

НОРМАТИВНИЙ ДОКУМЕНТ

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

НД ТЗІ 2.3-025-21

Том 2

Додаток А

Методика оцінювання груп заходів захисту класів AC, AT, AU, CA, CM, CP, IA, IP, IR, MA, MP, PA та PE

Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Київ 2021

Додаток А

Том 2

В додатку А тому 2 подається методика оцінювання заходів захисту для інформаційних систем (ІС) та інформації в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої визначена в законі та не становить державної таємниці, а саме класи: AC, AT, AU, CA, CM, CP, IA, IP, IR, MA, MP, PA та PE на наступних сторінках:

[I. КЛАС ЗАХОДІВ ЗАХИСТУ АС – УПРАВЛІННЯ ДОСТУПОМ 17](#_Toc89269687)

[II. КЛАС ЗАХОДІВ ЗАХИСТУ АТ – ОБІЗНАНІСТЬ ТА НАВЧАННЯ 125](#_Toc89269688)

[III. КЛАС ЗАХОДІВ ЗАХИСТУ АU – АУДИТ ТА ПІДЗВІТНІСТЬ 137](#_Toc89269689)

[IV. КЛАС ЗАХОДІВ ЗАХИСТУ CA – ОЦІНЮВАННЯ, АКРЕДИТАЦІЯ ТА МОНІТОРИНГ 179](#_Toc89269690)

[V. КЛАС ЗАХОДІВ ЗАХИСТУ CM – УПРАВЛІННЯ КОНФІГУРАЦІЄЮ 201](#_Toc89269691)

[VI. КЛАС ЗАХОДІВ ЗАХИСТУ CP – ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ 246](#_Toc89269692)

[VII. КЛАС ЗАХОДІВ ЗАХИСТУ IA – ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ 286](#_Toc89269693)

[VIII. КЛАС ЗАХОДІВ ЗАХИСТУ ІP – ІНДИВІДУАЛЬНА УЧАСТЬ 324](#_Toc89269694)

[IX. КЛАС ЗАХОДІВ ЗАХИСТУ IR – РЕАГУВАННЯ НА ІНЦИДЕНТИ 333](#_Toc89269695)

[X. КЛАС ЗАХОДІВ ЗАХИСТУ MA – ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ 361](#_Toc89269696)

[XI. КЛАС ЗАХОДІВ ЗАХИСТУ MP – ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ 394](#_Toc89269697)

[XII. КЛАС ЗАХОДІВ ЗАХИСТУ PA – АВТОРИЗАЦІЯ ПРИВАТНОСТІ 414](#_Toc89269698)

[XIII. КЛАС ЗАХОДІВ ЗАХИСТУ PE - ФІЗИЧНИЙ ЗАХИСТ ТА ЗАХИСТ РОБОЧОГО СЕРЕДОВИЩА 422](#_Toc89269699)

1. **КЛАС ЗАХОДІВ ЗАХИСТУ АС – УПРАВЛІННЯ ДОСТУПОМ**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| AC-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ ДОСТУПОМ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | |
| AC-1(a) | AC-1(a)[1] | AC-1(a)[1](1) | | Розробляє та документує політику (правила) управління доступом, яка: | | |
| AC-1(a)[1](1)(a)[1] | | містить мету, |
| AC-1(a)[1](1)(a)[2] | | містить сферу застосування, |
| AC-1(a)[1](1)(a)[3] | | містить ролі, |
| AC-1(a)[1](1)(a)[4] | | містить обов'язки, |
| AC-1(a)[1](1)(a)[5] | | містить зобов'язання керівництва, |
| AC-1(a)[1](1)(a)[6] | | містить координацію між організаційними підрозділами та систему контролю відповідності (compliances); |
| AC-1(a)[1](1)( b) | | відповідає чинному законодавству, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам |
| AC-1(a)[1](2) | | розробляє, документує процедури, що сприяють реалізації політики управління доступом та відповідних заходів управління доступом | | |
| AC-1(a)[2] | AC-1(a)[2](1) | | визначає персонал або ролі серед яких має бути поширена політика (правила) управління доступом, яка: | | |
| AC-1(a)[2](1)(a)[1] | | містить мету, |
| AC-1(a)[2](1)(a)[2] | | містить сферу застосування, |
| AC-1(a)[2](1)(a)[3] | | містить ролі, |
| AC-1(a)[2](1)(a)[4] | | містить обов'язки, |
| AC-1(a)[2](1)(a)[5] | | містить зобов'язання керівництва, |
| AC-1(a)[2](1)(a)[6] | | містить координацію між організаційними підрозділами та систему контролю відповідності (compliances); |
| AC-1(a)[2](1)(b) | | відповідає чинному законодавству, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам; |
| AC-1(a)[2](2) | | визначає персонал або ролі серед яких мають бути поширені процедури, що сприяють реалізації політики управління доступом та відповідних заходів управління доступом | | |
| AC-1(a)[3] | AC-1(a)[3](1) | | поширює серед визначеного організацією персоналу або ролей політику (правила) управління доступом, яка: | | |
| AC-1(a)[3](1)(а)[1] | | містить мету, |
| AC-1(a)[3](1)(а)[2] | | містить сферу застосування, |
| AC-1(a)[3](1)(а)[3] | | містить ролі, |
| AC-1(a)[3](1)(а)[4] | | містить обов'язки, |
| AC-1(a)[3](1)(а)[5] | | містить зобов'язання керівництва, |
| AC-1(a)[3](1)(а)[6] | | містить координацію між організаційними підрозділами та систему контролю відповідності (compliances); |
| AC-1(a)[3](1)(b) | | відповідає чинному законодавству, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам; |
| AC-1(a)[3](2) | | поширює серед визначеного організацією персоналу або ролей процедури, що сприяють реалізації політики управління доступом та відповідних заходів управління доступом | | |
| AC-1(b) | AC-1(b)[1] | визначає посадову особу для управління політикою та процедурами управління доступом | | | | |
| AC-1(b)[2] | призначає посаду для управління політикою та процедурами управління доступом | | | | |
| AC-1(с) | AC-1(с)[1] | AC-1(с)[1](1) | | AC-1(с)[1](1)[1] | визначає частоту перегляду поточної політики управління доступом | |
| AC-1(с)[1](1)[2] | переглядає поточну політику управління доступом з визначеною організацією частотою | |
| AC-1(с)[1](2) | | AC-1(с)[1](2)[1] | визначає частоту перегляду поточних процедур управління доступом | |
| AC-1(с)[1](2)[2] | переглядає поточні процедури управління доступом з визначеною організацією частотою | |
| AC-1(с)[2] | AC-1(с)[2](1) | | AC-1(с)[2](1)[1] | визначає частоту оновлення поточної політики управління доступом | |
| AC-1(с)[2](1)[2] | оновлює поточну політику управління доступом з визначеною організацією частотою | |
| AC-1(с)[2](2) | | AC-1(с)[2](2)[1] | визначає частоту оновлення поточних процедур управління доступом | |
| AC-1(с)[2](2)[2] | оновлює поточні процедури управління доступом з визначеною організацією частотою | |
| AC-1(d) | переконується, що процедури управління доступом реалізують політику та заходи управління доступом | | | | | |
| AC-1(e) | AC-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики управління доступом | | | |
| AC-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики управління доступом | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури управління доступом; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за управління доступом; персонал, відповідальний за інформаційну безпеку]. | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-2 | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | |
| AC-2(a) | визначає та задокументовує типи системних облікових записів, дозволених для використання в ІС для підтримки цілей, задач, функцій та процесів організації | | |
| AC-2(b) | призначає менеджерів облікових записів для управління системними обліковими записами | | |
| AC-2(c) | створює умови для групового та рольового членства | | |
| AC-2(d) | AC-2(d)[1] | визначає авторизованих користувачів інформаційної системи для кожного облікового запису | |
| AC-2(d)[2] | визначає членство в групі для кожного облікового запису | |
| AC-2(d)[3] | визначає ролі для кожного облікового запису; | |
| AC-2(d)[4] | визначає дозволи доступу (наприклад, привілеї) | |
| AC-2(d)[5] | визначає інші атрибути (за потреби) для кожного облікового запису | |
| AC-2(e) | AC-2(e)[1] | визначає особу або роль відповідальну за запити на створення системних облікових записів | |
| AC-2(e)[2] | вимагає схвалення визначеною організацією відповідальною особою або ролю запитів на створення системних облікових записів | |
| AC-2(f) | AC-2(f)[1] | визначає політики для створення системних облікових записів | |
| AC-2(f)[2] | визначає процедури для створення системних облікових записів | |
| AC-2(f)[3] | визначає умови для створення системних облікових записів | |
| AC-2(f)[4] | визначає політики для активації системних облікових записів | |
| AC-2(f)[5] | визначає процедури для активації системних облікових записів | |
| AC-2(f)[6] | визначає умови для активації системних облікових записів | |
| AC-2(f)[7] | визначає політики для зміни системних облікових записів | |
| AC-2(f)[8] | визначає процедури для зміни системних облікових записів | |
| AC-2(f)[9] | визначає умови для зміни системних облікових записів | |
| AC-2(f)[10] | визначає політики для деактивації системних облікових записів | |
| AC-2(f)[11] | визначає процедури для деактивації системних облікових записів | |
| AC-2(f)[12] | визначає умови для деактивації системних облікових записів | |
| AC-2(f)[13] | визначає політики для видалення системних облікових записів | |
| AC-2(f)[14] | визначає процедури для видалення системних облікових записів | |
| AC-2(f)[15] | визначає умови для видалення системних облікових записів | |
| AC-2(g) | впроваджує моніторинг використання системних облікових записів | | |
| AC-2(h) | AC-2(h)[1] | визначає часовий період протягом якого необхідно повідомляти адміністраторів облікових записів про те, що: | |
| AC-2(h)[1](1) | облікові записи більше не потрібні |
| AC-2(h)[1](2) | користувачі облікових записів звільнені або переведені |
| AC-2(h)[1](3) | використовуються індивідуальні системи або наявні зміни, які потребують нових знань |
| AC-2(h)[2] | повідомляє адміністраторів облікових записів протягом визначеного часового періоду про те, що: | |
| AC-2(h)[2](1) | облікові записи більше не потрібні |
| AC-2(h)[2](2) | користувачі облікових записів звільнені або переведені |
| AC-2(h)[2](3) | використовуються індивідуальні системи або наявні зміни, які потребують нових знань |
| AC-2(i) | AC-2(i)(1) | авторизує доступ до системи на основі дійсної авторизації доступу | |
| AC-2(i)(2) | авторизує доступ до системи на основі передбачуваного використання системи | |
| AC-2(i)(3) | авторизує доступ до системи на основі інших атрибутів, що вимагаються організацією | |
| AC-2(j) | AC-2(j)[1] | визначає частоту проведення перегляду облікових записів на відповідність вимогам управління обліковими записами | |
| AC-2(j)[2] | проводити перегляд облікових записів на відповідність вимогам управління обліковими записами з визначеною організацією частотою | |
| AC-2(k) | впроваджує процес повторного випуску облікових даних спільного/групового облікового запису (якщо він буде розгорнутий), коли особи виходять з групи | | |
| AC-2(e) | узгоджує процеси управління обліковими записами з процесами звільнення та переводу (передачі повноважень) персоналу | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; список активних системних облікових записів разом з іменем особи, пов’язаної з кожним обліковим записом; перелік умов для членства в групі та ролі; повідомлення або записи нещодавно переведених, відокремлених або припинених працівників; список недавно вимкнених облікових записів інформаційної системи разом з іменем особи, пов’язаної з кожним обліковим записом; записи авторизації доступу; огляди відповідності управління обліковим записом; записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Управління обліковими записами в організаційних процесах інформаційної системи; автоматизовані механізми здійснення управління рахунком]. | | | |

|  |  |  |
| --- | --- | --- |
| AC-2(1) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - АВТОМАТИЗОВАНЕ УПРАВЛІННЯ СИСТЕМНИМИ ОБЛІКОВИМИ ЗАПИСАМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AC-2(1)[1] | використовує автоматизовані механізми для підтримки управління системними обліковими записами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]. | |

|  |  |  |
| --- | --- | --- |
| AC-2(2) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ВИДАЛЕННЯ ТИМЧАСОВИХ ТА ЕКСТРЕНИХ ОБЛІКОВИХ ЗАПИСІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-2(2)[1] | організація визначає часовий період, після якого інформаційна система автоматично деактивує тимчасові облікові записи |
| AC-2(2)[2] | організація визначає часовий період, після якого інформаційна система автоматично видаляє тимчасові облікові записи |
| AC-2(2)[3] | організація визначає часовий період, після якого інформаційна система автоматично деактивує екстрені облікові записи |
| AC-2(2)[4] | організація визначає часовий період, після якого інформаційна система автоматично видаляє екстрені облікові записи |
| AC-2(2)[5] | інформаційна система автоматично деактивує тимчасові облікові записи після завершення визначеного організацією часового періоду |

|  |  |  |
| --- | --- | --- |
|  | AC-2(2)[6] | інформаційна система автоматично видаляє тимчасові облікові записи після завершення визначеного організацією часового періоду |
| AC-2(2)[7] | інформаційна система автоматично деактивує екстрені облікові записи після завершення визначеного організацією часового періоду |
| AC-2(2)[8] | інформаційна система автоматично видаляє екстрені облікові записи після завершення визначеного організацією часового періоду |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; сформований інформаційною системою перелік тимчасових облікових записів, вилучених та / або вимкнених; створений інформаційною системою перелік видалених та / або вимкнених аварійних облікових записів; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління рахунком; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-2(3) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДЕАКТИВАЦІЯ ОБЛІКОВИХ ЗАПИСІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| AC-2(3)[1] | організація визначає часовий період, після якого інформаційна система автоматично відключає неактивні облікові записи; | | |
| AC-2(3)[1][1] | інформаційна система автоматично відключає облікові записи якщо вони були неактивними впродовж визначеного організацією проміжку часу | |
| AC-2(3)[2] | організація визначає термін дії облікових записів | | |
| AC-2(3)[2][1] | інформаційна система автоматично відключає облікові записи коли їх термін дії минув | |
| AC-2(3)[3] | інформаційна система автоматично відключає облікові записи якщо вони більше не пов'язані з користувачем | | |
| AC-2(3)[4] | інформаційна система автоматично відключає облікові записи якщо вони порушують організаційну політику | | |
| AC-2(3)[5] | інформаційна система автоматично відключає облікові записи якщо вони більше не використовуються: | | |
| AC-2(3)[5]{1} | | додатками, |
| AC-2(3)[5]{2} | | послугами |
| AC-2(3)[5]{3} | | системою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; сформований інформаційною системою перелік тимчасових облікових записів, вилучених та / або вимкнених; створений інформаційною системою перелік видалених та / або вимкнених аварійних облікових записів; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-2(4) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДІЇ ПРИ АВТОМАТИЗОВАНОМУ АУДИТІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-2(4)[1] | інформаційна система автоматично перевіряє такі дії облікового запису: | |
| AC-2(4)[1][1] | створення |
| AC-2(4)[1][2] | модифікація |
| AC-2(4)[1][3] | включення |
| AC-2(4)[1][4] | відключення |
| AC-2(4)[1][5] | видалення |
| AC-2(4)[2] | організація визначає персонал або ролі, які повинні бути повідомлені про наступні дії в обліковому записі: | |
| AC-2(4)[2][1] | створення |
| AC-2(4)[2][2] | модифікація |
| AC-2(4)[2][3] | включення |
| AC-2(4)[2][4] | відключення |
| AC-2(4)[2][5] | видалення |
| AC-2(4)[3] | інформаційна система повідомляє визначений організацією персонал або ролі про наступні дії облікового запису: | |
| AC-2(4)[3][1] | створення |
| AC-2(4)[3][2] | модифікація |
| AC-2(4)[3][3] | включення |
| AC-2(4)[3][4] | відключення |
| AC-2(4)[3][5] | видалення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; повідомлення / сповіщення про створення, зміни, ввімкнення, вимкнення та видалення облікових записів; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-2(5) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ВИХІД З СИСТЕМИ ЗА НЕАКТИВНІСТЮ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-2(5)[1] | визначає часовий період очікуваної бездіяльності, який вимагає від користувачів виходу з системи. | |
| AC-2(5)[1][1] | вимагає, щоб користувачі вийшли з системи, коли досягається визначений організацією часовий період бездіяльності. |
| AC-2(5)[2] | визначає опис (сповіщення), коли користувачі повинні вийти з системи; | |
| AC-2(5)[2][1] | вимагає, щоб користувачі вийшли з системи, відповідно до визначеного організацією опису, коли потрібно вийти з системи. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; повідомлення про порушення безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; користувачів, які повинні відповідати політиці виходу з режиму бездіяльності]. | | |

|  |  |  |
| --- | --- | --- |
| AC-2(6) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДИНАМІЧНЕ УПРАВЛІННЯ ПРИВІЛЕЯМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-2(6)[1] | організація визначає перелік можливостей динамічного управління привілеями, що реалізуються інформаційною системою; |
| AC-2(6)[2] | інформаційна система реалізує визначений організацією перелік можливостей динамічного управління привілеями. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; системний перелік можливостей управління динамічними привілеями; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Інформаційна система, що реалізує можливості динамічного управління привілеями]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-2(7) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - СХЕМИ, ЗАСНОВАНІ НА РОЛЯХ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | |
| AC-2(7)(a) | AC-2(7)(a)[1] | створює привілейовані облікові записи користувачів відповідно до схеми доступу на основі ролей (role-based), яка реалізує дозволений доступ до системи та призначення привілеїв для ролей | |
| AC-2(7)(a)[2] | адмініструє привілейовані облікові записи користувачів відповідно до схеми доступу на основі ролей (role-based), яка реалізує дозволений доступ до системи та призначення привілеїв для ролей | |
| AC-2(7)(b) | проводить моніторинг призначень привілейованих ролей; | | |
| AC-2(7)(c) | AC-2(7)(c)[1] | | Визначає умови, коли призначені привілейовані ролі більше не потрібні |
| AC-2(7)(c)[2] | | скасовує доступ, коли привілейовані ролі більше не потрібні. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік привілейованих облікових записів користувачів та відповідної ролі, створений інформаційною системою; записи про вжиті дії, коли привілейоване призначення ролей більше не присвоюється; записи аудиту інформаційної системи; звіти про відстеження та моніторинг аудиту; записи моніторингу інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами; автоматизовані механізми моніторингу призначень привілейованих ролей]. | | | |

|  |  |  |
| --- | --- | --- |
| AC-2(8) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДИНАМІЧНЕ УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-2(8)[1] | організація визначає системні облікові записи, дії з якими будуть відбуватися динамічно |
| AC-2(8)[2] | інформаційна система динамічно створює визначені організацією облікові записи інформаційної системи |
| AC-2(8)[3] | інформаційна система динамічно активує визначені організацією облікові записи інформаційної системи |
| AC-2(8)[4] | інформаційна система динамічно управляє визначеними організацією облікові записи інформаційної системи |
| AC-2(8)[5] | інформаційна система динамічно деактивує визначені організацією облікові записи інформаційної системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; систематизований перелік облікових записів інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами] | |

|  |  |  |
| --- | --- | --- |
| AC-2(9) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ОБМЕЖЕННЯ НА ВИКОРИСТАННЯ СПІЛЬНИХ І ГРУПОВИХ ОБЛІКОВИХ ЗАПИСІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AC-2(9)[1] | визначає умови для створення спільних та групових облікових записів |
| AC-2(9)[2] | дозволяє використовувати лише ті спільні та групові облікові записи, які відповідають визначеним організацією умовам створення спільних та групових облікових записів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; сформований системою перелік спільних та групових облікових записів та пов'язаної з ними ролі; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління рахунком; системні та мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують управління спільними та груповими обліковими записами]. | |

|  |  |  |
| --- | --- | --- |
| AC-2(10) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ЗМІНА ДАНИХ СПІЛЬНИХ І ГРУПОВИХ ОБЛІКОВИХ ЗАПИСІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-2(10)[1] | інформаційна система змінює дані спільних облікових записів, коли члени групи залишають групу |
| AC-2(10)[2] | інформаційна система змінює дані групових облікових записів, коли члени групи залишають групу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи про припинення доступу до облікових записів; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-2(11) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - УМОВИ ВИКОРИСТАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-2(11)[1] | організація визначає ( один або кілька): | |
| AC-2(11)[1]{1} | обставини використання облікових записів інформаційної системи |
| AC-2(11)[1]{2} | організація визначає умови використання облікових записів інформаційної системи |
| AC-2(11)[2] | організація визначає облікові записи інформаційної системи, щодо яких мають бути визначені (один або кілька): | |
| AC-2(11)[2]{1} | обставини використання |
| AC-2(11)[2]{2} | умови використання |
| AC-2(11)[3] | інформаційна система забезпечує дотримання визначених організацією(один або кілька): | |
| AC-2(11)[3]{1} | обставин використання для визначених організацією облікових записів інформаційної системи |
| AC-2(11)[3]{2} | умов використання для визначених організацією облікових записів інформаційної системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; сформований системою перелік облікових записів інформаційної системи та пов'язані з ними призначення обставин використання та / або умов використання; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління облікових записів; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-2(12) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - МОНІТОРИНГ НЕТИПОВОГО ВИКОРИСТАННЯ ОБЛІКОВИХ ЗАПИСІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-2(12)(a) | AC-2(12)(a)[1] | визначає нетипове використання облікових записів інформаційної системи |
| AC-2(12)(a)[2] | здійснює моніторинг облікових записів інформаційної системи на предмет визначеного організацією нетипового використання облікових записів |
| AC-2(12)(b) | AC-2(12)(b)[1] | визначає персонал або ролі, які мають бути повідомлені про нетипове використання облікових записів інформаційної системи |
| AC-2(12)(b)[2] | повідомляє про нетипове використання облікових записів інформаційної системи визначений організацією персонал або ролі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи моніторингу інформаційної системи; записи аудиту інформаційної системи; спостереження аудиту та звіти про моніторинг; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]. | | |

|  |  |  |
| --- | --- | --- |
| AC-2(13) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДЕАКТИВАЦІЯ ОБЛІКОВИХ ЗАПИСІВ ОСІБ З ВИСОКИМ РІВНЕМ РИЗИКУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AC-2(13)[1] | визначає часовий період, протягом якого облікові записи користувачів, які представляють значний ризик, мають бути деактивовані |
| AC-2(13)[2] | деактивує облікові записи користувачів, які представляють значний ризик, в межах визначеного організацією періоду часу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; сформований системою список відключених облікових записів; перелік діяльності користувачів, що становлять значний організаційний ризик; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-2(14) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ТИПИ СПЕЦИФІЧНИХ ЗАБОРОНЕНИХ ОБЛІКОВИХ ЗАПИСІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-2(14)[1] | визначає типи специфічних заборонених облікових записів | |
| AC-2(14)[2] | AC-2(14)[2][1] | Забороняє створення спільних облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(14)[2][2] | Забороняє створення гостьових облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(14)[2][3] | Забороняє створення анонімних облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(14)[2][4] | Забороняє створення тимчасових облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(14)[2][5] | Забороняє створення екстрених облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(14)[3] | AC-2(14)[3][1] | Забороняє використання спільних облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(14)[3][2] | Забороняє використання гостьових облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(14)[3][3] | Забороняє використання анонімних облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(14)[3][4] | Забороняє використання тимчасових облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(14)[3][5] | Забороняє використання екстрених облікових записів для доступу до визначеної організацією типу інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; сформований системою список типів специфічних заборонених облікових записів; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-2(15) | УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ТИПИ СПЕЦИФІЧНИХ ЗАБОРОНЕНИХ ОБЛІКОВИХ ЗАПИСІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-2(15)[1] | визначає типи специфічних заборонених облікових записів | |
| AC-2(15)[2] | AC-2(15)[2][1] | Забороняє створення спільних облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(15)[2][2] | Забороняє створення гостьових облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(15)[2][3] | Забороняє створення анонімних облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(15)[2][4] | Забороняє створення тимчасових облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(15)[2][5] | Забороняє створення екстрених облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(15)[3] | AC-2(15)[3][1] | Забороняє використання спільних облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(15)[3][2] | Забороняє використання гостьових облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(15)[3][3] | Забороняє використання анонімних облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(15)[3][4] | Забороняє використання тимчасових облікових записів для доступу до визначеної організацією типу інформації. |
| AC-2(15)[3][5] | Забороняє використання екстрених облікових записів для доступу до визначеної організацією типу інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; сформований системою список типів специфічних заборонених облікових записів; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління обліковими записами; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]. | | |

|  |  |  |
| --- | --- | --- |
| AC-3 | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи | |
| AC-3[1] | застосовує інформаційна система затверджені дозволи для логічного доступу до інформації та системних ресурсів відповідно до застосовних політик контролю доступу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік затверджених дозволів (привілеїв користувача); записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу]. | |

|  |  |
| --- | --- |
| AC-3(1) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ОБМЕЖЕНИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ |
|  | [Вилучено: включено до складу AC-6] |

|  |  |  |
| --- | --- | --- |
| AC-3(2) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ПОДВІЙНА АВТОРИЗАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-3(2)[1] | організація визначає привілейовані команди та / або інші дії, щодо яких має виконуватися подвійна авторизація; |
| AC-3(2)[2] | інформаційна система застосовує подвійну авторизацію для визначених організацією привілейованих команд та / або інших визначених організацією дій. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу та подвійного дозволу; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; список привілейованих команд, що потребують подвійної авторизації; перелік дій, що вимагають подвійної авторизації; перелік затверджених дозволів (привілеїв користувача); інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Подвійні механізми авторизації, що реалізують політику контролю доступу]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| AC-3(3) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - МАНДАТНЕ УПРАВЛІННЯ ДОСТУПОМ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| AC-3(3)[1] | організація визначає мандатні правила контролю доступу, які слід застосовувати стосовно всіх суб’єктів та об'єктів; | | | |
| AC-3(3)[2] | організація визначає суб'єкти, щодо яких визначена організацією мандатна політика контролю доступу повинна бути застосована; | | | |
| AC-3(3)[3] | організація визначає об'єкти, щодо яких слід застосовувати визначені організацією мандатні політики контролю доступу; | | | |
| AC-3(3)[4] | організація визначає суб'єктів, яким може бути явно надано пільги таким чином, що вони не лімітуються обмеженнями, визначеними в інших місцях цього контролю; | | | |
| AC-3(3)[5] | організація визначає пільги, які можуть надаватися суб'єктам, визначеним організацією; | | | |
| AC-3(3)[6] | AC-3(3)[6](a) | AC-3(3)[6](a)[1] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що політика однаково застосовується для всіх суб'єктів у межах інформаційної системи; | |
| AC-3(3)[6](a)[2] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що політика однаково застосовується для всіх об'єктів у межах інформаційної системи; | |
| AC-3(3)[6](b) | AC-3(3)[6](b)(1) | AC-3(3)[6](b)(1)[1] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у передачі інформації несанкціонованим суб'єктам; |
| AC-3(3)[6](b)(1)[2] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у передачі інформації несанкціонованим об'єктам; |
| AC-3(3)[6](b)(2) | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у наданні своїх привілеїв іншим суб'єктам; | |
| AC-3(3)[6](b)(3) | AC-3(3)[6](b)(3)[1] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у зміні атрибуту безпеки: суб’єкти |
| AC-3(3)[6](b)(3)[2] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у зміні атрибуту безпеки: об’єкти |
| AC-3(3)[6](b)(3)[3] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у зміні атрибуту безпеки: Інформаційна система |
| AC-3(3)[6](b)(3)[4] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у зміні атрибуту безпеки: системні компоненти; |
| AC-3(3)[6](b)(4) | AC-3(3)[6](b)(4)[1] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у виборі атрибутів безпеки, які будуть пов'язані з новоствореними об'єктами; |
| AC-3(3)[6](b)(4)[2] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у виборі атрибутів безпеки, які будуть пов'язані зі зміненими об'єктами |
| AC-3(3)[6](b)(4)[3] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у виборі значень атрибутів, які будуть пов'язані з новоствореними об'єктами |
| AC-3(3)[6](b)(4)[4] | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у виборі значень атрибутів, які будуть пов'язані зі зміненими об'єктами |
| AC-3(3)[6](b)(5) | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що суб'єкт, якому було надано доступ до інформації, обмежується у зміні правил, що регулюють управління доступом; | |
| AC-3(3)[6](c) | інформаційна система застосовує визначені організацією мандатні політики контролю доступу щодо всіх суб'єктів та об'єктів, де політика визначає, що визначеним організацією суб'єктам можуть бути явно надані визначені організацією привілеї, так що вони не обмежуються будь-яким з перелічених вище обмежень. | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; правила мандатного контролю доступу; процедури щодо забезпечення доступу; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік предметів та об’єктів (тобто користувачів та ресурсів), які потребують виконання обов'язкових політик контролю доступу; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують мандатний контроль доступу] | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| AC-3(4) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ДИСКРЕЦІЙНЕ УПРАВЛІННЯ ДОСТУПОМ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| AC-3(4)[1] | організація визначає дискреційну політику контролю доступу; | | | |
| AC-3(4)[2] | організація визначає суб’єкти щодо яких застосовується політика дискреційного управління доступом | | | |
| AC-3(4)[3] | організація визначає об'єкти щодо яких застосовується політика дискреційного управління доступом | | | |
| AC-3(4)[4] | інформаційна система застосовує визначені організацією дискреційні політики контролю доступу щодо визначених суб'єктів та об'єктів, де політика визначає, що суб'єкту надано доступ до інформації та може (один або кілька): | | | |
| AC-3(4)[4](a) | передавати інформацію будь-яким іншим; | | |
| AC-3(4)[4](a){1} | | суб’єктам |
| AC-3(4)[4](a){2} | | об’єктам |
| AC-3(4)[4](b) | інформаційна система застосовує визначені організацією дискреційні політики контролю доступу щодо визначених суб'єктів та об'єктів, де політика визначає, що суб'єкту надано доступ до інформації та може надавати свої привілеї іншим суб'єктам; | | |
| AC-3(4)[4](c) | інформаційна система застосовує визначені організацією дискреційні політики контролю доступу щодо визначених суб'єктів та об'єктів, де політика визначає, що суб'єкту надано доступ до інформації та може змінити атрибути безпеки: | | |
| AC-3(4)[4](c)[1] | суб’єкти, | |
| AC-3(4)[4](c)[2] | об’єкти, | |
| AC-3(4)[4](c)[3] | інформаційна система, | |
| AC-3(4)[4](c)[4] | компоненти інформаційної системи; | |
| AC-3(4)[4](d) | AC-3(4)[4](d)[1] | інформаційна система застосовує визначені організацією дискреційні політики контролю доступу щодо визначених суб'єктів та об'єктів, де політика визначає, що суб'єкту надано доступ до інформації та може вибирати атрибути захисту, які потрібно асоціювати з новоствореними об’єктами; | |
| AC-3(4)[4](d)[2] | інформаційна система застосовує визначені організацією дискреційні політики контролю доступу щодо визначених суб'єктів та об'єктів, де політика визначає, що суб'єкту надано доступ до інформації та може вибирати атрибути захисту, які потрібно асоціювати з переглянутими об’єктами; | |
| AC-3(4)[4](e) | інформаційна система застосовує визначені організацією дискреційні політики контролю доступу щодо визначених суб'єктів та об'єктів, де політика визначає, що суб'єкту надано доступ до інформації та може змінити правила управління доступом. | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; дискреційна політика контролю доступу; процедури щодо забезпечення доступу; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік предметів та об’єктів (тобто користувачів та ресурсів), які потребують застосування дискреційних політик контролю доступу; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують дискреційну політику контролю доступу]. | | | | |

|  |  |  |
| --- | --- | --- |
| AC-3(5) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ІНФОРМАЦІЯ ЩОДО БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-3(5)[1] | організація визначає інформацію, що належить до безпеки, до якої інформаційна система забороняє доступ, за винятком випадків, коли вона знаходиться в безпечному непрацездатному стані системи; |
| AC-3(5)[2] | інформаційна система перешкоджає доступу до визначеної організацією інформації, що відповідає безпеці, за винятком безпечних, неробочих станів системи. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що запобігають доступу до інформації, що стосується безпеки, в межах інформаційної системи]. | |

|  |  |
| --- | --- |
| AC-3(6) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ЗАХИСТ ІНФОРМАЦІЇ КОРИСТУВАЧА ТА СИСТЕМИ |
|  | [Вилучено: Включено в MP-4 та SC-28]. |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-3(7) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ РОЛЕЙ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-3(7)[1] | організація визначає ролі для контролю доступу до інформаційної системи; | |
| AC-3(7)[2] | організація визначає користувачів, уповноважених виконувати визначені організацією ролі; | |
| AC-3(7)[3] | інформаційна система контролює доступ на основі визначених організацією ролей та користувачів, уповноважених виконувати такі ролі; | |
| AC-3(7)[4] | AC-3(7)[4][1] | інформаційна система застосовує рольову політику контролю доступу щодо визначених суб’єктів, |
| AC-3(7)[4][2] | інформаційна система застосовує рольову політику контролю доступу щодо визначених об’єктів; |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; рольові політики контролю доступу; процедури щодо забезпечення доступу; план безпеки, проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік ролей, користувачів та пов'язаних з ними привілеїв, необхідних для контролю доступу до інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують рольову політику контролю доступу]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-3(8) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - АНУЛЮВАННЯ ПРАВ ДОСТУПУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| AC-3(8)[1] | організація визначає правила, що регулюють терміни відкликання дозволів на доступ; | | |
| AC-3(8)[2] | AC-3(8)[2][1] | інформаційна система примушує скасовувати дозволи доступу внаслідок зміни атрибутів захисту суб'єктів на основі визначених організацією правил, що регулюють терміни відкликання дозволів на доступ. | |
| AC-3(8)[2][2] | інформаційна система примушує скасовувати дозволи доступу внаслідок зміни атрибутів захисту об'єктів на основі визначених організацією правил, що регулюють терміни відкликання дозволів на доступ. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; правила, що регулюють скасування дозволів на доступ, записів аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу] | | | |
| AC-3(9) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - КЕРОВАНА ПЕРЕДАЧА (ПУБЛІКАЦІЯ) ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| AC-3(9)[1] | AC-3(9)[1][1] | організація визначає інформаційну систему, уповноважений приймати інформацію, випущену поза встановленою межею інформаційної системи, яка випускає таку інформацію; | |
| AC-3(9)[1][2] | організація визначає компонент системи, уповноважений приймати інформацію, випущену поза встановленою межею інформаційної системи, яка випускає таку інформацію; | |
| AC-3(9)[2] | організація визначає заходи безпеки, які повинні надаватися певною інформаційною системою або компонентом системи, які отримують інформацію, випущену з інформаційної системи за межами встановленої межі системи; | | |
| AC-3(9)[3] | AC-3(9)[3](a) | AC-3(9)[3](a)[1] | Передавати (публікувати) інформацію за межами встановленої межі системи, можливо якщо визначена організацією приймаюча система забезпечує визначені організацією заходи безпеки; |
| AC-3(9)[3](a)[2] | Передавати (публікувати) інформацію за межами встановленої межі системи, можливо якщо визначена організацією приймаючий компонент системи забезпечує визначені організацією заходи безпеки; |
| AC-3(9)[3](b) | Використовує визначені організацією заходи безпеки для підтвердження відповідності інформації, призначеної для керованих передач (публікації). | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік заходів безпеки, що надаються інформаційною системою, яка приймає або її компонентами; список заходів безпеки, що підтверджують доречність інформації, призначеної для публікації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу]. | | | |

|  |  |  |
| --- | --- | --- |
| AC-3(10) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - АУДИТОРСЬКИЙ ПЕРЕГЛЯД МЕХАНІЗМІВ КОНТРОЛЮ ДОСТУПУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AC-3(10)[1] | визначає умови за яких застосовується аудиторський перегляд механізмів автоматизованого управління доступу |
| AC-3(10)[2] | визначає ролі які застосовують аудиторський перегляд механізмів автоматизованого управління доступу |
| AC-3(10)[3] | застосовує аудиторський перегляд механізмів автоматизованого управління доступу при визначених організацією умовах визначеними організацією ролями. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; умови для використання аудиторського перегляду автоматизованих механізмів контролю доступу; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу]. | |

|  |  |  |
| --- | --- | --- |
| AC-3(11) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ОБМЕЖЕННЯ ДОСТУПУ ДО СПЕЦІАЛЬНОЇ ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AC-3(12)[1] | визначає типи інформації до яких має бути обмежено доступ |
| AC-3(12)[2] | обмежує прямий доступ до сховищ даних, що містять визначені організацією типи інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-3(12) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ВСТАНОВЛЕННЯ ТА ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ДОДАТКІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-3(12)(a) | AC-3(12)(a)[1] | визначає системні програми та функції до яких буде встановлено доступ у процесі інсталяції. |
| AC-3(12)(a)[2] | вимагає від додатків встановити у процесі інсталяції доступ до визначених організацією системних програм та функції. |
| AC-3(12)(b) | Впровадити механізм примусового застосування, щоб запобігти доступу, відмінного від заявленого. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-3(13) | ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ АТРИБУТІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-3(13)[1] | AC-3(13)[1][1] | визначає атрибути для прийняття рішень про доступ |
| AC-3(13)[1][2] | управляє доступом на основі визначених організацією атрибутів для прийняття рішень про доступ. |
| AC-3(13)[2] | AC-3(13)[2][1] | визначає суб'єкти доступу на основі атрибутів |
| AC-3(13)[2][2] | здійснює політику управління доступу на основі атрибутів (atribute-based) для визначених суб'єктів доступу |
| AC-3(13)[3] | AC-3(13)[3][1] | визначає об'єкти доступу на основі атрибутів |
| AC-3(13)[3][2] | здійснює політику управління доступу на основі атрибутів (atribute-based) для визначених об'єктів доступу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-4 | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-4[1] | AC-4[1][1] | організація визначає політику управління інформаційним потоком для управління потоком інформації всередині системи; |
| AC-4[1][2] | організація визначає політику управління інформаційним потоком для управління потоком інформації між взаємопов'язаними системами; |
| AC-4[2] | AC-4[2][1] | інформаційна система застосовує затверджені дозволи на контроль потоку інформації всередині системи на основі визначених організацією політик управління потоком інформації. |
| AC-4[2][2] | інформаційна система застосовує затверджені дозволи на контроль потоку інформації між взаємопов'язаними системами на основі визначених організацією політик управління потоком інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційних потоків; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; конфігурація базової лінії інформації; перелік дозволів на потік інформації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-4(1) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - АТРИБУТИ БЕЗПЕКИ ОБ'ЄКТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-4(1)[1] | організація визначає політику управління потоком інформації як основу для прийняття рішень щодо контролю потоку; | |
| AC-4(1)[2] | організація визначає атрибути безпеки, пов'язані з об'єктами інформації, джерела та призначення; | |
| AC-4(1)[3] | AC-4(1)[3][1] | організація визначає інформацію пов'язану з визначеними організацією атрибутами безпеки |
| AC-4(1)[3][2] | організація визначає джерело пов'язане з визначеними організацією атрибутами безпеки |
| AC-4(1)[3][3] | організація визначає об'єкти призначення пов'язані з визначеними організацією атрибутами безпеки |
| AC-4(1)[4] | інформаційна система використовує визначені організацією атрибути безпеки, пов'язані з визначеними організацією об'єктами інформації, джерелами та об'єктом призначення, щоб застосовувати визначені організацією політики управління інформаційними потоками як основу для прийняття рішень щодо управління потоком. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік атрибутів безпеки та пов'язаних з ними об’єктів інформації, джерела та призначення, що застосовують політику управління інформаційним потоком; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | | |

|  |  |  |
| --- | --- | --- |
| AC-4(2) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ДОМЕНИ ОБРОБКИ ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(2)[1] | організація визначає політику управління потоком інформації, як основу для прийняття рішень щодо контролю потоку; |
| AC-4(2)[2] | інформаційна система використовує захищені домени обробки даних для забезпечення визначених організацією політик управління інформаційним потоком, як основи для прийняття рішень щодо управління потоком. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; архітектура безпеки інформаційної системи та супутня документація; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку]  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | |

|  |  |  |
| --- | --- | --- |
| AC-4(3) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ДИНАМІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ ПОТОКОМ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(3)[1] | організація визначає політику щодо забезпечення динамічного контролю інформаційного потоку; |
| AC-4(3)[2] | інформаційна система здійснює динамічне управління потоком інформації на основі визначених організацією політик. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; архітектура безпеки інформаційної системи та супутня документація; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-4(4) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - УПРАВЛІННЯ ПОТОКОМ ЗАШИФРОВАНОЇ ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| AC-4(4)[1] | AC-4(4)[1][1] | організація визначає процедури, які слід використовувати для запобігання обходу механізмів перевірки контенту зашифрованої інформації; | |
| AC-4(4)[1][2] | організація визначає метод, який слід використовувати для запобігання обходу механізмів перевірки контенту зашифрованої інформації; | |
| AC-4(4)[2] | AC-4(4)[2][1] | інформаційна система запобігає обходу механізмів перевірки контенту зашифрованої інформації, виконуючи: | |
| AC-4(4)[2][1]{1} | дешифрування інформації |
| AC-4(4)[2][1]{2} | блокування потоку зашифрованої інформації; |
| AC-4(4)[2][1]{3} | завершення сеансів зв'язку при спробі передачі зашифрованої інформації; |
| AC-4(4)[2][1]{4} | визначені організацією процедури. |
| AC-4(4)[2][1]{5} | визначені організацією методи. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | | | |

|  |  |  |
| --- | --- | --- |
| AC-4(5) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ВБУДОВУВАННЯ ТИПІВ ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(5)[1] | організація визначає обмеження, які слід застосовувати щодо вбудовування типів даних в інші типи даних; |
| AC-4(5)[2] | інформаційна система впроваджує визначені організацією обмеження щодо вбудовування типів даних в інші типи даних. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік обмежень, які мають бути застосовані щодо вбудовування типів даних в інші типи даних; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що впроваджують політику реалізації інформаційного потоку]. | |

|  |  |  |
| --- | --- | --- |
| AC-4(6) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - МЕТАДАНІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(6)[1] | організація визначає метадані, які слід використовувати як засіб забезпечення контролю за потоком інформації; |
| AC-4(6)[2] | інформаційна система здійснює управління інформаційним потоком на основі визначених організацією метаданих. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; типи метаданих, що застосовуються для забезпечення прийняття рішень щодо управління інформаційним потоком; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику забезпечення впровадження інформаційного потоку]. | |

|  |  |  |
| --- | --- | --- |
| AC-4(7) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - МЕХАНІЗМИ ОДНОСТОРОННЬОГО ПОТОКУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(7)[1] | організація визначає односторонні інформаційні потоки, що забезпечуються інформаційною системою; |
| AC-4(7)[2] | інформаційна система застосовує визначені організацією односторонні інформаційні потоки за допомогою апаратних механізмів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; апаратні механізми інформаційної системи та пов'язані з ними конфігурації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Апаратні механізми, що реалізують політику застосування інформаційного потоку] | |

|  |  |  |
| --- | --- | --- |
| AC-4(8) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ФІЛЬТРИ ПОЛІТИКИ БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(8)[1] | організація визначає фільтри політики безпеки, які використовуються як основа для виконання рішень щодо контролю потоку; |
| AC-4(8)[2] | організація визначає інформаційні потоки, щодо яких слід застосовувати та виконувати рішення щодо контролю потоків; |
| AC-4(8)[3] | інформаційна система здійснює управління інформаційними потоками, використовуючи визначені організацією фільтри політики безпеки як основу для прийняття рішень щодо управління потоками для визначених організацією інформаційних потоків. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік фільтрів політик безпеки, що регулюють рішення щодо управління потоком; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Адміністратори системи / мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | |

|  |  |  |
| --- | --- | --- |
| AC-4(9) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПЕРЕВІРКИ, ЩО ПРОВОДИТЬ ПЕРСОНАЛ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(9)[1] | організація визначає інформаційні потоки, що вимагають застосування перевірки людиною; |
| AC-4(9)[2] | організація визначає умови, за яких слід застосовувати перевірки людиною для визначених організацією інформаційних потоків; |
| AC-4(9)[3] | інформаційна система примушує використовувати перевірки людиною для організаційно визначених інформаційних потоків у визначених організацією умовах. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи перевірки людиною щодо інформаційних потоків; перелік умов, що потребують перевірки людиною на інформаційні потоки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Адміністратори системи / мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, відповідальний за виконання потоку інформації; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що застосовують використання оглядів людей]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-4(10) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - АКТИВАЦІЯ ТА ДЕАКТИВАЦІЯ ФІЛЬТРІВ ПОЛІТИКИ БЕЗПЕКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-4(10)[1] | організація визначає привілейованих адміністраторів, що мають можливість управляти фільтрами політик безпеки. | |
| AC-4(10)[2] | організація визначає фільтри політик безпеки, які привілейовані адміністратори мають можливість активувати та деактивувати; | |
| AC-4(10)[3] | організація визначає умови, за яких привілейовані адміністратори мають можливість активувати та деактивувати визначені організацією фільтри політики безпеки; | |
| AC-4(10)[4] | інформаційна система впроваджує можливість для привілейованих адміністраторів: | |
| AC-4(10)[4][1] | активувати фільтри політики безпеки, що визначаються організацією за визначених організацією умов. |
| AC-4(10)[4][2] | деактивувати фільтри політики безпеки, що визначаються організацією за визначених організацією умов. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; інформаційна політика інформаційного потоку; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; список фільтрів політик безпеки, увімкнутих та вимкнутих привілейованими адміністраторами; записи аудиту інформаційної системи; інші відповідні документи чи записи]  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за включення / відключення фільтрів політики безпеки; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | | |

|  |  |  |
| --- | --- | --- |
| AC-4(11) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - КОНФІГУРАЦІЯ ФІЛЬТРІВ ПОЛІТИКИ БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(11)[1] | визначає організація фільтри політики безпеки, які привілейовані адміністратори мають можливість налаштовувати для підтримки різних політик безпеки; |
| AC-4(11)[2] | інформаційна система впроваджує можливість для привілейованих адміністраторів налаштовувати визначені організацією фільтри політик безпеки для підтримки різних політик безпеки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР:Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік фільтрів політик безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за налаштування фільтрів політики безпеки; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | |

|  |  |  |
| --- | --- | --- |
| AC-4(12) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ІДЕНТИФІКАТОРИ ТИПУ ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(12)[1] | організація визначає ідентифікатори типів даних, які використовуватимуться при передачі інформації між різними доменами безпеки, для перевірки даних, важливих для прийняття рішень про потік інформації; |
| AC-4(12)[2] | інформаційна система при передачі інформації між різними доменами безпеки використовує визначені організацією ідентифікатори типу даних для перевірки даних, важливих для прийняття рішень про інформаційний потік. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік ідентифікаторів типу даних; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Адміністратори системи / мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | |

|  |  |  |
| --- | --- | --- |
| AC-4(13) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ДЕКОМПОЗИЦІЯ НА ВІДПОВІДНІ ПОЛІТИЦІ СУБКОМПОНЕНТИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(13)[1] | організація визначає відповідні для політики субкомпоненти для декомпозиції інформації для подання до механізмів виконання політики при передачі такої інформації між різними доменами безпеки; |
| AC-4(13)[2] | інформаційна система при передачі інформації між різними захищеними доменами, здійснює декомпозицію інформації на визначені організацією субкомпоненти, що відповідають політиці, для представлення у механізмах реалізації політики. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Адміністратори системи / мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | |

|  |  |  |
| --- | --- | --- |
| AC-4(14) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ОБМЕЖЕННЯ ФІЛЬТРА ПОЛІТИКИ БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(14)[1] | організація визначає фільтри політик безпеки, які потрібно впроваджувати, такі що вимагають повністю перелічених форматів, що обмежують структуру даних та вміст при передачі інформації між різними доменами безпеки; |
| AC-4(14)[2] | інформаційна система при передачі інформації між різними доменами безпеки реалізує визначені організацією фільтри політики безпеки, що вимагають перелічення усіх форматів, що обмежують структуру даних та вміст. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік фільтрів політик безпеки; перелік фільтрів політики щодо вмісту даних; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Адміністратори системи / мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | |

|  |  |  |
| --- | --- | --- |
| AC-4(15) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОЇ ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(15)[1] | організація визначає несанкціоновану інформацію, яку слід виявити при передачі інформації між різними доменами безпеки; |
| AC-4(15)[2] | організація визначає політику безпеки, яка вимагає заборонити передачу визначеної організацією несанкціонованої інформації між різними доменами безпеки, коли виявляється наявність такої інформації; |
| AC-4(15)[3] | інформаційна система при передачі інформації між різними доменами безпеки вивчає інформацію на наявність визначеної організацією несанкціонованої інформації відповідно до визначеної організацією політики безпеки. |
| AC-4(15)[4] | інформаційна система при передачі інформації між різними доменами безпеки при виявленні визначеної організацією несанкціонованої інформації забороняє передавати таку інформацію відповідно до визначеної організацією політики безпеки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік несанкціонованих типів інформації та пов'язаної з ними інформації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | |

|  |  |
| --- | --- |
| AC-4(16) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПЕРЕДАЧА ІНФОРМАЦІЇ ПРО ВЗАЄМОПОВ’ЯЗАНІ СИСТЕМИ |
|  | [Вилучено: Включено в АС-4] |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-4(17) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - АВТЕНТИФІКАЦІЯ ДОМЕНУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-4(17)[1] | Унікально ідентифікувати джерела призначення за допомогою(один або кілька): | |
| AC-4(17)[1]{1} | організації для передачі інформації |
| AC-4(17)[1]{2} | системи для передачі інформації |
| AC-4(17)[1]{3} | програми для передачі інформації |
| AC-4(17)[1]{4} | служби для передачі інформації |
| AC-4(17)[1]{5} | індивідуума для передачі інформації |
| AC-4(17)[2] | Унікально ідентифікувати пункти призначення за допомогою(один або кілька): | |
| AC-4(17)[2]{1} | організації для передачі інформації |
| AC-4(17)[2][2] | системи для передачі інформації |
| AC-4(17)[2][3] | програми для передачі інформації |
| AC-4(17)[2][4] | служби для передачі інформації |
| AC-4(17)[2][5] | індивідуума для передачі інформації |
| AC-4(17)[3] | Унікально автентифікувати джерела призначення за допомогою(один або кілька): | |
| AC-4(17)[3]{1} | організації для передачі інформації |
| AC-4(17)[3]{2} | системи для передачі інформації |
| AC-4(17)[3]{3} | програми для передачі інформації |
| AC-4(17)[3]{4} | служби для передачі інформації |
| AC-4(17)[3]{5} | індивідуума для передачі інформації |
| AC-4(17)[4] | Унікально автентифікувати пункти призначення за допомогою(один або кілька): | |
| AC-4(17)[4]{1} | організації для передачі інформації |
| AC-4(17)[4]{2} | системи для передачі інформації |
| AC-4(17)[4]{3} | програми для передачі інформації |
| AC-4(17)[4]{4} | служби для передачі інформації |
| AC-4(17)[4]{5} | індивідуума для передачі інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік несанкціонованих типів інформації та пов'язаної з ними інформації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку]. | | |

|  |  |  |
| --- | --- | --- |
| AC-4(18) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПРИВ'ЯЗКА АТРИБУТУ БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-4(18)[1] | організація визначає обов'язкові методи, які будуть використовуватися для сприяння реалізації політики потоку інформації; |
| AC-4(18)[2] | інформаційна система пов'язує атрибути безпеки з інформацією, використовуючи методи прив'язки, які організація визначила, для полегшення застосування політики потоку інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика посилення інформаційного потоку; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; список методів прив’язки для прив’язки атрибутів безпеки до інформації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за виконання потоку інформації; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення функціонування потоку інформації] | |

|  |  |  |
| --- | --- | --- |
| AC-4(19) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПЕРЕВІРКА МЕТАДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи | |
| AC-4(19)[1] | інформаційна система при передачі інформації між різними доменами безпеки застосовує ту саму політику безпеки фільтрації до метаданих, як й до корисних навантажень даних. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика посилення інформаційного потоку; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік критеріїв фільтрації політик безпеки, застосованих до метаданих та корисних навантажень даних; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за виконання потоку інформації; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення інформаційного потоку]. | |

|  |  |  |
| --- | --- | --- |
| AC-4(20) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ЗАТВЕРДЖЕНІ РІШЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AC-4(20)[1] | визначає рішення в затверджених змінах для управління потоком інформації через домени безпеки; |
| AC-4(20)[2] | визначає інформацію, для якої визначені організацією рішення у затверджених конфігураціях повинні використовуватися для контролю потоку такої інформації через домени безпеки; |
| AC-4(20)[3] | використовує визначені організацією рішення у затверджених конфігураціях для управління потоком визначеної організацією інформації через домени безпеки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика посилення інформаційного потоку; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік рішень у затверджених конфігураціях; затверджені базові лінії конфігурації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за виконання потоку інформації; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення функціонування потоку інформації]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-4(21) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ФІЗИЧНЕ ТА ЛОГІЧНЕ ВІДДІЛЕННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| AC-4(21)[1] | організація визначає механізми, які будуть використовуватися для поділу інформаційних потоків: | | |
| AC-4(21)[1]{1} | логічно | |
| AC-4(21)[1]{2} | фізично | |
| AC-4(21)[2] | організація визначає методи, які будуть використовуватися для поділу інформаційних потоків: | | |
| AC-4(21)[2]{1} | логічно | |
| AC-4(21)[2]{2} | фізично | |
| AC-4(21)[3] | організація визначає необхідний поділ інформаційних потоків за типами інформації; | | |
| AC-4(21)[4] | AC-4(21)[4]{1} | Організація відокремлює потоки інформації логічно, використовуючи визначені організацією: | |
| AC-4(21)[4]{1}{1} | механізми для досягнення визначеного організацією необхідного поділу за типами інформації. |
| AC-4(21)[4]{1}{2} | методи для досягнення визначеного організацією необхідного поділу за типами інформації. |
| AC-4(21)[4]{2} | Організація відокремлює потоки інформації фізично, використовуючи визначені організацією: | |
| AC-4(21)[4]{2}{1} | механізми для досягнення визначеного організацією необхідного поділу за типами інформації. |
| AC-4(21)[4]{2}{2} | методи для досягнення визначеного організацією необхідного поділу за типами інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика посилення інформаційного потоку; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік необхідного поділу інформаційних потоків за типами інформації; перелік механізмів та / або заходів, використовуваних для логічного або фізичного поділу інформаційних потоків; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал з обов'язками щодо забезпечення потоку інформації; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення функціонування потоку інформації] | | | |

|  |  |  |
| --- | --- | --- |
| AC-4(22) | УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ЄДИНИЙ ДОСТУП | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація | |
| AC-4(22)[1] | Забезпечує доступ з одного пристрою до обчислювальних платформ, що знаходяться в декількох різних захищених доменах, одночасно запобігаючи передачі будь-якого потоку інформації між різними захищеними доменами. |
| AC-4(22)[2] | Забезпечує доступ з одного пристрою до додатків, що знаходяться в декількох різних захищених доменах, одночасно запобігаючи передачі будь-якого потоку інформації між різними захищеними доменами. |
| AC-4(22)[3] | Забезпечує доступ з одного пристрою до даних, що знаходяться в декількох різних захищених доменах, одночасно запобігаючи передачі будь-якого потоку інформації між різними захищеними доменами. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури розв’язання питань розподілу відповідальності та розподілу обов'язків; налаштування конфігурації інформаційної системи та супутня документація; перелік підрозділів відповідальності та розподілу обов'язків; авторизація доступу до інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення відповідних підрозділів відповідальності та розподілу обов'язків; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику розділення обов'язків] | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-5 | РОЗМЕЖУВАННЯ ОБОВ'ЯЗКІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-5(a) | AC-5(a)[1] | визначає обов'язки окремих осіб; |
| AC-5(a)[2] | розмежовує обов’язки визначені організацією окремих осіб; |
| AC-5(b) | розробляє документи з розмежування обов'язків фізичних осіб | |
| AC-5(c) | встановлює правила авторизації доступу для підтримки розмежування обов'язків | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури розв’язання питань розподілу відповідальності та розмежування обов'язків; налаштування конфігурації інформаційної системи та супутня документація; перелік розподілу відповідальності та обов'язків; авторизація доступу до інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення відповідних підрозділів відповідальності та розподілу обов'язків; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику розподілу обов'язків]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-6 | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи | | |
| AC-6[1] | організація встановлює принцип мінімізації повноважень, дозволяючи лише авторизований доступ для користувачів та процесів, що діють від імені користувачів | |
| AC-6[2] | організація визначає завдання організації. | |
| AC-6[3] | організація визначає організаційні функції. | |
| AC-6[4] | Організація впроваджує принцип мінімізації повноважень, дозволяючи лише авторизований доступ для: | |
| AC-6[4]{1} | користувачів, здійснювати лише такі авторизовані звернення, які необхідні для виконання визначених завдань відповідно до цілей (призначення, місії) організації та бізнес-функцій |
| AC-6[4]{2} | процесам, що діють від імені користувачів, здійснювати лише такі авторизовані звернення, які необхідні для виконання визначених завдань відповідно до цілей (призначення, місії) організації та бізнес-функцій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; перелік призначених дозволів доступу (привілеїв користувача); налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення мінімізація повноважень, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують мінімізацію повноважень]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-6(1) | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - АВТОРИЗОВАНИЙ ДОСТУП ДО ФУНКЦІЙ БЕЗПЕКИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | |
| AC-6(1)[1] | визначає функці безпеки, які розгорнуті в: | | |
| AC-6(1)[1][1] | апаратних засобах, що стосується безпеки | |
| AC-6(1)[1][2] | програмному забезпеченні , що стосується безпеки | |
| AC-6(1)[1][3] | вбудованому програмному забезпеченні, що стосується безпеки | |
| AC-6(1)[2] | визначає інформацю, що стосується безпеки | | |
| AC-6(1)[3] | AC-6(1)[3][1] | явно надає доступ до визначених функції безпеки, які розгорнуті в: | |
| AC-6(1)[3][1][1] | апаратних засобах, що стосується безпеки |
| AC-6(1)[3][1][2] | програмному забезпеченні , що стосується безпеки |
| AC-6(1)[3][1][3] | вбудованому програмному забезпеченні, що стосується безпеки |
| AC-6(1)[3][2] | явно надає доступ до визначеної інформації, що стосується безпеки. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; перелік функцій безпеки (розгорнутих в апаратному, програмному забезпеченні та прошивці) та інформації, що стосується безпеки, доступ до якої має бути недвозначно авторизований; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень]. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| AC-6(2) | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - НЕПРИВІЛЕЙОВАНИЙ ДОСТУП ДО НЕЗАХИЩЕНИХ ФУНКЦІЙ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | |
| AC-6(2)[1] | AC-6(2)[1]{1} | визначає функції безпеки до яких мають доступ: | | | |
| AC-6(2)[1]{1} | | | користувачі облікових записів інформаційних систем |
| AC-6(2)[1]{2} | | | ролі інформаційних систем |
| AC-6(2)[1]{2} | визначає інформацію, що стосується безпеки, до якої мають доступ: | | | |
| AC-6(2)[2]{1} | | користувачі облікових записів інформаційних систем | |
| AC-6(2)[2]{2} | | ролі інформаційних систем | |
| AC-6(2)[2] | AC-6(2)[2]{1} | Вимагати від користувачів системних облікових записів, які мають доступ до визначених організацією: | | | |
| AC-6(2)[2]{1}{1} | функцій безпеки, використовувати непривілейовані облікові записи або ролі під час доступу до незахищених функцій. | | |
| AC-6(2)[2]{1}{2} | інформації, що стосується безпеки, використовувати непривілейовані облікові записи або ролі під час доступу до незахищених функцій. | | |
| AC-6(2)[2]{2} | Вимагати від ролей, які мають доступ до визначених організацією: | | | |
| AC-6(2)[2]{2}{1} | функцій безпеки, використовувати непривілейовані облікові записи або ролі під час доступу до незахищених функцій. | | |
| AC-6(2)[2]{2}{2} | інформації, що стосується безпеки, використовувати непривілейовані облікові записи або ролі під час доступу до незахищених функцій. | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; перелік функцій безпеки, що генеруються системою, або інформації про підвищену безпеку, призначеної для облікових записів або ролей інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення найменших пільг, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень]. | | | | | |

|  |  |  |
| --- | --- | --- |
| AC-6(3) | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - МЕРЕЖЕВИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ КОМАНД | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AC-6(3)[1] | визначає привілейовані команди, для яких доступ до мережі повинен бути дозволений тільки для невідкладних операційних потреб; |
| AC-6(3)[2] | визначає невідкладні операційні потреби, для яких мережевий доступ до визначених організацією привілейованих команд, повинен бути виключно авторизований; |
| AC-6(3)[3] | авторизує мережевий доступ до визначених організацією привілейованих команд тільки для визначених організацією невідкладних операційних потреб |
| AC-6(3)[4] | документує обґрунтування авторизованого доступу до мережі до визначених організацією привілейованих команд у плані безпеки інформаційної системи. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; план безпеки; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; перелік операційних потреб для авторизації доступу до мережі до привілейованих команд; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень]. | |

|  |  |  |
| --- | --- | --- |
| AC-6(4) | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - РОЗДІЛЬНІ ДОМЕНИ ОБРОБКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи | |
| AC-6(4)[1] | надає інформаційна система окремі домени обробки для більш точного розподілу користувальницьких повноважень. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-6(5) | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ПРИВІЛЕЙОВАНІ ОБЛІКОВІ ЗАПИСИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-6(5)[1] | AC-6(5)[1]{1} | визначає персонал, для яких мають бути обмежені привілейовані облікові записи в інформаційній системі; |
| AC-6(5)[1]{2} | визначає ролі, для яких мають бути обмежені привілейовані облікові записи в інформаційній системі; |
| AC-6(5)[2] | обмежує привілейовані облікові записи в інформаційній системі згідно з визначеними організацією: | |
| AC-6(5)[2]{1} | персоналом |
| AC-6(5)[2]{2} | ролями |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; перелік визначених системою привілейованих облікових записів; перелік персоналу системної адміністрації; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень]. | | |

|  |  |  |
| --- | --- | --- |
| AC-6(6) | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ПРИВІЛЕЙОВАНИЙ ДОСТУП КОРИСТУВАЧАМИ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-6(6)[1] | забороняє організація привілейований доступ до інформаційної системи користувачам, що не належать до організації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; список згенерованих системою привілейованих облікових записів; перелік не організаційних користувачів; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що забороняють привілейований доступ до інформаційної системи]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-6(7) | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ПЕРЕГЛЯД ПОВНОВАЖЕНЬ КОРИСТУВАЧА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-6(7)(a) | AC-6(7)(a)[1] | визначає посади або класи користувачів, яким призначаються повноваження; |
| AC-6(7)(a)[2] | визначає частоту перегляду повноважень, присвоєних визначеним організацією посадам або класам користувачів для перевірки потреби в таких повноваженнях; |
| AC-6(7)(a)[3] | переглядає повноваження, призначені визначеним організацією ролям або класам користувачів з визначеною організацією частотою, щоб підтвердити потребу в таких повноваженнях; |
| AC-6(7)(b) | AC-6(7)(b){1} | При необхідності перепризначає для правильного відображення цілей (місії) організації та потреб організації. |
| AC-6(7)(b){2} | При необхідності знімає повноваження, для правильного відображення цілей (місії) організації та потреб організації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; список згенерованих системою ролей або класів користувачів та призначених привілеїв; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перевірка відповідності повноважень, призначених ролям, класів або користувачам; записи про видалення або перепризначення повноважень для ролей або класів користувачів; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перегляд мінімізації повноважень, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують перегляд прав користувачів]. | | |

|  |  |  |
| --- | --- | --- |
| AC-6(8) | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - РІВНІ ПРИВІЛЕЇВ ДЛЯ ВИКОНАННЯ КОДУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-6(8)[1] | організація визначає програмне забезпечення, на рівні привілеїв вищому, ніж доступний користувачу, який використовує програмне забезпечення; |
| AC-6(8)[2] | інформаційна система запобігає виконанню визначеного організацією програмного забезпечення на вищих рівнях привілеїв, ніж користувачі, що виконують це програмне забезпечення. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; перелік програмного забезпечення, яке не повинно виконуватись на вищих рівнях привілеїв, ніж мають користувачі, що виконують програмне забезпечення; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень для виконання програмного забезпечення]. | |

|  |  |  |
| --- | --- | --- |
| AC-6(9) | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - АУДИТ ВИКОРИСТАННЯ ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AC-6(9)[1] | Проводить аудит виконання привілейованих функцій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік пільгових функцій, що підлягають аудиту; перелік ревізованих подій; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перегляд мінімізації повноважень, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми аудиту виконання функцій мінімізації повноважень]. | |

|  |  |  |
| --- | --- | --- |
| AC-6(10) | МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ЗАБОРОНА НЕПРИВІЛЕЙОВАНИМ КОРИСТУВАЧАМ ВИКОНУВАТИ ПРИВІЛЕЙОВАНІ ФУНКЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-6(10)[1] | інформаційна система запобігає виконувати непривілейованим користувачам привілейовані функції для відключення впроваджених гарантій безпеки або контрзаходів; |
| AC-6(10)[2] | інформаційна система запобігає виконувати непривілейованим користувачам привілейовані функції для обходу гарантій безпеки або контрзаходів; |
| AC-6(10)[3] | інформаційна система запобігає виконувати непривілейованим користувачам привілейовані функції для зміни впроваджених гарантій безпеки або контрзаходів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік пільгових функцій та пов'язаних з ними призначень облікових записів користувачів; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень для непривілейованих користувачів]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-7 | НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| AC-7(a) | AC-7(a)[1] | організація визначає кількість послідовних недійсних спроб входу, дозволених користувачу інформаційною системою протягом визначеного організацією часу; | |
| AC-7(a)[2] | організація визначає часовий період, дозволений користувачу інформаційної системи для визначеної організацією кількості послідовних невдалих спроб входу; | |
| AC-7(a)[3] | інформаційна система виконує обмеження визначеної організацією кількості послідовних невдалих спроб входу користувачем протягом визначеного організацією періоду часу; | |
| AC-7(b) | AC-7(b)[1] | організація визначає період часу блокування облікового запису або вузла, який повинен автоматично застосовуватися інформаційною системою при перевищенні максимальної кількості невдалих спроб входу; | |
| AC-7(b)[2] | організація визначає алгоритм затримки входу до облікового запису або вузла, який повинен автоматично застосовуватися інформаційною системою при перевищенні максимальної кількості невдалих спроб входу; | |
| AC-7(b)[3] | AC-7(b)[3][1] | інформаційна система при перевищенні максимальної кількості невдалих спроб входу автоматично блокує обліковий запис або вузол на визначений організацією часовий період; |
| AC-7(b)[3][2] | інформаційна система при перевищенні максимальної кількості невдалих спроб входу автоматично блокує обліковий запис або вузол до розблокування адміністратором; |
| AC-7(b)[3][3] | інформаційна система при перевищенні максимальної кількості невдалих спроб входу автоматично затримує наступний запит на вхід відповідно до визначеного організацією алгоритму затримки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури вирішення невдалих спроб входу; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за безпеку інформації; розробники системи; системні або мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для невдалих спроб входу]. | | | |

|  |  |
| --- | --- |
| AC-7(1) | НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - АВТОМАТИЧНЕ БЛОКУВАННЯ ОБЛІКОВОГО ЗАПИСУ |
|  | [Вилучено: Включено в АС-7] |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-7(2) | НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - ОЧИЩЕННЯ АБО СТИРАННЯ МОБІЛЬНОГО ПРИСТРОЮ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-7(2)[1] | організація визначає мобільні пристрої, які потрібно очистити чи стерти після визначеної організацією кількості послідовних, невдалих спроб входу пристрою; | |
| AC-7(2)[2] | AC-7(2)[2][1] | організація визначає вимоги очищення чи стирання, які слід використовувати, коли визначені організацією мобільні пристрої очищаються чи стираються після організаційно визначеної кількості послідовних, невдалих спроб входу пристрою; |
| AC-7(2)[2][2] | організація визначає методи очищення чи стирання, які слід використовувати, коли визначені організацією мобільні пристрої очищаються або стираються після організаційно визначеної кількості послідовних, невдалих спроб входу пристрою; |
| AC-7(2)[3] | організація визначає кількість послідовних, невдалих спроб входу, дозволених для доступу до мобільних пристроїв до того, як інформаційна система очистить чи стирає інформацію з таких пристроїв; | |
| AC-7(2)[4] | інформаційна система очищує або стирає інформацію з визначених організацією мобільних пристроїв на основі визначених організацією вимог або методів очищення чи стирання після визначеної організацією кількості послідовних, невдалих спроб входу. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури вирішення невдалих спроб входу на мобільні пристрої; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік мобільних пристроїв, які потрібно очистити або стерти після визначених організацією послідовних, невдалих спроб входу для пристрою; перелік вимог чи методів очищення або витирання для мобільних пристроїв; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для невдалих спроб входу пристрою]. | | |

|  |  |  |
| --- | --- | --- |
| AC-7(3) | НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - ОБМЕЖЕННЯ НА СПРОБИ БІОМЕТРИЧНОГО ВХОДУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-7(3)[1] | організація визначає кількість невдалих спроб входу за допомогою біометрики |
| AC-7(3)[2] | організація обмежує кількість невдалих спроб входу за допомогою біометрики. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури вирішення невдалих спроб входу за допомогою біометрики; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для невдалих спроб входу за допомогою біометрики]. | |

|  |  |  |
| --- | --- | --- |
| AC-7(4) | НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - ВИКОРИСТАННЯ АЛЬТЕРНАТИВНОГО ФАКТОРА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-7(4)[1] | Дозволити використання одного або декількох додаткових факторів автентифікації після перевищення визначених організацією кількості послідовних невдалих спроб входу в систему. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для невдалих спроб входу]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| AC-8 | ПОПЕРЕДЖЕННЯ ПРО ВИКОРИСТАННЯ СИСТЕМИ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| AC-8(a) | AC-8(a)[1] | організація визначає попередження про використання системи або банер, які повинні відображатися інформаційною системою користувачам перед наданням доступу до системи; | | |
| AC-8(a)[2] | інформаційна система відображає для користувачів визначене організацією попередження про використання системи або банер перед наданням доступу до інформаційної системи, які надають повідомлення про конфіденційність та безпеку, відповідно до чинних законів, нормативних документів, наказів, директив, політик, правил, стандартів та керівних принципів та зазначає що: | | |
| AC-8(a)[2](1) | перед тим, як надавати доступ до системи, демонструвати користувачам визначене організацією сповіщення або банер про використання системи, які зазначають, що користувачі здійснюють доступ до урядової системи | |
| AC-8(a)[2](2) | AC-8(a)[2](2)[1] | перед тим, як надавати доступ до системи, демонструвати користувачам визначене організацією сповіщення або банер про використання системи, які зазначають, що використання системи може контролюватися |
| AC-8(a)[2](2)[2] | перед тим, як надавати доступ до системи, демонструвати користувачам визначене організацією сповіщення або банер про використання системи, які зазначають, що використання системи може реєструватися |
| AC-8(a)[2](2)[3] | перед тим, як надавати доступ до системи, демонструвати користувачам визначене організацією сповіщення або банер про використання системи, які зазначають, що Використання системи може підлягати аудиту |
| AC-8(a)[2](3) | перед тим, як надавати доступ до системи, демонструвати користувачам визначене організацією сповіщення або банер про використання системи, які зазначають, що несанкціоноване використання системи забороняється та приводить до кримінальної та цивільної відповідальності | |
| AC-8(a)[2](4) | перед тим, як надавати доступ до системи, демонструвати користувачам визначене організацією сповіщення або банер про використання системи, які зазначають, що використання системи означає згоду на моніторинг та запис дій користувача | |
| AC-8(b) | інформаційна система зберігає повідомлення або банер на екрані, доки користувачі не визнають умови використання та не приймуть явних дій для входу в систему або подальшого доступу до системи; | | | |
| AC-8(c) | AC-8(c)(1) | AC-8(c)(1)[1] | для загальнодоступних систем, організація визначає умови використання системи які відображаються інформаційною системою до надання подальшого доступу; | |
| AC-8(c)(1)[2] | для загальнодоступних систем, інформаційна система демонструє інформацію про визначені організацією умови використання системи перед наданням подальшого доступу; | |
| AC-8(c)(2) | AC-8(c)(2)[1] | загальнодоступна інформаційна система демонструє посилання, якщо такі є, на моніторинг, які узгоджуються з акомодацією приватності для таких систем, які зазвичай забороняють такі дії | |
| AC-8(c)(2)[2] | загальнодоступна інформаційна система демонструє посилання, якщо такі є, на запис, які узгоджуються з акомодацією приватності для таких систем, які зазвичай забороняють такі дії | |
| AC-8(c)(2)[3] | загальнодоступна інформаційна система демонструє посилання, якщо такі є, на аудит, які узгоджуються з акомодацією приватності для таких систем, які зазвичай забороняють такі дії | |
| AC-8(c)(3) | загальнодоступна інформаційна система має опис авторизованого використання системи | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політики конфіденційності та безпеки, процедури щодо сповіщення про використання системи; документально підтверджене повідомлення про використання інформаційних систем повідомленнями або банерами; записи аудиту інформаційної системи; підтвердження користувачем отримання повідомлення або банера; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; використання інформаційними системами повідомлень про сповіщення; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, відповідальний за надання юридичних консультацій; розробники системи]  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують сповіщення про використання системи]. | | | | |

|  |  |  |
| --- | --- | --- |
| AC-9 | СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) | |
|  | МЕТА ОЦІНКИ:  Визначте, чи | |
| AC-9[1] | інформаційна система повідомляє користувача при успішному вході (доступі) до системи про дату та час останнього входу (доступу). |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо попереднього повідомлення про вхід; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; повідомлення про сповіщення інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для повідомлення про попередній вхід до системи]. | |

|  |  |  |
| --- | --- | --- |
| AC-9(1) | СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) - НЕВДАЛІ СПРОБИ ВХОДУ ДО СИСТЕМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи | |
| AC-9(1)[1] | інформаційна система сповіщає користувача після успішного входу / доступу про кількість невдалих спроб входу / доступу з моменту останнього успішного входу / доступу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо попереднього повідомлення про вхід; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для попереднього повідомлення про вхід]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-9(2) | СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) - УСПІШНІ ТА НЕВДАЛІ СПРОБИ ВХОДУ ДО СИСТЕМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-9(2)[1] | AC-9(2)[1]{1} | організація визначає часовий період, протягом якого інформаційна система повинна сповіщати користувача про кількість успішних входів / доступу; |
| AC-9(2)[1]{2} | організація визначає часовий період, протягом якого інформаційна система повинна сповіщати користувача про кількість невдалих спроб входу / доступу; |
| AC-9(2)[2] | інформаційна система після успішного входу / доступу до системи протягом визначеного організацією періоду часу повідомляє користувача про кількість(один або кілька): | |
| AC-9(2)[2]{1} | успішних входів (доступу) |
| AC-9(2)[2]{2} | невдалих спроб входу (доступу) |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо повідомлення про попередній вхід; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для повідомлення про попередній вхід]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-9(3) | СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) - ПОВІДОМЛЕННЯ ПРО ЗМІНИ В ОБЛІКОВОМУ ЗАПИСІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-9(3)[1] | організація визначає пов’язані з безпекою характеристики / параметри облікового запису користувача; | |
| AC-9(3)[2] | AC-9(3)[2][1] | організація визначає часовий період, протягом якого мають сповістити користувача про зміни, що відбулися в організаційно визначених характеристиках безпеки; |
| AC-9(3)[2][2] | організація визначає часовий період, протягом якого мають сповістити користувача про зміни, що відбулися в організаційно визначених параметрах облікового запису користувача; |
| AC-9(3)[3] | AC-9(3)[3][1] | інформаційна система сповіщає користувача, після успішного входу / доступу, про внесення змін до певних характеристик облікового запису користувача, визначених організацією протягом визначеного організацією періоду часу. |
| AC-9(3)[3][2] | інформаційна система сповіщає користувача, після успішного входу / доступу, про внесення змін до певних параметрів облікового запису користувача, визначених організацією протягом визначеного організацією періоду часу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо попереднього повідомлення про вхід; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для повідомлення про попередній вхід]. | | |

|  |  |  |
| --- | --- | --- |
| AC-9(4) | СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) – ДОДАТКОВА ІНФОРМАЦІЯ ПРО ВХІД | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-9(4)[1] | організація визначає інформацію, яку слід сповіщати користувачеві на додаток до дати та часу останнього входу (доступу); |
| AC-9(4)[2] | інформаційна система після успішного входу (доступу) повідомляє користувача про інформацію, визначену організацією, яка повинна бути включена на додаток до дати та часу останнього входу (доступу). |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо попереднього повідомлення про вхід; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для повідомлення про попередній вхід]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-10 | УПРАВЛІННЯ ПАРАЛЕЛЬНОЮ СЕСІЄЮ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-10[1] | AC-10[1]{1} | організація визначає облікові записи для інформаційної системи, які підпадають під політику управління паралельною сесією. Та чи або: |
| AC-10[1]{2} | організація визначає типи облікових записів для інформаційної системи, які підпадають під політику управління паралельною сесією |
| AC-10[2] | AC-10[2][1] | організація визначає кількість одночасних сеансів, дозволених для кожного визначеного організацією облікового запису; |
| AC-10[2][2] | організація визначає кількість одночасних сеансів, дозволених для кожного визначеного організацією типу облікового запису; |
| AC-10[3] | AC-10[3][1] | інформаційна система обмежує кількість одночасних сесій для кожного визначеного організацією облікового запису до визначеної організацією кількості дозволених одночасних сесій. |
| AC-10[3][2] | інформаційна система обмежує кількість одночасних сесій для кожного визначеного організацією типу облікового запису до визначеної організацією кількості дозволених одночасних сесій. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються паралельного контролю сеансу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для паралельного контролю сеансу]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-11 | БЛОКУВАННЯ ПРИСТРОЮ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-11(a) | AC-11(a)[1] | організація визначає часовий період бездіяльності користувача, після якого інформаційна система ініціює блокування сеансу; |
| AC-11(a)[2] | інформаційна система перешкоджає подальшому доступу до системи шляхом ініціювання блокування сеансу після визначеного організацією часового періоду бездіяльності користувача; |
| AC-11(a)[3] | інформаційна система перешкоджає подальшому доступу до системи шляхом ініціювання блокування сеансу після отримання запиту від користувача; |
| AC-11(b) | інформаційна система зберігає блокування сеансу, поки користувач не відновить доступ, використовуючи встановлені процедури ідентифікації та автентифікації. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо блокування сеансу; процедури щодо ідентифікації та автентифікації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для блокування сеансу]. | | |

|  |  |  |
| --- | --- | --- |
| AC-11(1) | БЛОКУВАННЯ ПРИСТРОЮ - ПРИХОВАНІ ДИСПЛЕЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи | |
| AC-11(1)[1] | інформаційна система приховує через блокування сеансу інформацію, попередньо видиму на дисплеї, загальнодоступним зображенням. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо блокування сеансу; екран дисплея з активованим блокуванням сеансу; проектна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Механізми блокування сеансу інформаційної системи] | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-12 | ПРИПИНЕННЯ СЕАНСУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-12[1] | AC-12[1][1] | організація визначає умови, що вимагають відключення сеансу; |
| AC-12[1][2] | організація визначає тригерні події, що вимагають відключення сеансу; |
| AC-12[2] | AC-12[2][1] | інформаційна система автоматично припиняє сеанс користувача після того, як трапляються визначені організацією умови, що вимагають відключення сеансу. |
| AC-12[2][2] | інформаційна система автоматично припиняє сеанс користувача після того, як трапляються визначені організацією тригерні події, що вимагають відключення сеансу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються припинення сеансу; проектна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік умов або подій запуску, які вимагають відключення сеансу; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують припинення сеансу користувача]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-12(1) | ПРИПИНЕННЯ СЕАНСУ - ІНІЦІЙОВАНЕ КОРИСТУВАЧЕМ БЛОКУВАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-12(1) | AC-12(1)[1] | визначає організація інформаційні ресурси, для отримання доступу до яких необхідна автентифікація користувачів; |
| AC-12(1)[2] | інформаційна система забезпечує можливість виходу для сеансів зв'язку, що визначаються користувачем, коли аутентифікація використовується для отримання доступу до визначених організацією інформаційних ресурсів; |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються припинення сеансу; повідомлення виходу користувача; проектна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Механізми блокування сеансу інформаційної системи]. | | |

|  |  |  |
| --- | --- | --- |
| AC-12(2) | ПРИПИНЕННЯ СЕАНСУ - ПОВІДОМЛЕННЯ ПРО ПРИПИНЕННЯ СЕАНСУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-12(2)[1] | інформаційна система відображає покладне повідомлення про вихід користувачів із системи зі зазначенням достовірної інформації про припинення аутентифікованих сеансів зв'язку. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються припинення сеансу; повідомлення виходу користувача; проектна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Механізми блокування сеансу інформаційної системи]. | |

|  |  |  |
| --- | --- | --- |
| AC-12(3) | ПРИПИНЕННЯ СЕАНСУ - ЗАСТЕРЕЖНЕ ПОВІДОМЛЕННЯ ПРО ТЕ, ЩО ЧАС СЕСІЇ ДОБІГАЄ КІНЦЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-12(3)[1] | інформаційна система відображає виразне повідомлення користувачам, що вказує, що час сесії добігає кінця. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються припинення сеансу; повідомлення виходу користувача; проектна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Механізми блокування сеансу інформаційної системи]. | |

|  |  |
| --- | --- |
| AC-13 | НАГЛЯД ТА ОГЛЯД - УПРАВЛІННЯ ДОСТУПОМ |
|  | [Вилучено: включено в АС-2 й АС-6]. |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-14 | ДОЗВОЛЕНІ ДІЇ БЕЗ ІДЕНТИФІКАЦІЇ АБО АВТЕНТИФІКАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-14(a) | AC-14(a)[1] | визначає дії користувача, які можуть виконуватися в інформаційній системі без ідентифікації, що відповідає організаційним завданням або функціям; |
| AC-14(a)[2] | визначає дії користувача, які можуть виконуватися в інформаційній системі без автентифікації, що відповідає організаційним завданням або функціям; |
| AC-14(a)[3] | ідентифікує визначені організацією дії користувачів, які можуть виконуватися в системі без ідентифікації або автентифікації відповідно до організаційних завдань та функцій |
| AC-14(b) | AC-14(b)[1] | документує та визначає відповідне обґрунтування в плані безпеки системи дій користувача, які не потребують ідентифікації |
| AC-14(b)[2] | документує та визначає відповідне обґрунтування в плані безпеки системи дій користувача, які не потребують автентифікації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури вирішення дозволених дій без ідентифікації чи автентифікації; налаштування конфігурації інформаційної системи та супутня документація; план безпеки; перелік дій користувача, які можна виконати без ідентифікації чи автентифікації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку] | | |

|  |  |
| --- | --- |
| AC-14(1) | ДОЗВОЛЕНІ ДІЇ БЕЗ ІДЕНТИФІКАЦІЇ АБО АВТЕНТИФІКАЦІЇ - НЕОБХІДНЕ ВИКОРИСТАННЯ |
|  | [Вилучено: включено до AC-14]. |

|  |  |
| --- | --- |
| AC-15 | АВТОМАТИЗОВАНЕ МАРКУВАННЯ |
|  | [Вилучено: включено до MP-3]. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| AC-16 | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | |
| AC-16(a) | AC-16(a)[1] | AC-16(a)[1]{1} | визначає типи атрибутів безпеки, які мають бути пов'язані з інформацією на зберіганні; | |
| AC-16(a)[1]{2} | визначає типи атрибутів безпеки, які мають бути пов'язані з інформацією при обробці | |
| AC-16(a)[1]{3} | визначає типи атрибутів безпеки, які мають бути пов'язані з інформацією при передачі | |
| AC-16(a)[2] | AC-16(a)[2]{1} | визначає типи атрибутів приватності, які мають бути пов'язані з інформацією на зберіганні; | |
| AC-16(a)[2]{2} | визначає типи атрибутів приватності, які мають бути пов'язані з інформацією при обробці | |
| AC-16(a)[2]{3} | визначає типи атрибутів приватності, які мають бути пов'язані з інформацією при передачі | |
| AC-16(a)[3] | визначає значення атрибутів безпеки для визначених організацією типів атрибутів безпеки; | | |
| AC-16(a)[4] | визначає значення атрибутів приватності для визначених організацією типів атрибутів безпеки; | | |
| AC-16(a)[5] | AC-16(a)[5]{1} | | Визначає засоби для асоціювання (пов’язання): визначених організацією типів атрибутів безпеки та приватності, що приймають визначені організацією значення атрибутів безпеки та приватності з інформацією яка зберігається |
| AC-16(a)[5]{2} | | Визначає засоби для асоціювання (пов’язання): визначених організацією типів атрибутів безпеки та приватності, що приймають визначені організацією значення атрибутів безпеки та приватності з інформацією яка обробляється |
| AC-16(a)[5]{3} | | Визначає засоби для асоціювання (пов’язання): визначених організацією типів атрибутів безпеки та приватності, що приймають визначені організацією значення атрибутів безпеки та приватності з інформацією яка передається |
| AC-16(b) | AC-16(b)[1] | забезпечує, щоб пов’язані атрибути безпеки та приватності створювалися разом з інформацією | | |
| AC-16(b)[2] | забезпечує, щоб пов’язані атрибути безпеки та приватності зберігались разом з інформацією | | |
| AC-16(c) | AC-16(c)[1] | визначає інформаційні системи, для яких слід встановити дозволені організаційно визначені атрибути безпеки; | | |
| AC-16(c)[2] | визначає атрибути безпеки, дозволені для організаційно визначених інформаційних систем; | | |
| AC-16(c)[3] | встановлює дозволені атрибути безпеки, визначені організацією, для визначених організацією інформаційних систем; | | |
| AC-16(d) | AC-16(d)[1] | AC-16(d)[1][1] | встановлює дозволені значення для атрибутів безпеки; | |
| AC-16(d)[1][2] | встановлює дозволені діапазони для атрибутів безпеки; | |
| AC-16(d)[1][3] | встановлює дозволені значення для атрибутів приватності; | |
| AC-16(d)[1][4] | встановлює дозволені діапазони для атрибутів приватності; | |
| AC-16(d)[2] | **AC-16(d)[2][1]** | присвоює визначені організацією значення для для кожного з встановлених атрибутів безпеки | |
| **AC-16(d)[2][2]** | присвоює визначені організацією діапазони для для кожного з встановлених атрибутів безпеки; | |
| **AC-16(d)[2][3]** | присвоює визначені організацією значення для для кожного з встановлених атрибутів приватності | |
| **AC-16(d)[2][4]** | присвоює визначені організацією діапазони для для кожного з встановлених атрибутів приватності; | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, пов'язані з асоціацією атрибутів безпеки з інформацією, що зберігається, обробляється та передається; проектна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Організаційна спроможність підтримувати асоціацію атрибутів безпеки з інформацією, що зберігається, обробляється та передається]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-16(1) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ДИНАМІЧНЕ ПОВ’ЯЗАННЯ АТРИБУТІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-16(1)[1] | організація визначає суб'єкти, з якими атрибути безпеки повинні динамічно асоціюватися при створенні та об'єднанні інформації; | |
| AC-16(1)[2] | організація визначає об'єкти, з якими атрибути безпеки повинні динамічно асоціюватися при створенні та об'єднанні інформації; | |
| AC-16(1)[3] | організація визначає політики безпеки, що вимагають від інформаційної системи динамічного асоціювання атрибутів безпеки з визначеними організацією суб’єктами та об'єктами | |
| AC-16(1)[4] | AC-16(1)[4][1] | інформаційна система динамічно пов’язує атрибути безпеки з визначеними організацією суб'єктами відповідно до визначених організацією політик безпеки та приватності, у міру створення та об'єднання інформації |
| AC-16(1)[4][2] | інформаційна система динамічно пов’язує атрибути безпеки з визначеними організацією об'єктами відповідно до визначених організацією політик безпеки та приватності, у міру створення та об'єднання інформації |
| AC-16(1)[4][3] | інформаційна система динамічно пов’язує атрибути приватності з визначеними організацією суб'єктами відповідно до визначених організацією політик безпеки та приватності, у міру створення та об'єднання інформації |
| AC-16(1)[4][4] | інформаційна система динамічно пов’язує атрибути приватності з визначеними організацією об'єктами відповідно до визначених організацією політик безпеки та приватності, у міру створення та об'єднання інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на динамічну асоціацію атрибутів безпеки з інформацією; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують динамічну асоціацію атрибутів безпеки з інформацією]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-16(2) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ЗМІНА ЗНАЧЕНЬ АТРИБУТІВ АВТОРИЗОВАНИМИ ОСОБАМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-16(2)[1] | AC-16(2)[1][1] | інформаційна система надає уповноваженим особам можливість визначати значення відповідних атрибутів безпеки |
| AC-16(2)[1][2] | інформаційна система надає уповноваженим особам можливість змінювати значення відповідних атрибутів безпеки |
| AC-16(2)[1][3] | інформаційна система надає уповноваженим особам можливість визначати значення відповідних атрибутів приватності |
| AC-16(2)[1][4] | інформаційна система надає уповноваженим особам можливість змінювати значення відповідних атрибутів приватності |
| AC-16(2)[2] | AC-16(2)[2][1] | інформаційна система надає уповноваженим процесам, що діють від імені фізичних осіб можливість визначати значення відповідних атрибутів безпеки |
| AC-16(2)[2][2] | інформаційна система надає уповноваженим процесам, що діють від імені фізичних осіб можливість змінювати значення відповідних атрибутів безпеки |
| AC-16(2)[2][3] | інформаційна система надає уповноваженим процесам, що діють від імені фізичних осіб можливість визначати значення відповідних атрибутів приватності |
| AC-16(2)[2][4] | інформаційна система надає уповноваженим процесам, що діють від імені фізичних осіб можливість змінювати значення відповідних атрибутів приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на зміну значень атрибутів безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; список осіб, уповноважених змінювати атрибути безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за зміну значень атрибутів безпеки; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що дозволяють змінювати значення атрибутів безпеки]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-16(3) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПІДТРИМКА СИСТЕМОЮ ПОВ’ЯЗАННЯ АТРИБУТІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-16(3)[1] | AC-16(3)[1][1] | організація визначає атрибути безпеки, пов'язані з організаційно визначеними суб'єктами та об'єктами; |
| AC-16(3)[1][2] | організація визначає атрибути приватності, пов'язані з організаційно визначеними суб'єктами та об'єктами; |
| AC-16(3)[2] | AC-16(3)[2][1] | організація визначає суб'єкти, що вимагають пов’язання та цілісності атрибутів безпеки з суб'єктами та об'єктами, які повинні підтримуватися; |
| AC-16(3)[2][2] | організація визначає об'єкти, що вимагають пов’язання та цілісності атрибутів безпеки з суб'єктами та об'єктами, які повинні підтримуватися; |
| AC-16(3)[3] | AC-16(3)[3][1] | інформаційна система підтримує пов’язання визначених організацією атрибутів безпеки та приватності з визначених організацією суб'єктів та об'єктів. |
| AC-16(3)[3][2] | інформаційна система підтримує цілісність визначених організацією атрибутів безпеки та приватності з визначених організацією суб'єктів та об'єктів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо об'єднання атрибутів безпеки до інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за захист інформації; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують об’єднання та цілісність атрибутів безпеки з інформацією]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-16(4) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПОВ’ЯЗАННЯ АТРИБУТІВ АВТОРИЗОВАНИМИ ОСОБАМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-16(4)[1] | AC-16(4)[1][1] | організація визначає атрибути безпеки, пов'язані з організаційно визначеними авторизованими особами; |
| AC-16(4)[1][2] | організація визначає атрибути приватності, пов'язані з організаційно визначеними авторизованими особами; |
| AC-16(4)[2] | AC-16(4)[2][1] | організація визначає суб'єкти, що вимагають пов’язання та цілісності атрибутів безпеки з авторизованими особами, які повинні підтримуватися; |
| AC-16(4)[2][2] | організація визначає об'єкти, що вимагають пов’язання та цілісності атрибутів безпеки з авторизованими особами, які повинні підтримуватися; |
| AC-16(4)[3] | AC-16(4)[3][1] | інформаційна система впроваджує можливість пов’язувати уповноваженими особами визначені організацією атрибути безпеки з визначеними організацією суб'єктами. |
| AC-16(4)[3][2] | інформаційна система впроваджує можливість пов’язувати уповноваженими особами визначені організацією атрибути безпеки з визначеними організацією об'єктами. |
| AC-16(4)[3][3] | інформаційна система впроваджує можливість пов’язувати уповноваженими особами визначені організацією атрибути приватності з визначеними організацією суб'єктами |
| AC-16(4)[3][4] | інформаційна система впроваджує можливість пов’язувати уповноваженими особами визначені організацією атрибути приватності з визначеними організацією об'єктами. |
| AC-16(4)[3][5] | інформаційна система впроваджує можливість пов’язувати уповноваженими процесами, що діють від імені фізичних осіб, визначені організацією атрибути безпеки з визначеними організацією суб'єктами. |
| AC-16(4)[3][6] | інформаційна система впроваджує можливість пов’язувати уповноваженими процесами, що діють від імені фізичних осіб, визначені організацією атрибути безпеки з визначеними організацією об'єктами. |
| AC-16(4)[3][7] | інформаційна система впроваджує можливість пов’язувати уповноваженими процесами, що діють від імені фізичних осіб, визначені організацією атрибути приватності з визначеними організацією суб'єктами. |
| AC-16(4)[3][8] | інформаційна система впроваджує можливість пов’язувати уповноваженими процесами, що діють від імені фізичних осіб, визначені організацією атрибути приватності з визначеними організацією об'єктами. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури стосовно об'єднання атрибутів безпеки з інформацією; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; список користувачів, уповноважених асоціювати атрибути безпеки до інформації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за асоціацію атрибутів безпеки до інформації; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи]  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують об’єднання атрибутів безпеки з інформацією користувачами]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-16(5) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ВІДОБРАЖЕННЯ АТРИБУТІВ НА ПРИСТРОЯХ ВИВЕДЕННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| AC-16(5)[1] | AC-16(5)[1][1] | організація визначає спеціальні інструкції щодо поширення інформації, що використовуються для кожного об'єкта, який інформаційна система передає на пристрої виведення; | |
| AC-16(5)[1][2] | організація визначає спеціальні інструкції щодо обробки інформації, що використовуються для кожного об'єкта, який інформаційна система передає на пристрої виведення | |
| AC-16(5)[1][3] | організація визначає спеціальні інструкції щодо наступного розподілу інформації, що використовуються для кожного об'єкта, який інформаційна система передає на пристрої виведення | |
| AC-16(5)[2] | Визначає організація ідентифікацію, в зручній для людини формі про стандартні угоди про присвоєння імен. | | |
| AC-16(5)[3] | **AC-16(5)[3][1]** | **AC-16(5)[3][1][1]** | Відображати атрибути безпеки в зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати визначені організацією спеціальні інструкції щодо поширення інформації, використовуючи визначену організацією ідентифікацію, в зручній для людини формі про стандартні угоди про присвоєння імен. |
| **AC-16(5)[3][1][2]** | Відображати атрибути безпеки в зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати визначені організацією спеціальні інструкції щодо обробки інформації, використовуючи визначену організацією ідентифікацію, в зручній для людини формі про стандартні угоди про присвоєння імен. |
| **AC-16(5)[3][1][3]** | Відображати атрибути безпеки в зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати визначені організацією спеціальні інструкції щодо наступного розподілу інформації, використовуючи визначену організацією ідентифікацію, в зручній для людини формі про стандартні угоди про присвоєння імен. |
| **AC-16(5)[3][2]** | **AC-16(5)[3][2][1]** | Відображати атрибути приватності в зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати визначені організацією спеціальні інструкції щодо поширення інформації, використовуючи визначену організацією ідентифікацію, в зручній для людини формі про стандартні угоди про присвоєння імен. |
| **AC-16(5)[3][2][2]** | Відображати атрибути приватності в зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати визначені організацією спеціальні інструкції щодо обробки інформації, використовуючи визначену організацією ідентифікацію, в зручній для людини формі про стандартні угоди про присвоєння імен. |
| **AC-16(5)[3][2][3]** | Відображати атрибути приватності в зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати визначені організацією спеціальні інструкції щодо наступного розподілу інформації, використовуючи визначену організацією ідентифікацію, в зручній для людини формі про стандартні угоди про присвоєння імен. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються відображення атрибутів безпеки у читаній для людини формі; спеціальні інструкції щодо розповсюдження, поводження чи поширення; типи зрозумілих для людини, ідентифікованих організацією стандартних угод про іменування; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за безпеку інформації; розробники системи].  Перевірка: [ВИБІР: Пристрої виведення системи, що відображають атрибути захисту у читаному для людини вигляді на кожному об'єкті]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-16(6) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПІДТРИМКА ПОВ’ЯЗАННЯ АТРИБУТІВ ОРГАНІЗАЦІЄЮ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-16(6)[1] | AC-16(6)[1][1] | організація визначає атрибути безпеки, пов'язані з організаційно визначеними суб'єктами та об'єктами; |
| AC-16(6)[1][2] | організація визначає атрибути приватності, пов'язані з організаційно визначеними суб'єктами та об'єктами; |
| AC-16(6)[2] | AC-16(6)[2][1] | організація визначає суб'єкти, що вимагають пов’язання та цілісності атрибутів безпеки з суб'єктами та об'єктами, які повинні підтримуватися; |
| AC-16(6)[2][2] | організація визначає об'єкти, що вимагають пов’язання та цілісності атрибутів безпеки з суб'єктами та об'єктами, які повинні підтримуватися; |
| AC-16(6)[3] | AC-16(6)[3][1] | визначає політику безпеки, яка дозволяє персоналу асоціювати та підтримувати зв'язок визначених організацією ознак безпеки з організаційно визначеними суб'єктами та об'єктами; |
| AC-16(6)[3][2] | визначає політику приватності, яка дозволяє персоналу асоціювати та підтримувати зв'язок визначених організацією ознак безпеки з організаційно визначеними суб'єктами та об'єктами; |
| AC-16(6)[4] | AC-16(6)[4][1] | вимагає від персоналу пов’язувати асоціацію визначених організацією атрибутів безпеки та приватності з визначеними організацією суб'єктами та об'єктами відповідно до визначеної організацією політики безпеки та приватності |
| AC-16(6)[4][2] | вимагає від персоналу підтримувати асоціацію визначених організацією атрибутів безпеки та приватності з визначеними організацією суб'єктами та об'єктами відповідно до визначеної організацією політики безпеки та приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, пов'язані з об'єднанням атрибутів безпеки з суб’єктами та об'єктами; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за асоціацію та підтримку асоціації атрибутів безпеки з суб’єктами та об'єктами; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують асоціації атрибутів безпеки з суб’єктами та об'єктами]. | | |

|  |  |  |
| --- | --- | --- |
| AC-16(7) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПОСЛІДОВНА ІНТЕРПРЕТАЦІЯ АТРИБУТІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-16(7)[1] | забезпечує організація послідовну інтерпретацію атрибутів безпеки, що передаються між розподіленими компонентами системи. |
| AC-16(7)[2] | забезпечує організація послідовну інтерпретацію атрибутів приватності, що передаються між розподіленими компонентами системи. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються послідовної інтерпретації атрибутів безпеки, що передаються між компонентами розподіленої інформаційної системи; процедури щодо забезпечення доступу; процедури щодо забезпечення інформаційного потоку; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення послідовної інтерпретації атрибутів безпеки, які використовуються в діях щодо забезпечення доступу і забезпечення потоку інформації; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу та забезпечення інформаційного потоку]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-16(8) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ТЕХНІКИ ТА ТЕХНОЛОГІЇ ПОВ'ЯЗАННЯ АТРИБУТІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-16(8)[1] | AC-16(8)[1][1] | організація визначає техніки, які слід застосовувати при асоціації атрибутів безпеки з інформацією; |
| AC-16(8)[1][2] | організація визначає технології, які слід застосовувати при асоціації атрибутів безпеки з інформацією; |
| AC-16(8)[2] | організація визначає рівень гарантії, який повинен надаватися, коли інформаційна система впроваджує визначені організацією технології або технології для прив'язки атрибутів безпеки до інформації; | |
| AC-16(8)[3] | AC-16(8)[3][1] | інформаційна система реалізує визначені організацією техніки з визначеним організацією рівнем гарантії пов’язання атрибутів безпеки з інформацією |
| AC-16(8)[3][2] | інформаційна система реалізує визначені організацією техніки з визначеним організацією рівнем гарантії пов’язання атрибутів приватності з інформацією |
| AC-16(8)[3][3] | інформаційна система реалізує визначені організацією технології з визначеним організацією рівнем гарантії пов’язання атрибутів безпеки з інформацією |
| AC-16(8)[3][4] | інформаційна система реалізує визначені організацією технології з визначеним організацією рівнем гарантії пов’язання атрибутів приватності з інформацією |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, пов'язані з об'єднанням атрибутів безпеки з інформацією; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за асоціацію атрибутів безпеки з інформацією; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують методи або технології, що асоціюють атрибути безпеки з інформацією]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-16(9) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПЕРЕПРИЗНАЧЕННЯ АТРИБУТІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-16(9)[1] | AC-16(9)[1][1] | визначає техніки для затвердження механізмів переоцінки, використовуваних для перерозподілу асоціації атрибутів безпеки з інформацією; |
| AC-16(9)[1][2] | визначає процедури для затвердження механізмів переоцінки, використовуваних для перерозподілу асоціації атрибутів безпеки з інформацією; |
| AC-16(9)[2] | AC-16(9)[2][1] | перепризначення атрибутів безпеки, пов'язаних з інформацією, здійснювати лише за допомогою механізмів перегляду, перевірених з використанням визначених організацією технік або процедур |
| AC-16(9)[2][2] | перепризначення атрибутів приватності, пов'язаних з інформацією, здійснювати лише за допомогою механізмів перегляду, перевірених з використанням визначених організацією технік або процедур |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на перерозподіл атрибутів безпеки інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перерозподіл об'єднання атрибутів безпеки до інформації; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують методи або процедури перерозподілу об'єднання атрибутів безпеки до інформації]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-16(10) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - КОНФІГУРАЦІЯ АТРИБУТІВ УПОВНОВАЖЕНИМИ ОСОБАМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи. | | |
| AC-16(10)[1] | AC-16(10)[1][1] | надати уповноваженим особам можливість визначати тип атрибутів безпеки, доступних для пов'язання з суб’єктами та об'єктами |
| AC-16(10)[1][2] | надати уповноваженим особам можливість визначати тип атрибутів приватності, доступних для пов'язання з суб’єктами та об'єктами |
| AC-16(10)[1][3] | надати уповноваженим особам можливість визначати значення атрибутів безпеки, доступних для пов'язання з суб’єктами та об'єктами |
| AC-16(10)[1][4] | надати уповноваженим особам можливість визначати значення атрибутів приватності, доступних для пов'язання з суб’єктами та об'єктами |
| AC-16(10)[2] | AC-16(10)[2][1] | надати уповноваженим особам можливість змінювати тип атрибутів безпеки, доступних для пов'язання з суб’єктами та об'єктами |
| AC-16(10)[2][2] | надати уповноваженим особам можливість змінювати тип атрибутів приватності, доступних для пов'язання з суб’єктами та об'єктами |
| AC-16(10)[2][3] | надати уповноваженим особам можливість змінювати значення атрибутів безпеки, доступних для пов'язання з суб’єктами та об'єктами |
| AC-16(10)[2][4] | надати уповноваженим особам можливість змінювати значення атрибутів приватності, доступних для пов'язання з суб’єктами та об'єктами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на налаштування атрибутів безпеки уповноваженими особами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення або зміну атрибутів безпеки, пов'язаних з інформацією; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливість визначення або зміни атрибутів безпеки]. | | |

|  |  |  |
| --- | --- | --- |
| AC-16(11) | АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - АУДИТ ЗМІН | |
|  | МЕТА ОЦІНКИ:  Визначте, чи.організація: | |
| AC-16(11)[1] | проводить аудит змін атрибутів безпеки |
| AC-16(11)[2] | проводить аудит змін атрибутів приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на налаштування атрибутів безпеки уповноваженими особами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення або зміну атрибутів безпеки, пов'язаних з інформацією; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливість визначення або зміни атрибутів безпеки]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-17 | ВІДДАЛЕНИЙ ДОСТУП | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-17(a) | AC-17(a)[1] | встановлює та задокументовує обмеження на використання щодо здійснення кожного типу віддаленого доступу, |
| AC-17(a)[2] | встановлює та задокументовує вимоги до конфігурації або підключення щодо здійснення кожного типу віддаленого доступу, |
| AC-17(a)[3] | встановлює та задокументовує рекомендації щодо здійснення кожного типу віддаленого доступу щодо здійснення кожного типу віддаленого доступу |
| AC-17(b) | авторизує віддалений доступ до системи перш ніж будуть дозволені такі підключення | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання віддаленого доступу (включаючи обмеження); план управління конфігурацією; план безпеки; налаштування конфігурації інформаційної системи та супутня документація; авторизація віддаленого доступу; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління з'єднаннями віддаленого доступу; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Можливість віддаленого доступу до інформаційної системи]. | | |

|  |  |  |
| --- | --- | --- |
| AC-17(1) | ВІДДАЛЕНИЙ ДОСТУП - АВТОМАТИЗОВАНИЙ МОНІТОРИНГ ТА УПРАВЛІННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи інформаційна система: | |
| AC-17(1)[1] | проводить моніторинг методами віддаленого доступу |
| AC-17(1)[2] | проводить управління методами віддаленого доступу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на віддалений доступ до інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; записи моніторингу інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми моніторингу та контролю методів віддаленого доступу]. | |

|  |  |  |
| --- | --- | --- |
| AC-17(2) | ВІДДАЛЕНИЙ ДОСТУП - ЗАХИСТ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ЗА ДОПОМОГОЮ ШИФРУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи інформаційна система | |
| AC-17(2)[1] | запроваджує криптографічні механізми для захисту конфіденційності сесій віддаленого доступу |
| AC-17(2)[2] | запроваджує криптографічні механізми для захисту цілісності сесій віддаленого доступу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на віддалений доступ до інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; криптографічні механізми та пов'язана з ними конфігураційна документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Криптографічні механізми, що захищають конфіденційність та цілісність сеансів віддаленого доступу]. | |

|  |  |  |
| --- | --- | --- |
| AC-17(3) | ВІДДАЛЕНИЙ ДОСТУП - КЕРОВАНІ ТОЧКИ КОНТРОЛЮ ДОСТУПУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-17(3)[1] | організація визначає кількість керованих точок контролю доступу до мережі, через які слід здійснювати маршрутизацію всього віддаленого доступу; |
| AC-17(3)[2] | інформаційна система спрямовує всі віддалені доступи через визначену в організації кількість керованих точок контролю доступу до мережі. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на віддалений доступ до інформаційної системи; проєктна документація інформаційної системи; перелік усіх керованих точок контролю доступу до мережі; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що здійснюють маршрутизацію всього віддаленого доступу через керовані точки контролю доступу до мережі]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-17(4) | ВІДДАЛЕНИЙ ДОСТУП - ПРИВІЛЕЙОВАНІ КОМАНДИ ТА ДОСТУП | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | |
| AC-17(4)(a) | AC-17(4)(a)[1] | AC-17(4)(a)[1][1] | визначає необхідність авторизації при виконанні привілейованих команд до інформації, що належать до безпеки, через віддалений доступ; |
| AC-17(4)(a)[1][2] | визначає необхідність авторизації при виконанні доступу до інформації, що належать до безпеки, через віддалений доступ; |
| AC-17(4)(a)[2] | AC-17(4)(a)[2][1] | надає авторизацію на виконання привілейованих команд до інформації, що стосується безпеки, через віддалений доступ лише для визначених організацією потреб; |
| AC-17(4)(a)[2][2] | надає авторизацію на доступ до інформації, що стосується безпеки, через віддалений доступ лише для визначених організацією потреб; |
| AC-17(4)(b) | документує обґрунтування такого доступу в плані безпеки інформаційної системи. | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на віддалений доступ до інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; план безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують управління віддаленим доступом]. | | | |

|  |  |
| --- | --- |
| AC-17(5) | ВІДДАЛЕНИЙ ДОСТУП - МОНІТОРИНГ ДЛЯ НЕАВТОРИЗОВАНИХ ПІДКЛЮЧЕНЬ |
|  | [Вилучено: Включено в СІ-4]. |

|  |  |  |
| --- | --- | --- |
| AC-17(6) | ВІДДАЛЕНИЙ ДОСТУП - ЗАХИСТ ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AC-17(6)[1] | забезпечує захист інформації щодо механізмів віддаленого доступу від неавторизованого використання |
| AC-17(6)[2] | забезпечує захист інформації щодо механізмів віддаленого доступу від розкриття |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються віддаленого доступу до інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за впровадження або моніторинг віддаленого доступу до інформаційної системи; користувачі інформаційної системи, що володіють знаннями про механізми віддаленого доступу; організаційний персонал, відповідальний за інформаційну безпеку]. | |

|  |  |
| --- | --- |
| AC-17(7) | ВІДДАЛЕНИЙ ДОСТУП - ДОДАТКОВИЙ ЗАХИСТ ДЛЯ ДОСТУПУ ДО ФУНКЦІЙ БЕЗПЕКИ |
|  | [Вилучено: Включено в AC-3 (10)]. |

|  |  |
| --- | --- |
| AC-17(8) | ВІДДАЛЕНИЙ ДОСТУП - ДЕАКТИВАЦІЯ НЕЗАХИЩЕНИХ ПРОТОКОЛІВ МЕРЕЖІ |
|  | [Вилучено: Включено в CM-7]. |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-17(9) | ВІДДАЛЕНИЙ ДОСТУП - ВІДКЛЮЧЕННЯ АБО ДЕАКТИВАЦІЯ ДОСТУПУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-17(9)[1] | визначає часовий проміжок, протягом якого слід оперативно відключити або деактивувати доступ до інформаційної системи; | |
| AC-17(9)[2] | AC-17(9)[2][1] | забезпечує можливість оперативного відключення віддаленого доступу до інформаційної системи протягом періоду часу, визначеного організацією. |
| AC-17(9)[2][2] | забезпечує можливість оперативної дезактивації віддаленого доступу до інформаційної системи протягом періоду часу, визначеного організацією. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо відключення або дезактивації віддаленого доступу до інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; план безпеки, записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливість відключення або дезактивації віддаленого доступу до інформаційної системи]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-18 | БЕЗДРОТОВИЙ ДОСТУП | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-18(a) | AC-18(a)[1] | встановлює обмеження на використання щодо здійснення бездротового доступу |
| AC-18(a)[2] | встановлює вимоги до конфігурації або підключення щодо здійснення бездротового доступу |
| AC-18(a)[3] | встановлює рекомендації щодо здійснення бездротового доступу |
| AC-18(b) | авторизує бездротовий доступ до інформаційної системи перед тим, як дозволяти такі з'єднання. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання бездротового доступу (включаючи обмеження); план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; авторизація бездротового доступу; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління бездротовими з'єднаннями доступу; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Можливість управління бездротовим доступом до інформаційної системи]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-18(1) | БЕЗДРОТОВИЙ ДОСТУП - АВТЕНТИФІКАЦІЯ ТА ШИФРУВАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи інформаційна система: | | |
| AC-18(1)[1] | AC-18(1)[1]{1} | забезпечує захист бездротового доступу до системи за допомогою автентифікації користувачів |
| AC-18(1)[1]{2} | забезпечує захист бездротового доступу до системи за допомогою автентифікації пристроїв |
| AC-18(1)[2] | забезпечує захист бездротового доступу до системи за допомогою шифрування | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання бездротового зв'язку (включаючи обмеження); проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні f,j мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують захист бездротового доступу до інформаційної системи]. | | |

|  |  |
| --- | --- |
| AC-18(2) | БЕЗДРОТОВИЙ ДОСТУП - МОНІТОРИНГ НЕАВТОРИЗОВАНИХ ПІДКЛЮЧЕНЬ |
|  | [Вилучено: Включено в SI-4]. |

|  |  |  |
| --- | --- | --- |
| AC-18(3) | БЕЗДРОТОВИЙ ДОСТУП - ВІДКЛЮЧЕННЯ БЕЗДРОТОВОЇ МЕРЕЖІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація | |
| AC-18(3)[1] | відключає, у разі відсутності необхідності у використанні, вбудовані в системні компоненти можливості бездротових мереж до їх виклику та розгортання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання бездротового зв'язку (включаючи обмеження); проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми управління відключенням можливостей бездротової мережі, внутрішньо вбудованими в компоненти інформаційної системи]. | |

|  |  |  |
| --- | --- | --- |
| AC-18(4) | БЕЗДРОТОВИЙ ДОСТУП - ОБМЕЖЕННЯ НАЛАШТУВАННЯ КОРИСТУВАЧАМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AC-18(4)[1] | встановити користувачів, яким дозволено самостійно налаштовувати можливості бездротової мережі; |
| AC-18(4)[2] | явно авторизує визначених користувачів, яким дозволено самостійно налаштовувати можливості бездротової мережі. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання бездротового зв'язку (включаючи обмеження); проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що дозволяють незалежне налаштування користувачем можливостей бездротової мережі]. | |

|  |  |  |
| --- | --- | --- |
| AC-18(5) | БЕЗДРОТОВИЙ ДОСТУП - АНТЕНИ ТА РІВЕНЬ ПОТУЖНОСТІ ПЕРЕДАЧІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AC-18(5)[1] | вибирає радіо антени, щоб зменшити ймовірність того, що корисні сигнали можуть прийматися за межами контрольованих організацією меж; |
| AC-18(5)[2] | калібрує рівні потужності передачі, щоб зменшити ймовірність того, що корисні сигнали можуть прийматися за контрольованими організацією межами. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання бездротового зв'язку (включаючи обмеження); проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Можливість бездротового доступу, що захищає корисні сигнали від несанкціонованого доступу за межами контрольованих організацією меж]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-19 | КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-19(a) | AC-19(a)[1] | встановлює обмеження на використання щодо впровадження мобільних пристроїв, контрольованих організацією |
| AC-19(a)[2] | встановлює вимоги до конфігурації щодо впровадження мобільних пристроїв, контрольованих організацією |
| AC-19(a)[3] | встановлює вимоги до підключення щодо впровадження мобільних пристроїв, контрольованих організацією |
| AC-19(a)[4] | встановлює рекомендації щодо впровадження мобільних пристроїв, контрольованих організацією |
| AC-19(b) | авторизує підключення мобільних пристроїв до систем, які експлуатуються організацією | |
| AC-19(c) | AC-19(c)[1] | забезпечує захист мобільних пристроїв, що знаходяться поза контрольованих зон |
| AC-19(c)[2] | забезпечує контроль мобільних пристроїв, що знаходяться поза контрольованих зон |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на контроль доступу для використання мобільних пристроїв (включаючи обмеження); план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; дозволи на підключення мобільних пристроїв до організаційних інформаційних систем; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, що використовує мобільні пристрої для доступу до організаційних інформаційних систем; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Можливість контролю доступу, що дозволяє авторизувати з'єднання мобільних пристроїв з організаційними інформаційними системами]. | | |

|  |  |
| --- | --- |
| AC-19(1) | КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ВИКОРИСТАННЯ ПИСЬМОВИХ ТА ПОРТАТИВНИЙ ПРИСТРОЇВ ДЛЯ ЗБЕРІГАННЯ ДАНИХ |
|  | [Вилучено: Включено в MP-7]. |

|  |  |
| --- | --- |
| AC-19(2) | КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ПОРТАТИВНИХ ПРИСТРОЇВ ЗБЕРІГАННЯ ДАНИХ |
|  | [Вилучено: Включено в MP-7]. |

|  |  |
| --- | --- |
| AC-19(3) | КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ВИКОРИСТАННЯ ПОРТАТИВНИХ ПРИСТРОЇВ ЗБЕРІГАННЯ ДАНИХ З НЕІДЕНТИФІКОВАНИМ ВЛАСНИКОМ |
|  | [Вилучено: Включено в MP-7]. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AC-19(4) | КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ОБМЕЖЕННЯ ДЛЯ ЗАСЕКРЕЧЕНОЇ ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | |
| AC-19(4)(a) | AC-19(4)(a){1} | забороняє використання незахищених мобільних пристроїв на об'єктах, де експлуатуються системи, що обробляють секретну інформацію, якщо це спеціально не дозволено уповноваженою особою | |
| AC-19(4)(a){2} | забороняє використання незахищених мобільних пристроїв на об'єктах, де експлуатуються системи, що зберігають секретну інформацію, якщо це спеціально не дозволено уповноваженою особою | |
| AC-19(4)(a){3} | забороняє використання незахищених мобільних пристроїв на об'єктах, де експлуатуються системи, що передають секретну інформацію, якщо це спеціально не дозволено уповноваженою особою | |
| AC-19(4)(b) | AC-19(4)(b)(1) | забезпечити наступні обмеження на осіб, яким дозволено уповноваженою особою використовувати незахищені мобільні пристрої в установах, що містять системи обробки, зберігання або передачі секретної інформації: підключення незахищених мобільних пристроїв до засекречених систем заборонено | |
| AC-19(4)(b)(2) | забезпечити наступні обмеження на осіб, яким дозволено уповноваженою особою використовувати незахищені мобільні пристрої в установах, що містять системи обробки, зберігання або передачі секретної інформації: підключення незахищених мобільних пристроїв до не засекречених систем вимагає схвалення уповноваженої посадової особи | |
| AC-19(4)(b)(3) | AC-19(4)(b)(3){1} | забезпечити наступні обмеження на осіб, яким дозволено уповноваженою особою використовувати незахищені мобільні пристрої в установах, що містять системи обробки, зберігання або передачі секретної інформації: використання внутрішніх модемів у незахищених мобільних пристроях заборонено |
| AC-19(4)(b)(3){2} | забезпечити наступні обмеження на осіб, яким дозволено уповноваженою особою використовувати незахищені мобільні пристрої в установах, що містять системи обробки, зберігання або передачі секретної інформації: використання зовнішніх модемів у незахищених мобільних пристроях заборонено |
| AC-19(4)(b)(3){3} | забезпечити наступні обмеження на осіб, яким дозволено уповноваженою особою використовувати незахищені мобільні пристрої в установах, що містять системи обробки, зберігання або передачі секретної інформації: використання бездротових інтерфейсів у незахищених мобільних пристроях заборонено |
| AC-19(4)(b)(4) | AC-19(4)(b)(4)[1] | визначає посадовими особами з захисту інформації, відповідальних за огляди та перевірки некласифікованих мобільних пристроїв та інформацію, що зберігається на цих пристроях; |
| AC-19(4)(b)(4)[2] | некласифіковані мобільні пристрої та інформація, що зберігається на цих пристроях, підлягають випадковим оглядам або перевіркам посадовими особами з захисту інформації, визначеними організацією |
| AC-19(4)(b)(4)[3] | якщо, за результатами перевірки некласифікованих мобільних пристроїв, секретна інформація знайдена, застосовується політика обробки інцидентів. |
| AC-19(4)(c) | AC-19(4)(c)[1] | визначає політику безпеки для обмеження підключення захищених мобільних пристроїв до засекречених систем; | |
| AC-19(4)(c)[2] | обмежує підключення захищених мобільних пристроїв до засекречених систем відповідно до визначених організацією політик безпеки. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; політика поводження з інцидентами; процедури, спрямовані на контроль доступу для мобільних пристроїв; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; доказова документація щодо випадкових перевірок та оглядів мобільних пристроїв; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за випадкові огляди або перевірки мобільних пристроїв; організаційний персонал, що використовує мобільні пристрої в приміщеннях, які призначені для обробки, зберігання або передачі секретної інформації інформаційних систем; організаційний персонал, відповідальний за реагування на інциденти; системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що забороняють використовувати внутрішні або зовнішні модеми або бездротові інтерфейси з мобільними пристроями]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-19(5) | КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ПОВНЕ ШИФРУВАННЯ ПРИСТРОЇВ ТА СХОВИЩ ІНФОРМАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| **AC-19(5)[1]** | визначає мобільні пристрої, для яких необхідне повне шифрування пристрою або шифрування сховищ інформації для захисту конфіденційності та цілісності інформації на таких пристроях; | |
| **AC-19(5)[2]** | організація має застосувати: | |
| **AC-19(5)[2]{1}** | повне шифрування пристроїв для захисту конфіденційності та цілісності інформації на визначених організацією мобільних пристроях |
| **AC-19(5)[2]{2}** | шифрування сховищ інформації для захисту конфіденційності та цілісності інформації на визначених організацією мобільних пристроях |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, спрямовані на контроль доступу для мобільних пристроїв; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; механізм шифрування і пов'язана з ним конфігураційна документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за контроль доступу для мобільних пристроїв; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Механізми шифрування, що захищають конфіденційність та цілісність інформації на мобільних пристроях]. | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| AC-20 | ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | |
| AC-20[1] | встановлює умови, що відповідають будь-яким довірчим відносинам, встановленим з іншими організаціями які (один або кілька): | | | |
| AC-20[1]{1} | володіють зовнішні системи, що дозволяють уповноваженим особам: | | |
| **AC-20[1]{1}(a)** | надавати доступ до інформаційної системи із зовнішніх інформаційних систем; | |
| **AC-20[1]{1}(b)** | **AC-20[1]{1}(b){1}** | обробляти керовану організацією інформацію за допомогою зовнішніх інформаційних систем. |
| **AC-20[1]{1}(b){2}** | зберігати керовану організацією інформацію за допомогою зовнішніх інформаційних систем. |
| **AC-20[1]{1}(b){3}** | передавати керовану організацією інформацію за допомогою зовнішніх інформаційних систем. |
| AC-20[1]{2} | експлуатують зовнішні системи, що дозволяють уповноваженим особам: | | |
| **AC-20[1]{2}(a)** | надавати доступ до інформаційної системи із зовнішніх інформаційних систем; | |
| **AC-20[1]{2}(b)** | **AC-20[1]{2}(b){1}** | обробляти керовану організацією інформацію за допомогою зовнішніх інформаційних систем. |
| **AC-20[1]{2}(b){2}** | зберігати керовану організацією інформацію за допомогою зовнішніх інформаційних систем. |
| **AC-20[1]{2}(b){3}** | передавати керовану організацією інформацію за допомогою зовнішніх інформаційних систем. |
| AC-20[1]{3} | підтримують зовнішні системи, що дозволяють уповноваженим особам: | | |
| **AC-20[1]{3}(a)** | надавати доступ до інформаційної системи із зовнішніх інформаційних систем; | |
| **AC-20[1]{3}(b)** | **AC-20[1]{3}(b){1}** | обробляти керовану організацією інформацію за допомогою зовнішніх інформаційних систем. |
| **AC-20[1]{3}(b){2}** | зберігати керовану організацією інформацію за допомогою зовнішніх інформаційних систем. |
| **AC-20[1]{3}(b){3}** | передавати керовану організацією інформацію за допомогою зовнішніх інформаційних систем. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо використання зовнішніх інформаційних систем; зовнішні інформаційні системи та умови; перелік типів програм, доступних із зовнішніх інформаційних систем; категоризація максимальної безпеки для інформації, що обробляється, зберігається або передається у зовнішніх інформаційних системах; налаштування конфігурації інформаційної системи та супутня документація; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за визначення умов та обставин використання зовнішніх інформаційних систем для доступу до організаційних систем; системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку]  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують умови використання зовнішніх інформаційних систем]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-20(1) | ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ОБМЕЖЕННЯ НА АВТОРИЗОВАНЕ ВИКОРИСТАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-20(1){1} | дозволяє організація уповноваженим особам використовувати зовнішню інформаційну систему для доступу до інформаційної системи лише тоді, коли організація: | |
| **AC-20(1)[1](a)** | перевіряє реалізацію необхідних заходів безпеки на зовнішній системі, як зазначено в політиці безпеки та приватності організації, а також планах безпеки та приватності; |
| **AC-20(1)[1](b)** | зберігає затверджені угоди про підключення або обробку системи з організаційною структурою, на якій розміщена зовнішня система |
| AC-20(1){2} | дозволяє організація уповноваженим особам використовувати зовнішню інформаційну систему для доступу обробки, зберігання керованої інформації лише тоді, коли організація: | |
| AC-20(1){2}(a) | перевіряє реалізацію необхідних заходів безпеки на зовнішній системі, як зазначено в політиці безпеки та приватності організації, а також планах безпеки та приватності; |
| AC-20(1){2}(b) | зберігає затверджені угоди про підключення або обробку системи з організаційною структурою, на якій розміщена зовнішня система |
| AC-20(1){3} | дозволяє організація уповноваженим особам використовувати зовнішню інформаційну систему для доступу до передавачі організації керованої інформацію лише тоді, коли організація: | |
| AC-20(1){3}(a) | перевіряє реалізацію необхідних заходів безпеки на зовнішній системі, як зазначено в політиці безпеки та приватності організації, а також планах безпеки та приватності; |
| AC-20(1){3}(b) | зберігає затверджені угоди про підключення або обробку системи з організаційною структурою, на якій розміщена зовнішня система |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються використання зовнішніх інформаційних систем; план безпеки; угоди про підключення або обробку інформаційних систем; документи з управління облікового запису; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують обмеження на використання зовнішніх інформаційних систем]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-20(2) | ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ПЕРЕНОСНІ ПРИСТРОЇ ЗБЕРІГАННЯ ДАНИХ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-20(2)[1] | організація визначає обмеження використання портативних пристроїв зберігання даних | |
| AC-20(2)[2] | AC-20(2)[2]{1} | обмежує використання портативних пристроїв зберігання даних, які знаходяться під контролем організації, уповноваженими особами на зовнішніх системах |
| AC-20(2)[2]{2} | забороняє використання портативних пристроїв зберігання даних, які знаходяться під контролем організації, уповноваженими особами на зовнішніх системах |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо використання зовнішніх інформаційних систем; план безпеки; налаштування конфігурації інформаційної системи та супутня документація; угоди про підключення або роботу з інформаційними системами; документи з управління обліковими записами; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за обмеження або заборону використання пристроїв зберігання даних, керованих організацією, у зовнішніх інформаційних системах; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують обмеження на використання портативних пристроїв зберігання даних]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-20(3) | ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - СИСТЕМИ ТА КОМПОНЕНТИ, ЩО НЕ ЗНАХОДЯТЬСЯ У ВЛАСНОСТІ ОРГАНІЗАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AC-20(3)[1] | організація визначає обмеження використання систем та компонентів системи, що не знаходяться у власності організації | |
| AC-20(3)[2] | AC-20(3)[2]{1} | обмежує використання систем та компонентів системи, що не знаходяться у власності організації, для обробки, зберігання або передачі організаційної інформації |
| AC-20(3)[2]{2} | забороняє використання систем та компонентів системи, що не знаходяться у власності організації, для обробки, зберігання або передачі організаційної інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо використання зовнішніх інформаційних систем; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; угоди про підключення або обробку інформаційної системи; документи з управління рахунками; записи аудиту інформаційної системи, інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за обмеження або заборону використання інформаційних систем, компонентів системи чи пристроїв, що не належать до організації; системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують обмеження щодо використання не організаційних систем або компонентів або пристроїв]. | | |

|  |  |  |
| --- | --- | --- |
| AC-20(4) | ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ПРИСТРОЇ ДЛЯ ЗБЕРІГАННЯ ДАНИХ, ЯКІ МОЖУТЬ МАТИ ДОСТУП ДО МЕРЕЖІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| **AC-20(4)[1]** | визначає пристрої для зберігання даних, які можуть мати доступ до мережі; |
| **AC-20(4)[2]** | забороняє використовувати визначені організацією пристрої для зберігання даних, які можуть мати доступ до мережі у зовнішніх інформаційних системах. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються використання мережевих пристроїв зберігання даних у зовнішніх інформаційних системах; план безпеки, проєктна документація на інформаційні системи; налаштування конфігурації інформаційної системи та супутня документація; угоди про підключення або роботу з інформаційною системою; перелік мережевих доступних пристроїв зберігання даних, заборонених до використання у зовнішніх інформаційних системах; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за заборону використання мережевих пристроїв зберігання даних у зовнішніх інформаційних системах; системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що забороняють використовувати мережеві пристрої зберігання даних у зовнішніх інформаційних системах]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-21 | РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| **AC-21(a)** | **AC-21(a)[1]** | визначає обставини обміну інформацією, коли необхідна обережність користувача; |
| **AC-21(a)[2]** | полегшує обмін інформацією, дозволяючи уповноваженим користувачам визначати, чи санкціоновані права доступу, призначені партнеру спільного доступу, відповідають обмеженням доступу до інформації для визначених організацією обставин обміну інформацією; |
| **AC-21(b)** | **AC-21(b)[1]** | визначає автоматизовані механізми або ручні процеси, які слід використовувати для надання допомоги користувачам у прийнятті рішень щодо обміну та співпраці; |
| **AC-21(b)[2]** | використовує визначені організацією автоматизовані механізми або ручні процеси, щоб допомогти користувачам у прийнятті рішень щодо обміну та співпраці |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо співпраці з користувачами та обміну інформацією (включаючи обмеження); проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; список користувачів, уповноважених приймати рішення щодо обміну та співпраці; перелік обставин обміну інформацією, що вимагає обачності від користувача; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за прийняття рішень щодо обміну та співпраці; системні або мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми або ручний процес, що реалізує авторизацію доступу, що підтримує рішення щодо обміну інформацією та співпраці користувачів]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-21(1) | РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ - АВТОМАТИЧНА ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AC-21(1)[1] | забезпечує інформаційна система прийняття рішень про обмін інформацією авторизованими користувачами на підставі: | |
| **AC-21(1)[1]** | авторизації доступу партнерів по обміну інформацією; |
| **AC-21(1)[2]** | обмеження доступу до інформації, яку передають. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються взаємодії з користувачами та обміну інформацією (включаючи обмеження); проєктна документація інформаційної системи; налаштування інформаційної системи та супутня документація; список користувачів, уповноважених приймати рішення щодо обміну та співпраці; перелік обставин обміну інформацією, які вимагають розсуду користувача; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Системні або мережеві адміністратори; організаційний персонал відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують авторизацію доступу, що підтримують рішення щодо обміну інформацією та співпраці користувачів]. | | |

|  |  |  |
| --- | --- | --- |
| AC-21(2) | РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ - ПОШУК І ПЕРЕВІРКА ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| **AC-21(2)[1]** | організація визначає обмеження щодо обміну інформацією, які слід застосовувати за допомогою служб пошуку та перевірки інформації; |
| **AC-21(2)[2]** | інформаційна система впроваджує сервіси пошуку та перевірки інформації, які застосовують визначені організацією обмеження щодо обміну інформацією. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються взаємодії з користувачами та обміну інформацією (включаючи обмеження); проєктна документація інформаційної системи; налаштування інформаційної системи та супутня документація; сформований системою перелік обмежень доступу щодо інформації, яку потрібно передавати; записи щодо пошуку та перевірки інформації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу до служб пошуку та перевірки інформаційних систем; системні або мережеві адміністратори; організаційний персонал відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Служби пошуку та перевірки інформаційної системи, що застосовують обмеження щодо обміну інформацією]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AC-22 | ПУБЛІЧНО ДОСТУПНИЙ КОНТЕНТ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| **AC-22(a)** | призначає осіб, уповноважених розміщувати інформацію у загальнодоступній інформаційній системі; | |
| **AC-22(b)** | навчає уповноважених осіб тому, щоб загальнодоступна інформація не містила інформацію з обмеженим доступом; | |
| **AC-22(c)** | переглядає запропонований зміст інформації перед публікацією в загальнодоступній інформаційній системі, щоб переконатися, що там не міститься інформація з обмеженим доступом; | |
| **AC-22(d)** | **AC-22(d)[1]** | визначає частоту перегляду вмісту в загальнодоступній інформаційній системі на предмет наявності там інформації з обмеженим доступом; |
| **AC-22(d)[2]** | перевіряє вміст інформації у загальнодоступній інформаційній системі на предмет наявності там інформації з обмеженим доступом з визначеною організацією частотою; |
| **AC-22(d)[3]** | видаляє інформацію з обмеженим доступом із загальнодоступної інформаційної системи, якщо вона виявлена. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури звернення до загальнодоступного контенту; перелік користувачів, які мають право публікувати загальнодоступний вміст в організаційних інформаційних системах; навчальні матеріали та / або записи; записи оглядів загальнодоступної інформації; записи відповідей на непублічну інформацію на загальнодоступних вебсайтах; журнали системного аудиту; записи про навчання поінформованості з безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за управління загальнодоступною інформацією, розміщеною в організаційних інформаційних системах; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують управління загальнодоступним контентом]. | | |

|  |  |  |
| --- | --- | --- |
| AC-23 | ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| **AC-23[1]** | визначає техніки виявлення та попередження витоку даних, які будуть використовуватися для визначених організацією об'єктів зберігання з метою для своєчасного виявлення та захисту від несанкціонованого інтелектуального аналізу даних; |
| **AC-23[2]** | визначає об'єкти зберігання даних, що мають бути захищенні від несанкціонованого інтелектуального аналізу даних; |
| **AC-23[3]** | використовує визначені організацією техніки виявлення та попередження витоку даних, для своєчасного виявлення та захисту від несанкціонованого інтелектуального аналізу даних. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури, що стосуються методів інтелектуального аналізу даних; процедури, спрямовані на захист об'єктів зберігання даних від інтелектуального аналізу даних; проєктна документація інформаційної системи; конфігурація інформаційної системи та супутня документація; журнали аудиту інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи]  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за впровадження методів виявлення та запобігання обробці даних для об'єктів зберігання даних; організаційний персонал відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують запобігання та виявлення інтелектуального аналізу даних]. | |

|  |  |  |
| --- | --- | --- |
| AC-24 | РІШЕННЯ ЩОДО УПРАВЛІННЯ ДОСТУПОМ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| **AC-24[1]** | визначає рішення щодо управління доступом, які повинні застосовуватися до кожного запиту щодо доступу до виконання доступу; |
| **AC-24[2]** | встановлює процедури для забезпечення прийнятих організацією рішень щодо управління доступом, які повинні застосовуватися до кожного запиту щодо доступу до виконання доступу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури розв’язання питань контролю доступу; проєктна документація інформаційної системи; налаштування інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за встановлення процедур щодо прийняття рішень щодо контролю доступу до інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що застосовують встановлені рішення та процедури контролю доступу]. | |

|  |  |  |
| --- | --- | --- |
| AC-24(1) | РІШЕННЯ ЩОДО УПРАВЛІННЯ ДОСТУПОМ - ІНФОРМАЦІЯ ПРО ПЕРЕДАЧУ АВТОРИЗОВАНОГО ДОСТУПУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| **AC-24(1)[1]** | організація визначає інформацію про авторизацію доступу, яку інформаційна система передає в визначені організацією інформаційні системи, які забезпечують прийняття рішень щодо управління доступом; |
| **AC-24(1)[2]** | організація визначає заходи безпеки, які повинні використовуватися, коли інформаційна система передає визначену організацією інформацію про авторизацію до визначених організацією інформаційних систем, які застосовують рішення щодо контролю доступу; |
| **AC-24(1)[3]** | організація визначає інформаційні системи, що застосовують рішення щодо контролю доступу; |
| **AC-24(1)[4]** | інформаційна система передає визначену організацією інформацію про дозвіл доступу, використовуючи визначені організацією заходи безпеки, до визначених організацією інформаційних систем, що застосовують рішення щодо управління доступом. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні та мережеві адміністратори; організаційний персонал відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу]. | |

|  |  |  |
| --- | --- | --- |
| AC-24(2) | РІШЕННЯ ЩОДО УПРАВЛІННЯ ДОСТУПОМ - ВІДСУТНІСТЬ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА АБО ПРОЦЕСУ, ЩО ДІЄ ВІД ІМЕНІ КОРИСТУВАЧА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| **AC-24(2)[1]** | організація визначає атрибути безпеки, які підтримують рішення контролю доступу, які не включають ідентифікацію користувача або процеси, що діють від імені користувача |
| **AC-24(2)[2]** | інформаційна система виконує рішення щодо контролю доступу на основі визначених організацією атрибутів безпеки, які не включають ідентифікацію користувача або процесу, що діє від імені користувача. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація інформаційної системи; налаштування інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні та мережеві адміністратори; організаційний персонал відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу]. | |

|  |  |  |
| --- | --- | --- |
| AC-25 | ДИСПЕТЧЕР ДОСТУПУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| **AC-25[1]** | організація визначає політику контролю доступу, щодо якої інформаційна система реалізує диспетчер доступу для здійснення такої політики; |
| **AC-25[2]** | інформаційна система реалізує диспетчер доступу для визначених організацією політик управління доступом, який захищений від несанкціонованого доступу, завжди викликається та досить малий, щоб підлягати аналізу та тестуванню, повнота якого може бути гарантована. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за забезпечення доступу; системні та мережеві адміністратори; організаційний персонал відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу]. | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ АТ – ОБІЗНАНІСТЬ ТА НАВЧАННЯ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| AT-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ ПІДВИЩЕННЯ ОБІЗНАНОСТІ ТА НАВЧАННЯ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| AT-1(a) | AT-1(a)[1] | AT-1(a)[1](1) | | | Розробляє та документує політику (правила) обізнаності та навчання , яка: | | | | | | | | |
| AT-1(a)[1](1)(a) | | Містить: | | | | | | |
| AT-1(a)[1](1)(a)[1] | | | | мету, | | |
| AT-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| AT-1(a)[1](1)(a)[3] | | | | ролі, | | |
| AT-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| AT-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| AT-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| AT-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| AT-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| AT-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| AT-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| AT-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| AT-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| AT-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| AT-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| AT-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| AT-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики (правил) обізнаності та навчання та відповідних заходів управління доступом | | | | | | | | |
| AT-1(a)[2] | AT-1(a)[2]{1} | | | AT-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика (правил) обізнаності та навчання | | | | | |
| AT-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики (правил) обізнаності та навчання та пов'язаних з нею заходів планування безпеки та приватності | | | | | |
| AT-1(a)[2]{2} | | | AT-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика (правил) обізнаності та навчання | | | | | |
| AT-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики (правил) обізнаності та навчання та пов'язаних з нею заходів планування безпеки та приватності | | | | | |
| AT-1(a)[3] | AT-1(a)[3]{1} | | | AT-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику (правила) обізнаності та навчання , яка: | | | | | | | |
| AT-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| AT-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| AT-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| AT-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| AT-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| AT-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| AT-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| AT-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| AT-1(a)[3](1)(b) | | | Відповідає: | | | | |
| AT-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| AT-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| AT-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| AT-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| AT-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| AT-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| AT-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| AT-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації політики (правил) обізнаності та навчання та відповідних заходів управління доступом | | | | | | | |
| AT-1(a)[3]{2} | | | AT-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику (правила) обізнаності та навчання , яка: | | | | | | | |
| AT-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| AT-1(a)[3]{2}(1)(а)[1] | | мету, | |
| AT-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| AT-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| AT-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| AT-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| AT-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| AT-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| AT-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| AT-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| AT-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| AT-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| AT-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| AT-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| AT-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| AT-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| AT-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики (правил) обізнаності та навчання та пов'язаних з нею заходів планування безпеки та приватності | | | | | | | |
| AT-1(b) | AT-1(b)[1] | визначає посадову особу для управління політикою та процедурами обізнаності та навчання | | | | | | | | | | | |
| AT-1(b)[2] | призначає посаду для управління політикою та процедурами планування обізнаності та навчання | | | | | | | | | | | |
| AT-1(с) | AT-1(с)[1] | AT-1(с)[1](1) | | AT-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики (правил) обізнаності та навчання | | | | | | | |
| AT-1(с)[1](1)[2] | | переглядає поточну політику (правила) обізнаності та навчання з визначеною організацією частотою | | | | | | | |
| AT-1(с)[1](2) | | AT-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур обізнаності та навчання | | | | | | | |
| AT-1(с)[1](2)[2] | | переглядає поточні процедури політики (правил) обізнаності та навчання з визначеною організацією частотою | | | | | | | |
| AT-1(с)[2] | AT-1(с)[2](1) | | AT-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики (правил) обізнаності та навчання | | | | | | | |
| AT-1(с)[2](1)[2] | | оновлює поточну політику (правила) обізнаності та навчання з визначеною організацією частотою | | | | | | | |
| AT-1(с)[2](2) | | AT-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур політики (правил) обізнаності та навчання | | | | | | | |
| AT-1(с)[2](2)[2] | | оновлює поточні процедури планування обізнаності та навчання з визначеною організацією частотою | | | | | | | |
| AT-1(d) | переконується, що процедури планування політики (правил) обізнаності та навчання реалізують політику та заходи планування обізнаності та навчання | | | | | | | | | | | | |
| AT-1(e) | AT-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики (правил) обізнаності та навчання | | | | | | | | | | |
| AT-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики (правил) обізнаності та навчання | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури політики (правил) обізнаності та навчання інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику (правила) обізнаності та навчання ; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AT-2 | НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| **AT-2(a)** | впроваджує базові тренінги з підвищення обізнаності у сфері безпеки та приватності для користувачів системи (включаючи менеджерів, керівників компаній та підрядників) в рамках початкового навчання для нових користувачів | |
| **AT-2(b)** | впроваджує базові тренінги з підвищення обізнаності у сфері безпеки та приватності для користувачів системи (включаючи менеджерів, керівників компаній та підрядників) за потребою у разі змін у системі | |
| **AT-2(c)** | AT-2(c)[1] | Визначає частоту впровадження базових тренінгів з підвищення обізнаності у сфері безпеки та приватності для користувачів системи (включаючи менеджерів, керівників компаній та підрядників) |
| AT-2(c)[2] | впроваджує базові тренінги з підвищення обізнаності у сфері безпеки та приватності для користувачів системи (включаючи менеджерів, керівників компаній та підрядників) після закінчення встановленого терміну |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; відповідні кодекси федеральних норм; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план безпеки; навчальні записи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за навчання з підвищення безпеки; організаційний персонал з обов'язками інформаційної безпеки; організаційний персонал, що складається із загальної спільноти користувачів інформаційної системи].  Перевірка: [ВИБІР: Автоматизовані механізми управління навчанням з питань безпеки.] | | |

|  |  |  |
| --- | --- | --- |
| AT-2(1) | НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - ПРАКТИЧНІ ЗАНЯТТЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AT-2(1)[1] | включає до програми навчання практичні заняття (вправи) з тренування обізнаності, які імітують інциденти в області безпеки та приватності. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, який бере участь у навчанні з підвищення безпеки; організаційний персонал, відповідальний за навчання з підвищення безпеки; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують моделювання кібератак у практичних вправах]. | |

|  |  |  |
| --- | --- | --- |
| AT-2(2) | НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - ВНУТРІШНІ ЗАГРОЗИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи | |
| AT-2(2)[1] | включає організація до програми навчання вправи з розпізнавання та виявлення потенційних індикаторів внутрішніх загроз. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, який бере участь у навчанні з підвищення безпеки; організаційний персонал, відповідальний за базове навчання з підвищення безпеки; організаційний персонал, відповідальний за інформаційну безпеку]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AT-2(3) | НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА СОЦІАЛЬНИЙ ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | |
| AT-2(3)[1] | включає до програми навчання вправи з підвищення обізнаності щодо розпізнавання та повідомлення про: | | |
| AT-2(3)[1][1] | потенційні атаки, з використанням методів: | |
| AT-2(3)[1][1][1] | соціальної інженерії |
| AT-2(3)[1][1][2] | інтелектуального аналізу соціальних даних. |
| AT-2(3)[1][2] | фактичні атаки, з використанням методів: | |
| AT-2(3)[1][2][1] | соціальної інженерії |
| AT-2(3)[1][2][2] | інтелектуального аналізу соціальних даних. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, який бере участь у навчанні з підвищення безпеки; організаційний персонал, відповідальний за базове навчання з підвищення безпеки; організаційний персонал, відповідальний за інформаційну безпеку]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AT-3 | РОЛЬОВЕ НАВЧАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| **AT-3(a)** | AT-3(a)[1] | Визначає ролі для яких має бути забезпечене проведення навчання з питань безпеки та приватності на основі ролей перед тим, як надати доступ до системи або допустити до виконання обов'язків |
| AT-3(a)[2] | забезпечує проведення навчання з питань безпеки та приватності на основі ролей для працівників з визначеними ролями та обов'язками перед тим, як надати доступ до системи або допустити до виконання обов'язків |
| **AT-3(b)** | AT-3(b)[1] | Визначає ролі для яких має бути забезпечене проведення навчання з питань безпеки та приватності на основі ролей за потребою у разі зміни системи |
| AT-3(b)[2] | забезпечує проведення навчання з питань безпеки та приватності на основі ролей для працівників з визначеними ролями та обов'язками за потребою у разі зміни системи |
| **AT-3(c)** | AT-3(c)[1] | Визначає частоту проведення навчання з питань безпеки та приватності на основі ролей |
| AT-3(c)[2] | Визначає ролі для яких має бути забезпечене проведення навчання з питань безпеки та приватності на основі ролей після закінчення встановленого терміну |
| AT-3(c)[3] | забезпечує проведення навчання з питань безпеки та приватності на основі ролей для працівників з визначеними ролями та обов'язками після закінчення встановленого терміну |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються впровадження тренінгів з безпеки; кодекси федеральних нормативних актів; навчальний план з питань безпеки; навчальні матеріали з безпеки; план безпеки; навчальні записи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за навчання безпеки на основі ролей; організаційний персонал з призначеними ролями та обов'язками безпеки інформаційної системи].  Перевірка: [ВИБІР: автоматизовані механізми управління навчанням безпеки на основі ролей]. | | |

|  |  |  |
| --- | --- | --- |
| AT-3(1) | РОЛЬОВЕ НАВЧАННЯ - ЗАХОДИ БЕЗПЕКИ РОБОЧОГО СЕРЕДОВИЩА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| **AT-3(1)[1]** | визначає персонал або ролі, які мають бути забезпечені початковим навчанням та підвищенням кваліфікації з питань застосування та експлуатації заходів з забезпечення захисту робочого середовища; |
| **AT-3(1)[2]** | визначає періодичність проведення підвищення кваліфікації в галузі операцій та функціонування заходів захисту робочого середовища; |
| **AT-3(1)[3]** | забезпечує підвищення кваліфікації в галузі зайнятості та функціонування заходів захисту робочого середовища, з визначеною організацією періодичністю. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються впровадження тренінгів з безпеки; навчальний план з питань безпеки; навчальні матеріали з безпеки; план безпеки; навчальні записи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за навчання безпеки на основі ролей; організаційний персонал, відповідальний за використання та управління заходами безпеки навколишнього середовища]. | |

|  |  |  |
| --- | --- | --- |
| AT-3(2) | РОЛЬОВЕ НАВЧАННЯ - ФІЗИЧНІ ЗАХОДИ БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| **AT-3(2)[1]** | визначає персонал або ролі, які мають бути забезпечені початковою та перепідготовкою в галузі використання та експлуатації заходів фізичної безпеки; |
| **AT-3(2)[2]** | визначає частоту проведення підвищення кваліфікації в галузі зайнятості та експлуатації засобів фізичної безпеки; |
| **AT-3(2)[3]** | забезпечує підвищення кваліфікації щодо використання та експлуатації заходів контролю фізичної безпеки з визначеною організацією періодичністю. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються впровадження тренінгів з безпеки; навчальний план з питань безпеки; навчальні матеріали з безпеки; план безпеки; навчальні записи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за навчання безпеки на основі ролей; організаційний персонал, відповідальний за використання та керування фізичними засобами безпеки]. | |

|  |  |  |
| --- | --- | --- |
| AT-3(3) | РОЛЬОВЕ НАВЧАННЯ - ПРАКТИЧНІ ЗАНЯТТЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація | |
| AT-3(3)[1] | включає практичні заняття з безпеки та приватності, які мають підкріпити досягнення цілей навчання. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал відповідальний за навчання безпеки на основі ролей; організаційний персонал, який бере участь у навчанні з підвищення безпеки]. | |

|  |  |  |
| --- | --- | --- |
| AT-3(4) | РОЛЬОВЕ НАВЧАННЯ - ПІДОЗРІЛІ ЗВ’ЯЗКИ ТА АНОМАЛЬНА ПОВЕДІНКА СИСТЕМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| **AT-3(4)[1]** | визначає показники шкідливого коду; |
| **AT-3(4)[2]** | забезпечує навчання свого персоналу щодо визначених організацією показників шкідливого коду для розпізнавання підозрілих зв'язків та аномальної поведінки в організаційних інформаційних системах. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються впровадження тренінгів з безпеки; навчальний план з питань безпеки; навчальні матеріали з безпеки; план безпеки; навчальні записи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за навчання ролі з безпеки; організаційний персонал, який бере участь у навчанні з підвищення безпеки]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AT-3(5) | РОЛЬОВЕ НАВЧАННЯ - ПІДОЗРІЛІ ЗВ’ЯЗКИ ТА АНОМАЛЬНА ПОВЕДІНКА СИСТЕМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| **AT-3(5)[1]** | Забезпечує персонал, який обробляє персональні дані початковим навчанням з: | |
| AT-3(5)[1](a) | організаційних повноважень щодо збору персональних даних |
| AT-3(5)[1](b) | авторизованого використання персональних даних |
| AT-3(5)[1](c) | змісту повідомлень про систему записів |
| AT-3(5)[1](d) | авторизованого обміну персональними даними зі зовнішніми сторонами |
| AT-3(5)[1](e) | наслідків несанкціонованого використання або спільного використання персональних даних |
| **AT-3(5)[2]** | Визначає для персоналу, який обробляє персональні дані частоту проведення навчання з: | |
| AT-3(5)[2](a) | організаційних повноважень щодо збору персональних даних |
| AT-3(5)[2](b) | авторизованого використання персональних даних |
| AT-3(5)[2](c) | змісту повідомлень про систему записів |
| AT-3(5)[2](d) | авторизованого обміну персональними даними зі зовнішніми сторонами |
| AT-3(5)[2](e) | наслідків несанкціонованого використання або спільного використання персональних даних |
| **AT-3(5)[3]** | Забезпечує персонал, який обробляє персональні дані, періодичним (з визначеною організацією частотою) навчання з: | |
| AT-3(5)[3](a) | організаційних повноважень щодо збору персональних даних |
| AT-3(5)[3](b) | авторизованого використання персональних даних |
| AT-3(5)[3](c) | змісту повідомлень про систему записів |
| AT-3(5)[3](d) | авторизованого обміну персональними даними зі зовнішніми сторонами |
| AT-3(5)[3](e) | наслідків несанкціонованого використання або спільного використання персональних даних |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються впровадження тренінгів з безпеки; навчальний план з питань безпеки; навчальні матеріали з безпеки; план безпеки; навчальні записи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за навчання ролі з безпеки; організаційний персонал, який бере участь у навчанні з підвищення безпеки]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AT-4 | НАВЧАЛЬНІ ЗАПИСИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| **AT-4(a)** | Документує та відстежує індивідуальні навчальні заходи з забезпечення безпеки та приватності, включаючи: | |
| **AT-4(a)[1]** | базову підготовку з питань безпеки та приватності визначених посадових осіб |
| **AT-4(a)[2]** | спеціальну підготовку з питань безпеки та приватності визначених посадових осіб |
| **AT-4(b)** | AT-4(b)[1] | Визначає період часу протягом якого організація має зберігати індивідуальні записи про навчання |
| AT-4(b)[2] | Зберігає індивідуальні записи про навчання протягом визначеного періоду часу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються записів навчання з безпеки; обізнаність із безпеки та навчальні записи; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал з обов'язками щодо зберігання записів з безпеки].  Перевірка: [ВИБІР ВІД: Автоматизовані механізми, що підтримують управління записами навчань з безпеки]. | | |

|  |  |
| --- | --- |
| AT-5 | КОНТАКТИ З ГРУПАМИ БЕЗПЕКИ ТА АСОЦІАЦІЯМИ |
|  | Вилучено: включено в PM-15. |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ АU – АУДИТ ТА ПІДЗВІТНІСТЬ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| AU-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ АУДИТУ ТА ПІДЗВІТНОСТІ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| AU-1(a) | AU-1(a)[1] | AU-1(a)[1](1) | | | Розробляє та документує політику аудиту та підзвітності, яка: | | | | | | | | |
| AU-1(a)[1](1)(a) | | Містить: | | | | | | |
| AU-1(a)[1](1)(a)[1] | | | | мету, | | |
| AU-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| AU-1(a)[1](1)(a)[3] | | | | ролі, | | |
| AU-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| AU-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| AU-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| AU-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| AU-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| AU-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| AU-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| AU-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| AU-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| AU-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| AU-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| AU-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| AU-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики аудиту та підзвітності, а також пов'язаних з ними заходів аудиту та підзвітності; | | | | | | | | |
| AU-1(a)[2] | AU-1(a)[2]{1} | | | AU-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика аудиту та підзвітності | | | | | |
| AU-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики аудиту та підзвітності та пов'язаних з нею заходів захисту політики аудиту та підзвітності | | | | | |
| AU-1(a)[2]{2} | | | AU-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика аудиту та підзвітності | | | | | |
| AU-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики аудиту та підзвітності та пов'язаних з нею заходів захисту політики аудиту та підзвітності | | | | | |
| AU-1(a)[3] | AU-1(a)[3]{1} | | | AU-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику аудиту та підзвітності | | | | | | | |
| AU-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| AU-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| AU-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| AU-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| AU-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| AU-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| AU-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| AU-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| AU-1(a)[3](1)(b) | | | Відповідає: | | | | |
| AU-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| AU-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| AU-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| AU-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| AU-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| AU-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| AU-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| AU-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації захисту аудиту та підзвітності та відповідних заходів аудиту та підзвітності | | | | | | | |
| AU-1(a)[3]{2} | | | AU-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику захисту аудиту та підзвітності, яка: | | | | | | | |
| AU-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| AU-1(a)[3]{2}(1)(а)[1] | | мету, | |
| AU-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| AU-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| AU-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| AU-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| AU-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| AU-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| AU-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| AU-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| AU-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| AU-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| AU-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| AU-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| AU-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| AU-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| AU-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики аудиту та підзвітності та пов'язаних з нею заходів аудиту та підзвітності | | | | | | | |
| AU-1(b) | AU-1(b)[1] | визначає посадову особу для управління політикою та процедурами аудиту та підзвітності | | | | | | | | | | | |
| AU-1(b)[2] | призначає посаду для управління політикою та процедурами аудиту та підзвітності | | | | | | | | | | | |
| AU-1(с) | AU-1(с)[1] | AU-1(с)[1](1) | | AU-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики аудиту та підзвітності | | | | | | | |
| AU-1(с)[1](1)[2] | | переглядає поточну політику аудиту та підзвітності з визначеною організацією частотою | | | | | | | |
| AU-1(с)[1](2) | | AU-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур аудиту та підзвітності | | | | | | | |
| AU-1(с)[1](2)[2] | | переглядає поточні процедури аудиту та підзвітності з визначеною організацією частотою | | | | | | | |
| AU-1(с)[2] | AU-1(с)[2](1) | | AU-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики аудиту та підзвітності | | | | | | | |
| AU-1(с)[2](1)[2] | | оновлює поточну політику аудиту та підзвітності з визначеною організацією частотою | | | | | | | |
| AU-1(с)[2](2) | | AU-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур аудиту та підзвітності | | | | | | | |
| AU-1(с)[2](2)[2] | | оновлює поточні процедури аудиту та підзвітності з визначеною організацією частотою | | | | | | | |
| AU-1(d) | переконується, що процедури аудиту та підзвітності реалізують політику та заходи аудиту та підзвітності | | | | | | | | | | | | |
| AU-1(e) | AU-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики аудиту та підзвітності | | | | | | | | | | |
| AU-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики аудиту та підзвітності | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури аудиту та підзвітності; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику аудиту та підзвітності; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-2 | ПОДІЇ АУДИТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| **AU-2(a)** | **AU-2(a)[1]** | визначає типи подій аудиту, які мають бути перевірені; |
| **AU-2(a)[2]** | перевіряє визначені організацією типи подій аудиту. |
| **AU-2(b)** | координує функції аудиту безпеки з іншими організаційними підрозділами, які вимагають інформації пов’язаної з аудитом, для посилення взаємної підтримки та допомоги у виборі типів подій, що перевіряються | |
| **AU-2(c)** | дає обгрунтування того, чому типи подій, що перевіряються вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов'язаних з безпекою та приватністю | |
| **AU-2(d)** | **AU-2(d)[1]** | визначає підмножину аудиторських подій, визначених у AU-2(a)[1], які підлягають аудиту в межах інформаційної системи; |
| **AU-2(d)[2]** | визначає, що підмножина аудиторських подій, визначених у AU-2(a)[1], підлягає аудиту в межах інформаційної системи; |
| **AU-2(d)[3]** | визначає частоту (або ситуацію, що вимагає) аудиту для кожної виявленої події. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури вирішення аудиторських подій; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; аудиторські події інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал з обов'язками інформаційної безпеки; системні / мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують аудит інформаційної системи]. | | |

|  |  |
| --- | --- |
| AU-2(1) | ПОДІЇ АУДИТУ - УЗАГАЛЬНЕННЯ ЗАПИСІВ ПРО АУДИТ З ДЕКІЛЬКОХ ДЖЕРЕЛ |
|  | [Вилучено: Включено в АU-12]. |

|  |  |
| --- | --- |
| AU-2(2) | ПОДІЇ АУДИТУ - ВИБІР ПОДІЇ АУДИТУ ЗА КОМПОНЕНТАМИ |
|  | [Вилучено: Включено в АU-12]. |

|  |  |  |
| --- | --- | --- |
| AU-2(3) | ПОДІЇ АУДИТУ - ПЕРЕГЛЯД ТА ОНОВЛЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| **AU-2(3)[1]** | визначає частоту перегляду аудиторських подій; |
| **AU-2(3)[2]** | визначає частоту оновлення аудиторських подій; |
| **AU-2(3)[3]** | перевіряє аудиторські події з визначеною організацією частотою. |
| **AU-2(3)[4]** | оновлює аудиторські події з визначеною організацією частотою. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури вирішення аудиторських подій; план безпеки; перелік визначених організацією аудиторських заходів; перевірка та оновлення аудиторських подій; записи аудиту інформаційної системи; повідомлення про випадки інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують огляд та оновлення аудиторських подій]. | |

|  |  |
| --- | --- |
| AU-2(4) | ПОДІЇ АУДИТУ - ПРИВІЛЕЙОВАНІ ФУНКЦІЇ |
|  | [Вилучено: Включено в AC-6 (9)]. |

|  |  |  |
| --- | --- | --- |
| AU-3 | ЗМІСТ ЗАПИСІВ АУДИТУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи інформаційна система: | |
| **AU-3[1]** | система генерує записи аудиту, що містять інформацію, яка встановлює який тип події стався; |
| **AU-3[2]** | система генерує записи аудиту, що містять інформацію, яка встановлює коли подія сталася; |
| **AU-3[3]** | система генерує записи аудиту, що містять інформацію, яка встановлює де відбулася подія; |
| **AU-3[4]** | система генерує записи аудиту, що містять інформацію, яка встановлює джерело події; |
| **AU-3[5]** | система генерує записи аудиту, що містять інформацію, яка встановлює результат події; |
| **AU-3[6]** | система генерує записи аудиту, що містять інформацію, яка встановлює ідентичність будь-яких осіб або суб'єктів, пов'язаних з цією подією |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються змісту аудиторських записів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік визначених організацією аудиторських заходів; записи аудиту інформаційної системи; повідомлення про випадки інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують аудит інформаційної системи аудиторських подій]. | |

|  |  |  |
| --- | --- | --- |
| AU-3(1) | ЗМІСТ ЗАПИСІВ АУДИТУ - ДОДАТКОВА ІНФОРМАЦІЯ ПРО АУДИТ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| **AU-3(1)[1]** | організація визначає додаткову, більш детальну інформацію, яка повинна міститися в аудиторських записах, які формує інформаційна система; |
| **AU-3(1)[2]** | інформаційна система формує аудиторські записи, що містять визначену організацією додаткову, більш детальну інформацію. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються змісту аудиторських записів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік визначених організацією аудиторських заходів; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал з обов'язками пов’язаними з інформаційною безпекою; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР: Можливість аудиту інформаційної системи]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-3(2) | ЗМІСТ ЗАПИСІВ АУДИТУ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ ПЛАНОВАНИМ ЗМІСТОМ ЗАПИСІВ АУДИТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| **AU-3(2)[1]** | організація визначає компоненти інформаційної системи, які генерують аудиторські записи, вміст яких повинен централізовано керуватися та конфігуруватися інформаційною системою; | |
| **AU-3(2)[2]** | **AU-3(2)[2][1]** | інформаційна система забезпечує централізоване управління контенту, який слід враховувати в записах аудиту, створених за допомогою системних компонентів, визначених організацією |
| **AU-3(2)[2][2]** | інформаційна система забезпечує конфігурацію контенту, який слід враховувати в записах аудиту, створених за допомогою системних компонентів, визначених організацією |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються змісту аудиторських записів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік визначених організацією аудиторських заходів; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР ВІД: Можливість інформаційної системи, що реалізує централізоване управління та конфігурацію вмісту записів аудиту]. | | |

|  |  |  |
| --- | --- | --- |
| AU-3(3) | ЗМІСТ ЗАПИСІВ АУДИТУ - ОБМЕЖЕННЯ ЕЛЕМЕНТІВ ПЕРСОНАЛЬНИХ ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| **AU-4[1]** | визначає елементи персональних даних, згідно з визначеними в оцінці ризику приватності |
| **AU-4[2]** | обмежує персональні дані, що міститься в записах аудиту, до таких елементів, які визначені в оцінці ризику приватності. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури, пов'язані з можливостями зберігання аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; вимоги до зберігання записів аудиту; можливість зберігання записів аудиту для компонентів інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР: Перевірити ємність пам’яті запису та відповідні налаштування конфігурації]. | |

|  |  |  |
| --- | --- | --- |
| AU-4 | МІСТКІСТЬ ЗБЕРІГАННЯ ЗАПИСІВ АУДИТУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| **AU-4[1]** | визначає вимоги до зберігання записів аудиту; |
| **AU-4[2]** | розподіляє ємність для зберігання записів аудиту відповідно до визначених організацією вимог зберігання записів аудиту. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури, пов'язані з можливостями зберігання аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; вимоги до зберігання записів аудиту; можливість зберігання записів аудиту для компонентів інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР: Перевірити ємність пам’яті запису та відповідні налаштування конфігурації]. | |

|  |  |  |
| --- | --- | --- |
| AU-4(1) | МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ - ПЕРЕДАЧА ДО АЛЬТЕРНАТИВНОГО СХОВИЩА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| **AU-4(1)[1]** | організація визначає частоту завантаження аудиторських записів на іншу систему чи носій інформації, ніж система, що перевіряється; |
| **AU-4(1)[2]** | інформаційна система вивантажує аудиторські записи на іншу систему або носій інформації, ніж система, що перевіряється, з визначеною організацією частотою. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури, пов'язані з можливостями зберігання аудиту; процедури, спрямовані на передачу записів аудиту інформаційної системи до вторинних або альтернативних систем; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; журнали передач аудиторських записів до вторинних або альтернативних систем; записи аудиту інформаційної системи, передані вторинним або альтернативним системам; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за планування можливостей зберігання аудиту; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори].  Перевірка: [ВИБІР ВІД: Автоматизовані механізми, що підтримують передачу аудиторських записів на іншу систему]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-5 | РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-5[1] | організація визначає персонал, який має бути сповіщено в разі збою обробки даних аудиту. | |
| AU-5[2] | організація визначає посади, які мають бути сповіщені в разі збою обробки даних аудиту. | |
| AU-5[3] | організація визначає період часу за який мають бути сповіщені персонал або посади в разі збою обробки даних аудиту. | |
| AU-5[4] | AU-5[4]{1} | сповіщати визначений організацією персонал в разі збою обробки даних аудиту у визначений організацією період часу. |
| AU-5[4]{2} | сповіщати визначені організацією посади в разі збою обробки даних аудиту у визначений організацією період часу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація інформаційної системи; план безпеки; налаштування конфігурації інформаційної системи та супутня документація; перелік персоналу, який повинен бути повідомлений у разі відмови аудиторської обробки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують відповідь інформаційної системи на помилки обробки аудиту]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-5(1) | РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-5(1)[1] | організація визначає(один або кілька): | |
| AU-5(1)[1]{1} | персонал, які попереджають коли обсяг записів аудиту, що зберігаються досягає максимуму місткості сховища. |
| AU-5(1)[1]{2} | ролі, які попереджають коли обсяг записів аудиту, що зберігаються досягає максимуму місткості сховища. |
| AU-5(1)[1]{3} | місця, які попереджають коли обсяг записів аудиту, що зберігаються досягає максимуму місткості сховища. |
| AU-5(1)[2] | організація визначає періоду часу за який попереджають персонал, ролі та / або місця коли обсяг записів аудиту, що зберігаються досягає максимуму місткості сховища. | |
| AU-5(1)[3] | організація попереджає визначений організацією(один або кілька): | |
| AU-5(1)[3]{1} | персонал у межах визначеного організацією періоду часу, коли обсяг записів аудиту, що зберігаються досягає максимуму місткості сховища |
| AU-5(1)[3]{2} | ролі у межах визначеного організацією періоду часу, коли обсяг записів аудиту, що зберігаються досягає максимуму місткості сховища |
| AU-5(1)[3]{3} | місця у межах визначеного організацією періоду часу, коли обсяг записів аудиту, що зберігаються досягає максимуму місткості сховища |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація інформаційної системи; план безпеки; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал з обов'язками інформаційної безпеки; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують попередження про обмеження зберігання аудиту]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-5(2) | РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - ТРИВОЖНЕ СПОВІЩЕННЯ В РЕАЛЬНОМУ ЧАСІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-5(2)[1] | організацією визначає | |
| AU-5(2)[1]{1} | персонал, який сповіщають у випадку, коли відбуваються події збою аудиту |
| AU-5(2)[1]{2} | ролі, який сповіщають у випадку, коли відбуваються події збою аудиту |
| AU-5(2)[1]{3} | місця, який сповіщають у випадку, коли відбуваються події збою аудиту |
| AU-5(2)[2] | сповіщають у випадку, коли відбуваються події збою аудиту. визначений організацією: | |
| AU-5(2)[3] | AU-5(2)[2]{1} | персонал та / або |
| AU-5(2)[2]{2} | ролі та / або |
| AU-5(2)[2]{3} | місця. |
| AU-5(2)[4] | організація визначає період реального часу за який необхідно забезпечити сповіщення визначених організацією персоналу, ролей та / або місць у випадку, коли відбуваються події збою аудиту. | |
| AU-5(2)[5] | організація визначає події, пов’язані зі збоями помилками аудиту, які вимагають тривоги в реальному часі. | |
| AU-5(2)[6] | організація забезпечує сповіщення у визначений організацією період реального часу визначених організацією персоналу, ролей та / або місць, коли відбуваються визначені організацією події, пов’язані зі збоями помилками аудиту, які вимагають тривоги в реальному часі. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація інформаційної системи; план безпеки; налаштування конфігурації інформаційної системи та супутня документація; записи сповіщень або сповіщень у режимі реального часу, коли виникають збої в обробці аудиту; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал з обов'язками інформаційної безпеки; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують попередження аудиту в режимі реального часу, коли відбуваються пошкодження аудиту, визначені організацією]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-5(3) | РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - НАЛАШТУВАННЯ ПОРОГОВОГО ОБСЯГУ ТРАФІКУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-5(3)[1] | Організація здійснює налаштування порогових значень обсягу трафіку комунікаційних мереж, що відображають обмеження на можливості аудиту. | |
| AU-5(3)[2] | AU-5(3)[2]{1} | Організація відхиляє мережевий трафік, якщо він перевищує цей поріг. |
| AU-5(3)[2]{2} | Організація затримує мережевий трафік, якщо він перевищує цей поріг. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація інформаційної системи; план безпеки; налаштування конфігурації інформаційної системи та супутня документація; конфігурація порогів обсягу трафіку мережевих комунікацій; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР ВІД: Можливість інформаційної системи, що реалізує налаштовані пороги обсягу трафіку]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-5(4) | РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - ВИМКНЕННЯ У РАЗІ ВІДМОВИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-5(4)[1] | організація визначає збої аудиту за яких застосовують вимкнення системи | |
| AU-5(4)[2] | якщо не існує альтернативної можливості аудиту, організація застосовує: | |
| AU-5(4)[2]{1} | повне вимикання системи; |
| AU-5(4)[2]{2} | часткове вимикання системи; |
| AU-5(4)[2]{3} | знижений режим роботи з обмеженням доступної цільової функціональності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація інформаційної системи; план безпеки; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР ВІД: Можливість роботи інформаційної системи, яка викликає вимкнення системи або погіршує режим роботи в разі відмови аудиторської обробки]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-6 | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-6[a][1] | організація визначає неналежну або незвичайну діяльність | |
| AU-6[a][2] | організація визначає частоту з якою слід переглядати та аналізувати записи системного аудиту для виявлення визначеної організацією неналежної або незвичайної діяльності. | |
| AU-6[a][3] | організація переглядає та аналізує записи системного аудиту для виявлення визначеної організацією неналежної або незвичайної діяльності з визначеною організацією частотою. | |
| AU-6[b][1] | AU-6[b][1]{1} | організація визначає персонал якому відправляють звіт про аудит. |
| AU-6[b][1]{2} | організація визначає посаду якої відправляють звіт про аудит. |
| AU-6[b][2] | організація відправляє звіт про аудит визначеним організацією персоналу або посадам. | |
| AU-6[с][1] | AU-6[с][1][1] | налаштовує організація рівні огляду аудиту в рамках системи, коли змінюється рівень ризику на основі інформації від правоохоронних органів, розвідувальної інформації або від інших достовірних джерел інформації. |
| AU-6[с][1][2] | налаштовує організація рівні огляду аналізу в рамках системи, коли змінюється рівень ризику на основі інформації від правоохоронних органів, розвідувальної інформації або від інших достовірних джерел інформації. |
| AU-6[с][1][3] | налаштовує організація рівні огляду звітності в рамках системи, коли змінюється рівень ризику на основі інформації від правоохоронних органів, розвідувальної інформації або від інших достовірних джерел інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; звіти про результати аудиту; записи про дії, вжиті у відповідь на огляди / аналітичні записи аудиту; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит, аналіз та звітність; організаційний персонал, відповідальний за інформаційну безпеку]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-6(1) | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - АВТОМАТИЗОВАНА ІНТЕГРАЦІЯ ПРОЦЕСІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-6(1)[1] | AU-6(1)[1][1] | організація використовує автоматизовані механізми для інтеграції аудиту, аналізу та звітності для підтримки організаційних процесів розслідування та реагування на підозрілі дії |
| AU-6(1)[1][2] | організація використовує автоматизовані механізми для інтеграції аудиту, аналізу та звітності для підтримки організаційних процесів розслідування та реагування на підозрілі дії |
| AU-6(1)[1][3] | організація використовує автоматизовані механізми для інтеграції аудиту, аналізу та звітності для підтримки організаційних процесів розслідування та реагування на підозрілі дії |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; процедури щодо розслідування та реагування на підозрілі дії; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит, аналіз та звітність; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що інтегрують процеси огляду, аналізу та звітності аудиту]. | | |

|  |  |
| --- | --- |
| AU-6(2) | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - АВТОМАТИЗОВАНІ СПОВІЩЕННЯ ПРО ПОРУШЕННЯ БЕЗПЕКУ |
|  | [Вилучено: Включено до SI-4] |

|  |  |  |
| --- | --- | --- |
| AU-6(3) | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ЗІСТАВЛЯННЯ СХОВИЩ АУДИТУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-6(3)[1] | Організація аналізує та зіставляє записи аудиту в різних сховищах, задля забезпечення ситуативної обізнаності в масштабах організації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи в різних сховищах; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит, аналіз та звітність; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують аналіз та кореляцію аудиторських записів]. | |

|  |  |  |
| --- | --- | --- |
| AU-6(4) | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ЦЕНТРАЛІЗОВАНИЙ ПЕРЕГЛЯД ТА АНАЛІЗ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-6(4)[1] | забезпечити можливість централізованого перегляду та аналізу записів аудиту з декількох компонентів у системі. |
| AU-6(4)[2] | впровадити можливість централізованого перегляду та аналізу записів аудиту з декількох компонентів у системі. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; план безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит, аналіз та звітність; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБРАТИ З: Здатність інформаційної системи до централізації огляду та аналізу аудиторських записів]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-6(5) | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ІНТЕГРОВАНИЙ АНАЛІЗ АУДИТОРСЬКИХ ЗАПИСІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-6(5)[1] | AU-6(5)[1]{1} | організація визначає дані, зібрані з інших джерел які допомагають у подальшому підвищенні здатності виявляти неприйнятну або незвичайну діяльність |
| AU-6(5)[1]{2} | організація визначає інформацію, зібрану з інших джерел яка допомагає у подальшому підвищенні здатності виявляти неприйнятну або незвичайну діяльність |
| AU-6(5)[2] | для подальшого підвищення здатності виявляти неприйнятну або незвичайну діяльність організація інтегрує аналіз записів аудиту з аналізом (один або кілька з нижченаведених): | |
| AU-6(5)[2]{1} | інформації про сканування уразливостей; |
| AU-6(5)[2]{2} | даних про продуктивність; |
| AU-6(5)[2]{3} | інформації про моніторинг системи; |
| AU-6(5)[2]{4} | визначених організацією даних / інформації, зібраних з інших джерел. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; інтегрований аналіз записів аудиту, інформація про сканування вразливості, дані про продуктивність, інформація про моніторинг мережі та супутня документація; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який має аудиторські перевірки, аналіз та звітність; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість інтегрувати аналіз аудиторських записів з аналізом джерел даних або інформації]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-6(6) | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - КОРЕЛЯЦІЯ З ФІЗИЧНИМ МОНІТОРИНГОМ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-6(6)[1] | організація зіставляє інформацію зі записів аудиту з інформацією, отриманою від моніторингу фізичного доступу, для подальшого підвищення здатності ідентифікувати: | |
| AU-6(6)[1]{1} | підозрілу діяльність, |
| AU-6(6)[1]{2} | неприйнятну діяльність, |
| AU-6(6)[1]{3} | незвичайну діяльність |
| AU-6(6)[1]{4} | зловмисну діяльність |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; процедури щодо моніторингу фізичного доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; документація, що надає докази співвіднесеної інформації, отриманої з аудиторських записів та записів моніторингу фізичного доступу; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який має аудиторські перевірки, аналіз та звітність; організаційний персонал, відповідальний за контроль фізичного доступу; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість співвідносити інформацію з аудиторських записів з інформацією з моніторингу фізичного доступу]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AU-6(7) | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ДОЗВОЛЕНІ ДІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| AU-6(7)[1] | організація визначає дозволені дії для кожного(один або кілька): | | |
| AU-6(7)[1]{1} | системного процесу, пов'язаного з: | |
| AU-6(7)[1]{1}[1] | переглядом інформації про аудит. |
| AU-6(7)[1]{1}[2] | аналізом інформації про аудит. |
| AU-6(7)[1]{1}[3] | поданням інформації про аудит. |
| AU-6(7)[1]{2} | ролі, пов'язаного з:. | |
| AU-6(7)[1]{2}[1] | переглядом інформації про аудит. |
| AU-6(7)[1]{2}[2] | аналізом інформації про аудит. |
| AU-6(7)[1]{2}[3] | поданням інформації про аудит. |
| AU-6(7)[1]{3} | користувача, пов'язаного з: | |
| AU-6(7)[1]{3}[1] | переглядом інформації про аудит. |
| AU-6(7)[1]{3}[2] | аналізом інформації про аудит. |
| AU-6(7)[1]{3}[3] | поданням інформації про аудит. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються процесу, ролі та / або дозволених користувачами дій з огляду аудиту, аналізу та звітності; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит, аналіз та звітність; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують дозволені дії щодо огляду, аналізу та звітності аудиторської інформації]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-6(8) | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - АНАЛІЗ ПОВНОГО ТЕКСТУ ПРИВІЛЕЙОВАНИХ КОМАНД | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| AU-6(8)[1] | виконує повний аналіз тексту привілейованих команд аудиту у: | |
| AU-6(8)[1]{1} | фізично окремому компоненті, яка може виконувати такий аналіз. |
| AU-6(8)[1]{2} | підсистемі системи, які можуть виконувати такий аналіз. |
| AU-6(8)[1]{3} | іншій системі, які можуть виконувати такий аналіз. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; інструменти аналізу тексту; документація з аналізу тексту перевірених привілейованих команд; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який має обов'язки з аудиту, аналізу та звітності; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість виконувати повний аналіз тексту аудитованих команд привілеїв]. | | |

|  |  |  |
| --- | --- | --- |
| AU-6(9) | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - КОРЕЛЯЦІЯ З ІНФОРМАЦІЄЮ З НЕТЕХНІЧНИХ ДЖЕРЕЛ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-6(9)[1] | Організація зіставляє інформацію з нетехнічних джерел з інформацією аудиту з метою посилення організаційної обізнаності. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; документація, що забезпечує докази співвіднесеної інформації, отриманої з аудиторських записів та визначених організацією нетехнічних джерел; перелік видів інформації з нетехнічних джерел для співвідношення з аудиторською інформацією; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ: Організаційний персонал, відповідальний за аудит, аналіз та звітність; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливість співвідносити інформацію з нетехнічних джерел]. | |

|  |  |
| --- | --- |
| AU-6(10) | ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - РЕГУЛЮВАННЯ РІВНЯ АУДИТУ |
|  | [Вилучено: Включено до AU-6] |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AU-7 | СКОРОЧЕННЯ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| AU-7[1] | забезпечує можливості скорочення записів аудиторських перевірок та звітів, до рівня, який: | | |
| AU-7[1][a] | AU-7[1][a][1] | підтримує перевірку на вимогу |
| AU-7[1][a][2] | підтримує аналіз на вимогу |
| AU-7[1][a][3] | підтримує звітність аудиту на вимогу |
| AU-7[1][a][4] | розслідування (постфактум) інцидентів безпеки |
| AU-7[1][b] | AU-7[1][b]{1} | не змінює оригінальний вміст упорядкування записів аудиту |
| AU-7[1][b]{2} | не змінює оригінальний час упорядкування записів аудиту |
| AU-7[2] | реалізує можливості скорочення записів аудиторських перевірок та звітів, до рівня, який: | | |
| AU-7[2][a] | AU-7[2][a][1] | підтримує перевірку на вимогу та розслідуванням (постфактум) інцидентів безпеки |
| AU-7[2][a][2] | підтримує аналіз на вимогу та розслідуванням (постфактум) інцидентів безпеки |
| AU-7[2][a][3] | підтримує звітність аудиту на вимогу та розслідуванням (постфактум) інцидентів безпеки |
| AU-7[1][a][4] | розслідування (постфактум) інцидентів безпеки |
| AU-7[2][b] | AU-7[2][b]{1} | не змінює оригінальний вміст упорядкування записів аудиту |
| AU-7[2][b]{2} | не змінює оригінальний час упорядкування записів аудиту |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо скорочення аудиту та формування звітів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; засоби зменшення аудиту, огляду, аналізу та звітності; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал зі скороченням аудиту та створенням звітів; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Скорочення аудиту та створення звітів]. | | | |

|  |  |  |
| --- | --- | --- |
| AU-7(1) | СКОРОЧЕННЯ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ - АВТОМАТИЧНА ОБРОБКА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-7(1)[1] | організація визначає поля в записах аудиту з метою обробки аудиторських записів на події, що представляють інтерес |
| AU-7(1)[2] | забезпечити можливість обробки записів аудиту для подій, що представляють інтерес, на основі визначених організацією полей в записах аудиту |
| AU-7(1)[3] | реалізувати можливість обробки записів аудиту для подій, що представляють інтерес, на основі визначених організацією полей в записах аудиту |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо скорочення аудиту та формування звітів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; засоби зменшення аудиту, огляду, аналізу та звітності; критерії (поля) аудиту, що встановлюють цікаві події; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал зі скороченням аудиту та створенням звітів; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБРАТИ З: Скорочення аудиту та створення звітів]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-7(2) | СКОРОЧЕННЯ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ - АВТОМАТИЧНЕ СОРТУВАННЯ ТА ПОШУК | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-7(2)[1] | організація визначає поля в межах записів аудиту, що беруть участь в автоматичному сортуванні та пошуці. | |
| AU-7(2)[2] | AU-7(2)[2][1] | Забезпечити можливість сортування записів аудиту для подій, що представляють інтерес, на основі змісту визначених організацією полях в межах записів аудиту |
| AU-7(2)[2][2] | Забезпечити можливість пошуку записів аудиту для подій, що представляють інтерес, на основі змісту визначених організацією полях в межах записів аудиту |
| AU-7(2)[2][3] | реалізувати можливість сортування записів аудиту для подій, що представляють інтерес, на основі змісту визначених організацією полях в межах записів аудиту |
| AU-7(2)[2][4] | реалізувати можливість пошуку записів аудиту для подій, що представляють інтерес, на основі змісту визначених організацією полях в межах записів аудиту |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо скорочення аудиту та формування звітів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; засоби скорочення аудиту, огляду, аналізу та звітності; критерії (поля) аудиту, що встановлюють цікаві події; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал зі скорочення аудиту та створенням звітів; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка: [ВИБРАТИ З: Скорочення аудиту та створення звітів]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AU-8 | ПОЗНАЧКА ЧАСУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| AU-8(a) | Організація використовує внутрішньосистемний годинник для створення позначок часу для записів аудиту | | |
| AU-8(b) | AU-8(b)[1] | Організація визначає точність вимірювання часу. | |
| AU-8(b)[2] | Застосовувати позначки часу для збереження записів аудиту, які можуть бути зіставлені з (організація визначає точність вимірювання часу): | |
| AU-8(b)[2]{1} | координованим універсальним часом |
| AU-8(b)[2]{2} | середнім часом за Гринвічем |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються генерації часових позначок; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують генерацію часових позначок]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-8(1) | ПОЗНАЧКА ЧАСУ - СИНХРОНІЗАЦІЯ З АВТОРИТЕТНИМ ДЖЕРЕЛОМ ЧАСУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| **AU-8(1)(a)** | **AU-8(1)(a)[1]** | організація визначає офіційне джерело часу, з яким повинні порівнюватися годинник внутрішньої інформаційної системи; |
| **AU-8(1)(a)[2]** | організація визначає частоту для порівняння годин внутрішньої інформаційної системи з авторитетним джерелом часу, визначеним організацією; |
| **AU-8(1)(a)[3]** | інформаційна система порівнює внутрішній час інформаційної системи з визначеним організацією авторитетним джерелом часу з визначеною організацією частотою; |
| **AU-8(1)(b)** | **AU-8(1)(b)[1]** | організація визначає часовий проміжок, який, якщо перевищить різницю в часі між внутрішніми системними та авторитетними джерелами часу, призведе до синхронізації внутрішніх системних годин з авторитетним джерелом часу; |
| **AU-8(1)(b)[2]** | інформаційна система синхронізує внутрішні годинники інформаційної системи з авторитетним джерелом часу, коли різниця у часі перевищує визначений організацією часовий період. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються генерації часових позначок; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують синхронізацію годинників внутрішньої інформаційної системи.]. | | |

|  |  |  |
| --- | --- | --- |
| AU-8(2) | ПОЗНАЧКА ЧАСУ - ВТОРИННЕ АВТОРИТЕТНЕ ДЖЕРЕЛО ЧАСУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-8(2)(a) | організація визначає вторинне авторитетне джерело часу, яке знаходиться в іншому географічному регіоні, ніж первинне джерело часу. |
| AU-8(2)(b) | синхронізувати внутрішньосистемні годинники з вторинним авторитетним джерелом часу, якщо первинне авторитетне джерело часу недоступно |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються генерації часових позначок; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують авторитетні джерела часу внутрішньої інформаційної системи]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-9 | ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-9[1] | забезпечити захист інформації аудиту від: | |
| AU-9[1][1] | несанкціонованого доступу, |
| AU-9[1][2] | несанкціонованої модифікацій |
| AU-9[1][3] | несанкціонованого видалення. |
| AU-9[2] | забезпечити захист інструментів аудиту від: | |
| AU-9[2][1] | несанкціонованого доступу, |
| AU-9[2][2] | несанкціонованої модифікацій |
| AU-9[2][3] | несанкціонованого видалення. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист аудиторської інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація, записи аудиту інформаційної системи; інструменти аудиту; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують захист аудиторської інформації]. | | |

|  |  |  |
| --- | --- | --- |
| AU-9(1) | ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - АПАРАТНІ НОСІЇ ІНФОРМАЦІЇ ОДНОРАЗОВОГО ЗАПИСУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-9(1)[1] | журнали аудиту мають бути записані на апаратні носії інформації з одноразовим записом. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист аудиторської інформації; проєктна документація інформаційної системи; налаштування апаратних засобів інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; носій інформації для зберігання інформації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Інформаційна система, що зберігає контрольні журнали.]. | |

|  |  |  |
| --- | --- | --- |
| AU-9(2) | ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ЗБЕРІГАННЯ НА ОКРЕМИХ ФІЗИЧНИХ СИСТЕМАХ АБО КОМПОНЕНТАХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-9(2)[1] | організація визначає частоту з якою необхідно зберігати записи аудиту |
| AU-9(2)[2] | зберігати записи аудиту з визначеною організацією з частотою у репозиторії, який є частиною фізично іншої системи або компонента системи, ніж система або компонент, який перевіряється. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, спрямовані на захист аудиторської інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація, система або носій, що зберігають резервні копії записів аудиту інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують резервне копіювання аудиторських записів]. | |

|  |  |  |
| --- | --- | --- |
| AU-9(3) | ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - КРИПТОГРАФІЧНИЙ ЗАХИСТ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-9(3)[1] | запровадити криптографічні механізми для захисту цілісності інформації аудиту |
| AU-9(3)[2] | запровадити криптографічні механізми для захисту цілісності інструментів аудиту |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист аудиторської інформації; проєктна документація інформаційної системи; налаштування апаратних засобів інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація, записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Криптографічні механізми, що захищають цілісність аудиторської інформації та інструментів]. | |

|  |  |  |
| --- | --- | --- |
| AU-9(4) | ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ДОСТУП, ЯКИЙ НАДАЄТЬСЯ ЧЕРЕЗ ЧЛЕНСТВО В ПІДМНОЖИНИ ПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-9(4)[1] | організація визначає підмножини привілейованих користувачів |
| AU-9(4)[2] | авторизувати доступ до управління функціональністю аудиту тільки для визначеної організацією підмножини привілейованих користувачів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист аудиторської інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація, створений системою список привілейованих користувачів з доступом до управління функціями аудиту; авторизація доступу; список контролю доступу; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми управління доступом до функцій аудиту]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-9(5) | ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ПОДВІЙНА АВТОРИЗАЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-9(5)[1] | організація визначає аудиторську інформацію необхідну для здійснення подвійної авторизації | |
| AU-9(5)[2] | для визначеної організацією аудиторської інформації організація здійснює подвійну авторизацію (один або кілька): | |
| AU-9(5)[2]{1} | переміщення |
| AU-9(5)[2]{2} | видалення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист аудиторської інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація, авторизація доступу; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують виконання подвійної авторизації]. | | |

|  |  |  |
| --- | --- | --- |
| AU-9(6) | ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ДОСТУП ТІЛЬКИ ДЛЯ ЧИТАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-9(6)[1] | організація визначає підмножини привілейованих користувачів для яких доступ авторизовано тільки для читання. |
| AU-9(6)[2] | авторизувати доступ лише для читання інформації аудиту для визначеної організацією підмножини привілейованих користувачів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист аудиторської інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація, створений системою список привілейованих користувачів із доступом до інформації аудиту лише для читання; авторизація доступу; список контролю доступу; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми управління доступом до аудиторської інформації]. | |

|  |  |  |
| --- | --- | --- |
| AU-9(7) | ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ЗБЕРІГАННЯ НА КОМПОНЕНТІ ІНШОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-9(7)[1] | організація зберігає інформацію про аудит на компоненті, що працює з іншою операційною системою, ніж система або компонент, який проходить аудит |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист аудиторської інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація, створений системою список привілейованих користувачів із доступом до інформації аудиту лише для читання; авторизація доступу; список контролю доступу; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аудит та підзвітність; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми управління доступом до аудиторської інформації]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-10 | НЕСПРОСТОВНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-10[1] | організація визначає дії, які повинні бути покриті захистом неспростовності | |
| AU-10[2] | AU-10[2]{1} | забезпечити захист від окремих осіб, які навмисно заперечують факти виконання визначених організацією дій, які повинні бути покриті захистом неспростовності |
| AU-10[2]{2} | забезпечити захист від процесів, що діють від імені фізичної особи, які навмисно заперечують факти виконання визначених організацією дій, які повинні бути покриті захистом неспростовності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо неспростовності; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість неспростовності]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-10(1) | НЕСПРОСТОВНІСТЬ - АСОЦІАЦІЯ ІДЕНТИЧНОСТІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-10(1)(a) | AU-10(1)(a)[1] | організація визначає міцність зв'язування особистість джерела інформації з інформацією |
| AU-10(1)(a)[2] | організація зв'язує особистість джерела інформації з інформацією з визначеною організацією міцністю зв'язування. |
| AU-10(1)(b) | впровадити засоби, якими уповноважені особи можуть визначити особу виробника інформації | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо неспростовності; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість неспростовності]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-10(2) | НЕСПРОСТОВНІСТЬ - РАТИФІКАЦІЯ ПРИВ'ЯЗКИ ІНФОРМАЦІЇ ПРО ІДЕНТИЧНІСТЬ ВИРОБНИКА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-10(2)(a) | AU-10(2)(a)[1] | організація визначає частоту з якою підтверджують прив'язку інформації про ідентичність джерела до інформації |
| AU-10(2)(a)[2] | організація підтверджує прив'язку інформації про ідентичність джерела до інформації з визначеною організацією частотою. |
| AU-10(2)(b) | AU-10(2)(b)[1] | організація визначає дії у разі помилки перевірки |
| AU-10(2)(b)[2] | організація має виконати визначені організацією дії у разі помилки перевірки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо неспростовності; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; ратифікаційні записи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість неспростовності]. | | |

|  |  |  |
| --- | --- | --- |
| AU-10(3) | НЕСПРОСТОВНІСТЬ - ЛАНЦЮЖОК ЗБЕРЕЖЕННЯ ДОКАЗІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-10(3)[1] | підтримувати перегляд ідентичності в межах встановленого ланцюжка збереження доказів для всієї переглянутої або оприлюдненої інформації. |
| AU-10(3)[2] | підтримувати перегляд повноважень в межах встановленого ланцюжка збереження доказів для всієї переглянутої або оприлюдненої інформації. |
| AU-10(3)[3] | підтримувати випуск в межах встановленого ланцюжка збереження доказів для всієї переглянутої або оприлюдненої інформації. |
| AU-10(3)[4] | підтримувати випуск повноважень в межах встановленого ланцюжка збереження доказів для всієї переглянутої або оприлюдненої інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо неспростовності; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи інформаційних оглядів та випусків; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість неспростовності]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| AU-10(4) | НЕСПРОСТОВНІСТЬ - ВАЛІДАЦІЯ ЗВ'ЯЗКУ ІДЕНТИЧНОСТІ ПЕРЕГЛЯДАЧА ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| **AU-10(4)(a)** | **AU-10(4)(a)[1]** | організація визначає домени безпеки між якими передається інформація. | |
| **AU-10(4)(a)[2]** | **AU-10(4)(a)[2]{1}** | підтвердить прив'язку особистості рецензента до інформації в точках передачі або видачі до її випуску або передачі між визначеними організацією домени безпеки |
| **AU-10(4)(a)[2]{2}** | підтвердить прив'язку особистості рецензента до інформації в точках передачі або видачі до її випуску або передачі між визначеними організацією домени безпеки |
| **AU-10(4)(b)** | **AU-10(4)(b)[1]** | організація визначає дії, які слід виконати у разі помилки перевірки | |
| **AU-10(4)(b)[2]** | організація виконує визначені дії у разі помилки перевірки | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо неспростовності; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; валідаційні записи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість неспростовності]. | | | |

|  |  |
| --- | --- |
| AU-10(5) | НЕСПРОСТОВНІСТЬ - ЦИФРОВІ ПІДПИСИ |
|  | [Вилучено: Включено до SI-13] |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-11 | ЗБЕРЕЖЕННЯ ЗАПИСІВ АУДИТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-11[1] | організація визначає період часу зберігання записів аудиту, відповідно політиці зберігання записів | |
| AU-11[2] | зберігає записи аудиту впродовж визначеного організацією періоду часу, відповідно політиці зберігання записів, щоб забезпечити підтримку розслідувань (постфактум): | |
| AU-11[2][1] | інцидентів безпеки щодо збереження даних аудиту. |
| AU-11[2][2] | інцидентів приватності щодо збереження даних аудиту. |
| AU-11[3] | зберігати записи аудиту впродовж визначеного організацією періоду часу, відповідно політиці зберігання записів, щодо збереження даних аудиту для задоволення вимог: | |
| AU-11[3][1] | нормативних документів |
| AU-11[3][2] | організаційних документів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; політика та процедури збереження записів аудиту; план безпеки; визначений організацією термін зберігання аудиторських записів; архіви записів аудиту; журнали аудиту; аудиторські записи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за збереження записів аудиту; організаційний персонал, відповідальний за захист інформації системні або мережеві адміністратори]. | | |

|  |  |  |
| --- | --- | --- |
| AU-11(1) | ЗБЕРЕЖЕННЯ ЗАПИСІВ АУДИТУ - ДОВГОСТРОКОВА МОЖЛИВІСТЬ ОТРИМАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-11(1)[1] | організація визначає заходи, необхідні для реалізації довгострокової можливості отримання записів аудиту |
| AU-11(1)[2] | впровадити визначені організацією заходи, щоб гарантувати, що довгострокові записи аудиту, створені системою, можуть бути отримані. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; політика та процедури збереження записів аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; архіви записів аудиту; журнали аудиту; аудиторські записи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за збереження записів аудиту; організаційний персонал, відповідальний за захист інформації системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість збереження записів аудиту]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-12 | ГЕНЕРАЦІЯ ДАНИХ АУДИТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-12(a)[1] | організація визначає системні компоненти необхідні для генерації даних аудиту | |
| AU-12(a)[2] | забезпечити генерацію даних аудиту для типів подій, що перевіряються в AU-2 в визначених організацією системних компонентах | |
| AU-12(b)[1] | задля вибору, які типи подій, що перевіряються повинні перевірятися окремими компонентами системи, організація визначає: | |
| AU-12(b)[1]{1} | персонал, |
| AU-12(b)[1]{2} | посади. |
| AU-12(b)[2] | Дозволити: | |
| AU-12(b)[2]{1} | *визначеному організацією персоналу* вибирати, які типи подій, що перевіряються повинні перевірятися окремими компонентами системи |
| AU-12(b)[2]{2} | *або посадам* вибирати, які типи подій, що перевіряються повинні перевірятися окремими компонентами системи |
| AU-12(c)[1] | генерувати записи аудиту для типів подій, визначених в AU-2 (d). з вмістом згідно AU-3 | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, спрямовані на створення аудиторських записів; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік аудиторських подій; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за створення записів аудиту; організаційний персонал, відповідальний за захист інформації системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість створення записів аудиту]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-12(1) | ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - ЗАГАЛЬНОСИСТЕМНИЙ ТА СИНХРОНІЗОВАНИЙ ЗА ЧАСОМ ЖУРНАЛУ АУДИТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-12(1)[1] | організація визначає системні компоненти необхідні для генерації даних аудиту | |
| AU-12(1)[2] | організація визначає допустимий рівень для взаємозв'язку між мітками часу окремих записів в журналах аудиту | |
| AU-12(1)[3] | організація компонує записи аудиту з визначеними організацією системними компонентами в загальносистемний: | |
| AU-12(1)[3]{1} | логічний журнал аудиту, який синхронізований за часом в межах визначеного організацією допустимого рівня для взаємозв'язку між мітками часу окремих записів в журналах аудиту |
| AU-12(1)[3]{2} | фізичний журнал аудиту, який синхронізований за часом в межах визначеного організацією допустимого рівня для взаємозв'язку між мітками часу окремих записів в журналах аудиту |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, спрямовані на створення аудиторських записів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; загальносистемний журнал аудиту (логічний або фізичний); записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за створення записів аудиту; організаційний персонал, відповідальний за захист інформації системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість створення записів аудиту]. | | |

|  |  |  |
| --- | --- | --- |
| AU-12(2) | ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - СТАНДАРТИЗОВАНІ ФОРМАТИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-12(2){1} | організація створює загальносистемний (логічний) журнал аудиту, що складається з записів аудиту в стандартизованому форматі |
| AU-12(2){2} | організація створює загальносистемний (фізичний) журнал аудиту, що складається з записів аудиту в стандартизованому форматі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, спрямовані на створення аудиторських записів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; загальносистемний журнал аудиту (логічний або фізичний); записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за створення записів аудиту; організаційний персонал, відповідальний за захист інформації системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість створення записів аудиту]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-12(3) | ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - ЗМІНИ, ЩО ВНОСЯТЬ АВТОРИЗОВАНІ ОСОБИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-12(3)[1] | AU-12(3)[1]{1} | організація визначає окремих осіб, яким дозволено змінювати аудит, |
| AU-12(3)[2] | AU-12(3)[1]{2} | організація визначає окремі ролі, яким дозволено змінювати аудит |
| AU-12(3)[3] | організація визначає системні компоненти, на якому будуть виконуватися зміни аудиту. | |
| AU-12(3)[4] | організація визначає критерії вибору подій аудиту, до яких необхідно вносити зміни. | |
| AU-12(3)[5] | організація визначає часові пороги зміни подій аудиту | |
| AU-12(3)[6] | AU-12(3)[6][1] | Забезпечити можливість для визначених організацією окремих осіб або ролей змінити аудит, який буде виконуватися на визначених організацією системних компонентах на основі визначених організацією критеріїв вибору подій в межах визначених організацією часових порогів |
| AU-12(3)[6][2] | реалізувати можливість для визначених організацією окремих осіб або ролей змінити аудит, який буде виконуватися на визначених організацією системних компонентах на основі визначених організацією критеріїв вибору подій в межах визначених організацією часових порогів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, спрямовані на створення аудиторських записів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; сформований системою список осіб або посад, уповноважених змінювати аудит, який слід виконувати; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за створення записів аудиту; організаційний персонал, відповідальний за захист інформації системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість створення записів аудиту]. | | |

|  |  |  |
| --- | --- | --- |
| AU-12(4) | ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - АУДИТ ЗАПИТІВ ПЕРСОНАЛЬНОЇ ІДЕНТИФІКАЦІЙНОЇ ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| AU-12(4)[1] | забезпечити можливості аудиту параметрів подій запитів користувачів для наборів даних, що містять персональну ідентифікаційну інформацію. |
| AU-12(4)[2] | реалізувати можливості аудиту параметрів подій запитів користувачів для наборів даних, що містять персональну ідентифікаційну інформацію. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, спрямовані на створення аудиторських записів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; сформований системою список осіб або посад, уповноважених змінювати аудит, який слід виконувати; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за створення записів аудиту; організаційний персонал, відповідальний за захист інформації системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість створення записів аудиту]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-13 | МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-13[1] | AU-13[1]{1} | організація визначає відкриті джерела інформації для отримання свідчень про несанкціоноване розкриття корпоративної інформації |
| AU-13[1]{2} | організація визначає відкриті інформаційні сайти для отримання свідчень про несанкціоноване розкриття корпоративної інформації |
| AU-13[2] | організація визначає частоту, з якою організація має відстежувати відкриті джерела інформації та/або інформаційні сайти для отримання свідчень про несанкціоноване розкриття корпоративної інформації. | |
| AU-13[3] | організація відстежує визначені організацією відкриті джерела інформації та/або інформаційні сайти з визначеною організацією частотою для отримання свідчень про несанкціоноване розкриття корпоративної інформації | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо моніторингу розкриття інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; моніторингові записи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за моніторинг інформації з відкритим кодом та / або інформаційних сайтів; організаційний персонал, відповідальний за інформаційну безпеку]  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують моніторинг для розкриття інформації]. | | |

|  |  |  |
| --- | --- | --- |
| AU-13(1) | МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ - ВИКОРИСТАННЯ АВТОМАТИЧНИХ ЗАСОБІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-13(1)[1] | організація використовує автоматизовані механізми, щоб визначити, чи була інформація про організацію несанкціоновано розкрита |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо моніторингу розкриття інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; автоматизовані засоби моніторингу; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за моніторинг розкриття інформації; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують моніторинг для розкриття інформації]. | |

|  |  |  |
| --- | --- | --- |
| AU-13(2) | МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ - ОГЛЯД САЙТІВ, ЩО ПІДЛЯГАЮТЬ МОНІТОРИНГУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-13(2)[1] | організація визначає частоту з якою проводять огляд відкритих інформаційних сайтів, що підлягають моніторингу |
| AU-13(2)[2] | організація проводить огляд відкритих інформаційних сайтів, що підлягають моніторингу з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо моніторингу розкриття інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; огляди інформаційних сайтів з відкритим кодом, що контролюються; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за моніторинг інформаційних сайтів з відкритим кодом; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують моніторинг для розкриття інформації]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-14 | АУДИТ СЕСІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-14[1] | організація забезпечує спроможність авторизованим користувачам вибирати сеанс користувача для: | |
| AU-14[1]{1} | збору |
| AU-14[1]{2} | запису |
| AU-14[1]{3} | перегляду |
| AU-14[1]{4} | прослуховування |
| AU-14[2] | організація реалізує спроможність авторизованим користувачам вибирати сеанс користувача для: | |
| AU-14[2]{1} | збору |
| AU-14[2]{2} | запису |
| AU-14[2]{3} | перегляду |
| AU-14[2]{4} | прослуховування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо аудиту сесії користувача; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість аудиту сесій користувача]. | | |

|  |  |  |
| --- | --- | --- |
| AU-14(1) | АУДИТ СЕСІЇ - СИСТЕМА ЗАПУСКУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-14(1)[1] | організація автоматично ініціює аудит сесії при запуску системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо аудиту сесій користувача; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБІР ВІД: Автоматизовані механізми, що реалізують можливість аудиту сесій користувача]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-14(2) | АУДИТ СЕСІЇ - ЗАХОПЛЕННЯ ТА ЗАПИС ІНФОРМАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-14(2)[1] | організація забезпечує спроможність авторизованих користувачів для | |
| AU-14(2)[1][1] | захоплення вмісту, пов'язаного з користувацьким сеансом |
| AU-14(2)[1][2] | запису вмісту, пов'язаного з користувацьким сеансом |
| AU-14(2)[1][3] | реєстрації вмісту, пов'язаного з користувацьким сеансом |
| AU-14(2)[2] | організація реалізує спроможність авторизованих користувачів для | |
| AU-14(2)[2][1] | захоплення вмісту, пов'язаного з користувацьким сеансом |
| AU-14(2)[2][2] | запису вмісту, пов'язаного з користувацьким сеансом |
| AU-14(2)[2][3] | реєстрації вмісту, пов'язаного з користувацьким сеансом |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо аудиту сеансів користувача; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість аудиту сеансів користувача]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| AU-14(3) | АУДИТ СЕСІЇ - ДИСТАНЦІЙНЕ СПОСТЕРЕЖЕННЯ ТА ПРОСЛУХОВУВАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| AU-14(3)[1] | організація забезпечує спроможність авторизованих користувачів віддалено: | |
| AU-14(3)[1][1] | переглядати вміст повідомлень, у реальному часі |
| AU-14(3)[1][2] | прослуховувати вміст повідомлень, у реальному часі |
| AU-14(3)[2] | організація реалізує спроможність авторизованих користувачів віддалено: | |
| AU-14(3)[2][1] | переглядати вміст повідомлень, у реальному часі |
| AU-14(3)[2][1] | прослуховувати вміст повідомлень, у реальному часі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури щодо аудиту сесії користувача; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість аудиту сеансів користувача]. | | |

|  |  |  |
| --- | --- | --- |
| AU-15 | АЛЬТЕРНАТИВНА МОЖЛИВІСТЬ АУДИТУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-15[1] | організація визначає альтернативні функції перевірки |
| AU-15[2] | надати можливість альтернативної перевірки у разі збою функції первинної перевірки, яка реалізує визначені організацією альтернативні функції перевірки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, пов'язані з можливістю альтернативного аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; тестові записи щодо можливості альтернативного аудиту; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за надання можливості альтернативного аудиту; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують альтернативні можливості аудиту]. | |

|  |  |  |
| --- | --- | --- |
| AU-16 | МІЖОРГАНІЗАЦІЙНИЙ АУДИТ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-16[1] | організація визначає методи для координації інформації серед зовнішніх організацій, коли інформація аудиту передається через (за) межі організації (системи). |
| AU-16[2] | організація визначає інформацію |
| AU-16[3] | організація використовує визначені організацією методи для координації визначеної організацією інформації серед зовнішніх організацій, коли інформація аудиту передається через (за) межі організації (системи). |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються методів координації аудиторської інформації серед зовнішніх організацій; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; методи координації аудиторської інформації серед зовнішніх організацій; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за координацію аудиторської інформації серед зовнішніх організацій; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують міжорганізаційний аудит (якщо застосовується)]. | |

|  |  |  |
| --- | --- | --- |
| AU-16(1) | МІЖОРГАНІЗАЦІЙНИЙ АУДИТ - ЗБЕРЕЖЕННЯ ІДЕНТИЧНОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-16(1)[1] | організація вимагає, щоб ідентичність особистості зберігалася в крос-організаційних аудиторських журналах |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури розв’язання питань міжорганізаційного аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з відповідальністю за міжорганізаційний аудит; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що впроваджують міжорганізаційний аудит (якщо застосовується)]. | |

|  |  |  |
| --- | --- | --- |
| AU-16(2) | МІЖОРГАНІЗАЦІЙНИЙ АУДИТ - ОБМІН ІНФОРМАЦІЄЮ АУДИТУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| AU-16(2)[1] | організація визначає організації до яких надають інформацію про міжорганізаційний аудит |
| AU-16(2)[2] | організація визначає міжорганізаційну угоду про розподіл. |
| AU-16(2)[3] | надати інформацію про міжорганізаційний аудит до організацій, визначених організацією на основі визначеної організацією міжорганізаційної угоди про розподіл. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються міжорганізаційного обміну аудиторською інформацією; міжорганізаційні угоди про обмін; угоди про обмін даними; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обмін інформацією міжорганізаційного аудиту; організаційний персонал, відповідальний за інформаційну безпеку]. | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ CA – ОЦІНЮВАННЯ, АКРЕДИТАЦІЯ ТА МОНІТОРИНГ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CA-1 | ПОЛІТИКА І ПРОЦЕДУРИ ОЦІНЮВАННЯ, АКРЕДИТАЦІЇ ТА МОНІТОРИНГУ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| CA-1(a) | CA-1(a)[1] | CA-1(a)[1](1) | | | Розробляє та документує політику оцінювання, акредитації та моніторингу, яка: | | | | | | | | |
| CA-1(a)[1](1)(a) | | Містить: | | | | | | |
| CA-1(a)[1](1)(a)[1] | | | | мету, | | |
| CA-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| CA-1(a)[1](1)(a)[3] | | | | ролі, | | |
| CA-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| CA-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| CA-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| CA-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| CA-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| CA-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| CA-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| CA-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| CA-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| CA-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| CA-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| CA-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| CA-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики оцінювання, акредитації та моніторингу, а також пов'язаних з ними заходів оцінювання, акредитації та моніторингу; | | | | | | | | |
| CA-1(a)[2] | CA-1(a)[2]{1} | | | CA-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика оцінювання, акредитації та моніторингу | | | | | |
| CA-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики оцінювання, акредитації та моніторингу та пов'язаних з нею заходів захисту політики оцінювання, акредитації та моніторингу | | | | | |
| CA-1(a)[2]{2} | | | CA-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика оцінювання, акредитації та моніторингу | | | | | |
| CA-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики оцінювання, акредитації та моніторингу та пов'язаних з нею заходів захисту політики оцінювання, акредитації та моніторингу | | | | | |
| CA-1(a)[3] | CA-1(a)[3]{1} | | | CA-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику оцінювання, акредитації та моніторингу | | | | | | | |
| CA-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| CA-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| CA-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| CA-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| CA-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| CA-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| CA-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| CA-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| CA-1(a)[3](1)(b) | | | Відповідає: | | | | |
| CA-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| CA-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| CA-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| CA-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| CA-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| CA-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| CA-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| CA-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації захисту оцінювання, акредитації та моніторингу та відповідних заходів оцінювання, акредитації та моніторингу | | | | | | | |
| CA-1(a)[3]{2} | | | CA-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику захисту оцінювання, акредитації та моніторингу, яка: | | | | | | | |
| CA-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| CA-1(a)[3]{2}(1)(а)[1] | | мету, | |
| CA-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| CA-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| CA-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| CA-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| CA-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| CA-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| CA-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| CA-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| CA-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| CA-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| CA-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| CA-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| CA-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| CA-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| CA-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики оцінювання, акредитації та моніторингу та пов'язаних з нею заходів оцінювання, акредитації та моніторингу | | | | | | | |
| CA-1(b) | CA-1(b)[1] | визначає посадову особу для управління політикою та процедурами оцінювання, акредитації та моніторингу оцінювання, акредитації та моніторингу | | | | | | | | | | | |
| CA-1(b)[2] | призначає посаду для управління політикою та процедурами оцінювання, акредитації та моніторингу | | | | | | | | | | | |
| CA-1(с) | CA-1(с)[1] | CA-1(с)[1](1) | | CA-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики оцінювання, акредитації та моніторингу | | | | | | | |
| CA-1(с)[1](1)[2] | | переглядає поточну політику оцінювання, акредитації та моніторингу з визначеною організацією частотою | | | | | | | |
| CA-1(с)[1](2) | | CA-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур оцінювання, акредитації та моніторингу | | | | | | | |
| CA-1(с)[1](2)[2] | | переглядає поточні процедури оцінювання, акредитації та моніторингу з визначеною організацією частотою | | | | | | | |
| CA-1(с)[2] | CA-1(с)[2](1) | | CA-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики оцінювання, акредитації та моніторингу | | | | | | | |
| CA-1(с)[2](1)[2] | | оновлює поточну політику оцінювання, акредитації та моніторингу з визначеною організацією частотою | | | | | | | |
| CA-1(с)[2](2) | | CA-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур оцінювання, акредитації та моніторингу | | | | | | | |
| CA-1(с)[2](2)[2] | | оновлює поточні процедури оцінювання, акредитації та моніторингу з визначеною організацією частотою | | | | | | | |
| CA-1(d) | переконується, що процедури оцінювання, акредитації та моніторингу реалізують політику та заходи оцінювання, акредитації та моніторингу | | | | | | | | | | | | |
| CA-1(e) | CA-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики оцінювання, акредитації та моніторингу | | | | | | | | | | |
| CA-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики оцінювання, акредитації та моніторингу | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури оцінювання, акредитації та моніторингу; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику оцінювання, акредитації та моніторингу; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CA-2 | ОЦІНЮВАННЯ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| CA-2(a)[1] | розробити план оцінювання безпеки, який описує сферу оцінки, та охоплює: | | | | |
| CA-2(a)[1](1) | | CA-2(a)[1](1)[1] | | заходи захисту, що підлягають оцінюванню |
| CA-2(a)[1](1)[2] | | удосконалені заходи захисту, що підлягають оцінюванню |
| CA-2(a)[1](2) | | процедури оцінювання, які будуть використовуватися для визначення ефективності заходів | | |
| CA-2(a)[1](3) | | CA-2(a)[1](3)[1] | | середовище оцінювання, |
| CA-2(a)[1](3)[2] | | групу оцінювання, |
| CA-2(a)[1](3)[3] | | ролі з оцінювання |
| CA-2(a)[1](3)[4] | | обов'язки з оцінювання |
| CA-2(a)[2] | розробити план оцінювання приватності, який описує сферу оцінки, та охоплює: | | | | |
| CA-2(a)[2](1) | | CA-2(a)[2](1)[1] | | заходи захисту, що підлягають оцінюванню |
| CA-2(a)[2](1)[2] | | удосконалені заходи захисту, що підлягають оцінюванню |
| CA-2(a)[2](2) | | процедури оцінювання, які будуть використовуватися для визначення ефективності заходів | | |
| CA-2(a)[2](3) | | CA-2(a)[2](3)[1] | | середовище оцінювання, |
| CA-2(a)[2](3)[2] | | групу оцінювання, |
| CA-2(a)[2](3)[3] | | ролі з оцінювання |
| CA-2(a)[2](3)[4] | | обов'язки з оцінювання |
| CA-2(b){1} | CA-2(b){1}[1] | | забезпечити розгляд плану оцінювання уповноваженою офіційною особою | | |
| CA-2(b){1}[2] | | забезпечити затвердження плану оцінювання уповноваженою офіційною особою | | |
| CA-2(b){2} | CA-2(b){2}[1] | | забезпечити розгляд плану оцінювання призначеним для проведення оцінювання представником | | |
| CA-2(b){2}[2] | | забезпечити затвердження плану оцінювання призначеним для проведення оцінювання представником | | |
| CA-2(c) | CA-2(c)[1] | | визначає частоту оцінювання заходів захисту в системі та в її середовищі функціонування для визначення, як коректно реалізовані заходи безпеки, наскільки діють за призначенням і дають бажаний результат щодо дотримання встановлених вимог безпеки та приватності | | |
| CA-2(c)[2] | | проводить оцінювання заходів захисту в системі та в її середовищі функціонування для визначення, як коректно реалізовані заходи безпеки, наскільки діють за призначенням і дають бажаний результат щодо дотримання встановлених вимог безпеки та приватності з визначеною частотою | | |
| CA-2(d) | підготовити звіт про оцінку безпеки та приватності, який документує результати оцінювання | | | | |
| CA-2(e) | CA-2(e)[1] | CA-2(e)[1]{1} | | організація визначає уповноважену особу, що відповідає за контроль за результатами оцінювання безпеки та приватності | |
| CA-2(e)[1]{2} | | організація визначає посаду, що відповідає за контроль за результатами оцінювання безпеки та приватності | |
| CA-2(e)[2] | надати результати оцінювання з безпеки та приватності уповноваженій особі - визначеній організацією особі або посади. | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури щодо планування оцінки безпеки; процедури, що стосуються оцінок безпеки; план оцінки безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за оцінку безпеки; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують оцінку безпеки, розробку плану оцінки безпеки та / або звітність про оцінку безпеки]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CA-2(1) | ОЦІНЮВАННЯ - НЕЗАЛЕЖНІ ЕКСПЕРТИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CA-2(1){1} | Залучати незалежних експертів з оцінки для проведення: | |
| CA-2(1){1}[1] | оцінювання безпеки |
| CA-2(1){1}[2] | оцінювання приватності |
| CA-2(1){2} | Залучати незалежні групи з оцінки для проведення: | |
| CA-2(1){2}[1] | оцінювання безпеки |
| CA-2(1){2}[2] | оцінювання приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, що стосуються оцінок безпеки; пакет дозволів на безпеку (включаючи план безпеки, план оцінки безпеки, звіт про оцінку безпеки, план дій та основні етапи, заяву про авторизацію); інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за оцінку безпеки; організаційний персонал, відповідальний за інформаційну безпеку]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CA-2(2) | ОЦІНЮВАННЯ - СПЕЦІАЛІЗОВАНІ ОЦІНКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CA-2(2)[1] | організація обирає одну або декілька з наступних спеціалізованих оцінок: | |
| CA-2(2)[1]{1} | поглиблений моніторинг; |
| CA-2(2)[1]{2} | сканування уразливостей; |
| CA-2(2)[1]{3} | тестування на шкідливих користувачів; |
| CA-2(2)[1]{4} | оцінка внутрішньої загрози; |
| CA-2(2)[1]{5} | тестування продуктивності; |
| CA-2(2)[1]{6} | тестування навантаження; |
| CA-2(2)[1]{7} | організаційно визначені інші форми оцінки. |
| CA-2(2)[2] | організація визначає, як проводити спеціалізовану оцінку: | |
| CA-2(2)[2]{1} | з попередженням; |
| CA-2(2)[2]{2} | без попередження |
| CA-2(2)[3] | організація визначає частоту з якою проводить спеціалізовані оцінки. | |
| CA-2(2)[4] | організація включає як частину оцінювання заходів безпеки та приватності з визначеною організацією частотою, з попередженням або без попередження, (один або кілька): | |
| CA-2(2)[4]{1} | поглиблений моніторинг; |
| CA-2(2)[4]{2} | сканування уразливостей; |
| CA-2(2)[4]{3} | тестування на шкідливих користувачів; |
| CA-2(2)[4]{4} | оцінка внутрішньої загрози; |
| CA-2(2)[4]{5} | тестування продуктивності; |
| CA-2(2)[4]{6} | тестування навантаження; |
| CA-2(2)[4]{7} | організаційно визначені інші форми оцінки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, що стосуються оцінок безпеки; план безпеки; план оцінки безпеки; звіт про оцінку безпеки; докази оцінки безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за оцінку безпеки; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують оцінку заходів безпеки]. | | |

|  |  |  |
| --- | --- | --- |
| CA-2(3) | ОЦІНЮВАННЯ - ЗОВНІШНІ ОРГАНІЗАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CA-2(3)[1] | організація визначає систему, яка приймає результати оцінок заходів захисту інформації та персональних даних |
| CA-2(3)[2] | зовнішня організація визначає організацію, яка надає результати оцінок заходів захисту інформації та персональних даних |
| CA-2(3)[3] | організація визначає вимоги до результатів оцінок заходів захисту інформації та персональних даних |
| CA-2(3)[4] | прийняти результати оцінок заходів захисту інформації та персональних даних: визначеною організацією системою, що надані: організацією, визначеною зовнішньою організацією, коли оцінювання відповідає: визначеним організацією вимогам. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, що стосуються оцінок безпеки; план безпеки; вимоги щодо оцінки безпеки; план оцінки безпеки; звіт про оцінку безпеки; докази оцінки безпеки; план дій та віхи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за оцінку безпеки; організаційний персонал, відповідальний за захист інформації персонал, який виконує оцінки безпеки для зазначеної зовнішньої організації]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CA-3 | СИСТЕМНІ ВЗАЄМОДІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CA-3(a) | авторизувати з'єднання системи з іншими системами з використанням Угод про безпеку з'єднань | | |
| CA-3(b) | задокументувати для кожної взаємодії | | |
| CA-3(b)[1] | характеристики інтерфейсу, | |
| CA-3(b)[2] | вимоги безпеки та приватності, | |
| CA-3(b)[3] | характер переданої інформації | |
| CA-3(с) | CA-3(с)[1] | CA-3(с)[1][1] | організація визначає частоту перегляду угод про безпеку мережевого з'єднання |
| CA-3(с)[1][2] | організація визначає частоту оновлення угод про безпеку мережевого з'єднання |
| CA-3(с)[2] | CA-3(с)[2][1] | здійснювати перегляд угод про безпеку мережевого з'єднання з визначеною організацією частотою |
| CA-3(с)[2][2] | здійснювати оновлення угод про безпеку мережевого з'єднання з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика контролю доступу; процедури, що стосуються з'єднань інформаційної системи; системна та комунікаційна політика захисту; Угоди про безпеку взаємозв'язку інформаційної системи; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за розробку, впровадження або затвердження угод про взаємозв'язок інформаційної системи; організаційний персонал, відповідальний за захист інформації персонал, що керує системою (системами), на яку поширюється Угода про безпеку взаємозв’язку]. | | | |

|  |  |  |
| --- | --- | --- |
| CA-3(1) | СИСТЕМНІ ВЗАЄМОДІЇ - НЕЗАХИЩЕНІ З’ЄДНАННЯ СИСТЕМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CA-3(1)[1] | організація визначає незахищені системи яким заборонено безпосереднє підключення до зовнішньої мережі без використання визначених організацією засобів захисту периметру |
| CA-3(1)[2] | організація визначає засоби захисту периметру, які використовуються визначеними організацією незахищеними системи |
| CA-3(1)[3] | організація забороняє безпосереднє підключення визначених організацією незахищених систем до зовнішньої мережі без використання визначених організацією засобів захисту периметру. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика контролю доступу; процедури, що стосуються з'єднань інформаційної системи; системна та комунікаційна політика захисту; угоди про безпеку взаємозв'язку інформаційної системи; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; звіт про оцінку безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління прямими підключеннями до зовнішніх мереж; мережеві адміністратори; організаційний персонал, відповідальний за захист інформації персонал, що управляє безпосередньо підключеними зовнішніми мережами]  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують управління зовнішніми мережевими з'єднаннями]. | |

|  |  |  |
| --- | --- | --- |
| CA-3(2) | СИСТЕМНІ ВЗАЄМОДІЇ - ЗАХИЩЕНІ З’ЄДНАННЯ СИСТЕМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CA-3(2)[1] | організація визначає засоби захисту периметру для прямого підключення системи до зовнішньої мережі. |
| CA-3(2)[2] | організація забороняє пряме підключення системи до зовнішньої мережі без використання визначених організацією засобів захисту периметру |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика контролю доступу; процедури, що стосуються з'єднань інформаційної системи; системна та комунікаційна політика захисту; угоди про безпеку взаємозв'язку інформаційної системи; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; звіт про оцінку безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління прямими підключеннями до зовнішніх мереж; мережеві адміністратори; організаційний персонал, відповідальний за захист інформації; персонал, що управляє безпосередньо підключеними зовнішніми мережами]  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують управління зовнішніми мережевими з'єднаннями]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CA-3(3) | СИСТЕМНІ ВЗАЄМОДІЇ - НЕСЕКРЕТНІ З’ЄДНАННЯ СИСТЕМИ БЕЗПЕКИ, ЩО НЕ Є НАЦІОНАЛЬНИМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CA-3(3)[1] | організація визначає: | |
| CA-3(3)[1][1] | некласифіковані системи безпеки, яким забороняється безпосереднє підключення до зовнішньої мережі без використання визначених організацією засобів захисту периметру. |
| CA-3(3)[1][2] | ненаціональні системи безпеки, яким забороняється безпосереднє підключення до зовнішньої мережі без використання визначених організацією засобів захисту периметру. |
| CA-3(3)[2] | організація визначає засоби захисту периметру | |
| CA-3(3)[3] | організація забороняє безпосереднє підключення визначеної організацією некласифікованої, ненаціональної системи безпеки до зовнішньої мережі без використання визначених організацією засобів захисту периметру | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика контролю доступу; процедури, що стосуються з'єднань інформаційної системи; системна та комунікаційна політика захисту; угоди про безпеку взаємозв'язку інформаційної системи; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; звіт про оцінку безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: організаційний персонал, відповідальний за управління прямими підключеннями до зовнішніх мереж; мережеві адміністратори; організаційний персонал, відповідальний за захист інформації персонал, що управляє безпосередньо підключеними зовнішніми мережами]  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують управління зовнішніми мережевими з'єднаннями]. | | |

|  |  |  |
| --- | --- | --- |
| CA-3(4) | СИСТЕМНІ ВЗАЄМОДІЇ - ПІДКЛЮЧЕННЯ ДО ЗАГАЛЬНОДОСТУПНИХ МЕРЕЖ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CA-3(4)[1] | організація визначає системи, яким заборонено пряме підключення до загальнодоступної мережі |
| CA-3(4)[2] | організація забороняє пряме підключення визначених організацією систем до загальнодоступної мережі. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика контролю доступу; процедури, що стосуються з'єднань інформаційної системи; системна та комунікаційна політика захисту; угоди про безпеку взаємозв'язку інформаційної системи; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; звіт про оцінку безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми підтримки управління загальнодоступними мережевими підключеннями]. | |

|  |  |  |
| --- | --- | --- |
| CA-3(5) | СИСТЕМНІ ВЗАЄМОДІЇ - ОБМЕЖЕННЯ ЗВ'ЯЗКУ ЗІ ЗОВНІШНІМИ СИСТЕМАМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CA-3(5)[1] | організація визначає системи, яким дозволено підключатися до зовнішніх систем при впровадженні політики «заборони на все», даючи дозвіл за винятком. |
| CA-3(5)[2] | організація впроваджує політику «заборони на все», даючи дозвіл за винятком, щоб дозволити визначеним організацією системам підключатися до зовнішніх систем. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика контролю доступу; процедури, що стосуються з'єднань інформаційної системи; системна та комунікаційна політика захисту; угоди про взаємозв’язок інформаційної системи; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; звіт про оцінку безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління з'єднаннями із зовнішніми інформаційними системами; мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують обмеження на зовнішні підключення до системи]. | |

|  |  |  |
| --- | --- | --- |
| CA-3(6) | ВЗАЄМОДІЇ СИСТЕМ - ВТОРИННІ ТА ТРЕТИННІ ЗВ'ЯЗКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CA-3(6)(a) | визначити вторинні та третинні зв’язки з взаємопов'язаними системами |
| CA-3(6)(b) | вжити заходів для забезпечення розриву зв'язків, коли заходи захисту, що впроваджені на ідентифікованих вторинних та третинних системах не можуть бути перевірені або підтверджені. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика контролю доступу; процедури, що стосуються з'єднань інформаційної системи; системна та комунікаційна політика захисту; угоди про взаємозв’язок інформаційної системи; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; звіт про оцінку безпеки; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління з'єднаннями із зовнішніми інформаційними системами; мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують обмеження на зовнішні підключення до системи]. | |

|  |  |
| --- | --- |
| CA-4 | СЕРТИФІКАЦІЯ БЕЗПЕКИ |
|  | [Вилучено: Включено до CA-2]. |

|  |  |  |  |
| --- | --- | --- | --- |
| CA-5 | ПЛАН ДІЙ ТА КОНТРОЛЬНІ ПОКАЗНИКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CA-5(a) | з метою документування запланованих коригувальних дій організації для усунення недоліків та зауважень, які виявлені у ході оцінювання заходів захисту, а також для зменшення або усунення відомих вразливостей в системі, розробити для системи: | |
| CA-5(a)[1] | план усунення недоліків |
| CA-5(a)[2] | контрольні показники |
| CA-5(b) | CA-5(b)[1] | організація визначає частоту оновлювання чинного плану усунення недоліків та контрольних показників |
| CA-5(b)[2] | організація оновлює чинний план усунення недоліків та контрольні показники з визначеною організацією частотою на основі результатів оцінювання заходів, аналізу наслідків та безперервного моніторингу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури щодо плану дій та віхи; план безпеки; план оцінки безпеки; звіт про оцінку безпеки; докази оцінки безпеки; план дій та віхи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з планом дій та основних етапів розробки та реалізацією обов'язків; відповідальні за розробку та впровадження; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми розробки, впровадження та підтримання плану дій та віхи]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CA-5(1) | ПЛАН ДІЙ ТА КОНТРОЛЬНІ ПОКАЗНИКИ - АВТОМАТИЗАЦІЯ ПІДТРИМКИ ЗАДЛЯ ТОЧНОСТІ ТА ВЖИВАНОСТІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CA-5(1)[1] | впровадити автоматизовані механізми для забезпечення того, щоб план усунення недоліків для системи був: | |
| CA-5(1)[1][1] | точним, |
| CA-5(1)[1][2] | актуальним |
| CA-5(1)[1][3] | доступним |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури щодо плану дій та віхи; проєктна документація інформаційної системи, налаштування конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; план дій та віхи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з планом дій та основних етапів розробки та реалізацією обов'язків; відповідальними за розробку та впровадження; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми розробки, впровадження та підтримки плану дій та віхи]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CA-6 | АВТОРИЗАЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CA-6(a) | Призначити відповідальну за систему та будь-які загальні заходи захисту, успадкованих системою: | |
| CA-6(a){1} | старшого керівника, |
| CA-6(a){2} | менеджера |
| CA-6(a){3} | іншу уповноважену посадову особу |
| CA-6(b) | Переконатися перед початком функціонування системи, що посадова особа: | |
| CA-6(b)[1] | акредитує систему на функціонування за призначенням; |
| CA-6(b)[2] | акредитує загальні заходи захисту, що успадковані системою. |
| CA-6(c) | CA-6(c)[1] | організація визначає частоту з якою оновлюють акредитацію |
| CA-6(c)[2] | організація оновлює акредитацію з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, що стосуються дозволу безпеки; пакет дозволів на безпеку (включаючи план безпеки; звіт про оцінку безпеки; план дій та основні етапи; заява про авторизацію); інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за повноваження щодо безпеки організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що полегшують авторизацію та оновлення безпеки]. | | |

|  |  |  |
| --- | --- | --- |
| CA-6(1) | АКРЕДИТАЦІЯ - СПІЛЬНА АКРЕДИТАЦІЯ - ОДНА І ТА Ж ОРГАНІЗАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CA-6(1)[1] | впровадити спільний процес акредитації для системи, що включає кількох уповноважених посадових осіб однієї організації, що здійснюють акредитацію. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, що стосуються дозволу безпеки; пакет дозволів на безпеку (включаючи план безпеки; звіт про оцінку безпеки; план дій та основні етапи; заява про авторизацію); інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за повноваження щодо безпеки організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що полегшують авторизацію та оновлення безпеки]. | |

|  |  |  |
| --- | --- | --- |
| CA-6(2) | АКРЕДИТАЦІЯ - СПІЛЬНА АКРЕДИТАЦІЯ - РІЗНІ ОРГАНІЗАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CA-6(2)[1] | впровадити спільний процес акредитації для системи, що включає кількох уповноважених посадових осіб з принаймні однією уповноваженою посадовою особою з організації, що є зовнішньою організацією, що здійснює акредитацію. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, що стосуються дозволу безпеки; пакет дозволів на безпеку (включаючи план безпеки; звіт про оцінку безпеки; план дій та основні етапи; заява про авторизацію); інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за повноваження щодо безпеки організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що полегшують авторизацію та оновлення безпеки]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CA-7 | БЕЗПЕРЕРВНИЙ МОНІТОРИНГ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| CA-7[1] | організація розробляє стратегію безперервного моніторингу безпеки та приватності. | | | |
| CA-7[2] | організація впроваджує програму безперервного моніторингу безпеки та приватності, яка включає: | | | |
| CA-7[2](a) | CA-7[2](a)[1] | організація визначає метрики для безперервного моніторингу | |
| CA-7[2](a)[2] | організація встановлює показники безпеки та приватності, які необхідно відстежувати (визначені організацією метрики). | |
| CA-7[2](b) | CA-7[2](b)[1] | організація встановлює частоту для моніторингу | |
| CA-7[2](b)[2] | організація встановлює частоту для безперервної оцінки ефективності заходів захисту; | |
| CA-7[2](c) | поточні оцінки заходів захисту відповідно до стратегії безперервного моніторингу організації | | |
| CA-7[2](d) | постійний моніторинг стану безпеки та приватності відповідно до встановлених організацією метрик та відповідно до стратегії безперервного моніторингу організації | | |
| CA-7[2](e) | співставлення та аналіз інформації, яка пов'язана з безпекою та приватністю, яка була отримана в результаті оцінок та моніторингу безпеки та приватності | | |
| CA-7[2](f) | дії реагування за результатами аналізу інформації, пов'язаної з безпекою та приватністю | | |
| CA-7[2](g) | CA-7[2](g)[1] | CA-7[2](g)[1]{1} | організація визначає персонал, яким повідомляють про статус безпеки та приватності організації та систем |
| CA-7[2](g)[1]{2} | організація визначає ролі, яким повідомляють про статус безпеки та приватності організації та систем |
| CA-7[2](g)[2] | організація визначає частоту з якою повідомляють визначні організацією ролі та персонал про статус безпеки та приватності організації та систем | |
| CA-7[2](g)[3] | повідомлення про статус безпеки та приватності організації та систем визначені організацією персонал або ролі з визначеною організацією частотою | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, спрямовані на постійний моніторинг заходів безпеки інформаційної системи; процедури, спрямовані на управління конфігурацією; план безпеки; звіт про оцінку безпеки; план дій та віхи; записи моніторингу інформаційної системи; записи управління конфігурацією, аналіз впливу на безпеку; звіти про стан; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з постійними обов'язками моніторингу; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Механізми, що здійснюють постійний моніторинг]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CA-7(1) | БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - НЕЗАЛЕЖНА ОЦІНКА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CA-7(1)[1] | CA-7(1)[1]{1} | залучити незалежних експертів з оцінки, щоб постійно спостерігати за заходами захисту в системі. |
| CA-7(1)[1]{2} | залучити групи з оцінки, щоб постійно спостерігати за заходами захисту в системі. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, спрямовані на постійний моніторинг заходів безпеки інформаційної системи; план безпеки; звіт про оцінку безпеки; план дій та віхи; записи моніторингу інформаційної системи; аналізи впливу на безпеку; звіти про стан; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з постійними обов'язками моніторингу; організаційний персонал, відповідальний за інформаційну безпеку]. | | |

|  |  |
| --- | --- |
| CA-7(2) | Безперервний моніторинг - Види оцінок |
|  | [Вилучено: Включено до CA-2] |

|  |  |  |  |
| --- | --- | --- | --- |
| CA-7(3) | БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - АНАЛІЗ ТЕНДЕНЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CA-7(3)[1] | забезпечити моніторинг ризиків, що є невід'ємною частиною стратегії постійного моніторингу, що включає наступне: | |
| CA-7(3)[1](a) | моніторинг ефективності |
| CA-7(3)[1](b) | моніторинг відповідності |
| CA-7(3)[1](c) | моніторинг змін |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Стратегія постійного моніторингу; оцінка безпеки та політика авторизації; процедури, спрямовані на постійний моніторинг заходів безпеки інформаційної системи; план безпеки; звіт про оцінку безпеки; план дій та віхи; записи моніторингу інформаційної системи; аналізи впливу на безпеку; звіти про стан; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з постійними обов'язками моніторингу; організаційний персонал, відповідальний за інформаційну безпеку]. | | |

|  |  |  |
| --- | --- | --- |
| CA-8 | ТЕСТУВАННЯ НА ПРОНИКНЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CA-8[1] | організація визначає частоту з якою проводить тестування на проникнення. |
| CA-8[2] | організація визначає інформаційну систему у якій проводить тестування на проникнення |
| CA-8[3] | організація проводить тестування на проникнення з визначеною організацією частотою у визначеній організацією інформаційній системі. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, спрямовані на тестування на проникнення; план безпеки; план оцінки безпеки; звіт про випробування на проникнення; звіт про оцінку безпеки; докази оцінки безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за оцінку безпеки; організаційний персонал, відповідальний за інформаційну безпеку, системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують тестування на проникнення]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CA-8(1) | ТЕСТУВАННЯ НА ПРОНИКНЕННЯ - НЕЗАЛЕЖНА КОМАНДА АБО АГЕНТ НА ПРОНИКНЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CA-8(1){1} | CA-8(1){1}{1} | залучити незалежного агента проникнення для виконання тесту на проникнення систем |
| CA-8(1){1}{2} | залучити незалежного агента проникнення для виконання тесту на проникнення системних компонентів |
| CA-8(1){2} | CA-8(1){2}{1} | залучити команду проникнення для виконання тесту на проникнення систем |
| CA-8(1){2}{2} | залучити команду проникнення для виконання тесту на проникнення системних компонентів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, спрямовані на тестування на проникнення; план безпеки; план оцінки безпеки; звіт про випробування на проникнення; звіт про оцінку безпеки; докази оцінки безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за оцінку безпеки; організаційний персонал, відповідальний за інформаційну безпеку]. | | |

|  |  |  |
| --- | --- | --- |
| CA-8(2) | ТЕСТУВАННЯ НА ПРОНИКНЕННЯ - ЧЕРВОНА КОМАНДА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CA-8(2)[1] | організація визначає червону команду для імітації спроби супротивників скомпрометувати організаційні системи відповідно до чинних правил взаємодії. |
| CA-8(2)[2] | залучити визначені організацією червону команду, щоб імітувати спроби супротивників скомпрометувати організаційні системи відповідно до чинних правил взаємодії |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, спрямовані на тестування на проникнення; процедури щодо вправ червоної команди; план безпеки; план оцінки безпеки; результати вправ червоної команди; звіт про випробування на проникнення; звіт про оцінку безпеки; правила заручення; докази оцінки безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за оцінку безпеки; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують використання вправ червоної команди]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CA-8(3) | ТЕСТУВАННЯ НА ПРОНИКНЕННЯ - МОЖЛИВОСТІ ПЕРЕВІРКИ НА ПРОНИКНЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CA-8(3)[1] | організація визначає частоту спроби обійти або зламати заходи безпеки, пов'язані з фізичними точками доступу до об'єкта в тестуванні на проникнення | |
| CA-8(3)[2] | спроби обійти або зламати заходи безпеки, пов'язані з фізичними точками доступу до об'єкта при тестуванні на проникнення організація проводить: | |
| CA-8(3)[2]{1} | з попередженням; |
| CA-8(3)[2]{2} | без попередження |
| CA-8(3) | організація впроваджує процес тестування на проникнення, який включає визначену організацією частоту, з попередженням або без попередження, спроби обійти або зламати заходи безпеки, пов'язані з фізичними точками доступу до об'єкта | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Оцінка безпеки та політика авторизації; процедури, спрямовані на тестування на проникнення; процедури щодо вправ червоної команди; план безпеки; план оцінки безпеки; результати вправ червоної команди; звіт про випробування на проникнення; звіт про оцінку безпеки; правила заручення; докази оцінки безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за оцінку безпеки; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують використання вправ червоної команди]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CA-9 | ВНУТРІШНІ СИСТЕМНІ З’ЄДНАННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CA-9(a) | CA-9(a)[1] | CA-9(a){1} | організація визначає системні компоненти які беруть участь у внутрішніх системних з’єднаннях |
| CA-9(a){2} | організація визначає класи компонентів які беруть участь у внутрішніх системних з’єднаннях |
| CA-9(a)[2] | авторизувати внутрішні підключення (системні компоненти або класи компонентів, що організація визначила) до системи. | |
| CA-9(b) | задокументувати, для кожного внутрішнього з’єднання, | | |
| CA-9(b)[1] | характеристики інтерфейсу, | |
| CA-9(b)[2] | вимоги безпеки та приватності, | |
| CA-9(b)[3] | характеру переданої інформації | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика контролю доступу; процедури, що стосуються з'єднань інформаційної системи; системна та комунікаційна політика захисту; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; список компонентів або класів компонентів, дозволених як внутрішні системні з'єднання; звіт про оцінку безпеки; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за розробку, впровадження або дозвіл внутрішніх системних з'єднань; організаційний персонал, відповідальний за інформаційну безпеку]. | | | |

|  |  |  |
| --- | --- | --- |
| CA-9(1) | ВНУТРІШНІ СИСТЕМНІ З’ЄДНАННЯ - ВІДПОВІДНІСТЬ ПЕРЕВІРКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| CA-9(1)[1] | виконує перевірку безпеки та приватності компонентів складової системи до встановлення внутрішнього з'єднання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика контролю доступу; процедури, що стосуються з'єднань інформаційної системи; системна та комунікаційна політика захисту; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; список компонентів або класів компонентів, дозволених як внутрішні системні з'єднання; звіт про оцінку безпеки; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за розробку, впровадження або дозвіл внутрішніх системних з'єднань; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують перевірку відповідності]. | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ CM – УПРАВЛІННЯ КОНФІГУРАЦІЄЮ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CM-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ КОНФІГУРАЦІЄЮ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| CM-1(a) | CM-1(a)[1] | CM-1(a)[1](1) | | | Розробляє та документує політику управління конфігурацією, яка: | | | | | | | | |
| CM-1(a)[1](1)(a) | | Містить: | | | | | | |
| CM-1(a)[1](1)(a)[1] | | | | мету, | | |
| CM-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| CM-1(a)[1](1)(a)[3] | | | | ролі, | | |
| CM-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| CM-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| CM-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| CM-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| CM-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| CM-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| CM-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| CM-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| CM-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| CM-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| CM-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| CM-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| CM-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики управління конфігурацією, а також пов'язаних з ними заходів управління конфігурацією; | | | | | | | | |
| CM-1(a)[2] | CM-1(a)[2]{1} | | | CM-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика управління конфігурацією | | | | | |
| CM-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики управління конфігурацією та пов'язаних з нею заходів захисту політики управління конфігурацією | | | | | |
| CM-1(a)[2]{2} | | | CM-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика управління конфігурацією | | | | | |
| CM-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики управління конфігурацією та пов'язаних з нею заходів захисту політики управління конфігурацією | | | | | |
| CM-1(a)[3] | CM-1(a)[3]{1} | | | CM-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику управління конфігурацією | | | | | | | |
| CM-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| CM-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| CM-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| CM-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| CM-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| CM-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| CM-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| CM-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| CM-1(a)[3](1)(b) | | | Відповідає: | | | | |
| CM-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| CM-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| CM-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| CM-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| CM-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| CM-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| CM-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| CM-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації захисту управління конфігурацією та відповідних заходів управління конфігурацією | | | | | | | |
| CM-1(a)[3]{2} | | | CM-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику захисту управління конфігурацією, яка: | | | | | | | |
| CM-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| CM-1(a)[3]{2}(1)(а)[1] | | мету, | |
| CM-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| CM-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| CM-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| CM-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| CM-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| CM-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| CM-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| CM-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| CM-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| CM-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| CM-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| CM-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| CM-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| CM-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| CM-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики управління конфігурацією та пов'язаних з нею заходів управління конфігурацією | | | | | | | |
| CM-1(b) | CM-1(b)[1] | визначає посадову особу для управління політикою та процедурами управління конфігурацією | | | | | | | | | | | |
| CM-1(b)[2] | призначає посаду для управління політикою та процедурами управління конфігурацією | | | | | | | | | | | |
| CM-1(с) | CM-1(с)[1] | CM-1(с)[1](1) | | CM-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики управління конфігурацією | | | | | | | |
| CM-1(с)[1](1)[2] | | переглядає поточну політику управління конфігурацією з визначеною організацією частотою | | | | | | | |
| CM-1(с)[1](2) | | CM-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур управління конфігурацією | | | | | | | |
| CM-1(с)[1](2)[2] | | переглядає поточні процедури управління конфігурацією з визначеною організацією частотою | | | | | | | |
| CM-1(с)[2] | CM-1(с)[2](1) | | CM-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики управління конфігурацією | | | | | | | |
| CM-1(с)[2](1)[2] | | оновлює поточну політику управління конфігурацією з визначеною організацією частотою | | | | | | | |
| CM-1(с)[2](2) | | CM-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур управління конфігурацією | | | | | | | |
| CM-1(с)[2](2)[2] | | оновлює поточні процедури управління конфігурацією з визначеною організацією частотою | | | | | | | |
| CM-1(d) | переконується, що процедури управління конфігурацією реалізують політику та заходи управління конфігурацією | | | | | | | | | | | | |
| CM-1(e) | CM-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики управління конфігурацією | | | | | | | | | | |
| CM-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики управління конфігурацією | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури управління конфігурацією; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику управління конфігурацією; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CM-2 | БАЗОВА КОНФІГУРАЦІЇ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | |
| CM-2(a) | CM-2(a)[1] | розробити за допомогою заходів конфігурації, поточні базові налаштування системи | | | |
| CM-2(a)[2] | задокументувати за допомогою заходів конфігурації, поточні базові налаштування системи | | | |
| CM-2(a)[3] | підтримувати за допомогою заходів конфігурації, поточні базові налаштування системи | | | |
| CM-2(b) | CM-2(b)[1] | CM-2(b)[1](1) | CM-2(b)[1](1)[1] | організація визначає частоту перегляду базових налаштувань системи | |
| CM-2(b)[1](1)[2] | організація переглядає базові налаштування системи з визначеною частотою | |
| CM-2(b)[1](2) | CM-2(b)[1](2)[1] | організація визначає обставини за яких необхідно переглядати базові налаштування системи | |
| CM-2(b)[1](2)[2] | організація переглядає базові налаштування системи за необхідності внаслідок визначених організацією обставин | |
| CM-2(b)[1](3) | CM-2(b)[1](3){1} | | організація переглядає базові налаштування системи коли встановлені нові компоненти системи |
| CM-2(b)[1](3){2} | | організація переглядає базові налаштування системи коли оновлені компоненти системи |
| CM-2(b)[2] | CM-2(b)[2](1) | CM-2(b)[2](1)[1] | організація визначає частоту оновлення базових налаштувань системи | |
| CM-2(b)[2](1)[2] | організація оновлює базові налаштування системи з визначеною частотою | |
| CM-2(b)[2](2) | CM-2(b)[2](2)[1] | організація визначає обставини за яких необхідно оновлювати базові налаштування системи | |
| CM-2(b)[2](2)[2] | організація оновлює базові налаштування системи за необхідності внаслідок визначених організацією обставин | |
| CM-2(b)[2](3) | CM-2(b)[2](3){1} | | організація оновлює базові налаштування системи коли встановлені нові компоненти системи |
| CM-2(b)[2](3){2} | | організація оновлює базові налаштування системи коли оновлені компоненти системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються базової конфігурації інформаційної системи; план управління конфігурацією; документація архітектури підприємства; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; зміни записів контролю; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління конфігурацією; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління конфігураціями базової лінії; автоматизовані механізми, що підтримують управління конфігурацією базової конфігурації]. | | | | | |

|  |  |
| --- | --- |
| CM-2(1) | БАЗОВА КОНФІГУРАЦІЯ - ПЕРЕГЛЯД ТА ОНОВЛЕННЯ |
|  | [Вилучено: Включено до CM-2]. |

|  |  |  |
| --- | --- | --- |
| CM-2(2) | Базова конфігурація - Автоматизація підтримки задля точності та вживаності | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-2 (2)[1] | використовувати автоматизовані механізми для підтримки найновішої, повної, точної та доступної базової конфігурації системи. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються базової конфігурації інформаційної системи; план управління конфігурацією; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи управління зміною конфігурації; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління конфігурацією; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління конфігураціями базової лінії; автоматизовані механізми, що реалізують підтримку базової конфігурації]. | |

|  |  |  |
| --- | --- | --- |
| CM-2(3) | Базова конфігурація - Зберігання попередніх версій конфігурацій | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-2 (3)[1] | організація визначає попередні версії базових конфігурацій системи необхідні для підтримки відкату |
| CM-2 (3)[2] | зберігати визначені організацією попередні версії базових конфігурацій системи для підтримки відкату |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються базової конфігурації інформаційної системи; план управління конфігурацією; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; копії попередніх версій конфігурації базової лінії; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління конфігурацією; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління конфігураціями базової лінії]. | |

|  |  |
| --- | --- |
| CM-2(4) | БАЗОВА КОНФІГУРАЦІЯ - НЕАВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ |
|  | [Вилучено: Включено до CM-7(4)]. |

|  |  |
| --- | --- |
| CM-2(5) | БАЗОВА КОНФІГУРАЦІЯ - АВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ |
|  | [Вилучено: Включено до CM-7(5)]. |

|  |  |  |
| --- | --- | --- |
| CM-2(6) | БАЗОВА КОНФІГУРАЦІЯ - РОЗРОБКА ТА СЕРЕДОВИЩЕ ТЕСТУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-2(6)[1] | підтримувати базову конфігурацію для розробки системи, які керуються окремо від операційної базової конфігурації. |
| CM-2(6)[2] | підтримувати базову конфігурацію для розробки тестових середовищ, які керуються окремо від операційної базової конфігурації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються базової конфігурації інформаційної системи; план управління конфігурацією; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління конфігурацією; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління конфігураціями базової лінії; автоматизовані механізми, що реалізують окремі базові конфігурації для середовищ розробки, тестування та експлуатації]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CM-2(7) | БАЗОВА КОНФІГУРАЦІЯ - КОНФІГУРАЦІЯ СИСТЕМ ТА КОМПОНЕНТІВ ДЛЯ СФЕР З ВИСОКИМ РИЗИКОМ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CM-2(7)(a) | CM-2(7)(a)[1] | CM-2(7)(a)[1]{1} | організація визначає системи для сфер з високим ризиком |
| CM-2(7)(a)[1]{2} | організація визначає компоненти систем для сфер з високим ризиком |
| CM-2(7)(a)[2] | організація визначає конфігурації для системи та компонентів систем для сфер високого ризику | |
| CM-2(7)(a)[3] | організація видає визначені організацією системи або компоненти систем з визначеними організацією конфігураціями особам, які перебувають у місцях, які організація вважає місцями зі значним ризиком | |
| CM-2(7)(b) | CM-2(7)(b)[1] | організація визначає запобіжні заходи безпеки до компонентів, після поїздок до місць, які організація вважає місцями зі значним ризиком | |
| CM-2(7)(b)[2] | організація застосовує визначені організацією запобіжні заходи безпеки до компонентів, коли особи повертаються з поїздки. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; план управління конфігурацією; процедури, що стосуються базової конфігурації інформаційної системи; процедури щодо встановлення та оновлення компонентів інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи оглядів та оновлень базової лінії конфігурації інформаційної системи; установки або оновлення компонентів інформаційної системи та пов'язані з ними записи; зміни записів контролю; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління конфігурацією; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління конфігураціями базової лінії]. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CM-3 | УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| CM-3(a) | визначити типи змін в системі, які контролюються конфігурацією | | | | |
| CM-3(b) | CM-3(b)[1] | | переглядати запропоновані зміни в конфігурації, контрольовані системою | | |
| CM-3(b)[2] | | зміни, в конфігурації, контрольовані системою, з явним урахуванням аналізу наслідків безпеки: | | |
| CM-3(b)[2]{1} | | схвалити |
| CM-3(b)[2]{2} | | відхилити |
| CM-3(c) | документувати рішення зі зміни конфігурації системи | | | | |
| CM-3(d) | впровадити схвалені зміни конфігурації в систему | | | | |
| CM-3(e) | CM-3(e)[1] | організація визначає певний період часу за який необхідно зберігати зміни конфігурації системи | | | |
| CM-3(e)[2] | зберігати записи змін конфігурації системі впродовж певного періоду часу визначеного організацією | | | |
| CM-3(f) | CM-3(f)[1] | здійснювати моніторинг дій, пов'язаних зі змінами конфігурації системи; | | | |
| CM-3(f)[2] | здійснювати аналіз дій, пов'язаних зі змінами конфігурації системи; | | | |
| CM-3(g) | CM-3(g)[1] | організація визначає елемент управління змінами конфігурації | | | |
| CM-3(g)[2] | організація визначає частоту виклику елементу управління змінами конфігурації | | | |
| CM-3(g)[3] | організація визначає умови зміни конфігурації за яких викликається елемент управління змінами конфігурації | | | |
| CM-3(g)[4] | координувати нагляд за діяльністю з управління змінами конфігурації за допомогою елементу управління змінами конфігурації, визначеного організацією, який викликається (виберіть один або кілька з наступного): | | | |
| CM-3(g)[4][1] | | | з визначеною організацією частотою |
| CM-3(g)[4][2] | | | за визначеними організацією умовами зміни конфігурації. |
| CM-3(g)[5] | впроваджувати нагляд за діяльністю з управління змінами конфігурації за допомогою елементу управління змінами конфігурації, визначеного організацією, який викликається (віберіть один або кілька з наступного): | | | |
| CM-3(g)[5][1] | | з визначеною організацією частотою | |
| CM-3(g)[5][2] | | за визначеними організацією умовами зміни конфігурації. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на управління зміною конфігурації інформаційної системи; план управління конфігурацією; документація архітектури та конфігурація інформаційної системи; план безпеки; зміни записів контролю; записи аудиту інформаційної системи; звіти про контроль аудиту та перегляд змін; порядок денний або хвилини з нарад з контролю за зміною конфігурації; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління зміною конфігурації; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; члени ради управління змінами чи подібні].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління зміною конфігурації; автоматизовані механізми, що реалізують контроль зміни конфігурації]. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CM-3(1) | УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - АВТОМАТИЗОВАНЕ ДОКУМЕНТУВАННЯ, ПОВІДОМЛЕННЯ ТА ЗАБОРОНА ВНЕСЕННЯ ЗМІН | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| CM-3(1)[1] | організація впроваджує автоматизовані механізми для: | | | |
| CM-3(1)[1](a) | документування запропонованих змін в системі | | |
| CM-3(1)[1](b) | CM-3(1)[1](b)[1] | | організація визначає затверджуючі органи влади. |
| CM-3(1)[1](b)[2] | | повідомлення визначених організацією органів влади, що затверджують, про запропоновані зміни в системі та схвалення запитів змін. |
| CM-3(1)[1](c) | CM-3(1)[1](c)[1] | | організація визначає період часу за який можливо виділити запропонованих змін в системі, які не були схвалені або відхилені |
| CM-3(1)[1](c)[2] | | виділення запропонованих змін в системі, які не були схвалені або відхилені за визначений організацією період часу |
| CM-3(1)[1](d) | заборони внесення змін до системи, доки не будуть отримані погодження | | |
| CM-3(1)[1](e) | документування всіх змін в системі. | | |
| CM-3(1)[1](f) | CM-3(1)[1](f)[1] | організація визначає персонал, який слід сповіщати, коли завершено затверджені зміни в системі. | |
| CM-3(1)[1](f)[2] | повідомлення визначеного організацією персоналу, коли завершено затверджені зміни в системі | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на управління зміною конфігурації інформаційної системи; план управління конфігурацією; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; автоматизовані механізми управління конфігурацією; налаштування конфігурації інформаційної системи та супутня документація; зміни записів контролю; записи аудиту інформаційної системи; зміни запитів на затвердження; зміни затверджень; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління зміною конфігурації; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління зміною конфігурації; автоматизовані механізми, що реалізують керування зміною конфігурації]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-3(2) | УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - ТЕСТУВАННЯ, ВАЛІДАЦІЯ ТА ДОКУМЕНТУВАННЯ ЗМІН | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-3(2)[1] | зміни у системі до повної їх реалізації необхідно: | |
| CM-3(2)[1][1] | тестувати, |
| CM-3(2)[1][2] | перевіряти |
| CM-3(2)[1][3] | документувати |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; план управління конфігурацією; процедури, спрямовані на управління зміною конфігурації інформаційної системи; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; тестові записи; валідаційні записи; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління зміною конфігурації; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління зміною конфігурації; автоматизовані механізми підтримки та / або впровадження тестування, перевірки та документування змін інформаційної системи]. | | |

|  |  |  |
| --- | --- | --- |
| CM-3(3) | УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - АВТОМАТИЗОВАНА РЕАЛІЗАЦІЯ ЗМІН | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-3(3)[1] | організація використовує автоматизовані механізми для реалізації змін до поточної базової конфігурації системи |
| CM-3(3)[2] | організація розгортає оновлені базові конфігурації через встановлену базу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; план управління конфігурацією; процедури, спрямовані на управління зміною конфігурації інформаційної системи; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; автоматизовані механізми управління конфігурацією; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління зміною конфігурації; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління зміною конфігурації; автоматизовані механізми впровадження змін до поточної базової інформаційної системи]. | |

|  |  |  |
| --- | --- | --- |
| CM-3(4) | УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - ПРЕДСТАВНИК БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-3(4)[1] | організація визначає представника з інформаційної безпеки |
| CM-3(4)[2] | організація визначає елемент керування зміною конфігурацій |
| CM-3(4)[3] | організація вимагає від визначеного організацією представника з інформаційної безпеки бути членом визначеного організацією елементу керування зміною конфігурацій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на управління зміною конфігурації інформаційної системи; план управління конфігурацією; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління зміною конфігурації; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління зміною конфігурації]. | |

|  |  |  |
| --- | --- | --- |
| CM-3(5) | УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - АВТОМАТИЧНЕ РЕАГУВАННЯ БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-3(5)[1] | організація визначає реагування безпеки, якщо базова конфігурація системи змінюється несанкціонованим чином |
| CM-3(5)[2] | організація реалізує автоматично визначені організацією реагування безпеки, якщо базова конфігурація системи змінюється несанкціонованим чином |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на управління зміною конфігурації інформаційної системи; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; попередження або сповіщення про несанкціоновані зміни базової конфігурації; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління зміною конфігурації; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління зміною конфігурації; автоматизовані механізми, що реалізують відповіді безпеки на зміни в базових конфігураціях]. | |

|  |  |  |
| --- | --- | --- |
| CM-3(6) | УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - УПРАВЛІННЯ КРИПТОГРАФІЄЮ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-3(6)[1] | організація визначає заходи безпеки. |
| CM-3(6)[2] | організація забезпечує, щоб криптографічні механізми, які використовуються для надання визначених організацією заходів безпеки, знаходяться під управлінням конфігурацією. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на управління зміною конфігурації інформаційної системи; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління зміною конфігурації; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління зміною конфігурації; криптографічні механізми, що реалізують організаційні гарантії безпеки]. | |

|  |  |  |
| --- | --- | --- |
| CM-4 | АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-4[1] | аналізувати зміни в системі, щоб визначити потенційну загрозу безпеці та приватності перед реалізацією змін |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на аналіз впливу на безпеку щодо змін в інформаційній системі; план управління конфігурацією; документація щодо аналізу впливу на безпеку; інструменти аналізу та пов'язані з ними результати; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аналіз впливу на безпеку; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси для аналізу впливу на безпеку]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-4(1) | АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ - ОКРЕМІ ВИПРОБУВАЛЬНІ СЕРЕДОВИЩА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-4(1)[1] | проаналізувати зміни в системі в окремому тестовому середовищі до впровадження змін в операційному середовищі, | |
| CM-4(1)[2] | шукати вплив на безпеку та приватність через | |
| CM-4(1)[2][1] | недоліки, |
| CM-4(1)[2][2] | слабкості, |
| CM-4(1)[2][3] | несумісність |
| CM-4(1)[2][4] | навмисне спричинення шкоди |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на аналіз впливу на безпеку щодо змін в інформаційній системі; план управління конфігурацією; документація щодо аналізу впливу на безпеку; інструменти аналізу та пов'язані з ними виходи на проєктну документацію інформаційної системи; документація архітектури та конфігурація інформаційної системи; зміни записів контролю; записи аудиту інформаційної системи; документальне підтвердження окремих випробувальних та експлуатаційних середовищ; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аналіз впливу на безпеку; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси для аналізу впливу на безпеку; автоматизовані механізми, що підтримують та / або здійснюють аналіз впливу змін на безпеку]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-4(2) | АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ - ВЕРИФІКАЦІЯ ФУНКЦІЙ БЕЗПЕКИ ТА ПРИВАТНОСТІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-4(2)[1] | Перевірити функції безпеки та приватності після системних змін, щоб переконатися, що функції: | |
| CM-4(2)[1] | впроваджені правильно, |
| CM-4(2)[2] | працюють за призначенням |
| CM-4(2)[3] | виробляють бажаний результат зі задоволення вимог безпеки та приватності для системи. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на аналіз впливу на безпеку щодо змін в інформаційній системі; план управління конфігурацією; документація щодо аналізу впливу на безпеку; інструменти аналізу та пов'язані з ними результати; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аналіз впливу на безпеку; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси для аналізу впливу на безпеку; автоматизовані механізми, що підтримують та / або реалізують перевірку функцій безпеки]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-5 | ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-5[1] | застосування фізичних обмежень доступу, пов'язаних зі змінами в системі, організація: | |
| CM-5[1][1] | визначає, |
| CM-5[1][2] | задокументовує, |
| CM-5[1][3] | затверджує |
| CM-5[1][4] | забезпечує. |
| CM-5[2] | застосування логічних обмежень доступу, пов'язаних зі змінами в системі, організація: | |
| CM-5[2][1] | визначає, |
| CM-5[2][2] | задокументовує, |
| CM-5[2][3] | затверджує |
| CM-5[2][4] | забезпечує. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до інформаційної системи; план управління конфігурацією; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; логічні схвалення доступу; затвердження фізичного доступу; доступ до облікових даних; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з логічними обов'язками контролю доступу; організаційний персонал з обов'язками фізичного контролю доступу; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління обмеженнями доступу для зміни; автоматизовані механізми підтримки / реалізації / забезпечення обмежень доступу, пов'язаних зі змінами в інформаційній системі]. | | |

|  |  |  |
| --- | --- | --- |
| CM-5(1) | ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - АУДИТ ТА ЗДІЙСНЕННЯ АВТОМАТИЧНОГО ДОСТУПУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-5(a) | організація здійснює обмеження доступу |
| CM-5(b) | організація генерує записи аудиторських перевірок виконаних дій. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до інформаційної системи; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління обмеженнями доступу для зміни; автоматизовані механізми, що здійснюють виконання обмежень доступу для змін до інформаційної системи; автоматизовані механізми, що підтримують аудит дій з примусового виконання]. | |

|  |  |  |
| --- | --- | --- |
| CM-5(2) | ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ПЕРЕГЛЯД ЗМІН В СИСТЕМІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-5(2)[1] | організація визначає частоту перегляду змін у системі |
| CM-5(2)[2] | організація визначає обставини за яких переглядають зміни в системі |
| CM-5(2)[3] | організація переглядає зміни в системі з частотою, визначеною організацією та при обставинах, визначених організацією, щоб визначити, чи відбулися неавторизовані зміни |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до інформаційної системи; план управління конфігурацією; план безпеки; огляди змін інформаційної системи; аудиторські та оглядові звіти; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за безпеку інформації; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління обмеженнями доступу для зміни; автоматизовані механізми, що підтримують / впроваджують огляд інформаційної системи, щоб визначити, чи відбулися несанкціоновані зміни]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-5(3) | ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ПІДПИСАНІ КОМПОНЕНТИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-5(3)[1] | CM-5(3)[1][1] | організація визначає програмні компоненти, які слід перевіряти на наявність цифрового підпису з використанням сертифіката, який визнається та схвалений організацією. |
| CM-5(3)[1][2] | організація визначає компоненти мікропрограм, які слід перевіряти на наявність цифрового підпису з використанням сертифіката, який визнається та схвалений організацією. |
| CM-5(3)[2] | без перевірки того, що компонент був підписаний цифровим підписом з використанням сертифіката, який визнається та схвалений організацією, запобігати встановленню: | |
| CM-5(3)[2][1] | визначених організацією програмних компонент, |
| CM-5(3)[2][2] | визначених організацією компонент мікропрограм. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до інформаційної системи; план управління конфігурацією; план безпеки; перелік компонентів програмного забезпечення та мікропрограмного забезпечення, які забороняються встановлювати без визнаного та затвердженого сертифіката; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за безпеку інформації; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління обмеженнями доступу для зміни; автоматизовані механізми, що перешкоджають встановленню компонентів програмного забезпечення та мікропрограмного забезпечення, не підписаних сертифікатом, визнаним та затвердженим організацією]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-5(4) | ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ПОДВІЙНА АВТОРИЗАЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-5(4)[1] | CM-5(4)[1][2] | організація визначає системні компоненти, щодо яких здійснюється подвійна авторизація за необхідності внесення до них змін. |
| CM-5(4)[1][2] | організація визначає інформацію на рівні системи, щодо яких здійснюється подвійна авторизація за необхідності внесення до них змін. |
| CM-5(4)[2] | організація здійснює подвійну авторизацію для внесення змін до системних компонентів та інформації на рівні системи, визначених організацією. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до інформаційної системи; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з подвійними обов'язками щодо виконання дозволу на впровадження змін інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління обмеженнями доступу для зміни; автоматизовані механізми, що реалізують подвійне виконання авторизації]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CM-5(5) | ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ОБМЕЖЕННЯ ПОВНОВАЖЕНЬ ДЛЯ ВИРОБНИЦТВА ТА ЕКСПЛУАТАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CM-5(5)(a) | CM-5(5)(a)[1] | обмежити повноваження для зміни компонентів системи у: | |
| CM-5(5)(a)[1]{1} | виробничому середовищі |
| CM-5(5)(a)[1]{2} | операційному середовищі |
| CM-5(5)(a)[2] | обмежити повноваження для зміни інформації, пов'язаної з системою, у: | |
| CM-5(5)(a)[2]{1} | виробничому середовищі |
| CM-5(5)(a)[2]{2} | операційному середовищі |
| CM-5(5)(b) | CM-5(5)(b)[1] | організація визначає частоту з якою необхідно переглядати повноваження | |
| CM-5(5)(b)[2] | організація визначає частоту з якою необхідно переоцінювати повноваження | |
| CM-5(5)(b)[3] | організація переглядає повноваження з визначеною організацією частотою | |
| CM-5(5)(b)[4] | організація переоцінює повноваження визначеною організацією з частотою | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до інформаційної системи; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; огляди привілеїв користувачів; повторне підтвердження прав користувачів; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за безпеку інформації; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління обмеженнями доступу для зміни; автоматизовані механізми, що підтримують та / або реалізують обмеження доступу для змін]. | | | |

|  |  |  |
| --- | --- | --- |
| CM-5(6) | ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ОБМЕЖЕННЯ ПОВНОВАЖЕНЬ ДЛЯ БІБЛІОТЕК | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-5(6)[1] | обмежити повноваження для зміни програмного забезпечення, яке перебуває в бібліотеках програмного забезпечення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до інформаційної системи; план управління конфігурацією; проєктна документація інформаційної системи; документація архітектури та конфігурація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за безпеку інформації; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління обмеженнями доступу для зміни; автоматизовані механізми, що підтримують та / або реалізують обмеження доступу для змін]. | |

|  |  |
| --- | --- |
| CM-5(7) | ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - АВТОМАТИЧНЕ ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ |
|  | [Вилучено: включено до SI-7]. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CM-6 | НАЛАШТУВАННЯ КОНФІГУРАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CM-6(a) | CM-6(a)[1] | організація встановлює загальні безпечні конфігурації | |
| CM-6(a)[2] | встановити та задокументувати параметри конфігурації компонентів, які застосовуються в системі, використовуючи визначені організацією загальні безпечні конфігурації, які відображають найбільш обмежений режим, який відповідає операційним вимогам | |
| CM-6(b) | організація реалізує конфігураційні установки. | | |
| CM-6(c) | CM-6(c)[1] | організація визначає компонентів системи, які стосуються конфігураційних параметрів | |
| CM-6(c)[2] | організація визначає оперативні вимоги, які стосуються конфігураційних параметрів | |
| CM-6(c)[3] | будь-які відхилення від встановлених конфігураційних параметрів для визначених організацією компонентів системи на основі визначених організацією оперативних вимог мають бути: | |
| CM-6(c)[3][1] | визначені, |
| CM-6(c)[3][2] | задокументовані |
| CM-6(c)[3][3] | затверджені |
| CM-6(d) | CM-6(d)[1] | відстежувати та керувати змінами конфігураційних параметрів відповідно до організаційної політики | |
| CM-6(d)[2] | відстежувати та керувати змінами конфігураційних параметрів відповідно до організаційної процедур | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на налаштування конфігурації інформаційної системи; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; контрольні списки налаштувань безпеки; докази, що підтверджують затверджені відхилення від встановлених параметрів конфігурації; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління конфігурацією безпеки; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління налаштуваннями конфігурації; автоматизовані механізми, що реалізують, контролюють та / або керують налаштуваннями конфігурації інформаційної системи; автоматизовані механізми, що ідентифікують та / або документують відхилення від встановлених параметрів конфігурації]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-6(1) | НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - АВТОМАТИЗОВАНЕ УПРАВЛІННЯ, ЗАСТОСУВАННЯ ТА ВЕРИФІКАЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-6(1)[1] | організація визначає системні компоненти | |
| CM-6(1)[2] | використовувати автоматизовані механізми для: | |
| CM-6(1)[2][1] | централізованого керування параметрів конфігурації для визначених організацією системних компонентів |
| CM-6(1)[2][2] | застосування параметрів конфігурації для визначених організацією системних компонентів |
| CM-6(1)[2][3] | перевірки параметрів конфігурації для визначених організацією системних компонентів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на налаштування конфігурації інформаційної системи; план управління конфігурацією; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; контрольні списки налаштувань безпеки; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління конфігурацією безпеки; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Організаційні процеси управління налаштуваннями конфігурації; автоматизовані механізми, реалізовані для централізованого управління, застосування та перевірки параметрів конфігурації інформаційної системи]. | | |

|  |  |  |
| --- | --- | --- |
| CM-6(2) | НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - РЕАГУВАННЯ НА НЕСАНКЦІОНОВАНІ ЗМІНИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-6(2)[1] | організація визначає заходи захисту для реагування на несанкціоновані зміни |
| CM-6(2)[2] | організація визначає налаштування, до яких мають застосовуватись заходи захисту для реагування на несанкціоновані зміни. |
| CM-6(2)[3] | організація використовує визначені організацією заходи захисту для реагування на несанкціоновані зміни налаштувань, визначених організацією. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на налаштування конфігурації інформаційної системи; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; попередження або сповіщення про несанкціоновані зміни в налаштуваннях конфігурації інформаційної системи; задокументовані відповіді на несанкціоновані зміни в налаштуваннях конфігурації інформаційної системи; зміни записів заходів; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління конфігурацією безпеки; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційний процес реагування на несанкціоновані зміни в налаштуваннях конфігурації інформаційної системи; автоматизовані механізми, що підтримують та / або реалізують гарантії безпеки для реагування на несанкціоновані зміни]. | |

|  |  |
| --- | --- |
| CM-6(3) | НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ ЗМІН |
|  | [Вилучено: Включено до SI-7] |

|  |  |
| --- | --- |
| CM-6(4) | НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - ДЕМОНСТРАЦІЯ ВІДПОВІДНОСТІ |
|  | [Вилучено: Включено до CM-4] |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CM-7 | МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CM-7(a) | налаштована система на надання лише найважливіших функцій | | |
| CM-7(b) | CM-7(b){1} | заборонити використання визначених організацією (один або кілька): | |
| CM-7(b){1}{1} | функцій, |
| CM-7(b){1}{2} | портів, |
| CM-7(b){1}{3} | протоколів |
| CM-7(b){1}{4} | служб |
| CM-7(b){2} | обмежити використання визначених організацією (один або кілька): | |
| CM-7(b){2}{1} | функцій, |
| CM-7(b){2}{2} | портів, |
| CM-7(b){2}{3} | протоколів |
| CM-7(b){2}{4} | служб |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; план управління конфігурацією; процедури, що стосуються найменшої функціональності в інформаційній системі; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; контрольні списки налаштувань безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками управління конфігурацією безпеки; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси, що забороняють або обмежують функції, порти, протоколи та / або послуги; автоматизовані механізми, що реалізують обмеження або заборону функцій, портів, протоколів та / або послуг]. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CM-7(1) | МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ПЕРІОДИЧНИЙ ПЕРЕГЛЯД | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| CM-7(а) | CM-7(а)[1] | організація визначає частоту з якою проводять перегляд системи | | |
| CM-7(а)[2] | CM-7(а)[2]{1} | проводити перегляд системи з визначеною організацією частотою для виявлення непотрібних (один або кілька): | |
| CM-7(а)[2]{1}[1] | функцій, |
| CM-7(а)[2]{1}[2] | портів, |
| CM-7(а)[2]{1}[3] | протоколів та |
| CM-7(а)[2]{1}[4] | послуг |
| CM-7(а)[2]{2} | проводити перегляд системи з визначеною організацією частотою для виявлення незахищених (один або кілька): | |
| CM-7(а)[2]{2}[1] | функцій, |
| CM-7(а)[2]{2}[2] | портів, |
| CM-7(а)[2]{2}[3] | протоколів та |
| CM-7(а)[2]{2}[4] | послуг |
| CM-7(b) | CM-7(b)[1] | CM-7(b)[1]{1} | організація визначає які в системі вважаються непотрібними: | |
| CM-7(b)[1]{1}[1] | функції, |
| CM-7(b)[1]{1}[2] | порти, |
| CM-7(b)[1]{1}[3] | протоколи |
| CM-7(b)[1]{1}[4] | послуги |
| CM-7(b)[1]{2} | організація визначає які в системі вважаються незахищеними: | |
| CM-7(b)[1]{2}[1] | функції, |
| CM-7(b)[1]{2}[2] | порти, |
| CM-7(b)[1]{2}[3] | протоколи |
| CM-7(b)[1]{2}[4] | послуги |
| CM-7(b)[2] | в системі, ті, що вважаються непотрібними та / або незахищеними, організація вимикає: | | |
| CM-7(b)[2][1] | функції, | |
| CM-7(b)[2][2] | порти, | |
| CM-7(b)[2][3] | протоколи | |
| CM-7(b)[2][4] | послуги | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються найменшої функціональності в інформаційній системі; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; контрольні списки налаштувань безпеки; задокументовані огляди функцій, портів, протоколів та / або послуг; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за перегляд функцій, портів, протоколів та служб інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси огляду або відключення незахищених функцій, портів, протоколів та / або послуг; автоматизовані механізми, що реалізують огляд та відключення незахищених функцій, портів, протоколів та / або послуг]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-7(2) | МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ЗАБОРОНА ВИКОНАННЯ ПРОГРАМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-7(2)[1] | організація визначає політики щодо використання програмних програм та обмежень | |
| CM-7(2)[2] | організація визначає правила, що встановлюють терміни та умови використання програмного забезпечення | |
| CM-7(2)[3] | заборонити виконання програми відповідно до (одного або декількох): | |
| CM-7(2)[3]{1} | визначеної організацією політики щодо використання програмних програм та обмежень; |
| CM-7(2)[3]{2} | правил, що встановлюють терміни та умови використання програмного забезпечення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються найменшої функціональності в інформаційній системі; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; специфікації щодо запобігання виконанню програм; налаштування конфігурації інформаційної системи та супутня документація; зміни записів заходів; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за безпеку інформації; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Організаційні процеси, що перешкоджають виконанню програми в інформаційній системі; організаційні процеси використання програмного забезпечення та обмеження; автоматизовані механізми, що запобігають виконанню програми в інформаційній системі; автоматизовані механізми, що підтримують та / або реалізують використання та обмеження програм]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-7(3) | МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ВІДПОВІДНІСТЬ РЕЄСТРАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-7(3)[1] | організація визначає вимоги до реєстрації для: | |
| CM-7(3)[1][1] | функцій, |
| CM-7(3)[1][2] | портів, |
| CM-7(3)[1][3] | протоколів |
| CM-7(3)[1][4] | послуг |
| CM-7(3)[2] | організація забезпечує відповідність визначеним організацією вимогам до реєстрації для: | |
| CM-7(3)[2][1] | функцій, |
| CM-7(3)[2][2] | портів, |
| CM-7(3)[2][3] | протоколів |
| CM-7(3)[2][4] | послуг |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються найменшої функціональності в інформаційній системі; план управління конфігурацією; план безпеки; налаштування конфігурації інформаційної системи та супутня документація; аудиторські перевірки та дотримання відповідності; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за безпеку інформації; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси, що забезпечують відповідність вимогам реєстрації для функцій, портів, протоколів та / або послуг; автоматизовані механізми, що реалізують відповідність вимогам реєстрації для функцій, портів, протоколів та / або послуг]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-7(4) | МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - НЕАВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - ЧОРНИЙ СПИСОК | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-7(4)(a) | організація визначає програмне забезпечення, що не має дозволу виконуватися в системі | |
| CM-7(4)(b) | CM-7(4)(b)[1] | організація визначає політику «дозволу всього, за винятком деяких» для заборони виконання неавторизованих програм у системі |
| CM-7(4)(b)[2] | організація впроваджує політику «дозволу всього, за винятком деяких» для заборони виконання неавторизованих програм у системі |
| CM-7(4)(c) | CM-7(4)(c)[1] | організація визначає частоту, з якою необхідно переглядати список неавторизованих програм |
| CM-7(4)(c)[2] | організація визначає частоту, з якою необхідно оновлювати список неавторизованих програм |
| CM-7(4)(c)[3] | організація переглядає список неавторизованих програм з визначеною організацією частотою |
| CM-7(4)(c)[4] | організація оновлює список неавторизованих програм з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються найменшої функціональності в інформаційній системі; план управління конфігурацією; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік програм, які не мають права виконувати в інформаційній системі; контрольні списки налаштувань безпеки; перегляд та оновлення записів, пов’язаних зі списком програм, що не мають дозволу; зміни записів заходів; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за виявлення програмного забезпечення, яке не має права виконуватися в інформаційній системі; організаційний персонал, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційний процес ідентифікації, перегляду та оновлення програм, які не мають права виконуватися в інформаційній системі; організаційний процес реалізації чорного списку; автоматизовані механізми підтримки та / або впровадження чорного списку]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-7(5) | МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - АВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ – БІЛИЙ СПИСОК | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-7(5)(а) | організація визначає програмне забезпечення, яке авторизоване виконуватися в систем | |
| CM-7(5)(b) | CM-7(5)(b)[1] | організація визначає політику «заборони всього, за винятком деяких», щоб дозволити виконання авторизованих програм в системі |
| CM-7(5)(b)[2] | організація впроваджує політику «заборони всього, за винятком деяких», щоб дозволити виконання авторизованих програм в системі |
| CM-7(5)(c) | CM-7(5)(c)[1] | організація визначає частоту, з якою необхідно переглядати список авторизованих програм |
| CM-7(5)(c)[2] | організація визначає частоту, з якою необхідно оновлювати список авторизованих програм |
| CM-7(5)(c)[3] | організація переглядає список авторизованих програм з визначеною організацією частотою |
| CM-7(5)(c)[4] | організація оновлює список авторизованих програм з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються найменшої функціональності в інформаційній системі; план управління конфігурацією; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік програм, дозволених до виконання в інформаційній системі; контрольні списки налаштувань безпеки; перегляд та оновлення записів, пов’язаних із переліком авторизованих програм; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за визначення програмного забезпечення, дозволеного до виконання в інформаційній системі; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційний процес ідентифікації, перегляду та оновлення програм, дозволених до виконання в інформаційній системі; організаційний процес реалізації білого списку; автоматизовані механізми, що реалізують білий список]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CM-8 | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CM-8(a) | організація розробляє та задокументовує процес інвентаризації компонентів системи, якій: | | |
| CM-8(a)(1) | точно описує поточну систему | |
| CM-8(a)(2) | включає всі компоненти в межах акредитації системи | |
| CM-8(a)(3) | визначає рівень деталізації, яка вважається необхідною для відстеження та звітування | |
| CM-8(a)(4) | CM-8(a)(4)[1] | організація визначає інформацію, яка вважається необхідною для досягнення ефективної підзвітності компоненту системи |
| CM-8(a)(4)[2] | включає інформацію, яка вважається необхідною для досягнення ефективної підзвітності компоненту системи |
| CM-8(b) | CM-8(b)[1] | організація визначає частоту, з якою необхідно переглядати опис компонентів системи | |
| CM-8(b)[2] | організація визначає частоту, з якою необхідно оновлювати опис компонентів системи | |
| CM-8(b)[3] | організація переглядає опис компонентів системи з визначеною організацією частотою | |
| CM-8(b)[4] | організація оновлює опис компонентів системи з визначеною організацією частотою | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; план управління конфігурацією; план безпеки; записи інвентаризації інформаційної системи; огляди запасів та оновлення записів; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інвентаризацію компонентів інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси розробки та документування інвентаризації компонентів інформаційної системи; автоматизовані механізми, що підтримують та / або реалізують інвентаризацію компонентів інформаційної системи]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-8(1) | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ - ОНОВЛЕННЯ ПІД ЧАС ВСТАНОВЛЕННЯ ТА ВИДАЛЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-8(1)[1] | організація оновлює інвентарний опис компонентів системи як складової частини процесу | |
| CM-8(1)[1][1] | інсталяції компонентів системи |
| CM-8(1)[1][2] | видалення компонентів системи |
| CM-8(1)[1][3] | оновлення компонентів системи. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; план управління конфігурацією; план безпеки; записи інвентаризації інформаційної системи; огляди запасів та оновлення записів; записи про встановлення компонентів; записи про видалення компонентів; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за оновлення інвентаризації компонентів інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси оновлення опису компонентів інформаційної системи; автоматизовані механізми, що реалізують оновлення інвентаризації компонентів інформаційної системи]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-8(2) | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ - АВТОМАТИЗОВАНА ПІДТРИМКА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-8(2)[1] | організація впроваджує автоматизовані механізми, які допоможуть підтримувати: | |
| CM-8(2)[1][1] | актуальний опис компонентів системи |
| CM-8(2)[1][2] | повний опис компонентів системи |
| CM-8(2)[1][3] | точний опис компонентів системи |
| CM-8(2)[1][4] | легко доступний опис компонентів системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; план управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи інвентаризації інформаційної системи; зміни записів контролю; записи технічного обслуговування інформаційних систем; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління автоматизованими механізмами, що реалізують інвентаризацію компонентів інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Організаційні процеси ведення інвентаризації компонентів інформаційної системи; автоматизовані механізми реалізації інвентаризації компонентів інформаційної системи]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CM-8(3) | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ - АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ КОМПОНЕНТІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CM-8(3)(a) | CM-8(3)(a)[1] | організація визначає частоту з якою необхідно впроваджувати автоматизовані механізми | |
| CM-8(3)(a)[2] | організація визначає частоту з якою необхідно використовувати автоматизовані механізми | |
| CM-8(3)(a)[3] | впровадити автоматизовані механізми з визначеною організацією частотою для виявлення наявності в системі: | |
| CM-8(3)(a)[3][1] | неавторизованих апаратних засобів, |
| CM-8(3)(a)[3][2] | програмного забезпечення |
| CM-8(3)(a)[3][3] | компонентів прошивки |
| CM-8(3)(a)[4] | використовувати автоматизовані механізми з визначеною організацією частотою для виявлення наявності в системі: | |
| CM-8(3)(a)[4][1] | неавторизованих апаратних засобів, |
| CM-8(3)(a)[4][2] | програмного забезпечення |
| CM-8(3)(a)[4][3] | компонентів прошивки |
| CM-8(3)(b) | CM-8(3)(b)[1] | CM-8(3)(b)[1]{1} | організація визначає персонал, який слід повідомляти при виявленні неавторизованих компонентів |
| CM-8(3)(b)[1]{2} | організація визначає посади, який слід повідомляти при виявленні неавторизованих компонентів |
| CM-8(3)(b)[2] | при виявленні неавторизованих компонентів виконувати наступні дії (один або кілька): | |
| CM-8(3)(b)[2]{1} | відключення доступу до мережі такими компонентами; |
| CM-8(3)(b)[2]{2} | ізолювати компоненти |
| CM-8(3)(b)[2]{3} | повідомити визначені організацією персонал або посади |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи інвентаризації інформаційної системи; оповіщення або сповіщення про несанкціоновані компоненти в інформаційній системі; записи моніторингу інформаційної системи; зміни записів контролю; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління автоматизованими механізмами, що реалізують виявлення несанкціонованих компонентів інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Організаційні процеси виявлення несанкціонованих компонентів інформаційної системи; автоматизовані механізми, що реалізують виявлення несанкціонованих компонентів інформаційної системи]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CM-8(4) | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ - ІНФОРМАЦІЯ ПРО ПІДЗВІТНІСТЬ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CM-8(4)[1] | включити в інвентаризаційну інформацію: | | |
| CM-8(4)[1][1] | компоненту системи, | |
| CM-8(4)[1][2] | засіб для ідентифікації осіб, відповідальних та підзвітних за управління цими компонентами за (один або більше): | |
| CM-8(4)[1][2]{1} | ім'ям; |
| CM-8(4)[1][2]{2} | позицією; |
| CM-8(4)[1][2]{3} | роллю |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; план управління конфігурацією; план безпеки; записи інвентаризації інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління запасами компонентів інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; системні або мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси ведення інвентаризації компонентів інформаційної системи; автоматизовані механізми реалізації інвентаризації компонентів інформаційної системи]. | | | |

|  |  |  |
| --- | --- | --- |
| CM-8(5) | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ - ВИКЛЮЧЕННЯ ДУБЛЮВАННЯ КОМПОНЕНТІВ ОБЛІКУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-8(5)(a) | перевірити, що всі компоненти в межах авторизації системи не дублюються в інших інвентарних описах системних компонентів |
| CM-8(5)(b) | якщо використовується централізована інвентаризація компонентів, перевірити, що компоненти не призначені для декількох систем |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; план управління конфігурацією; план безпеки; записи інвентаризації інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інвентаризацію інформаційної системи; організаційний персонал, відповідальний за визначення компонентів інформаційної системи в межах дозволу системи; організаційний персонал з обов'язками інформаційної безпеки; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси ведення інвентаризації компонентів інформаційної системи; автоматизовані механізми реалізації інвентаризації компонентів інформаційної системи]. | |

|  |  |  |
| --- | --- | --- |
| CM-8(6) | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ - ОЦІНЮВАНІ НАЛАШТУВАННЯ ТА ЗАТВЕРДЖЕНІ ВІДХИЛЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-8(6)[1] | внести перевірені налаштування компонентів до поточних розгорнутих конфігурацій в інвентаризаційний опис компонентів системи |
| CM-8(6)[2] | внести будь-які затверджені відхилення до поточних розгорнутих конфігурацій в інвентаризаційний опис компонентів системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи інвентаризації інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління запасами та оцінкою компонентів інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси ведення інвентаризації компонентів інформаційної системи; автоматизовані механізми реалізації інвентаризації компонентів інформаційної системи]. | |

|  |  |  |
| --- | --- | --- |
| CM-8(7) | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ - ЦЕНТРАЛІЗОВАНЕ СХОВИЩЕ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-8(7)[1] | організація впроваджує централізований репозитарій для інвентаризаційного опису компонентів системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; план управління конфігурацією; проєктна документація інформаційної системи; сховище інвентаризації інформаційної системи; записи інвентаризації інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління компонентами інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують інвентаризацію компонентів інформаційної системи в централізованому сховищі]. | |

|  |  |  |
| --- | --- | --- |
| CM-8(8) | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ - АВТОМАТИЗОВАНЕ ВІДСТЕЖЕННЯ МІСЦЯ ЗНАХОДЖЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-8(8)[1] | використовувати автоматизовані механізми для підтримки відстеження компонентів системи за географічним розташуванням |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; план управління конфігурацією; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; записи інвентаризації інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління компонентами інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; системні / мережеві адміністратори; розробники системи].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують інвентаризацію компонентів інформаційної системи; автоматизовані механізми, що підтримують відстеження компонентів інформаційної системи за географічним розташуванням]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CM-8(9) | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ - ПРИЗНАЧЕННЯ КОМПОНЕНТІВ СИСТЕМАМ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CM-8(9)(a) | CM-8(9)(a)[1] | організація визначає, які компоненти системи є придбані. | |
| CM-8(9)(a)[2] | організація призначає визначені організацією придбані компоненти системи системі | |
| CM-8(9)(b) | CM-8(9)(b)[1] | CM-8(9)(b)[1]{1} | організація визначає персонал який відповідає за належне виконання призначення компонентів систем |
| CM-8(9)(b)[1]{2} | організація визначає ролі які відповідають за належне виконання призначення компонентів системам |
| CM-8(9)(b)[2] | CM-8(9)(b)[2]{1} | отримати підтвердження від персоналу, визначеного організацією, про виконання призначення компонентів системам |
| CM-8(9)(b)[2]{2} | отримати підтвердження від ролі, визначеного організацією, про виконання призначення компонентів системам |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; підтвердження призначень компонентів інформаційної системи; записи інвентаризації інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління запасами компонентів інформаційної системи; власник інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси присвоєння компонентів системам; організаційні процеси визнання призначення компонентів системам; автоматизовані механізми, що здійснюють віднесення придбаних компонентів до інформаційної системи; автоматизовані механізми, що реалізують підтвердження віднесення придбаних компонентів до інформаційної системи]. | | | |

|  |  |  |
| --- | --- | --- |
| CM-8(10) | ІНВЕНТАРИЗАЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ - ВІДОБРАЖЕННЯ ДІЙ З ДАНИМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-8(10)[1] | розробити та задокументувати системний план дій з даними, згідно з яким обробляють персональну ідентифікаційну інформацію |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів інформаційної системи; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; підтвердження призначень компонентів інформаційної системи; записи інвентаризації інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління запасами компонентів інформаційної системи; власник інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси присвоєння компонентів системам; організаційні процеси визнання призначення компонентів системам; автоматизовані механізми, що здійснюють віднесення придбаних компонентів до інформаційної системи; автоматизовані механізми, що реалізують підтвердження віднесення придбаних компонентів до інформаційної системи]. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| CM-9 | ПЛАН УПРАВЛІННЯ КОНФІГУРАЦІЄЮ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| CM-9[1] | організація розробляє, задокументовує план управління конфігурацією системи, який: | | | | |
| CM-9[1](a) | CM-9[1](a)[1] | описує ролі управління конфігурацією | | |
| CM-9[1](a)[2] | описує відповідальність управління конфігурацією | | |
| CM-9[1](a)[3] | описує процеси управління конфігурацією | | |
| CM-9[1](a)[4] | описує процедури управління конфігурацією | | |
| CM-9[1](b) | встановлює процес ідентифікації елементів конфігурації: | | | |
| CM-9[1](b)[1] | протягом всього життєвого циклу розробки системи | | |
| CM-9[1](b)[2] | для управління конфігурацією елементів | | |
| CM-9[1](c) | CM-9[1](c)[1] | визначає елементи конфігурації для системи | | |
| CM-9[1](c)[2] | розміщує елементи конфігурації під управлінням конфігурації | | |
| CM-9[1](d) | CM-9[1](d)[1] | CM-9[1](d)[1]{1} | | організація визначає персонал, які розглядають та затверджують план управління конфігурацією системи |
| CM-9[1](d)[1]{2} | | організація визначає ролі, які розглядають та затверджують план управління конфігурацією системи |
| CM-9[1](d)[1] | CM-9[1](d)[1]{1} | | розглядає визначеним організацією персоналом або ролями план управління конфігурацією системи |
| CM-9[1](d)[1]{2} | | затверджує визначеним організацією персоналом або ролями план управління конфігурацією системи |
| CM-9[1](e) | CM-9[1](e)[1] | захищає план управління конфігурацією від несанкціонованого розкриття | | |
| CM-9[1](e)[2] | захищає план управління конфігурацією від несанкціонованої модифікації | | |
| CM-9[2] | організація реалізує план управління конфігурацією системи, який: | | | | |
| CM-9[2](a) | CM-9[2](a)[1] | описує ролі управління конфігурацією | | |
| CM-9[2](a)[2] | описує відповідальність управління конфігурацією | | |
| CM-9[2](a)[3] | описує процеси управління конфігурацією | | |
| CM-9[2](a)[4] | описує процедури управління конфігурацією | | |
| CM-9[2](b) | встановлює процес ідентифікації елементів конфігурації: | | | |
| CM-9[2](b)[1] | протягом всього життєвого циклу розробки системи | | |
| CM-9[1](b)[2] | для управління конфігурацією елементів | | |
| CM-9[2](c) | CM-9[2](c)[1] | визначає елементи конфігурації для системи | | |
| CM-9[2](c)[2] | розміщує елементи конфігурації під управлінням конфігурації | | |
| CM-9[2](d) | CM-9[2](d)[1] | CM-9[2](d)[1]{1} | організація визначає персонал, який розглядає та затверджує план управління конфігурацією системи | |
| CM-9[2](d)[1]{2} | організація визначає ролі, які розглядають та затверджують план управління конфігурацією системи | |
| CM-9[2](d)[2] | CM-9[2](d)[2]{1} | розглядає визначеним організацією персоналом або ролями план управління конфігурацією системи | |
| CM-9[2](d)[2]{2} | затверджує визначеним організацією персоналом або ролями план управління конфігурацією системи | |
| CM-9[2](e) | CM-9[2](e)[1] | захищає план управління конфігурацією від несанкціонованого розкриття | | |
| CM-9[2](e)[2] | захищає план управління конфігурацією від несанкціонованої модифікації | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на планування управління конфігурацією; план управління конфігурацією; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за розробку плану управління конфігурацією; організаційний персонал, відповідальний за впровадження та управління процесами, визначеними в плані управління конфігурацією; організаційний персонал, відповідальний за захист плану управління конфігурацією; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси розробки та документування плану управління конфігурацією; організаційні процеси ідентифікації та управління елементами конфігурації; організаційні процеси захисту плану управління конфігурацією; автоматизовані механізми, що реалізують план управління конфігурацією; автоматизовані механізми управління елементами конфігурації; автоматизовані механізми захисту плану управління конфігурацією]. | | | | | |

|  |  |  |
| --- | --- | --- |
| CM-9(1) | ПЛАН УПРАВЛІННЯ КОНФІГУРАЦІЄЮ - ВИЗНАЧЕННЯ ВІДПОВІДАЛЬНОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-9(1)[1] | встановити відповідальність за реалізацію процесу управління конфігурацією персоналу, який безпосередньо не бере участь у розробці системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури вирішення відповідальності за розробку процесів управління конфігурацією; план управління конфігурацією; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за розвиток процесів управління конфігурацією; організаційний персонал, відповідальний за інформаційну безпеку]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-10 | ОБМЕЖЕННЯ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-10(a) | використовувати програмне забезпечення та супутні документи відповідно до договірних угод та законів про авторські права | |
| CM-10(b) | відстежувати використання програмного забезпечення та пов'язаної документації, захищеної ліцензіями, для контролю | |
| CM-10(b)[1] | копіювання |
| CM-10(b)[2] | розповсюдження |
| CM-10(c) | контролювати та документувати використання технології однорангового обміну файлами, щоб гарантувати, що ця можливість не використовується для несанкціонованого: | |
| CM-10(c){1} | розповсюдження програмного забезпечення, захищеного авторським правом |
| CM-10(c){2} | відображення програмного забезпечення, захищеного авторським правом |
| CM-10(c){3} | виконання програмного забезпечення, захищеного авторським правом |
| CM-10(c){4} | відтворення програмного забезпечення, захищеного авторським правом |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури, спрямовані на обмеження використання програмного забезпечення; план управління конфігурацією; план безпеки; договори програмного забезпечення та закони про авторські права; документація на ліцензію на сайт; перелік обмежень щодо використання програмного забезпечення; звіти про відстеження ліцензій на програмне забезпечення; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; організаційний персонал, що працює, використовує та / або підтримує інформаційну систему; організаційний персонал з обов'язками управління ліцензіями на програмне забезпечення].  Перевірка: [ВИБРАТИ З: Організаційний процес відстеження використання програмного забезпечення, захищеного кількісними ліцензіями; організаційний процес контролю / документування використання технологій спільного використання однорангових файлів; автоматизовані механізми, що реалізують відстеження ліцензій на програмне забезпечення; автоматизовані механізми, що реалізують та контролюють використання технологій спільного використання однорангових файлів]. | | |

|  |  |  |
| --- | --- | --- |
| CM-10(1) | ОБМЕЖЕННЯ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ - ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ З ВІДКРИТИМ ВИХІДНИМ КОДОМ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CM-10(1)[1] | організація визначає обмеження на використання програмного забезпечення з відкритим вихідним кодом |
| CM-10(1)[2] | організація встановлює такі обмеження на використання програмного забезпечення з відкритим вихідним кодом визначені організацією обмеження |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури вирішення обмежень щодо використання програмного забезпечення з відкритим кодом; план управління конфігурацією; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за встановлення та виконання обмежень щодо використання програмного забезпечення з відкритим кодом; організаційний персонал з обов'язками інформаційної безпеки; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційний процес обмеження використання програмного забезпечення з відкритим кодом; автоматизовані механізми, що реалізують обмеження на використання програмного забезпечення з відкритим кодом]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CM-11 | ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CM-11(a) | CM-11(a)[1] | організація визначає правила, що регулюють встановлення програмного забезпечення користувачами |
| CM-11(a)[2] | організація встановлює правила, що регулюють встановлення програмного забезпечення користувачами |
| CM-11(b) | CM-11(b)[1] | організація визначає методи встановлення програмного забезпечення |
| CM-11(b)[2] | організація визначає правила (політики) встановлення програмного забезпечення |
| CM-11(b)[3] | організація застосує правила (політики) встановлення програмного забезпечення за допомогою наступних методів визначених організацією методів. |
| CM-11(c) | CM-11(c)[1] | організація визначає частоту з якою необхідно відстежувати відповідність правилам (політики). |
| CM-11(c)[2] | відстежувати відповідність правилам (політики) з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури звернення до встановленого користувачем програмного забезпечення; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; перелік правил, що регулюють встановлене користувачем програмне забезпечення; записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи; стратегія постійного моніторингу].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління програмним забезпеченням, встановленим користувачем; організаційний персонал, що працює, використовує та / або підтримує інформаційну систему; організаційний персонал, що здійснює контроль за дотриманням встановленої користувачем програмної політики; організаційний персонал, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].  Перевірка: [ВИБРАТИ З: Організаційні процеси, що керують встановленим користувачем програмним забезпеченням в інформаційній системі; автоматизовані механізми забезпечення правил / методів управління встановленням програмного забезпечення користувачами; автоматизовані механізми контролю за дотриманням політики]. | | |

|  |  |
| --- | --- |
| CM-11(1) | ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - ПОПЕРЕДЖЕННЯ ПРО НЕСАНКЦІОНОВАНУ ІНСТАЛЯЦІЮ |
|  | [Вилучено: Включено до CM-8(3)]. |

|  |  |  |
| --- | --- | --- |
| **CM-11(2)** | **ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - ВСТАНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ПРИВІЛЕЙОВАНИМ СТАТУСОМ** | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| **CM-11(2)[1]** | дозволяє користувачеві встановлювати програмне забезпечення лише при наявності привілейованого статусу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління конфігурацією; процедури звернення до встановленого користувачем програмного забезпечення; план управління конфігурацією; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; оповіщення / сповіщення про несанкціоновані установки програмного забезпечення; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління програмним забезпеченням, встановленим користувачем; організаційний персонал, що працює, використовує та / або підтримує інформаційну систему].  Перевірка: [ВИБРАТИ З: Організаційні процеси, що керують встановленим користувачем програмним забезпеченням в інформаційній системі; автоматизовані механізми заборони встановлення програмного забезпечення без пільгового статусу (наприклад, управління доступом)]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CM-12 | РОЗТАШУВАННЯ ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CM-12(a) | CM-12(a)[1] | організація визначає інформацію розташування якої необхідно контролювати | |
| CM-12(a)[2] | визначити місце розташування: | |
| CM-12(a)[2][1] | інформації, визначеної організацією |
| CM-12(a)[2][2] | конкретних компонентів системи, на яких зберігається інформація |
| CM-12(b) | визначити та задокументувати користувачів, які мають доступ до системи та компонентів системи, де зберігається інформація | | |
| CM-12(c) | задокументувати зміни в розташуванні (наприклад, системи або компонентів системи), де знаходиться інформація | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління розташуванням інформації; план безпеки; проєктна документація інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління розташуванням інформації; організаційний персонал, що працює, використовує та / або підтримує інформаційну систему].  Перевірка: [ВИБРАТИ З: Організаційні процеси, що керують розташуванням інформації] | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CM-12(1) | РОЗТАШУВАННЯ ІНФОРМАЦІЇ - АВТОМАТИЗОВАНІ ІНСТРУМЕНТИ ПІДТРИМКИ РОЗТАШУВАННЯ ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CM-12(1)[1] | організація визначає інформацію за типом | | |
| CM-12(1)[2] | організація визначає системні компоненти для впровадження належних заходів безпеки та приватності для захисту інформації про організацію та приватність особи. | | |
| CM-12(1)[2][1] | CM-12(1)[2][1][1] | організація використовує автоматизовані інструменти для ідентифікації визначеної організацією інформації за типом інформації, на визначених організацією системних компонентах, для впровадження належних заходів безпеки для захисту інформації про організацію |
| CM-12(1)[2][1][2] | організація використовує автоматизовані інструменти для ідентифікації визначеної організацією інформації за типом інформації, на визначених організацією системних компонентах, для впровадження належних заходів безпеки для захисту інформації про приватність особи |
| CM-12(1)[2][2] | CM-12(1)[2][2][1] | організація використовує автоматизовані інструменти для ідентифікації визначеної організацією інформації за типом інформації, на визначених організацією системних компонентах, для впровадження належних заходів приватності для захисту інформації про організацію |
| CM-12(1)[2][2][2] | організація використовує автоматизовані інструменти для ідентифікації визначеної організацією інформації за типом інформації, на визначених організацією системних компонентах, для впровадження належних заходів приватності для захисту інформації про приватність особи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління розташуванням інформації; план безпеки; проєктна документація інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління розташуванням інформації; організаційний персонал, що працює, використовує та / або підтримує інформаційну систему].  Перевірка: [ВИБРАТИ З: Організаційні процеси, що керують розташуванням інформації] | | | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ CP – ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CP-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| CP-1(a) | CP-1(a)[1] | CP-1(a)[1](1) | | | Розробляє та документує політику планування безперервної роботи, яка: | | | | | | | | |
| CP-1(a)[1](1)(a) | | Містить: | | | | | | |
| CP-1(a)[1](1)(a)[1] | | | | мету, | | |
| CP-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| CP-1(a)[1](1)(a)[3] | | | | ролі, | | |
| CP-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| CP-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| CP-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| CP-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| CP-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| CP-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| CP-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| CP-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| CP-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| CP-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| CP-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| CP-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| CP-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики планування безперервної роботи, а також пов'язаних з ними заходів а планування безперервної роботи; | | | | | | | | |
| CP-1(a)[2] | CP-1(a)[2]{1} | | | CP-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика планування безперервної роботи | | | | | |
| CP-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики планування безперервної роботи та пов'язаних з нею заходів захисту політики планування безперервної роботи | | | | | |
| CP-1(a)[2]{2} | | | CP-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика планування безперервної роботи | | | | | |
| CP-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики планування безперервної роботи та пов'язаних з нею заходів захисту політики планування безперервної роботи | | | | | |
| CP-1(a)[3] | CP-1(a)[3]{1} | | | CP-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику планування безперервної роботи | | | | | | | |
| CP-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| CP-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| CP-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| CP-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| CP-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| CP-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| CP-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| CP-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| CP-1(a)[3](1)(b) | | | Відповідає: | | | | |
| CP-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| CP-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| CP-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| CP-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| CP-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| CP-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| CP-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| CP-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації захисту планування безперервної роботи та відповідних заходів планування безперервної роботи | | | | | | | |
| CP-1(a)[3]{2} | | | CP-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику захисту планування безперервної роботи, яка: | | | | | | | |
| CP-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| CP-1(a)[3]{2}(1)(а)[1] | | мету, | |
| CP-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| CP-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| CP-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| CP-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| CP-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| CP-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| CP-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| CP-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| CP-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| CP-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| CP-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| CP-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| CP-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| CP-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| CP-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики планування безперервної роботи та пов'язаних з нею заходів планування безперервної роботи | | | | | | | |
| CP-1(b) | CP-1(b)[1] | визначає посадову особу для управління політикою та процедурами планування безперервної роботи | | | | | | | | | | | |
| CP-1(b)[2] | призначає посаду для управління політикою та процедурами планування безперервної роботи | | | | | | | | | | | |
| CP-1(с) | CP-1(с)[1] | CP-1(с)[1](1) | | CP-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики планування безперервної роботи | | | | | | | |
| CP-1(с)[1](1)[2] | | переглядає поточну планування безперервної роботи з визначеною організацією частотою | | | | | | | |
| CP-1(с)[1](2) | | CP-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур планування безперервної роботи | | | | | | | |
| CP-1(с)[1](2)[2] | | переглядає поточні процедури планування безперервної роботи з визначеною організацією частотою | | | | | | | |
| CP-1(с)[2] | CP-1(с)[2](1) | | CP-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики планування безперервної роботи | | | | | | | |
| CP-1(с)[2](1)[2] | | оновлює поточну політику планування безперервної роботи з визначеною організацією частотою | | | | | | | |
| CP-1(с)[2](2) | | CP-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур планування безперервної роботи | | | | | | | |
| CP-1(с)[2](2)[2] | | оновлює поточні процедури планування безперервної роботи з визначеною організацією частотою | | | | | | | |
| CP-1(d) | переконується, що процедури планування безперервної роботи реалізують політику та заходи планування безперервної роботи | | | | | | | | | | | | |
| CP-1(e) | CP-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики планування безперервної роботи | | | | | | | | | | |
| CP-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики планування безперервної роботи | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури планування безперервної роботи; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику планування безперервної роботи; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CP-2** | **ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ** | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | | | |
| **CP-2(a)** | **CP-2(a)[1]** | | розробити план забезпечення безперервної роботи системи, який: | | | | | | | | | |
| **CP-2(a)[1](1)** | | | | **CP-2(a)[1](1)[1]** | визначає основні завдання, щодо безперервної роботи | | | | |
| **CP-2(a)[1](1)[2]** | визначає функції щодо безперервної роботи | | | | |
| **CP-2(a)[1](1)[2]** | визначає пов'язані з ними вимоги щодо безперервної роботи | | | | |
| **CP-2(a)[1](2)** | | | | **CP-2(a)[1](2)[1]** | забезпечує цілі відновлення функціонування | | | | |
| **CP-2(a)[1](2)[2]** | забезпечує пріоритети відновлення функціонування | | | | |
| **CP-2(a)[1](2)[2]** | забезпечує відповідні показники відновлення функціонування | | | | |
| **CP-2(a)[1](3)** | | | | **CP-2(a)[1](3)[1]** | визначає ролі | | | | |
| **CP-2(a)[1](3)[2]** | визначає обов'язки | | | | |
| **CP-2(a)[1](3)[3]** | визначає відповідальних осіб з контактною інформацією | | | | |
| **CP-2(a)[1](4)** | | | | **CP-2(a)[1](4)[1]** | спрямований на підтримку основних завдань, попри | | | | |
| **CP-2(a)[1](4)[1][1]** | | системні збої, | | |
| **CP-2(a)[1](4)[1][2]** | | компрометації або | | |
| **CP-2(a)[1](4)[1][3]** | | помилки | | |
| **CP-2(a)[1](4)[2]** | спрямований на підтримку основних функцій, попри | | | | |
| **CP-2(a)[1](4)[2][1]** | | системні збої, | | |
| **CP-2(a)[1](4)[2][2]** | | компрометації або | | |
| **CP-2(a)[1](4)[2][3]** | | помилки | | |
| **CP-2(a)[1](5)** | | | | **CP-2(a)[1](5)[1]** | **CP-2(a)[1](5)[1][1]** | | спрямований на повне відновлення функціонування системи без погіршення запланованих заходів захисту інформації | | |
| **CP-2(a)[1](5)[1][2]** | | спрямований на повне відновлення функціонування системи без погіршення запланованих заходів захисту персональних даних | | |
| **CP-2(a)[1](5)[2]** | **CP-2(a)[1](5)[2][1]** | | спрямований на повне відновлення функціонування системи без погіршення реалізованих заходів захисту інформації | | |
| **CP-2(a)[1](5)[2][2]** | | спрямований на повне відновлення функціонування системи без погіршення реалізованих заходів захисту персональних даних | | |
| **CP-2(a)[1](6)** | | | | **CP-2(a)[1](6)[1]** | організація визначає персонал, який розглядає та схвалює план забезпечення безперервної роботи функціонування системи | | | | |
| **CP-2(a)[1](6)[2]** | організація визначає ролі, які розглядають та схвалюють план забезпечення безперервної роботи функціонування системи | | | | |
| **CP-2(a)[1](6)[3]** | організація розглядає визначеним організацією персоналом план забезпечення безперервної роботи функціонування системи | | | | |
| **CP-2(a)[1](6)[4]** | організація розглядає визначеними організацією ролями план забезпечення безперервної роботи функціонування системи | | | | |
| **CP-2(a)[1](6)[5]** | організація схвалює визначеним організацією персоналом план забезпечення безперервної роботи функціонування системи | | | | |
| **CP-2(a)[1](6)[6]** | організація схвалює визначеними організацією ролями план забезпечення безперервної роботи функціонування системи | | | | |
| **CP-2(a)[2]** | | розробити план забезпечення відновлення функціонування системи, який: | | | | | | | | | |
| **CP-2(a)[2](1)** | | | | **CP-2(a)[2](1)[1]** | | визначає основні завдання, щодо безперервної роботи | | | |
| **CP-2(a)[2](1)[2]** | | визначає функції щодо безперервної роботи | | | |
| **CP-2(a)[2](1)[2]** | | визначає пов'язані з ними вимоги щодо безперервної роботи | | | |
| **CP-2(a)[2](2)** | | | | **CP-2(a)[2](2)[1]** | | забезпечує цілі відновлення функціонування | | | |
| **CP-2(a)[2](2)[2]** | | забезпечує пріоритети відновлення функціонування | | | |
| **CP-2(a)[2](2)[2]** | | забезпечує відповідні показники відновлення функціонування | | | |
| **CP-2(a)[2](3)** | | | | **CP-2(a)[2](3)[1]** | | визначає ролі | | | |
| **CP-2(a)[2](3)[2]** | | визначає обов'язки | | | |
| **CP-2(a)[2](3)[3]** | | визначає відповідальних осіб з контактною інформацією | | | |
| **CP-2(a)[2](4)** | | | | **CP-2(a)[2](4)[1]** | | спрямований на підтримку основних завдань, попри | | | |
| **CP-2(a)[2](4)[1][1]** | | | системні збої, |
| **CP-2(a)[2](4)[1][2]** | | | компрометації або |
| **CP-2(a)[2](4)[1][3]** | | | помилки |
| **CP-2(a)[2](4)[2]** | | спрямований на підтримку основних функцій, попри | | | |
| **CP-2(a)[2](4)[2][1]** | | системні збої, | |
| **CP-2(a)[2](4)[2][2]** | | компрометації або | |
| **CP-2(a)[2](4)[2][3]** | | помилки | |
| **CP-2(a)[2](5)** | | | | **CP-2(a)[2](5)[1]** | | **CP-2(a)[2](5)[1][1]** | | спрямований на повне відновлення функціонування системи без погіршення запланованих заходів захисту інформації | |
| **CP-2(a)[2](5)[1][2]** | | спрямований на повне відновлення функціонування системи без погіршення запланованих заходів захисту персональних даних | |
| **CP-2(a)[2](5)[2]** | | **CP-2(a)[2](5)[2][1]** | | спрямований на повне відновлення функціонування системи без погіршення реалізованих заходів захисту інформації | |
| **CP-2(a)[2](5)[2][2]** | | спрямований на повне відновлення  функціонування системи без погіршення реалізованих заходів захисту персональних даних | |
| **CP-2(a)[2](6)** | | | | **CP-2(a)[2](6)[1]** | | організація визначає персонал, який розглядає та схвалює план відновлення функціонування системи | | | |
| **CP-2(a)[2](6)[2]** | | організація визначає ролі, які розглядають та схвалюють план відновлення функціонування системи | | | |
| **CP-2(a)[2](6)[3]** | | організація розглядає визначеним організацією персоналом план забезпечення відновлення функціонування системи | | | |
| **CP-2(a)[2](6)[4]** | | організація розглядає визначеними організацією ролями план відновлення функціонування системи | | | |
| **CP-2(a)[2](6)[5]** | | організація схвалює визначеним організацією персоналом план відновлення функціонування системи | | | |
| **CP-2(a)[2](6)[6]** | | організація схвалює визначеними організацією ролями план відновлення функціонування системи | | | |
| **CP-2(b)** | **CP-2(b)[1]** | | організація визначає ключовий персонал з непередбачених обставин, який ідентифікують за (один або кілька): | | | | | | | | | |
| **CP-2(b)[1]{1}** | | | | ім’ям | | | | | |
| **CP-2(b)[1]{2}** | | | | ролями | | | | | |
| **CP-2(b)[2]** | | організація визначає організаційні елементи з непередбачених обставин. | | | | | | | | | |
| **CP-2(b)[3]** | | поширити копії плану забезпечення безперервної роботи та відновлення функціонування серед: | | | | | | | | | |
| **CP-2(b)[3][1]** | | | | визначеного організацією ключового персоналу з непередбачених обставин | | | | | |
| **CP-2(b)[3][2]** | | | | організаційних елементів | | | | | |
| **CP-2(c)** | координувати діяльність з планування безперервної роботи з діяльністю по обробці інцидентів | | | | | | | | | | | |
| **CP-2(d)** | **CP-2(d)[1]** | | організація визначає частоту переглядів плану забезпечення безперервної роботи системи | | | | | | | | | |
| **CP-2(d)[2]** | | організація визначає частоту переглядів плану відновлення функціонування системи | | | | | | | | | |
| **CP-2(d)[3]** | | переглядати план забезпечення безперервної роботи системи з визначеною організацією частотою | | | | | | | | | |
| **CP-2(d)[4]** | | переглядати план забезпечення відновлення функціонування системи з визначеною організацією частотою | | | | | | | | | |
| **CP-2(e)** | оновлювати план забезпечення безперервної роботи та відновлення функціонування з урахуванням: | | | | | | | | | | | |
| **CP-2(e)[1]** | **CP-2(e)[1]{1}** | | | | змін в організації, | | | | | | |
| **CP-2(e)[1]{2}** | | | | змін в системі | | | | | | |
| **CP-2(e)[1]{3}** | | | | змін в середовищі експлуатації | | | | | | |
| **CP-2(e)[2]** | проблем, що виникають при : | | | | | | | | | | |
| **CP-2(e)[2]{1}** | | | | реалізації плану забезпечення безперервної роботи та відновлення функціонування; | | | | | | |
| **CP-2(e)[2]{2}** | | | | виконанні плану забезпечення безперервної роботи та відновлення функціонування; | | | | | | |
| **CP-2(e)[2]{3}** | | | | тестуванні плану забезпечення безперервної роботи та відновлення функціонування; | | | | | | |
| **CP-2(f)** | **CP-2(f)[1]** | організація визначає ключовий персонал з відновлення функціонування, який ідентифікують за (один або кілька): | | | | | | | | | | |
| **CP-2(f)[1]{1}** | | | ім’ям | | | | | | | |
| **CP-2(f)[1]{2}** | | | ролями | | | | | | | |
| **CP-2(f)[2]** | організація визначає організаційні елементи з відновлення функціонування. | | | | | | | | | | |
| **CP-2(f)[3]** | повідомляти про зміни плану забезпечення безперервної роботи та відновлення функціонування: | | | | | | | | | | |
| **CP-2(f)[3][1]** | | | визначений організацією ключовий персонал з відновлення функціонування | | | | | | | |
| **CP-2(f)[3][2]** | | | організаційних елементів з відновлення функціонування | | | | | | | |
| **CP-2(g)** | забезпечити захист плану забезпечення безперервної роботи та відновлення функціонування від | | | | | | | | | | | |
| **CP-2(g){1}** | | | несанкціонованого розкриття | | | | | | | | |
| **CP-2(g){2}** | | | несанкціонованої зміни | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для інформаційної системи; резервний план; план безпеки; докази оглядів та оновлень плану дій у надзвичайних ситуаціях; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; організаційний персонал, який несе відповідальність за вирішення інцидентів; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси розробки, огляду, оновлення та захисту плану дій у надзвичайних ситуаціях; автоматизовані механізми розробки, перегляду, оновлення та / або захисту плану надзвичайних ситуацій]. | | | | | | | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-2(1) | ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - КООРДИНАЦІЯ З ПОВ’ЯЗАНИМИ ПЛАНАМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| CP-2(1)[1] | координує розробку плану забезпечення безперервної роботи та відновлення функціонування зі структурними підрозділами, які відповідають за: | |
| CP-2(1)[1][1] | розробку пов'язаних планів |
| CP-2(1)[1][2] | реалізацію пов'язаних планів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для інформаційної системи; резервний план; плани дій у надзвичайних ситуаціях; плани відновлення після аварій; безперервність операційних планів; кризи комунікаційних планів; критичні інфраструктурні плани; план реагування на кіберінциденти; інсайдерські плани реалізації загроз; плани надзвичайних ситуацій для пасажирів; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; організаційний персонал, відповідальний за інформаційну безпеку; персонал, відповідальний за пов'язані плани]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-2(2) | ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ПЛАНУВАННЯ РЕСУРСІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-2(2)[1] | організація під час відновлення функціонування системи здійснює планування ресурсів, з метою забезпечення необхідного потенціалу для: | |
| CP-2(2)[1][1] | обробки інформації, |
| CP-2(2)[1][2] | обробки телекомунікацій |
| CP-2(2)[1][3] | підтримки навколишнього середовища |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для інформаційної системи; резервний план; документи з планування потенціалу; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; організаційний персонал, відповідальний за інформаційну безпеку]. | | |

|  |  |  |
| --- | --- | --- |
| CP-2(3) | ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ВІДНОВЛЕННЯ КРИТИЧНИХ ФУНКЦІЙ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-2(3)[1] | організація визначає період часу планувати відновлення критичних функцій |
| CP-2(3)[2] | планувати відновлення критичних функцій в межах визначеного організацією періоду часу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для інформаційної системи; резервний план; план безпеки; оцінка впливу на бізнес; інші пов'язані плани; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР ВІД: Організаційні процеси відновлення місій та ділових функцій]. | |

|  |  |  |
| --- | --- | --- |
| CP-2(4) | ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ВІДНОВЛЕННЯ ВСІХ ФУНКЦІЙ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-2(4)[1] | організація визначає період часу планувати відновлення всіх функцій |
| CP-2(4)[2] | планувати відновлення всіх функцій в межах визначеного організацією часового періоду |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для інформаційної системи; резервний план; план безпеки; оцінка впливу на бізнес; інші пов'язані плани; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси відновлення місій та ділових функцій]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-2(5) | ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - БЕЗПЕРЕРВНІСТЬ ВИКОНАННЯ КРИТИЧНИХ ФУНКЦІЙ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-2(5)[1] | планувати безперервність виконання критичних функцій з мінімальною втратою або без втрати безперервності роботи | |
| CP-2(5)[2] | підтримувати безперервну роботу до повного відновлення системи в місцях (один або кілька): | |
| CP-2(5)[2]{1} | первинної обробки |
| CP-2(5)[2]{2} | зберігання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для інформаційної системи; резервний план; оцінка впливу на бізнес; угоди про первинну обробку сайту; угоди про первинне зберігання; альтернативні угоди про обробку сайтів; альтернативні угоди про місце зберігання; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану дій на випадок надзвичайних ситуацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для продовження місій та ділових функцій]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-2(6) | ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - МІСЦЯ АЛЬТЕРНАТИВНОЇ ОБРОБКИ ТА ЗБЕРІГАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-2(6)[1] | Планувати перенесення виконання критичних функцій в альтернативні місця обробки (один або кілька): | |
| CP-2(6)[2] | CP-2(6)[2]{1} | зберігання з мінімальною втратою безперервності роботи |
| CP-2(6)[2]{2} | зберігання без втрати безперервності роботи |
| CP-2(6)[3] | підтримувати безперервність роботи під час відновлення системи на первинних майданчиках (один або кілька): | |
| CP-2(6)[3]{1} | обробки |
| CP-2(6)[3]{2} | зберігання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для інформаційної системи; резервний план; оцінка впливу на бізнес; альтернативні угоди про обробку сайтів; альтернативні угоди про місце зберігання; документація тестування плану дій на випадок надзвичайних ситуацій; результати випробувань плану дій на випадок надзвичайних ситуацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для передачі основних місій та бізнес-функцій на альтернативні місця для обробки / зберігання]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-2(7) | ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - КООРДИНАЦІЯ З ПРОВАЙДЕРАМИ ЗОВНІШНІХ ПОСЛУГ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-2(7)[1] | з метою забезпечення виконання вимог на випадок надзвичайних ситуацій, координувати план забезпечення безперервної роботи та відновлення функціонування з: | |
| CP-2(7)[1][1] | планами забезпечення безперервної роботи зовнішніх постачальників послуг, |
| CP-2(7)[1][2] | відновлення функціонування зовнішніх постачальників послуг, |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для інформаційної системи; резервний план; плани зовнішніх дій; постачальники послуг; договори про рівень обслуговування; план безпеки; Вимоги до плану дій у надзвичайних ситуаціях; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; зовнішні постачальники послуг; організаційний персонал, відповідальний за інформаційну безпеку]. | | |

|  |  |  |
| --- | --- | --- |
| CP-2(8) | ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ВИЗНАЧЕННЯ КРИТИЧНИХ АКТИВІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-2(8)[1] | визначити критичні активи системи, що підтримують критичні функції |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для інформаційної системи; резервний план; оцінка впливу на бізнес; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; організаційний персонал, відповідальний за інформаційну безпеку]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CP-3 | НАВЧАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CP-3[1] | організація забезпечує навчання користувачів системи щодо забезпечення безперервної роботи відповідно до визначених ролей та обов'язків: | | |
| CP-3[1](a) | CP-3[1](a)[1] | організація визначає період часу в межах якого необхідно взяти на себе відповідну роль та відповідальність з відновлення функціонування |
| CP-3[1](a)[2] | у межах визначеного організацією періоду часу взяти на себе відповідну роль та відповідальність з відновлення функціонування |
| CP-3[1](b) | у разі внесення змін у систему | |
| CP-3[1](c) | CP-3[1](c)[1] | визначеною організацією частоту навчання користувачів системи щодо забезпечення безперервної роботи відповідно до визначених ролей та обов'язків |
| CP-3[1](c)[2] | надалі з визначеною організацією частотою проводити навчання користувачів системи щодо забезпечення безперервної роботи відповідно до визначених ролей та обов'язків |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються навчання у надзвичайних ситуаціях; резервний план; навчальна програма з надзвичайних ситуацій; навчальний матеріал з надзвичайних ситуацій; план безпеки; записи про навчання у надзвичайних ситуаціях; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який займається плануванням, реалізацією плану та навчанням; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для навчання у надзвичайних ситуаціях]. | | | |

|  |  |  |
| --- | --- | --- |
| CP-3(1) | НАВЧАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ - ЗІМІТОВАНІ ПОДІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-3(1)[1] | впровадити моделювання подій в навчанні, щоб забезпечити ефективне реагування персоналу на кризові ситуації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються навчання у надзвичайних ситуаціях; резервний план; навчальна програма з надзвичайних ситуацій; навчальний матеріал з надзвичайних ситуацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який займається плануванням, реалізацією плану та навчанням; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для навчання у надзвичайних ситуаціях; автоматизовані механізми моделювання подій у надзвичайних ситуаціях]. | |

|  |  |  |
| --- | --- | --- |
| CP-3(2) | НАВЧАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ - АВТОМАТИЗОВАНІ НАВЧАЛЬНІ СЕРЕДОВИЩА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-3(2)[1] | впровадити автоматизовані механізми, щоб забезпечити більш досконале та реалістичне середовище навчання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються навчання у надзвичайних ситуаціях; резервний план; навчальна програма з надзвичайних ситуацій; навчальний матеріал з надзвичайних ситуацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який займається плануванням, реалізацією плану та навчанням; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для навчання у надзвичайних ситуаціях; автоматизовані механізми моделювання подій у надзвичайних ситуаціях]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CP-4 | ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CP-4(a) | CP-4(a)[1] | організація визначає частоту тестування плану забезпечення безперервної роботи та відновлення функціонування системи | |
| CP-4(a)[2] | організація визначає тести, які використовують при тестуванні плану забезпечення безперервної роботи та відновлення функціонування системи з метою визначення ефективності плану та організаційної готовності виконати план | |
| CP-4(a)[3] | організація проводить тестування плану забезпечення безперервної роботи та відновлення функціонування системи з визначеною організацією частотою, використовуючи тести, що визначила організація, з метою: | |
| CP-4(a)[3][1] | визначення ефективності плану |
| CP-4(a)[3][2] | організаційної готовності виконати план |
| CP-4(b) | організація переглядає результати тестування плану | | |
| CP-4(c) | організація, за необхідності, ініціює коригувальні дії | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, спрямовані на тестування плану дій на випадок надзвичайних ситуацій, резервний план; план безпеки; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану дій на випадок надзвичайних ситуацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за тестування плану дій на випадок надзвичайних ситуацій, перегляд або реагування на тести плану дій на випадок дій; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для тестування плану на випадок дій; автоматизовані механізми, що підтримують тестування плану на випадок дій та / або тестування плану на випадок надзвичайних ситуацій]. | | | |

|  |  |  |
| --- | --- | --- |
| CP-4(1) | ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - КООРДИНАЦІЯ З ПОВ'ЯЗАНИМ ПЛАНАМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-4(1)[1] | координувати тестування плану забезпечення безперервної роботи та відновлення функціонування з організаційними підрозділами, що відповідають за реалізацію пов'язаних планів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; політика реагування на інциденти; процедури, спрямовані на тестування плану дій на випадок дій у надзвичайних ситуаціях, документація тестування плану дій на випадок надзвичайних ситуацій; резервний план; плани безперервності бізнесу; плани відновлення після аварій; безперервність операційних планів; кризи комунікаційних планів; критичні інфраструктурні плани; плани реагування на кіберінциденти; плани надзвичайних ситуацій для виконуючих обов’язки; план безпеки; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками тестування плану на випадок надзвичайних ситуацій; організаційний персонал; персонал, відповідальний за відповідні плани; організаційний персонал, відповідальний за інформаційну безпеку]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CP-4(2) | ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - АЛЬТЕРНАТИВНА ПЛАТФОРМА ТЕСТУВАННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CP-4(2)[1] | організація тестує план забезпечення безперервної роботи та відновлення функціонування на альтернативній платформі тестування: | | |
| CP-4(2)[1](a) | CP-4(2)[1](a)[1] | ознайомлює персонал з об'єктом |
| CP-4(2)[1](a)[2] | ознайомлює персонал наявними ресурсами |
| CP-4(2)[1](b) | оцінює можливості альтернативної платформи тестування для підтримки безперервної роботи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, спрямовані на тестування плану дій на випадок дій у надзвичайних ситуаціях, резервний план; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану дій на випадок надзвичайних ситуацій; альтернативні угоди про обробку сайтів; угоди про рівень обслуговування; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для тестування плану на випадок дій у надзвичайних ситуаціях; автоматизовані механізми, що підтримують план на випадок надзвичайних ситуацій та / або тестування плану на випадок надзвичайних ситуацій]. | | | |

|  |  |  |
| --- | --- | --- |
| CP-4(3) | ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - АВТОМАТИЧНЕ ТЕСТУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-4(3)[1] | організація використовує автоматизовані механізми для більш ретельного та ефективного тестування плану забезпечення безперервної роботи та відновлення функціонування. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури, спрямовані на тестування плану дій на випадок надзвичайних ситуацій, резервний план; автоматизовані механізми, що підтримують тестування плану на випадок дій; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану дій на випадок надзвичайних ситуацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за тестування плану дій на випадок надзвичайних ситуацій; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для тестування плану на випадок дій; автоматизовані механізми, що підтримують тестування плану на випадок надзвичайних ситуацій]. | |

|  |  |  |
| --- | --- | --- |
| CP-4(4) | ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ПОВНЕ ВІДНОВЛЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-4(4)[1] | Включити повне відновлення системи до відомого стану як частину тестування плану забезпечення безперервної роботи та відновлення функціонування |
| CP-4(4)[2] | Включити повне повернення системи до відомого стану як частину тестування плану забезпечення безперервної роботи та відновлення функціонування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури щодо відновлення та відтворення інформаційної системи; резервний план; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану дій на випадок надзвичайних ситуацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками тестування плану на випадок надзвичайних ситуацій; організаційний персонал, відповідальний за відновлення та відтворення інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для тестування плану на випадок дій у надзвичайних ситуаціях; автоматизовані механізми, що підтримують тестування плану на випадок дій у надзвичайних ситуаціях; автоматизовані механізми підтримки відновлення та відтворення інформаційної системи]. | |

|  |  |
| --- | --- |
| CP-5 | ОНОВЛЕННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ |
|  | [Вилучено: Включено до СР-2]. |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-6 | АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-6(a) | створити альтернативне місце зберігання, включаючи необхідні угоди, що дозволяють | |
| CP-6(a)[1] | зберігати |
| CP-6(a)[2] | видавати інформацію резервного копіювання системи |
| CP-6(b) | переконатися, що в альтернативному місці зберігання впроваджені заходи захисту, аналогічні заходам захисту основної локації | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних місць зберігання; резервний план; альтернативні угоди про місце зберігання; угоди про первинне зберігання; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який має план дій у надзвичайних ситуаціях, чергує обов'язки на місці зберігання; організаційний персонал, відповідальний за відновлення інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси зберігання та отримання резервної інформації інформаційної системи на альтернативному місці зберігання; автоматизовані механізми, що підтримують та / або реалізують зберігання та пошук резервної копії інформації інформаційної системи на альтернативному місці зберігання]. | | |

|  |  |  |
| --- | --- | --- |
| CP-6(1) | АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ - ВІДДІЛЕННЯ ВІД ПЕРВИННОГО СХОВИЩА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-6(1)[1] | визначити альтернативне місце зберігання, яке відокремлено від основного місця зберігання, щоб зменшити сприйнятливість до тих самих загроз |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних місць зберігання; резервний план; альтернативний сайт зберігання; альтернативні угоди про місце зберігання; угоди про первинне зберігання; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який має план дій у надзвичайних ситуаціях, чергує обов'язки на місці зберігання; організаційний персонал, відповідальний за відновлення інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-6(2) | АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ - ЧАС ВІДНОВЛЕННЯ ТА ВСТАНОВЛЕННЯ ЦІЛЕЙ ВІДНОВЛЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-6(2)[1] | налаштувати альтернативне місце зберігання для полегшення операцій відновлення відповідно до | |
| CP-6(2)[1][1] | часу відновлення та |
| CP-6(2)[1][2] | встановлених цілей відновлення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних сайтів зберігання; резервний план; альтернативний сайт зберігання; альтернативні угоди про місце зберігання; альтернативні конфігурації сайту зберігання; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал з обов'язками тестування плану на випадок надзвичайних ситуацій; організаційний персонал, відповідальний за тестування пов'язаних планів; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для тестування плану на випадок дій у надзвичайних ситуаціях; автоматизовані механізми, що підтримують цілі відновлення часу / точок]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-6(3) | АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ - ДОСТУПНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-6(3)[1] | Визначити потенційні проблеми доступності для альтернативного місця зберігання в разі | |
| CP-6(3)[1]{1} | збоїв по всьому регіоні, |
| CP-6(3)[1]{2} | стихійних лих по всьому регіоні, |
| CP-6(3)[2] | в загальних рисах окреслити дії щодо пом'якшення наслідків | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних місць зберігання; резервний план; альтернативне місце зберігання; перелік можливих проблем із доступністю до альтернативного місця зберігання; дії щодо пом'якшення наслідків проблем із доступністю до альтернативного місця зберігання; оцінки організаційних ризиків; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який має план дій у надзвичайних ситуаціях, чергує обов'язки на місці зберігання; організаційний персонал, відповідальний за відновлення інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку]. | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CP-7 | АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК РОБОТИ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| CP-7(a) | CP-7(a)[1] | Організація визначає системні операції для: | | | | |
| CP-7(a)[1][1] | | основних завдань | | |
| CP-7(a)[1][2] | | основних функцій | | |
| CP-7(a)[2] | Організація визначає періоду часу, коли можливості основного майданчика недоступні, відповідно | | | | |
| CP-7(a)[2][1] | | термінам відновлення, | | |
| CP-7(a)[2][2] | | встановленим цілям відновлення | | |
| CP-7(a)[3] | Організація затверджує необхідні угоди, які дозволяють: | | | | |
| CP-7(a)[3][1] | | передачу визначених організацією системних операцій | | |
| CP-7(a)[3][2] | | Відновлення визначених організацією системних операцій | | |
| CP-7(a)[4] | Створити альтернативний майданчик для роботи, включаючи необхідні угоди, які дозволяють передачу та відновлення визначених організацією системних операцій для основних завдань та функцій в рамках визначеного організацією періоду часу, відповідно термінам відновлення та встановленим цілям відновлення, коли можливості основного майданчика недоступні | | | | |
| CP-7(b) | CP-7(b){1} | Забезпечити на альтернативному майданчику доступними для роботи | | | | |
| CP-7(b){1}[1] | інформацію, | | | |
| CP-7(b){1}[2] | обладнання та | | | |
| CP-7(b){1}[3] | прилади, необхідні для | | | |
| CP-7(b){1}[3][1] | | передачі та | |
| CP-7(b){1}[3][2] | | відновлення роботи | |
| CP-7(b){2} | CP-7(b){2}[1] | організацією встановлює періоду часу для передачі та відновлення роботи | | | |
| CP-7(b){2}[2] | укласти контракти протягом встановленого організацією періоду часу для: | | | |
| CP-7(b){2}[2][1] | | | передачі |
| CP-7(b){2}[2][2] | | | відновлення роботи |
| CP-7(c) | Впровадити на альтернативному майданчику роботи заходи захисту, які еквівалентні тим, що впровадженні на основному майданчику | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних місць обробки; резервний план; альтернативні угоди про обробку місць; угоди про первинну обробку місць; запасні запаси обладнання та запасів на альтернативній ділянці обробки; договори на обладнання та постачання; угоди про рівень обслуговування; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування надзвичайних ситуацій та / або альтернативну організацію майданчика; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси відновлення на альтернативному місці; автоматизовані механізми, що підтримують та / або реалізують відновлення на місці альтернативної обробки]. | | | | | | |

|  |  |  |
| --- | --- | --- |
| CP-7(1) | АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ВІДДІЛЕННЯ ВІД ОСНОВНОГО МАЙДАНЧИКА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-7(1)[1] | Визначити альтернативний майданчик для роботи, який відокремлений від основного майданчика, з метою зменшення сприйнятливості до тих самих загроз |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних майданчиків обробки; резервний план; альтернативна ділянка обробки; альтернативні угоди про обробку місць; угоди про первинну обробку сайту; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який має план дій у надзвичайних ситуаціях, чергує обов'язки по обробці місця; організаційний персонал, відповідальний за відновлення інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-7(2) | АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ДОСТУПНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-7(2)[1] | Організація визначає потенційні проблеми доступності для альтернативного майданчика для роботи в разі: | |
| CP-7(2)[1]{1} | збоїв або |
| CP-7(2)[1]{2} | катастрофи по всьому регіону |
| CP-7(2)[2] | окреслити чіткі заходи щодо пом'якшення наслідків | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних місць обробки; резервний план; альтернативна ділянка обробки; альтернативні угоди про обробку сайтів; угоди про первинну обробку сайту; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який має план дій у надзвичайних ситуаціях, чергує обов'язки по обробці місця; організаційний персонал, відповідальний за відновлення інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку]. | | |

|  |  |  |
| --- | --- | --- |
| CP-7(3) | АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ПРІОРИТЕТ ОБСЛУГОВУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-7(3)[1] | Організація визначає вимоги щодо організаційної доступності(включаючи вимоги щодо часу відновлення) |
| CP-7(3)[2] | Розробити угоди про альтернативний майданчик для роботи, які містять положення щодо пріоритету обслуговування відповідно до вимог щодо організаційної доступності (включаючи вимоги щодо часу відновлення). |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних місць обробки; резервний план; альтернативні угоди про обробку сайтів; угоди про рівень обслуговування; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який має план дій у надзвичайних ситуаціях, чергує обов'язки у місці обробки; організаційний персонал, відповідальний за відновлення інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, відповідальний за придбання / договірні угоди]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-7(4) | АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ПІДГОТОВКА ДЛЯ ВИКОРИСТАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-7(4)[1] | Підготувати альтернативний майданчик для роботи таким чином, щоб майданчик був готовий до використання як оперативний майданчик, що підтримує виконання | |
| CP-7(4)[1][1] | основних завдань |
| CP-7(4)[1][2] | основних функцій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних сайтів обробки; резервний план; альтернативний майданчик обробки; альтернативні угоди про обробку майданчиків; чергування конфігурацій сайту; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який має план дій у надзвичайних ситуаціях, чергує обов'язки по обробці місця; організаційний персонал, відповідальний за відновлення інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують відновлення на альтернативному місці обробки]. | | |

|  |  |
| --- | --- |
| CP-7(5) | АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ЕКВІВАЛЕНТНІ ЗАХОДИ БЕЗПЕКИ ІНФОРМАЦІЇ |
|  | [Вилучено: Включено до СР-7] |

|  |  |  |
| --- | --- | --- |
| CP-7(6) | АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - НЕЗДАТНІСТЬ ПОВЕРНУТИСЯ НА ОСНОВНИЙ МАЙДАНЧИК | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-7(6)[1] | Розробити план та підготуватися до обставин, що виключають повернення на основний майданчик для роботи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних місць обробки; резервний план; альтернативна ділянка обробки; альтернативні угоди щодо обробки сайтів; чергування конфігурацій сайту; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за відновлення інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CP-8 | ТЕЛЕКОМУНІКАЦІЙНІ ПОСЛУГИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CP-8[1] | Організація визначає системні операції для основних завдань та функцій | | |
| CP-8[2] | Організація визначає період часу за який необхідно відновити визначені організацією системні операції | | |
| CP-8[3] | Впровадити альтернативні телекомунікаційні послуги, включаючи необхідні угоди, що дозволять відновити визначені організацією системні операції для основних завдань та функцій в визначений організацією період часу, коли: | | |
| CP-8[3]{1} | основні можливості зв'язку недоступні на основному місці локації, | |
| CP-8[3]{2} | основні можливості зв'язку знаходяться на альтернативному майданчику для | |
| CP-8[3]{2}{1} | роботи або |
| CP-8[3]{2}{2} | зберігання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних телекомунікаційних послуг; резервний план; первинні та альтернативні угоди про послуги з телекомунікацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обов'язки щодо плану дій у галузі надзвичайних ситуацій; організаційний персонал, відповідальний за відновлення інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; організаційний персонал, відповідальний за придбання / договірні угоди].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми підтримки телекомунікацій]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CP-8(1) | ТЕЛЕКОМУНІКАЦІЙНІ ПОСЛУГИ - ПРІОРИТЕТ ПОСТАЧАННЯ ПОСЛУГ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CP-8(1)(a) | CP-8(1)(a)[1] | Організація визначає вимоги щодо організаційної доступності(включаючи вимоги щодо часу відновлення) | |
| CP-8(1)(a)[2] | Розробити основні угоди про надання телекомунікаційних послуг, які містять пріоритетні положення про надання послуг відповідно до вимог організаційної доступності (включаючи вимоги щодо часу відновлення); | |
| CP-8(1)(a)[3] | Розробити альтернативні угоди про надання телекомунікаційних послуг, які містять пріоритетні положення про надання послуг відповідно до вимог організаційної доступності (включаючи вимоги щодо часу відновлення); | |
| CP-8(1)(b) | CP-8(1)(b)[1] | Надсилати запит про пріоритети телекомунікаційних послуг для всіх телекомунікаційних послуг, що використовуються для забезпечення безперервності роботи, якщо (один або кілька): | |
| CP-8(1)(b)[1]{1} | основні телекомунікаційні послуги надаються загальним оператором |
| CP-8(1)(b)[1]{2} | альтернативні телекомунікаційні послуги надаються загальним оператором |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до первинних та альтернативних телекомунікаційних послуг; резервний план; первинні та альтернативні угоди про послуги з телекомунікацій; пріоритетна документація щодо послуг зв'язку; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обов'язки щодо плану дій у галузі надзвичайних ситуацій; організаційний персонал, відповідальний за відновлення інформаційної системи; організаційний персонал з обов'язками інформаційної безпеки; організаційний персонал, відповідальний за придбання / договірні угоди].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми підтримки телекомунікацій]. | | | |

|  |  |  |
| --- | --- | --- |
| CP-8(2) | ТЕЛЕКОМУНІКАЦІЙНІ ПОСЛУГИ - ЄДИНІ ТОЧКИ ВІДМОВИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-8(2)[1] | Отримати альтернативні телекомунікаційні послуги, з метою зменшення ймовірності спільного використання єдиної точки відмови з основними телекомунікаційними послугами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до первинних та альтернативних телекомунікаційних послуг; резервний план; первинні та альтернативні угоди про послуги з телекомунікацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обов'язки щодо плану дій у галузі надзвичайних ситуацій; організаційний персонал, відповідальний за відновлення інформаційної системи; первинні та альтернативні постачальники послуг зв'язку; організаційний персонал, відповідальний за інформаційну безпеку]. | |

|  |  |  |
| --- | --- | --- |
| CP-8(3) | ТЕЛЕКОМУНІКАЦІЙНІ ПОСЛУГИ - ВІДДІЛЕННЯ ОСНОВНИХ ТА АЛЬТЕРНАТИВНИХ ПРОВАЙДЕРІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-8(3)[1] | Отримувати альтернативні телекомунікаційні послуги від постачальників, які відокремлені від основних постачальників послуг, щоб зменшити сприйнятливості до тих самих загроз |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до первинних та альтернативних телекомунікаційних послуг; резервний план; первинні та альтернативні угоди про послуги з телекомунікацій; альтернативне місце постачальника послуг зв'язку; сайт провайдера первинних телекомунікаційних послуг; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обов'язки щодо плану дій у галузі надзвичайних ситуацій; організаційний персонал, відповідальний за відновлення інформаційної системи; первинні та альтернативні постачальники послуг зв'язку; організаційний персонал, відповідальний за інформаційну безпеку]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-8(4) | ТЕЛЕКОМУНІКАЦІЙНІ ПОСЛУГИ - ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ПОСТАЧАЛЬНИКА ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-8(4)(a) | CP-8(4)(a)[1] | вимагати, щоб постачальники основних телекомунікаційних послуг мали плани забезпечення безперервної роботи |
| CP-8(4)(a)[2] | вимагати, щоб постачальники альтернативних телекомунікаційних послуг мали плани забезпечення безперервної роботи |
| CP-8(4)(b) | переглядати плани забезпечення безперервної роботи постачальників телекомунікаційних послуг для забезпечення відповідності планам забезпечення безперервної роботи організації | |
| CP-8(4)(c) | CP-8(4)(c)[1] | Організація визначає частоту тестування планів забезпечення безперервної роботи та навчання постачальників телекомунікаційних послуг |
| CP-8(4)(c)[2] | отримати свідчення про тестування планів забезпечення безперервної роботи та навчання постачальників телекомунікаційних послуг з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до первинних та альтернативних телекомунікаційних послуг; резервний план; плани на випадок непередбачених ситуацій; докази тестування / навчання постачальників на випадок надзвичайних ситуацій; первинні та альтернативні угоди про послуги з телекомунікацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за планування на випадок надзвичайних ситуацій, виконання плану та тестування; первинні та альтернативні постачальники послуг зв'язку; організаційний персонал з обов'язками інформаційної безпеки; організаційний персонал, відповідальний за придбання / договірні угоди]. | | |

|  |  |  |
| --- | --- | --- |
| CP-8(5) | ТЕЛЕКОМУНІКАЦІЙНІ ПОСЛУГИ - ТЕСТУВАННЯ АЛЬТЕРНАТИВНИХ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-8(5)[1] | Організація визначає частоту з якою необхідно тестувати надання альтернативних телекомунікаційних послуг |
| CP-8(5)[2] | Тестувати надання альтернативних телекомунікаційних послуг з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування дій у надзвичайних ситуаціях; процедури звернення до альтернативних телекомунікаційних послуг; резервний план; докази тестування альтернативних телекомунікаційних послуг; альтернативні угоди про послуги з телекомунікацій; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за планування на випадок надзвичайних ситуацій, виконання плану та тестування; альтернативні постачальники послуг зв'язку; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують тестування альтернативних телекомунікаційних послуг]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CP-9 | РЕЗЕРВНЕ КОПІЮВАННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CP-9(a) | CP-9(a)[1] | організація визначає частоту резервного копіювання інформації користувачів, що міститься в системі, відповідно до: | |
| CP-9(a)[1][1] | часу відновлення |
| CP-9(a)[1][2] | встановлених цілей відновлення |
| CP-9(a)[2] | Проводити резервне копіювання інформації користувачів, що міститься в системі з визначеною організацією частотою, відповідно до часу відновлення та встановлених цілей відновлення | |
| CP-9(b) | CP-9(b)[1] | організація визначає частоту резервного копіювання системної інформації на системному рівні, що міститься в системі, відповідно до | |
| CP-9(b)[1][1] | завдань відновлення |
| CP-9(b)[1][2] | встановлених цілей відновлення |
| CP-9(b)[2] | Організація проводить резервне копіювання системної інформації на системному рівні, що міститься в системі з визначеною організацією частотою, відповідно до завдань відновлення і встановлених цілей відновлення | |
| CP-9(с) | CP-9(с)[1] | організація визначає частоту резервного копіювання системної документації, включаючи документацію, пов'язану зі забезпеченням безпеки, відповідно до | |
| CP-9(b)[1][1] | часу відновлення |
| CP-9(b)[1][2] | встановлених цілей відновлення |
| CP-9(с)[2] | Організація проводить резервне копіювання системної документації, включаючи документацію, пов'язану зі забезпеченням безпеки з визначеною організацією частотою, відповідно до часу відновлення та встановлених цілей відновлення | |
| CP-9(d) | Організація забезпечує для резервних копій інформації в місцях їх зберігання захист: | | |
| CP-9(d)[1] | конфіденційності, | |
| CP-9(d)[2] | цілісності | |
| CP-9(d)[3] | доступності | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання інформаційної системи; резервний план; резервне місце (місця) зберігання; журнали або записи інформаційної системи резервного копіювання; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за резервне копіювання інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для проведення резервних копій інформаційних систем; автоматизовані механізми підтримки та / або реалізації резервних копій інформаційних систем]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-9(1) | РЕЗЕРВНЕ КОПІЮВАННЯ - ВИПРОБУВАННЯ НА НАДІЙНІСТЬ ТА ЦІЛІСНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-9(1)[1] | Організація визначає частоту з якою необхідно тестувати носії резервних копій інформації | |
| CP-9(1)[2] | Організація повинна тестувати носії резервних копій інформації з визначеною організацією частотою для перевірки: | |
| CP-9(1)[2][1] | надійності носіїв |
| CP-9(1)[2][2] | цілісності інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання інформаційної системи; резервний план; результати тестування резервної копії інформаційної системи; документація на випробування плану дій на випадок непередбачених ситуацій; результати випробувань плану дій на випадок непередбачених ситуацій; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за резервне копіювання інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для проведення резервних копій інформаційних систем; автоматизовані механізми підтримки та / або реалізації резервних копій інформаційних систем]. | | |

|  |  |  |
| --- | --- | --- |
| CP-9(2) | РЕЗЕРВНЕ КОПІЮВАННЯ - ТЕСТУВАННЯ ВІДНОВЛЕННЯ З ВИКОРИСТАННЯМ ЗРАЗКІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-9(2)[1] | Використовувати зразок резервної копії інформації при відновленні вибраних системних функцій як частину тестування плану забезпечення безперервної роботи та відновлення функціонування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання інформаційної системи; резервний план; результати тестування резервної копії інформаційної системи; документація на випробування плану дій на випадок непередбачених ситуацій; результати випробувань плану дій на випадок непередбачених ситуацій; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за резервне копіювання інформаційної системи; організаційний персонал, який відповідає за планування на випадок непередбачених ситуацій / тестування плану дій на випадок непередбачених ситуацій; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для проведення резервних копій інформаційних систем; автоматизовані механізми підтримки та / або реалізації резервних копій інформаційних систем]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-9(3) | РЕЗЕРВНЕ КОПІЮВАННЯ - ВІДОКРЕМЛЕНЕ СХОВИЩЕ КРИТИЧНОЇ ІНФОРМАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-9(3)[1] | Організація визначає критичне системне програмне забезпечення та іншу інформацію, пов'язану з безпекою | |
| CP-9(3)[2] | Зберігати резервні копії визначеного організацією критичного системного програмного забезпечення та іншу інформацію, пов'язану з безпекою в | |
| CP-9(3)[2][1] | окремому сховищі, яке не пов'язані з системою |
| CP-9(3)[2][2] | або у вогнестійкому контейнері, який не пов'язаний з системою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання інформаційної системи; резервний план; резервне місце (місця) зберігання; конфігурації резервної копії інформаційної системи та супутня документація; журнали або записи інформаційної системи резервного копіювання; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за планування на випадок надзвичайних ситуацій та виконання плану; організаційний персонал, відповідальний за резервне копіювання інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку]. | | |

|  |  |
| --- | --- |
| CP-9(4) | РЕЗЕРВНЕ КОПІЮВАННЯ - ЗАХИСТ ВІД НЕАВТОРИЗОВАНИХ МОДИФІКАЦІЙ |
|  | [Вилучено: Включено до СР-9]. |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-9(5) | РЕЗЕРВНЕ КОПІЮВАННЯ - ПЕРЕДАЧА НА АЛЬТЕРНАТИВНЕ СХОВИЩЕ ЗБЕРІГАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-9(5)[1] | організація визначає період часу передачі резервних копій інформації системи на альтернативне сховище, відповідно до: | |
| CP-9(5)[1][1] | часу відновлення |
| CP-9(5)[1][2] | встановленим цілям відновлення |
| CP-9(5)[2] | організація визначає швидкість передачі, резервних копій інформації системи на альтернативне сховище, відповідно до: | |
| CP-9(5)[2][1] | часу відновлення |
| CP-9(5)[2][2] | встановленим цілям відновлення |
| CP-9(5)[3] | Організація переносить резервні копії інформації системи на альтернативне сховище: | |
| CP-9(5)[3][1] | у визначений організацією період часу, відповідні часу відновлення та встановленим цілям відновлення |
| CP-9(5)[3][2] | швидкість передачі, відповідні часу відновлення та встановленим цілям відновлення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання інформаційної системи; резервний план; журнали або записи інформаційної системи резервного копіювання; докази інформації про резервне копіювання системи, переданої на альтернативне місце зберігання; альтернативні угоди про місця зберігання; інші відповідні документи або записи]  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за резервне копіювання інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для передачі резервних копій інформаційної системи на альтернативне місце зберігання; автоматизовані механізми підтримки та / або реалізації резервних копій інформаційних систем; автоматизовані механізми, що підтримують та / або реалізують передачу інформації до альтернативного місця зберігання]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CP-9(6) | РЕЗЕРВНЕ КОПІЮВАННЯ - НАДЛИШКОВА ВТОРИННА СИСТЕМА | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| CP-9(6)[1] | Організація виконує резервне копіювання системи, підтримуючи надлишкову вторинну систему, яка: | | |
| CP-9(6)[1][1] | CP-9(6)[1][1][1] | не пов'язана з первинною системою та |
| CP-9(6)[1][2] | CP-9(6)[1][2]{1} | яку можна активувати без втрати інформації або |
| CP-9(6)[1][2]{2} | яку можна активувати без порушення роботи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання інформаційної системи; резервний план; результати тестування резервної копії інформаційної системи; результати випробувань плану дій на випадок непередбачених ситуацій; документація на випробування плану на випадок непередбачених ситуацій резервна вторинна система для резервного копіювання інформаційної системи; розташування надлишкових вторинних систем резервного копіювання; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за резервне копіювання інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за надлишкову вторинну систему].  Перевірка: [ВИБРАТИ З: Організаційні процеси для підтримки надлишкових вторинних систем; автоматизовані механізми підтримки та / або реалізації резервних копій інформаційних систем; автоматизовані механізми, що підтримують та / або реалізують передачу інформації до резервної вторинної системи]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-9(7) | РЕЗЕРВНЕ КОПІЮВАННЯ - ПОДВІЙНА АВТОРИЗАЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-9(7)[1] | Організація визначає резервні копії інформації | |
| CP-9(7)[2] | Організація використовує для визначених організацією резервних копій інформації подвійну авторизацію для: | |
| CP-9(7)[2][1] | видалення |
| CP-9(7)[2][2] | знищення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання інформаційної системи; резервний план; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; створений системою перелік подвійних повноважень або правил авторизації; журнали або записи видалення або знищення резервної інформації; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за резервне копіювання інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують подвійну авторизацію; автоматизовані механізми підтримки та / або реалізації видалення / знищення резервної інформації]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-9(8) | РЕЗЕРВНЕ КОПІЮВАННЯ - КРИПТОГРАФІЧНИЙ ЗАХИСТ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-9(8)[1] | організація визначає резервні копії інформації | |
| CP-9(8)[2] | Організація впроваджує криптографічні механізми для запобігання: | |
| CP-9(8)[2][1] | несанкціонованого розкриття визначених організацією резервних копій інформації |
| CP-9(8)[2][2] | змін визначених організацією резервних копій інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання інформаційної системи; резервний план; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; створений системою перелік подвійних повноважень або правил авторизації; журнали або записи видалення або знищення резервної інформації; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за резервне копіювання інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують подвійну авторизацію; автоматизовані механізми підтримки та / або реалізації видалення / знищення резервної інформації]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-10 | ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-10[1] | організація визначає період часу, відповідного: | |
| CP-10[1][1] | часу відновлення |
| CP-10[1][2] | встановлених цілей відновлення |
| CP-10[2] | організація забезпечує відновлення системи до відомого стану після збою, компрометації або помилок у межах визначеного організацією періоду часу, відповідного часу відновлення та встановлених цілей відновлення | |
| CP-10[3] | організація pабезпечує відтворення системи до відомого стану після збою, компрометації або помилок у межах визначеного організацією періоду часу, відповідного часу відновлення та встановлених цілей відновлення | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання інформаційної системи; резервний план; результати тестування резервної копії інформаційної системи; результати випробувань плану дій на випадок непередбачених ситуацій; документація на випробування плану на випадок непередбачених ситуацій резервна вторинна система для резервного копіювання інформаційної системи; розташування надлишкових вторинних систем резервного копіювання; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який несе відповідальність за планування, відновлення та / або відновлення; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси, що реалізують операції з відновлення та відновлення інформаційної системи; автоматизовані механізми, що підтримують та / або впроваджують операції з відновлення та відтворення інформаційної системи]. | | |

|  |  |
| --- | --- |
| CP-10(1) | ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ |
|  | [Вилучено: Включено до СР-4]. |

|  |  |  |
| --- | --- | --- |
| CP-10(2) | ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ВІДНОВЛЕННЯ ТРАНЗАКЦІЙ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-10(2)[1] | Реалізувати відновлення транзакцій для систем, що базуються на транзакціях |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури відновлення та відтворення інформаційної системи; резервний план; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація на випробування плану на випадок непередбачених ситуацій результати випробувань плану дій на випадок непередбачених ситуацій; записи відновлення транзакцій інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за відновлення транзакцій; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливість відновлення транзакцій]. | |

|  |  |
| --- | --- |
| CP-10(3) | ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - КОМПЕНСАЦІЙНІ ЗАХОДИ БЕЗПЕКИ |
|  | [Вилучено: Переадресовано через процедури адаптації]. |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-10(4) | ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ВІДНОВЛЕННЯ У МЕЖАХ ЧАСОВОГО ПЕРІОДУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-10(4)[1] | Організація визначає період відновлення компонентів системи | |
| CP-10(4)[2] | Організація забезпечує можливість відновлення компонентів системи в межах визначеного організацією періоду відновлення з: | |
| CP-10(4)[2][1] | інформації управління конфігурацією |
| CP-10(4)[2][2] | захищеною цілісністю, яка описує відомий робочий стан компонентів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика планування на випадок непередбачених ситуацій; процедури відновлення та відтворення інформаційної системи; резервний план; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація на випробування плану на випадок непередбачених ситуацій результати випробувань плану дій на випадок непередбачених ситуацій; докази операцій з відновлення та відтворення інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, відповідальний за відновлення та відтворення інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують відновлення / відтворення інформації інформаційної системи]. | | |

|  |  |
| --- | --- |
| CP-10(5) | ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ЗДАТНІСТЬ ВІДМОВОСТІЙКОСТІ |
|  | [Вилучено: Включено до SI-13]. |

|  |  |  |
| --- | --- | --- |
| CP-10(6) | ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ЗАХИСТ КОМПОНЕНТУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-10(6)[1] | Забезпечити захист компонентів системи, які використовуються для резервного копіювання |
| CP-10(6)[2] | Забезпечити захист компонентів системи, які використовуються для резервного відновлення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика планування на випадок непередбачених ситуацій; процедури відновлення та відтворення інформаційної системи; резервний план; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; логічні дані доступу; облікові дані фізичного доступу; записи авторизації логічного доступу; записи фізичних дозволів доступу; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, відповідальний за відновлення та відтворення інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для захисту апаратного забезпечення, прошивки та програмного забезпечення для резервного копіювання та відновлення; автоматизовані механізми, що підтримують і / або здійснюють захист резервного копіювання та відновлення апаратних засобів, програмно-апаратних та програмних]]. | |

|  |  |  |
| --- | --- | --- |
| CP-11 | АЛЬТЕРНАТИВНІ ПРОТОКОЛИ ЗВ’ЯЗКУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-11[1] | Організація визначає альтернативні протоколи зв'язку для підтримки збереження безперервності функціонування |
| CP-11[2] | Організація забезпечує можливість застосування визначених організацією альтернативних протоколів зв'язку для підтримки збереження безперервності функціонування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З:Політика планування на випадок непередбачених ситуацій; процедури, що стосуються альтернативних протоколів зв'язку; резервний план; план безперервності операцій; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік альтернативних протоколів зв'язку, що підтримують безперервність операцій; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за планування на випадок надзвичайних ситуацій та виконання плану; організаційний персонал з безперервністю оперативного планування та відповідальності за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З:Автоматизовані механізми, що використовують альтернативні протоколи зв'язку]. | |

|  |  |  |
| --- | --- | --- |
| CP-12 | БЕЗПЕЧНИЙ РЕЖИМ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| CP-12[1] | Організація визначає умови, за яких організація вводить безпечний режим роботи |
| CP-12[2] | Організація визначає обмеження в безпечному режимі роботи |
| CP-12[3] | Коли Організація виявляє визначені організацією умови, організація вводить безпечний режим роботи з визначеними організацією обмеженнями в безпечному режимі роботи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються безпечного режиму роботи інформаційної системи; резервний план; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; посібники з адміністрування інформаційної системи; посібники з експлуатації інформаційної системи; посібники з встановлення інформаційної системи; протоколи випробувань на випадок непередбачених ситуацій; записи про обробку інцидентів; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що реалізують безпечний режим роботи]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| CP-13 | АЛЬТЕРНАТИВНІ МЕХАНІЗМИ БЕЗПЕКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| CP-13[1] | Організація визначає: | |
| CP-13[1][1] | Альтернативні механізми безпеки |
| CP-13[1][2] | додаткові механізми безпеки |
| CP-13[2] | Організація визначає функції безпеки | |
| CP-13[3] | Організація використовує визначені організацією альтернативні механізми безпеки для реалізації визначених організацією функцій безпеки, коли основні засоби реалізації функцій безпеки недоступні або скомпрометовані. | |
| CP-13[4] | Організація використовує визначені організацією додаткові механізми безпеки для реалізації визначених організацією функцій безпеки, коли основні засоби реалізації функцій безпеки недоступні або скомпрометовані. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються альтернативних механізмів безпеки; резервний план; план безперервності операцій; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; протоколи випробувань на випадок непередбачених ситуацій; результати випробувань плану дій на випадок непередбачених ситуацій; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Можливість інформаційної системи, що реалізує альтернативні механізми безпеки]. | | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ IA – ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IA-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| IA-1(a) | IA-1(a)[1] | IA-1(a)[1](1) | | | Розробляє та документує політику ідентифікації та автентифікації, яка: | | | | | | | | |
| IA-1(a)[1](1)(a) | | Містить: | | | | | | |
| IA-1(a)[1](1)(a)[1] | | | | мету, | | |
| IA-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| IA-1(a)[1](1)(a)[3] | | | | ролі, | | |
| IA-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| IA-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| IA-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| IA-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| IA-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| IA-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| IA-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| IA-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| IA-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| IA-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| IA-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| IA-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| IA-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики ідентифікації та автентифікації, а також пов'язаних з ними заходів ідентифікації та автентифікації; | | | | | | | | |
| IA-1(a)[2] | IA-1(a)[2]{1} | | | IA-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика ідентифікації та автентифікації | | | | | |
| IA-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики ідентифікації та автентифікації та пов'язаних з нею заходів захисту політики ідентифікації та автентифікації | | | | | |
| IA-1(a)[2]{2} | | | IA-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика ідентифікації та автентифікації | | | | | |
| IA-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики ідентифікації та автентифікації та пов'язаних з нею заходів захисту політики ідентифікації та автентифікації | | | | | |
| IA-1(a)[3] | IA-1(a)[3]{1} | | | IA-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику ідентифікації та автентифікації | | | | | | | |
| IA-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| IA-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| IA-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| IA-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| IA-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| IA-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| IA-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| IA-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| IA-1(a)[3](1)(b) | | | Відповідає: | | | | |
| IA-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| IA-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| IA-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| IA-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| IA-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| IA-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| IA-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| IA-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації захисту ідентифікації та автентифікації та відповідних заходів ідентифікації та автентифікації | | | | | | | |
| IA-1(a)[3]{2} | | | IA-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику захисту ідентифікації та автентифікації, яка: | | | | | | | |
| IA-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| IA-1(a)[3]{2}(1)(а)[1] | | мету, | |
| IA-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| IA-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| IA-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| IA-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| IA-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| IA-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| IA-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| IA-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| IA-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| IA-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| IA-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| IA-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| IA-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| IA-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| IA-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики ідентифікації та автентифікації та пов'язаних з нею заходів ідентифікації та автентифікації | | | | | | | |
| IA-1(b) | IA-1(b)[1] | визначає посадову особу для управління політикою та процедурами ідентифікації та автентифікації | | | | | | | | | | | |
| IA-1(b)[2] | призначає посаду для управління політикою та процедурами ідентифікації та автентифікації | | | | | | | | | | | |
| IA-1(с) | IA-1(с)[1] | IA-1(с)[1](1) | | IA-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики ідентифікації та автентифікації | | | | | | | |
| IA-1(с)[1](1)[2] | | переглядає поточну політику ідентифікації та автентифікації з визначеною організацією частотою | | | | | | | |
| IA-1(с)[1](2) | | IA-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур ідентифікації та автентифікації | | | | | | | |
| IA-1(с)[1](2)[2] | | переглядає поточні процедури ідентифікації та автентифікації з визначеною організацією частотою | | | | | | | |
| IA-1(с)[2] | IA-1(с)[2](1) | | IA-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики ідентифікації та автентифікації | | | | | | | |
| IA-1(с)[2](1)[2] | | оновлює поточну політику ідентифікації та автентифікації з визначеною організацією частотою | | | | | | | |
| IA-1(с)[2](2) | | IA-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур ідентифікації та автентифікації | | | | | | | |
| IA-1(с)[2](2)[2] | | оновлює поточні процедури ідентифікації та автентифікації з визначеною організацією частотою | | | | | | | |
| IA-1(d) | переконується, що процедури ідентифікації та автентифікації реалізують політику та заходи ідентифікації та автентифікації | | | | | | | | | | | | |
| IA-1(e) | IA-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики ідентифікації та автентифікації | | | | | | | | | | |
| IA-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики ідентифікації та автентифікації | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури ідентифікації та автентифікації; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику ідентифікації та автентифікації; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-2 | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-2[1] | Організація унікально ідентифікує | |
| IA-2[1][1] | Користувачів, що діють від імені користувачів |
| IA-2[1][2] | процеси, що діють від імені користувачів |
| IA-2[2] | Організація унікально автентифікує користувачів або процеси, що діють від імені користувачів | |
| IA-2[2][1] | Користувачів, що діють від імені користувачів |
| IA-2[2][2] | процеси, що діють від імені користувачів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік рахунків інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; організаційний персонал, відповідальний за управління рахунками; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для однозначної ідентифікації та автентифікації користувачів; автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]. | | |

|  |  |  |
| --- | --- | --- |
| IA-2(1) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-2(1) | Реалізувати багатофакторну автентифікацію для доступу до привілейованих облікових записів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік рахунків інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, відповідальний за управління обліковими записами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують багатофакторну можливість автентифікації]. | |

|  |  |  |
| --- | --- | --- |
| IA-2(2) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-2(2)[1] | Організація реалізує багатофакторну автентифікацію для доступу до непривілейованих облікових записів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік облікових записів інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, відповідальний за управління обліковими записами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують багатофакторну можливість автентифікації]. | |

|  |  |
| --- | --- |
| IA-2(3) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ЛОКАЛЬНИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ |
|  | [Вилучено: Включено до ІА-2(1)]. |

|  |  |
| --- | --- |
| IA-2(4) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ЛОКАЛЬНИЙ ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ |
|  | [Вилучено: Включено до ІА-2(1)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-2(5) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ІНДИВІДУАЛЬНА АВТЕНТИФІКАЦІЯ З ГРУПОВОЮ АВТЕНТИФІКАЦІЄЮ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-2(5){1} | Коли використовуються спільні облікові записи, потрібно, щоб користувачі окремо проходили автентифікацію перед наданням доступу до: | |
| IA-2(5){1}{1} | спільних облікових записів |
| IA-2(5){1}{2} | або спільних ресурсів |
| IA-2(5){2} | Коли використовуються спільні автентифікатори, потрібно, щоб користувачі окремо проходили автентифікацію перед наданням доступу до спільних облікових записів або ресурсів | |
| IA-2(5){2}{1} | спільних облікових записів |
| IA-2(5){2}{2} | або спільних ресурсів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік облікових записів інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, відповідальний за управління обліковими записами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують можливість автентифікації для групових облікових записів]. | | |

|  |  |
| --- | --- |
| IA-2(6) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - МЕРЕЖЕВИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ – ОКРЕМИЙ ПРИСТРІЙ |
|  | [Вилучено: Включено до ІА-2(1)]. |

|  |  |
| --- | --- |
| IA-2(7) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - МЕРЕЖЕВИЙ ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ – ОКРЕМИЙ ПРИСТРІЙ |
|  | [Вилучено: Включено до ІА-2(1)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-2(8) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ДОСТУП ДО ОБЛІКОВИХ ЗАПИСІВ – СТІЙКІСТЬ ДО ВІДТВОРЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-2(8)[1] | Організація реалізує стійкі до відтворення механізми автентифікації для доступу до (один або кілька): | |
| IA-2(8)[1][1] | привілейованих облікових записів; |
| IA-2(8)[1][2] | непривілейованих облікових записів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік привілейованих облікових записів інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, відповідальний за управління обліковими записами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що підтримують та / або впроваджують стійкі до відтворення механізми автентифікації]. | | |

|  |  |
| --- | --- |
| IA-2(9) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ – СТІЙКІСТЬ ДО ВІДТВОРЕННЯ |
|  | [Вилучено: Включено до ІА-2(8)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-2(10) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ЄДИНА ТОЧКА ВХОДУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-2(10)[1] | організація визначає перелік системних облікових записів, для яких повинна бути передбачена можливість єдиного входу | |
| IA-2(10)[2] | організація визначає перелік послуг інформаційної системи, для яких повинна бути передбачена можливість єдиного входу | |
| IA-2(10)[3] | організація впроваджує можливість єдиного входу для: | |
| IA-2(10)[3][1] | системних облікових записів та |
| IA-2(10)[3][2] | послуг, визначених організацією |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються можливості єдиного входу для облікових записів та послуг інформаційної системи; процедури, що стосуються ідентифікації та автентифікації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік облікових записів та послуг інформаційної системи, що вимагають можливості єдиного входу; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, відповідальний за управління обліковими записами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що підтримують та / або впроваджують можливість єдиного входу для облікових записів та послуг інформаційної системи]. | | |

|  |  |
| --- | --- |
| IA-2(11) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ВІДДАЛЕНИЙ ДОСТУП - ОКРЕМИЙ ПРИСТРІЙ |
|  | [Вилучено: Включено до ІА-2(1)]. |

|  |  |  |
| --- | --- | --- |
| IA-2(12) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ПРИЙНЯТТЯ ПОВНОВАЖЕНЬ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИСТОЇ ІНФОРМАЦІЇ (PIV CREDENTIALS) | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-2(12)[1] | Прийняти повноваження облікових даних особистої ідентифікації |
| IA-2(12)[2] | електронним шляхом підтвердити повноваження облікових даних особистої ідентифікації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; Записи перевірки PIV; докази посвідчення особи PIV; Уповноваження PIV; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, відповідальний за управління обліковими записами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або впроваджують прийняття та перевірку облікових даних PIV]. | |

|  |  |
| --- | --- |
| IA-2(13) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - АВТЕНТИФІКАЦІЯ ПО ЗОВНІШНЬОМУ КАНАЛУ |
|  | [Вилучено: Включено до ІА-2(1)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-3 | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-3[1] | організація визначає типи пристроїв, які необхідно: | |
| IA-3[1][1] | унікально ідентифікувати перед установкою підключення |
| IA-3[1][2] | унікально автентифікувати перед установкою підключення. |
| IA-3[2] | організація унікально ідентифікує визначені організацією типи пристроїв, які перед установкою (один або кілька): | |
| IA-3[2][1] | Локального підключення; |
| IA-3[2][2] | Дистанційного підключення, |
| IA-3[2][3] | мережного підключення |
| IA-3[3] | організація унікально автентифікує визначені організацією типи пристроїв, які перед установкою (один або кілька): | |
| IA-3[3][1] | Локального підключення; |
| IA-3[3][2] | Дистанційного підключення, |
| IA-3[3][3] | мережного підключення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації пристрою; проєктна документація інформаційної системи; перелік пристроїв, що вимагають унікальної ідентифікації та автентифікації; звіти про підключення пристрою; налаштування конфігурації інформаційної системи та відповідна документація; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за ідентифікацію та автентифікацію пристрою; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують можливість ідентифікації та автентифікації пристрою]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IA-3(1) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - КРИПТОГРАФІЧНА ДВОБІЧНА АВТЕНТИФІКАЦІЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IA-3(1)[1] | IA-3(1)[1]{1} | Організація визначає певні пристрої, які необхідно автентифікувати перед встановленням підключення за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах та/або | |
| IA-3(1)[1]{2} | Організація визначає типи пристроїв, які необхідно автентифікувати перед встановленням підключення за допомогою двобічної автентифікації, яка заснована на криптографічних | |
| IA-3(1)[2] | IA-3(1)[2]{1} | Організація автентифікує певні пристрої, визначені організацією та/або перед встановленням (один або кілька): | |
| IA-3(1)[2]{1}{1} | локального підключення за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах; |
| IA-3(1)[2]{1}{2} | віддаленого підключення за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах; |
| IA-3(1)[2]{1}{3} | мережевого підключення за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах. та/або: |
| IA-3(1)[2]{2} | Організація автентифікує типи пристроїв перед встановленням (один або кілька): | |
| IA-3(1)[2]{2}{1} | локального підключення за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах; |
| IA-3(1)[2]{2}{2} | віддаленого підключення за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах; |
| IA-3(1)[2]{2}{3} | мережевого підключення за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації пристрою; проєктна документація інформаційної системи; перелік пристроїв, що вимагають унікальної ідентифікації та автентифікації; звіти про підключення пристрою; налаштування конфігурації інформаційної системи та відповідна документація; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за ідентифікацію та автентифікацію пристрою; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують можливість аутентифікації пристрою; криптографічно засновані двобічні механізми автентифікації]. | | | |

|  |  |
| --- | --- |
| IA-3(2) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - КРИПТОГРАФІЧНИЙ ДВОБІЧНА МЕРЕЖА АВТЕНТИФІКАЦІЯ |
|  | [Виключено: включено до ІА-3(1)]. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IA-3(3) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - ДИНАМІЧНИЙ РОЗПОДІЛ АДРЕСИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IA-3(3)(a) | IA-3(3)(a)[1] | У разі динамічного розподілу адреси визначити вимоги щодо оренди динамічного розміщення адреси, призначених для пристроїв відповідно до: | |
| IA-3(3)(a)[1][1] | інформації про оренду, визначеної організацією, та |
| IA-3(3)(a)[1][2] | інформації тривалість лізингу |
| IA-3(3)(a)[2] | У разі динамічного розподілу адреси визначити вимоги щодо тривалості лізингу, призначених для пристроїв відповідно до: | |
| IA-3(3)(a)[2][1] | інформації про оренду, визначеної організацією, та |
| IA-3(3)(a)[2][2] | інформації тривалість лізингу |
| IA-3(3)(b) | Проводить аудит інформації щодо оренди при призначенні на пристрій | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації пристрою; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; докази інформації про оренду та тривалості оренди, призначені пристроям; звіти про підключення пристрою; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за ідентифікацію та автентифікацію пристрою; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують можливість ідентифікації та автентифікації пристрою; автоматизовані механізми підтримки та / або реалізації динамічного розподілу адрес; автоматизовані механізми, що підтримують та / або імплантують аудит інформації про оренду]. | | | |

|  |  |  |
| --- | --- | --- |
| IA-3(4) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - АТЕСТАЦІЯ ПРИСТРОЮ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-3(4)[1] | організація визначає процес управління конфігурацією. |
| IA-3(4)[2] | організація здйснює ідентифікацію пристроїв на основі атестації за допомогою визначеного організацією процесу управління конфігурацією |
| IA-3(4)[3] | організація здйснює автентифікацію пристроїв на основі атестації за допомогою визначеного організацією процесу управління конфігурацією |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації пристрою; процедури, що стосуються управління конфігурацією пристрою; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи управління конфігурацією; змінити записи контролю; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за ідентифікацію та автентифікацію пристрою; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують можливість ідентифікації та автентифікації пристрою; автоматизовані механізми підтримки та / або реалізації управління конфігурацією; криптографічні механізми, що підтримують атестацію пристроїв]. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| IA-4 | УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| IA-4[1] | Управляти системними ідентифікаторами шляхом: | | | | |
| IA-4[1](a) | IA-4[1](a)[1] | IA-4[1](a)[1]{1} | | організація визначає персонал, який надає дозвіл для призначення ідентифікатора особі, групи, ролі або пристрою |
| IA-4[1](a)[1]{2} | | організація визначає ролі, які надають дозвіл для призначення ідентифікатора особі, групи, ролі або пристрою. |
| IA-4[1](a)[2] | організація надає дозвіл від визначеного організацією персоналу для призначення ідентифікатора | | |
| IA-4[1](a)[2]{1} | | особі, |
| IA-4[1](a)[2]{2} | | групи, |
| IA-4[1](a)[2]{3} | | ролі |
| IA-4[1](a)[2]{4} | | пристрою |
| IA-4[1](a)[3] | організація надає дозвіл від визначених організацією ролей для призначення ідентифікатора особі, групи, ролі або пристрою | | |
| IA-4[1](a)[3]{1} | | особі, |
| IA-4[1](a)[3]{2} | | групи, |
| IA-4[1](a)[3]{3} | | ролі |
| IA-4[1](a)[3]{4} | | пристрою |
| IA-4[1](b) | Вибору ідентифікатора, який ідентифікує | | | |
| IA-4[1](b){1} | | окрему особу, | |
| IA-4[1](b){2} | | групу, | |
| IA-4[1](b){3} | | роль | |
| IA-4[1](b){4} | | пристрій | |
| IA-4[1](c) | Призначення ідентифікатора: | | | |
| IA-4[1](c)[1] | | особі, | |
| IA-4[1](c)[2] | | групі, | |
| IA-4[1](c)[3] | | ролі або | |
| IA-4[1](c)[4] | | пристрою | |
| IA-4[1](d) | IA-4[1](d)[1] | | організація визначає період часу, впродовж якого необхідно запобігати повторному використанню ідентифікаторів. | |
| IA-4[1](d)[2] | | організація запобігає повторному використанню ідентифікаторів впродовж визначеного організацією періоду часу | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління рахунками; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік облікових записів інформаційної системи; перелік ідентифікаторів, що генеруються з фізичних пристроїв контролю доступу; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління ідентифікаторами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або впроваджують управління ідентифікаторами]. | | | | | |

|  |  |  |
| --- | --- | --- |
| IA-4(1) | УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ЗАБОРОНА ВИКОРИСТАННЯ ІДЕНТИФІКАТОРІВ ОБЛІКОВИХ ЗАПИСІВ ТАКИ САМИХ, ЯК Й ПУБЛІЧНІ ІДЕНТИФІКАТОРИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-4(1)[1] | Заборонити використання системних ідентифікаторів облікових записів, які збігаються з загальнодоступними ідентифікаторами для індивідуальних облікових записів електронної пошти |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління ідентифікаторами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або впроваджують управління ідентифікаторами]. | |

|  |  |
| --- | --- |
| IA-4(2) | УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - АВТОРИЗАЦІЯ СУПЕРВАЙЗЕРА |
|  | [Виключено: Включено до ІА-12(1)]. |

|  |  |
| --- | --- |
| IA-4(3) | УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - МНОЖИННІ ФОРМИ СЕРТИФІКАЦІЇ |
|  | [Виключено: Включено до ІА-12(2)]. |

|  |  |  |
| --- | --- | --- |
| IA-4(4) | УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ІДЕНТИФІКАЦІЯ СТАТУСУ КОРИСТУВАЧА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-4(4)[1] | організація визначає ознаку, що ідентифікує індивідуальний статус |
| IA-4(4)[2] | організація управляє індивідуальними ідентифікаторами, однозначно ідентифікуючи кожного індивідуума за визначену організацією ознакою, що ідентифікує індивідуальний статус |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; перелік характеристик, що ідентифікують індивідуальний статус; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління ідентифікаторами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або впроваджують управління ідентифікаторами]. | |

|  |  |  |
| --- | --- | --- |
| IA-4(5) | УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ДИНАМІЧНЕ УПРАВЛІННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-4(5)[1] | Організація динамічно управляє індивідуальними ідентифікаторами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління ідентифікаторами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують управління динамічним ідентифікатором]. | |

|  |  |  |
| --- | --- | --- |
| IA-4(6) | УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - КРОС-ОРГАНІЗАЦІЙНЕ УПРАВЛІННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-4(6)[1] | Організація визначає зовнішні організації з якими необхідно здійснювати координацію для крос-організаційного управління ідентифікаторами |
| IA-4(6)[2] | Організація здійснює координацію з визначеними організацією зовнішніми організаціями для крос-організаційного управління ідентифікаторами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління ідентифікаторами; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або впроваджують управління ідентифікаторами]. | |

|  |  |
| --- | --- |
| IA-4(7) | УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ОСОБИСТА РЕЄСТРАЦІЯ |
|  | [Виключено: Включено до ІА-12(4)]. |

|  |  |  |
| --- | --- | --- |
| IA-4(8) | УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ПОПАРНІ ПСЕВДОНІМНІ ІДЕНТИФІКАТОРИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-4(8)[1] | Організація створює попарні псевдонімні ідентифікатори |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління ідентифікаторами; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або впроваджують управління ідентифікаторами]. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| IA-5 | УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| IA-5[1] | Організація управляє системними автентифікаторами шляхом: | | | | |
| IA-5[1](a) | Перевірки, як частини початкового розподілу автентифікатора: | | | |
| IA-5[1](a){1} | особу, яка отримує автентифікатор | | |
| IA-5[1](a){2} | групу, яка отримує автентифікатор | | |
| IA-5[1](a){3} | роль, яка отримує автентифікатор | | |
| IA-5[1](a){4} | пристрій, який отримує автентифікатор | | |
| IA-5[1](b) | Створення вихідного вмісту автентифікатора для будь-яких автентифікаторів, випущених організацією | | | |
| IA-5[1](c) | Забезпечення того, щоб автентифікатори мали достатню стійкість механізму для їх несанкціонованого використання | | | |
| IA-5[1](d) | IA-5[1](d)[1] | Створення адміністративних процедур для початкового поширення автентифікатора, для: | | |
| IA-5[1](d)[1]{1} | | втрачених автентифікаторів |
| IA-5[1](d)[1]{2} | | скомпрометованих автентифікаторів |
| IA-5[1](d)[1]{3} | | або ушкоджених автентифікаторів |
| IA-5[1](d)[2] | Створення адміністративних процедур для відкликання автентифікаторів | | |
| IA-5[1](d)[3] | реалізацію адміністративних процедур для початкового поширення автентифікатора, для: | | |
| IA-5[1](d)[3]{1} | | втрачених автентифікаторів |
| IA-5[1](d)[3]{2} | | скомпрометованих автентифікаторів |
| IA-5[1](d)[3]{3} | | або ушкоджених автентифікаторів |
| IA-5[1](d)[4] | реалізацію адміністративних процедур для відкликання автентифікаторів | | |
| IA-5[1](e) | IA-5[1](e)[1] | Встановлення мінімальних обмежень тривалості життя та умов повторного використання для автентифікаторів: | | |
| IA-5[1](e)[1][1] | | життя повторного використання для автентифікаторів |
| IA-5[1](e)[1][2] | | умов повторного використання для автентифікаторів |
| IA-5[1](e)[2] | Встановлення максимальних обмежень тривалості: | | |
| IA-5[1](e)[2][1] | | життя повторного використання для автентифікаторів |
| IA-5[1](e)[2][2] | | умов повторного використання для автентифікаторів |
| IA-5[1](f) | IA-5[1](f)[1] | організація визначає період часу за типом автентифікатора за який змінюють автентифікатор | | |
| IA-5[1](f)[2] | організація визначає період часу за типом автентифікатора за який оновлюють автентифікатор | | |
| IA-5[1](f)[3] | організація змінює автентифікатори у встановлений організацією період часу за типом автентифікатора | | |
| IA-5[1](f)[4] | організація оновлює автентифікатори у встановлений організацією період часу за типом автентифікатора | | |
| IA-5[1](g) | IA-5[1](g)[1] | | організація захищає вміст автентифікатора від несанкціонованого розкриття | |
| IA-5[1](g)[2] | | організація захищає вміст автентифікатора від несанкціонованих модифікацій | |
| IA-5[1](h) | Вимогою до осіб, які використовують пристрої, використовувати спеціальні заходи безпеки для захисту автентифікаторів | | | |
| IA-5[1](i) | IA-5[1](i)[1] | Змінювати автентифікатори для облікових записів груп при зміні членства в цих облікових записах | | |
| IA-5[1](i)[2] | Змінювати автентифікатори для облікових записів ролей при зміні членства в цих облікових записах | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікатором; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік типів автентифікатора інформаційної системи; зміни записів заходів, пов’язаних з управлінням автентифікаторами інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З:Організаційний персонал, який відповідає за управління автентифікатором; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують можливості управління автентифікатором]. | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| IA-5(1) | УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТЕНТИФІКАЦІЯ НА ОСНОВІ ПАРОЛЯ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| IA-5(1)[1] | Для автентифікації на основі пароля необхідно: | | | | |
| IA-5(1)(a) | IA-5(1)(a)[1] | вести список: | | |
| IA-5(1)(a)[1][1] | часто використовуваних, | |
| IA-5(1)(a)[1][2] | очікуваних | |
| IA-5(1)(a)[1][3] | скомпрометованих паролів | |
| IA-5(1)(a)[2] | організація визначає частоту оновлення списку: | | |
| IA-5(1)(a)[2][1] | часто використовуваних, | |
| IA-5(1)(a)[2][2] | очікуваних | |
| IA-5(1)(a)[2][3] | скомпрометованих паролів | |
| IA-5(1)(a)[3] | організація оновлює список | | |
| IA-5(1)(a)[3][1] | часто використовуваних, | |
| IA-5(1)(a)[3][2] | очікуваних | |
| IA-5(1)(a)[3][3] | скомпрометованих паролів | |
| IA-5(1)(a)[4] | організація оновлює список коли підозрюється, що паролі організацій скомпрометовані: | | |
| IA-5(1)(a)[4]{1} | | прямо чи |
| IA-5(1)(a)[4]{2} | | опосередковано |
| IA-5(1)(b) | IA-5(1)(b)[1] | перевіряти, коли користувачі створюють паролі, що паролі не знаходяться у визначеному організацією списку найчастіше використовуваних, очікуваних або скомпрометованих паролів | | |
| IA-5(1)(b)[2] | перевіряти, коли користувачі оновлюють паролі, що паролі не знаходяться у визначеному організацією списку найчастіше використовуваних, очікуваних або скомпрометованих паролів | | |
| IA-5(1)(c) | передавати лише криптографічно захищені паролі | | | |
| IA-5(1)(d) | зберігати паролі за допомогою затвердженого алгоритму хешування, переважно використовуючи ключову хеш-функцію | | | |
| IA-5(1)(e) | вимагати негайного вибору нового пароля після відновлення облікового запису | | | |
| IA-5(1)(f) | дозволити користувачеві вибирати довгі паролі та фрази, включаючи пробіли та всі друковані символи | | | |
| IA-5(1)(g) | використовувати автоматизовані інструменти для допомоги користувачеві у виборі надійних автентифікаторів паролів | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; політика щодо паролів; процедури, що стосуються управління автентифікатором; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; конфігурації паролів та відповідна документація; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління автентифікатором; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або впроваджують можливість керування автентифікатором на основі паролів]. | | | | | |

|  |  |  |
| --- | --- | --- |
| IA-5(10) | УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ДИНАМІЧНЕ ЗВ’ЯЗУВАННЯ МАНДАТІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-5(10)[1] | Динамічно зв'язувати ідентичності та автентифікатори |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; план безпеки; проєктна документація інформаційної системи; автоматизовані механізми, що забезпечують динамічну прив'язку ідентифікаторів та автентифікаторів; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З:Організаційний персонал, який відповідає за управління ідентифікаторами; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що реалізують можливості управління ідентифікаторами; автоматизовані механізми, що реалізують динамічне забезпечення ідентифікаторів]. | |

|  |  |
| --- | --- |
| IA-5(11) | УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТЕНТИФІКАЦІЯ НА ОСНОВІ АПАРАТНИХ ТОКЕНІВ |
|  | [Вилучено: Включено до ІА-2(1)]. |

|  |  |  |
| --- | --- | --- |
| IA-5(12) | УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ЕФЕКТИВНІСТЬ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-5(12)[1] | організація визначає вимоги до якості біометрії |
| IA-5(12)[2] | Для біометричної автентифікації використовувати механізми, які задовольняють визначені організацією вимоги до якості біометрії |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікатором; план безпеки; проєктна документація інформаційної системи; автоматизовані механізми, що використовують біометричну автентифікацію для інформаційної системи; перелік вимог до якості біометричної автентифікації; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління автентифікатором; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або впроваджують можливість управління автентифікатором на основі біометричних даних]. | |

|  |  |  |
| --- | --- | --- |
| IA-5(13) | УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ЗАКІНЧЕННЯ ТЕРМІНУ КЕШУВАННЯ АВТЕНТИФІКАТОРІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-5(13)[1] | організація визначає періоду часу після якого необхідно заборонити використання кешованих автентифікаторів |
| IA-5(13)[2] | Заборонити використання кешованих автентифікаторів після визначеного організацією періоду часу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікатором; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління автентифікатором; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують можливості управління автентифікатором]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-5(14) | УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - УПРАВЛІННЯ ЗМІСТОМ ДОВІРЧИХ СХОВИЩ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-5(14)[1] | Для автентифікації на основі інфраструктури з відкритим ключем використовувати загальноорганізаційну методологію управління вмістом довірених сховищ інфраструктури відкритого ключа, встановлених на всіх платформах, включаючи: | |
| IA-5(14)[1][1] | мережі, |
| IA-5(14)[1][2] | операційні системи, |
| IA-5(14)[1][3] | браузери |
| IA-5(14)[1][4] | додатки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікатором; план безпеки; організаційна методологія управління вмістом довірчих сховищ відкритого ключа на всіх встановлених платформах; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація архітектури безпеки підприємства; документація з архітектури підприємства; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління автентифікатором; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують можливості управління автентифікатором на основі відкритого ключа; автоматизовані механізми, що підтримують та / або впроваджують можливість зберігання довіри відкритого ключа]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-5(15) | УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ПРОДУКТИ ТА ПОСЛУГИ, ЗАТВЕРДЖЕНІ УПРАВЛІННЯМ ЗАГАЛЬНИМИ ПОСЛУГАМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-5(15)[1] | Організація визначає уповноважений орган, що затверджує продукти та послуги | |
| IA-5(15)[2] | Використовувати лише схвалені уповноваженим органом | |
| IA-5(15)[2][1] | продукти |
| IA-5(15)[2][2] | послуги |
| IA-5(15)[3] | Використовувати лише затверджені уповноваженим органом | |
| IA-5(15)[3][1] | продукти |
| IA-5(15)[3][2] | послуги |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; план безпеки; проєктна документація інформаційної системи; автоматизовані механізми, що забезпечують динамічну прив'язку ідентифікаторів та автентифікаторів; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за управління ідентифікацією та автентифікацією; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або впроваджують можливості управління обліковим записом; автоматизовані механізми, що підтримують та / або реалізують можливості управління ідентифікацією та аутентифікацією для інформаційної системи]. | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| IA-5(16) | УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ПЕРЕДАЧА ОСОБИСТОЇ АБО ДОВІРЧОЇ АВТЕНТИФІКАЦІЇ ЗОВНІШНЬОЇ СТОРОНИ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| IA-5(16)[1] | IA-5(16)[1]{1} | організація визначає види автентифікатори  та / або | | | | |
| IA-5(16)[1]{2} | організація визначає конкретні автентифікатори | | | | |
| IA-5(16)[2] | організація визначає зареєстрований орган до якого передаються визначені організацією види та/або конкретні автентифікатори. | | | | | |
| IA-5(16)[3] | IA-5(16)[3]{1} | організація визначає персонал, який повинен бути авторизований для передачі визначених видів та/або конкретних автентифікаторів до визначеного організацією, зареєстрованого органу. | | | | |
| IA-5(16)[3]{2} | організація визначає ролі, які повинні бути авторизовані для передачі визначених видів та/або конкретних автентифікаторів до визначеного організацією, зареєстрованого органу. | | | | |
| IA-5(16)[4] | IA-5(16)[4]{1}  (та \ або) | Вимагати, щоб передача визначених організацією видів автентифікаторів: | | | | |
| IA-5(16)[4]{1}[1] | Особисто до визначеного організацією, зареєстрованого органу здійснювалася з авторизацією визначеними організацією | | | |
| IA-5(16)[4]{1}[1][1] | | | персоналом або |
| IA-5(16)[4]{1}[1][2] | | | ролями. |
| IA-5(16)[4]{1}[2] | довіреною зовнішньою стороною до визначеного організацією, зареєстрованого органу здійснювалася з авторизацією визначеними організацією | | | |
| IA-5(16)[4]{1}[2][1] | | персоналом або | |
| IA-5(16)[4]{1}[2][2] | | ролями. | |
| IA-5(16)[4]{2} | Вимагати, щоб передача визначених організацією конкретних автентифікаторів: | | | | |
| IA-5(16)[4]{1}[1] | Особисто до визначеного організацією, зареєстрованого органу здійснювалася з авторизацією визначеними організацією | | | |
| IA-5(16)[4]{1}[1][1] | персоналом або | | |
| IA-5(16)[4]{1}[1][2] | ролями. | | |
| IA-5(16)[4]{1}[2] | довіреною зовнішньою стороною до визначеного організацією, зареєстрованого органу здійснювалася з авторизацією визначеними організацією | | | |
| IA-5(16)[4]{1}[2][1] | персоналом або | | |
| IA-5(16)[4]{1}[2][2] | ролями. | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та аутентифікації; процедури, що стосуються управління ідентифікаторами; план безпеки; проєктна документація інформаційних систем; автоматизовані механізми, що забезпечують динамічну прив'язку ідентифікаторів та автентифікатор; настройки конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ ВІД: Організаційний персонал, який відповідає за управління ідентифікацією та автентифікацією; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ ВІД: Автоматизовані механізми, що підтримують та / або реалізують можливості управління обліковим записом; автоматизовані механізми, що підтримують та / або реалізують можливості управління ідентифікацією та аутентифікацією для інформаційної системи]. | | | | | | |

|  |  |  |
| --- | --- | --- |
| IA-5(17) | УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТОМАТИЗОВАНІ ЗАСОБИ ВИЯВЛЕННЯ АТАК ІЗ ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ АВТЕНТИФІКАТОРІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-5(17)[1] | Використовувати механізми виявлення атак із використанням штучно виготовлених артефактів для біометричних автентифікаторів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та аутентифікації; процедури, що стосуються управління ідентифікаторами; план безпеки; проєктна документація інформаційних систем; автоматизовані механізми, що забезпечують динамічну прив'язку ідентифікаторів і автентифікатор; настройки конфігурації інформаційної системи та супутня документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за управління ідентифікацією та автентифікацією; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості управління обліковим записом; автоматизовані механізми, що підтримують та / або реалізують можливості управління ідентифікацією та аутентифікацією для інформаційної системи]. | |

|  |  |  |
| --- | --- | --- |
| IA-6 | ЗВОРОТНИЙ ЗВ'ЯЗОК АВТЕНТИФІКАТОРА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-6[1] | Забезпечити виявлення прихованої зворотної передачі інформації автентифікації в процесі автентифікації для забезпечення захисту інформації від можливої експлуатації та використання неавторизованими особами. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політика ідентифікації та автентифікації; процедури звернення до відгуків автентифікатора; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують затемнення зворотного зв’язку інформації про автентифікацію під час автентифікації].: | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-7 | АВТЕНТИФІКАЦІЯ КРИПТОГРАФІЧНОГО МОДУЛЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-7[1] | Впровадити механізми автентифікації в криптографічний модуль, який відповідає, для такої автентифікації, вимогам: | |
| IA-7[1][1] | чинних законів |
| IA-7[1][2] | виконавчих розпоряджень |
| IA-7[1][3] | директив |
| IA-7[1][4] | політик |
| IA-7[1][5] | правил |
| IA-7[1][6] | стандартів |
| IA-7[1][7] | рекомендацій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються аутентифікації криптографічного модуля; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за аутентифікацію криптографічного модуля; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: : [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують аутентифікацію криптографічного модуля] | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-8 | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (НЕ ОРГАНІЗАЦІЙНІ КОРИСТУВАЧІ) | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-8[1] | Унікально ідентифікувати: | |
| IA-8[1]{1} | не організаційних користувачів |
| IA-8[1]{2} | процеси (що не належать організації), які діють від імені користувачів. |
| IA-8[2] | Унікально автентифікувати: | |
| IA-8[2]{1} | не організаційних користувачів |
| IA-8[2]{2} | процеси (що не належать організації), які діють від імені користувачів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік рахунків інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; організаційний персонал, відповідальний за управління обліковими записами].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації] | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-8(1) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (НЕ ОРГАНІЗАЦІЙНІ КОРИСТУВАЧІ) - ВИЗНАННЯ ПОСВІДЧЕНЬ ІДЕНТИФІКАЦІЙНИХ ДАНИХ ВІД ІНШИХ УСТАНОВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-8(1)[1] | облікові дані (посвідчення ідентифікаційних даних), видані іншими установами для встановлення особи: | |
| IA-8(1)[1][1] | приймають |
| IA-8(1)[1][2] | в електронному вигляді перевіряють |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; Записи перевірки PIV; докази посвідчення особи PIV; Уповноваження PIV; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал, відповідальний за управління рахунками].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, які приймають та перевіряють облікові дані PIV] | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-8(2) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (НЕ ОРГАНІЗАЦІЙНІ КОРИСТУВАЧІ) - ВИЗНАННЯ ЗОВНІШНІХ ПОСВІДЧЕНЬ ІДЕНТИФІКАЦІЙНИХ ДАНИХ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| IA-8(2)[1] | приймає тільки ті зовнішні облікові дані (посвідчення ідентифікаційних даних), що відповідають вимогам | |
| IA-8(2)[1][1] | нормативних документів |
| IA-8(2)[1][2] | стандартів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік продуктів, компонентів або послуг, затверджених FICAM, сторонніми документами для реєстрації, закупленими та реалізованими організацією; сторонні записи перевірки облікових даних; докази підтверджених FICAM повноважень сторонніх осіб; повноваження сторонніх облікових даних; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал, який відповідає за управління рахунками].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що приймають затверджені FICAM облікові дані] | | |

|  |  |
| --- | --- |
| IA-8(3) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (НЕ ОРГАНІЗАЦІЙНІ КОРИСТУВАЧІ) - ВИКОРИСТАННЯ ЗАТВЕРДЖЕНИХ ПРОДУКТІВ |
|  | [Вилучено: Включено до ІА-8(2)] |

|  |  |  |
| --- | --- | --- |
| IA-8(4) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (НЕ ОРГАНІЗАЦІЙНІ КОРИСТУВАЧІ) - ВИКОРИСТАННЯ ПРОФІЛЕЙ ВИДАНИХ УПОВНОВАЖЕНИМ ОРГАНОМ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-8(4)[1] | Для керування ідентифікацією забезпечити відповідність до профілів, що видані уповноваженим органом. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; політика придбання системи та послуг; процедури, що стосуються ідентифікації та автентифікації користувачів; процедури, що стосуються інтеграції вимог безпеки в процес придбання; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік профілів, виданих FICAM, та пов'язаних із ними, затверджених протоколів; документація про придбання; договори придбання для закупівель або послуг інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал, який відповідає за управління обліковими записами].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що підтримують та / або впроваджують відповідність із профілями, виданими FICAM]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-8(5) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (НЕ ОРГАНІЗАЦІЙНІ КОРИСТУВАЧІ) - ВИЗНАННЯ ПОСВІДЧЕНЬ ОСОБИ, ЩО ВИДАЮТЬСЯ НЕДЕРЖАВНИМИ ОРГАНАМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-8(5)[1] | облікові дані для підтвердження особи, що видаються недержавними органами: | |
| IA-8(5)[1][1] | приймати |
| IA-8(5)[1][2] | підтверджувати в електронному вигляді |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; Записи перевірки PIV-I; докази посвідчення особи PIV-I; Дозвільні документи PIV-I; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал, відповідальний за управління рахунками].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що приймають та перевіряють облікові дані PIV-I]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IA-8(6) | ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (НЕ ОРГАНІЗАЦІЙНІ КОРИСТУВАЧІ) - РОЗ’ЄДНАННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IA-8(6)[1] | IA-8(6)[1]{1} | організація визначає заходи, щоб диcоціювати атрибути користувача | |
| IA-8(6)[1]{2} | організація визначає заходи, щоб диcоціювати відносини затвердження облікових даних | |
| IA-8(6)[2] | IA-8(6)[2]{1} | Реалізувати визначені організацією заходи, щоб диcоціювати атрибути користувача між: | |
| IA-8(6)[2]{1}[1] | особами, |
| IA-8(6)[2]{1}[2] | постачальниками послуг облікового запису |
| IA-8(6)[2]{1}[3] | перевіряючими сторонами. |
| IA-8(6)[2]{2} | Реалізувати визначені організацією заходи, щоб диcоціювати відносини затвердження облікових даних між: | |
| IA-8(6)[2]{2}[1] | особами, |
| IA-8(6)[2]{2}[2] | постачальниками послуг облікового запису |
| IA-8(6)[2]{2}[3] | перевіряючими сторонами. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; Записи перевірки PIV-I; докази посвідчення особи PIV-I; Дозвільні документи PIV-I; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал, відповідальний за управління обліковими записами].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що приймають та перевіряють облікові дані PIV-I]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IA-9 | ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IA-9[1] | IA-9[1][1] | організація визначає системні служби, які необхідно ідентифікувати та автентифікувати перш ніж встановлювати зв'язок з пристроями, користувачами або іншими послугами чи додатками. | |
| IA-9[1][2] | організація визначає системні додатки, які необхідно ідентифікувати та автентифікувати перш ніж встановлювати зв'язок з пристроями, користувачами або іншими послугами чи додатками. | |
| IA-9[2] | IA-9[2][1] | Ідентифікувати визначені організацією системні служби, перш ніж встановлювати зв'язок з: | |
| IA-9[2][1]{1} | пристроями |
| IA-9[2][1]{2} | користувачами |
| IA-9[2][1]{3} | іншими послугами чи додатками |
| IA-9[2][2] | Ідентифікувати визначені організацією додатки, перш ніж встановлювати зв'язок з: | |
| IA-9[2][2]{1} | пристроями |
| IA-9[2][2]{2} | користувачами |
| IA-9[2][2]{3} | іншими послугами чи додатками |
| IA-9[2][3] | Автентифікувати визначені організацією системні служби, перш ніж встановлювати зв'язок з: | |
| IA-9[2][3]{1} | пристроями |
| IA-9[2][3]{2} | користувачами |
| IA-9[2][3]{3} | іншими послугами чи додатками |
| IA-9[2][4] | Автентифікувати визначені організацією додатки, перш ніж встановлювати зв'язок з: | |
| IA-9[2][4]{1} | пристроями |
| IA-9[2][4]{2} | користувачами |
| IA-9[2][4]{3} | іншими послугами чи додатками |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації послуг; план безпеки; проєктна документація інформаційної системи; гарантії безпеки, що використовуються для ідентифікації та автентифікації служб інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал з обов'язками щодо ідентифікації та автентифікації].  Перевірка: [ВИБРАТИ З: Гарантії безпеки, що реалізують можливість ідентифікації та автентифікації служби] | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-9(1) | ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ - ОБМІН ІНФОРМАЦІЄЮ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-9(1)[1] | Переконатися, що постачальники послуг інформацію ідентифікації: | |
| IA-9(1)[1][1] | отримують |
| IA-9(1)[1][2] | перевіряють |
| IA-9(1)[1][3] | передають |
| IA-9(1)[2] | Переконатися, що постачальники послуг інформацію автентифікації: | |
| IA-9(1)[2][1] | отримують |
| IA-9(1)[2][2] | перевіряють |
| IA-9(1)[2][3] | передають |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації послуг; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за ідентифікацію та автентифікацію; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; постачальники послуг].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливості ідентифікації та аутентифікації служби]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-9(2) | ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ - ПЕРЕДАЧА РІШЕНЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IA-9(2)[1] | визначає політику організації щодо передачі рішення щодо ідентифікації та автентифікації між визначеними організацією послугами | |
| IA-9(2)[2] | організація визначає послуги, відповідно до політик організації, між якими будуть передавати рішення щодо ідентифікації та автентифікації | |
| IA-9(2)[3] | IA-9(2)[3][1] | Передавати рішення щодо ідентифікації між визначеними організацією послугами відповідно до політик організації. |
| IA-9(2)[3][2] | Передавати рішення щодо автентифікації між визначеними організацією послугами відповідно до політик організації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації послуг; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; записи передачі; записи перевірки передачі; правила прийняття рішень щодо ідентифікації та аутентифікації між організаційними службами; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за ідентифікацію та автентифікацію; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливості ідентифікації та аутентифікації служби]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IA-10 | АДАПТИВНА АВТЕНТИФІКАЦІЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IA-10[1] | організація визначає додаткові методи автентифікації | | |
| IA-10[2] | організація визначає додаткові механізми автентифікації | | |
| IA-10[3] | IA-10[3]{1} | організація визначає обставини | |
| IA-10[3]{2} | організація визначає ситуації | |
| IA-10[4] | IA-10[4]{1} | Вимагати, щоб особи, які отримують доступ до системи, використовували визначені організацією додаткові методи автентифікації відповідно до конкретних визначених організацією: | |
| IA-10[4]{1}{1} | обставин |
| IA-10[4]{1}{2} | ситуацій |
| IA-10[4]{2} | Вимагати, щоб особи, які отримують доступ до системи, використовували визначені організацією додаткові механізми автентифікації відповідно до конкретних визначених організацією: | |
| IA-10[4]{2}{1} | обставин |
| IA-10[4]{2}{2} | ситуацій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються методів або механізмів адаптивної / додаткової ідентифікації та автентифікації; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; додаткові методи та механізми ідентифікації та автентифікації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал з обов'язками щодо ідентифікації та автентифікації].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IA-11 | ПОВТОРНА АВТЕНТИФІКАЦІЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IA-11[1] | IA-11[1]{1} | організація визначає обставини, що вимагають повторної автентифікації | |
| IA-11[1]{2} | організація визначає ситуації, що вимагають повторної автентифікації | |
| IA-11[2] | IA-11[2][1] | Вимагати від користувачів повторної автентифікації, при: | |
| IA-11[2][1]{1} | визначених організацією обставинах, що вимагають повторної автентифікації |
| IA-11[2][1]{2} | визначених організацією ситуаціях, що вимагають повторної автентифікації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються повторної автентифікації користувачів та пристроїв; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік обставин або ситуацій, що вимагають повторної автентифікації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал з обов'язками щодо ідентифікації та автентифікації].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації] | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IA-12 | ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IA-12(a) | Засвідчити особи користувачів, яким потрібні облікові записи для логічного доступу до систем на основі вимог гарантій відповідного рівня, як це зазначено у відповідних стандартах і рекомендаціях | | |
| IA-12(b) | Встановити ідентифікатори користувачів унікальні для особи | | |
| IA-12(c) | IA-12(c)[1] | Докази (свідчення) ідентичності особи: | |
| IA-12(c)[1][1] | Збирати |
| IA-12(c)[1][2] | затверджувати |
| IA-12(c)[1][3] | перевіряти |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються повторної автентифікації користувачів та пристроїв; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік обставин або ситуацій, що вимагають повторної автентифікації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал з обов'язками щодо ідентифікації та автентифікації].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації] | | | |

|  |  |  |
| --- | --- | --- |
| IA-12(1) | ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - АВТОРИЗАЦІЯ СУПЕРВАЙЗЕРА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-12(1)[1] | Вимагати, щоб процес реєстрації для отримання облікового запису для логічного доступу включав авторизацію супервайзера. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються повторної автентифікації користувачів та пристроїв; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік обставин або ситуацій, що вимагають повторної автентифікації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал з обов'язками щодо ідентифікації та автентифікації].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації] | |

|  |  |  |
| --- | --- | --- |
| IA-12(2) | ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПОСВІДЧЕННЯ ОСОБИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-12(2)[1] | Необхідно пред'явити до реєстраційного органу докази індивідуальної ідентифікації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються повторної автентифікації користувачів та пристроїв; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік обставин або ситуацій, що вимагають повторної автентифікації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал з обов'язками щодо ідентифікації та автентифікації].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації] | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IA-12(3) | ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПЕРЕВІРКА ТА ВЕРИФІКАЦІЯ ДОКАЗІВ ІДЕНТИЧНОСТІ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IA-12(3)[1] | організація визначає методи перевірки доказів ідентичності | | |
| IA-12(3)[2] | організація визначає методи верифікації доказів ідентичності | | |
| IA-12(3)[3] | Організація вимагає, щоб надані ідентифікаційні свідчення: | | |
| IA-12(3)[3][1] | перевірялися через визначені організацією:. | |
| IA-12(3)[3][1][1] | методи перевірки |
| IA-12(3)[3][1][2] | методи верифікації |
| IA-12(3)[3][2] | верифікувалися через визначені організацією: | |
| IA-12(3)[3][2][1] | методи перевірки |
| IA-12(3)[3][2][2] | методи верифікації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються повторної автентифікації користувачів та пристроїв; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік обставин або ситуацій, що вимагають повторної автентифікації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал з обов'язками щодо ідентифікації та автентифікації].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації] | | | |

|  |  |  |
| --- | --- | --- |
| IA-12(4) | ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ОЧНА ПЕРЕВІРКА ТА ВЕРИФІКАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | |
| IA-12(4)[1] | призначає орган реєстрації у якому необхідно очно підтверджувати та перевіряти свідчення щодо ідентифікації. |
| IA-12(4)[2] | Вимагає, щоб підтвердження свідчень щодо ідентифікації проводилися очно у призначеному органі реєстрації. |
| IA-12(4)[3] | Вимагає, щоб перевірка свідчень щодо ідентифікації проводилися очно у призначеному органі реєстрації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються очної перевірки та верифікації; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал з обов'язками щодо ідентифікації та автентифікації].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації] | |

|  |  |  |  |
| --- | --- | --- | --- |
| IA-12(5) | ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПІДТВЕРДЖЕННЯ АДРЕСИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | |
| IA-12(5){1} | вимагає, щоб для перевірки фізичної адреси реєстрації користувачів: | |
| IA-12(5){1}[1] | реєстраційний код доставляється через зовнішній канал. |
| IA-12(5){1}[2] | повідомлення про перевірку доставляється через зовнішній канал. |
| IA-12(5){2} | вимагає, щоб для перевірки цифрової адреси реєстрації користувачів: | |
| IA-12(5){2}[1] | реєстраційний код доставляється через зовнішній канал. |
| IA-12(5){2}[2] | повідомлення про перевірку доставляється через зовнішній канал. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються підтвердження адреси; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал з обов'язками щодо ідентифікації та автентифікації].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації] | | |

|  |  |  |
| --- | --- | --- |
| IA-12(6) | ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПРИЙНЯТТЯ ІДЕНТИФІКАЦІЙ СХВАЛЕНИХ ТРЕТЬОЮ СТОРОНОЮ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IA-12(6)[1] | організація визначає рівень гарантії ідентичності для прийняття ідентичності, що підтверджена третьою стороною. |
| IA-12(6)[2] | організація приймає ідентичність, що підтверджена третьою стороною на рівень гарантії ідентичності, визначений організацією. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика ідентифікації та автентифікації; процедури, що стосуються прийняття ідентифікацій схвалених третьою стороною; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за функціонування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; організаційний персонал з обов'язками щодо ідентифікації та автентифікації].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації] | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ ІP – ІНДИВІДУАЛЬНА УЧАСТЬ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IP-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ ІНДИВІДУАЛЬНОЇ УЧАСТІ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| IP-1(a) | IP-1(a)[1] | IP-1(a)[1](1) | | | Розробляє та документує політику індивідуальної участі, яка: | | | | | | | | |
| IP-1(a)[1](1)(a) | | Містить: | | | | | | |
| IP-1(a)[1](1)(a)[1] | | | | мету, | | |
| IP-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| IP-1(a)[1](1)(a)[3] | | | | ролі, | | |
| IP-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| IP-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| IP-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| IP-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| IP-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| IP-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| IP-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| IP-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| IP-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| IP-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| IP-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| IP-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| IP-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики індивідуальної участі, а також пов'язаних з ними заходів індивідуальної участі; | | | | | | | | |
| IP-1(a)[2] | IP-1(a)[2]{1} | | | IP-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика індивідуальної участі | | | | | |
| IP-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики індивідуальної участі та пов'язаних з нею заходів захисту політики індивідуальної участі | | | | | |
| IP-1(a)[2]{2} | | | IP-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика індивідуальної участі | | | | | |
| IP-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики індивідуальної участі та пов'язаних з нею заходів захисту політики індивідуальної участі | | | | | |
| IP-1(a)[3] | IP-1(a)[3]{1} | | | IP-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику індивідуальної участі | | | | | | | |
| IP-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| IP-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| IP-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| IP-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| IP-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| IP-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| IP-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| IP-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| IP-1(a)[3](1)(b) | | | Відповідає: | | | | |
| IP-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| IP-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| IP-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| IP-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| IP-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| IP-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| IP-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| IP-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації захисту індивідуальної участі та відповідних заходів індивідуальної участі | | | | | | | |
| IP-1(a)[3]{2} | | | IP-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику захисту індивідуальної участі, яка: | | | | | | | |
| IP-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| IP-1(a)[3]{2}(1)(а)[1] | | мету, | |
| IP-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| IP-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| IP-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| IP-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| IP-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| IP-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| IP-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| IP-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| IP-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| IP-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| IP-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| IP-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| IP-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| IP-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| IP-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики індивідуальної участі та пов'язаних з нею заходів індивідуальної участі | | | | | | | |
| IP-1(b) | IP-1(b)[1] | визначає посадову особу для управління політикою та процедурами індивідуальної участі | | | | | | | | | | | |
| IP-1(b)[2] | призначає посаду для управління політикою та процедурами індивідуальної участі | | | | | | | | | | | |
| IP-1(с) | IP-1(с)[1] | IP-1(с)[1](1) | | IP-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики індивідуальної участі | | | | | | | |
| IP-1(с)[1](1)[2] | | переглядає поточну політику індивідуальної участі з визначеною організацією частотою | | | | | | | |
| IP-1(с)[1](2) | | IP-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур індивідуальної участі | | | | | | | |
| IP-1(с)[1](2)[2] | | переглядає поточні процедури індивідуальної участі з визначеною організацією частотою | | | | | | | |
| IP-1(с)[2] | IP-1(с)[2](1) | | IP-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики індивідуальної участі | | | | | | | |
| IP-1(с)[2](1)[2] | | оновлює поточну політику індивідуальної участі з визначеною організацією частотою | | | | | | | |
| IP-1(с)[2](2) | | IP-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур індивідуальної участі | | | | | | | |
| IP-1(с)[2](2)[2] | | оновлює поточні процедури індивідуальної участі з визначеною організацією частотою | | | | | | | |
| IP-1(d) | переконується, що процедури індивідуальної участі реалізують політику та заходи індивідуальної участі | | | | | | | | | | | | |
| IP-1(e) | IP-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики індивідуальної участі | | | | | | | | | | |
| IP-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики індивідуальної участі | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури індивідуальної участі; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику індивідуальної участі; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| IP-2 | ЗГОДА | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| IP-2[1] | IP-2[1]{1} | Організація визначає інструменти, щоб користувачі дозволяли обробку своїх персональних даних перед їх збиранням | | | |
| IP-2[1]{2} | Організація визначає механізми, щоб користувачі дозволяли обробку своїх персональних даних перед їх збиранням | | | |
| IP-2[2] | IP-2[2]{1} | Впровадити визначені організацією інструменти, щоб користувачі дозволяли обробку своїх персональних даних перед їх збиранням, які: | | | |
| IP-2[2]{1}(a) | IP-2[2]{1}(a)[1] | Використовують просту форму | |
| IP-2[2]{1}(a)[2] | містять приклади для ілюстрації потенційних ризиків приватності; | |
| IP-2[2]{1}(b) | Надають засоби для користувачів, щоб відмовитися від авторизації | | |
| IP-2[2]{2} | Впровадити визначені організацією механізми, щоб користувачі дозволяли обробку своїх персональних даних перед їх збиранням, які: | | | |
| IP-2[2]{2}(a) | IP-2[2]{2}(a)[1] | | Використовують просту форму |
| IP-2[2]{2}(a)[2] | | містять приклади для ілюстрації потенційних ризиків приватності; |
| IP-2[2]{2}(b) | Надають засоби для користувачів, щоб відмовитися від авторизації | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР:: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | | | | |

|  |  |  |
| --- | --- | --- |
| IP-2(1) | ЗГОДА - УПРАВЛІННЯ АТРИБУТАМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IP-2(1)[1] | Дозволити суб'єктам даних налаштовувати дозволи на використання для обраних атрибутів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління атрибутами; процедури, що стосуються атрибутів, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують управління атрибутів]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| IP-2(2) | ЗГОДА - СВОЄЧАСНЕ ПОВІДОМЛЕННЯ ПРО ЗГОДУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IP-2(2)[1] | організація визначає частоту надання повноваження на обробку персональних даних | |
| IP-2(2)[2] | IP-2(2)[2]{1} | Надати повноваження на обробку персональних даних у поєднанні з діями відносно даних |
| IP-2(2)[2]{2} | Надати повноваження на обробку персональних даних у поєднанні з визначеною організацією частотою. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IP-3 | ВИПРАВЛЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IP-3[1] | Встановити процес для того, щоб особи, які мають неточні персональні дані, що зберігається організацією, могли: | |
| IP-3[1]{1} | скоригувати |
| IP-3[1]{2} | змінити неточні персональні дані; |
| IP-3[2] | впровадити процес для того, щоб особи, які мають неточні персональні дані, що зберігається організацією, могли: | |
| IP-3[2]{1} | скоригувати |
| IP-3[2]{2} | змінити неточні персональні дані; |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | |

|  |  |  |
| --- | --- | --- |
| IP-3(1) | ВИПРАВЛЕННЯ - ПОВІДОМЛЕННЯ ПРО ВНЕСЕННЯ ПОПРАВОК АБО ЗМІН | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IP-3(1)[1] | Повідомляти осіб про внесення змін або поправок в їх персональній дані |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| IP-3(2) | ВИПРАВЛЕННЯ - ЗВЕРНЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IP-3(2){1} | IP-3(2){1}[1] | організація визначає процес для осіб, які можуть оскаржити несприятливе рішення |
| IP-3(2){1}[2] | Впровадити визначений організацією процес для осіб, які можуть оскаржити несприятливе рішення. |
| IP-3(2){2} | IP-3(2){2}[1] | організація визначає процес для осіб, які можуть змінити некоректну інформацію |
| IP-3(2){2}[2] | Впровадити визначений організацією процес для осіб, які можуть змінити некоректну інформацію. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP-4 | ПОВІДОМЛЕННЯ ПРО ПРИВАТНІСТЬ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IP-4[a] | IP-4[a][1] | організація визначає частоту з якою повідомляє фізичних осіб про забезпечення приватності. | |
| IP-4[a][2] | Зробити повідомлення, про забезпечення приватності, доступним для фізичних осіб: | |
| IP-4[2][1] | під час першої взаємодії з організацією, |
| IP-4[2][2] | потім з визначеною організацією частотою |
| IP-4[b] | Забезпечити, що повідомлення про приватність є зрозумілими та простими, надають інформацію про обробку персональних даних простою та зрозумілою мовою. | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IP-4(1) | ПОВІДОМЛЕННЯ ПРО ПРИВАТНІСТЬ - СВОЄЧАСНЕ ПОВІДОМЛЕННЯ ПРО ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IP-4(1)[1] | організація визначає частоту надання дозволу на обробку даних | |
| IP-4(1)[2] | IP-4(1)[2]{1} | Надати дозвіл на обробку персональних даних у поєднанні з діями над даними |
| IP-4(1)[2]{2} | Надати дозвіл на обробку персональних даних з частотою, визначеною організацією. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IP-5 | ЗАЯВИ ПРО ПРИВАТНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IP-5(a) | IP-5(a){1} | Включати вимоги Законодавства про захист персональних даних до організаційних форм, які збирають персональні дані |
| IP-5(a){2} | Включати вимоги Законодавства про захист персональних даних в окремих формах, які можуть зберігатись окремими особами |
| IP-5(b) | Ознайомити в усній формі особу з Заявою про захист персональних даних до початку збору персональних даних. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | |

|  |  |  |
| --- | --- | --- |
| IP-6 | ІНДИВІДУАЛЬНИЙ ДОСТУП | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IP-6[1] | Забезпечити фізичним особам можливість отримати доступ до своїх персональних даних, що зберігаються в організації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ IR – РЕАГУВАННЯ НА ІНЦИДЕНТИ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IR-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ РЕАГУВАННЯ НА ІНЦИДЕНТИ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| IR-1(a) | IR-1(a)[1] | IR-1(a)[1](1) | | | Розробляє та документує політику реагування на інциденти, яка: | | | | | | | | |
| IR-1(a)[1](1)(a) | | Містить: | | | | | | |
| IR-1(a)[1](1)(a)[1] | | | | мету, | | |
| IR-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| IR-1(a)[1](1)(a)[3] | | | | ролі, | | |
| IR-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| IR-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| IR-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| IR-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| IR-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| IR-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| IR-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| IR-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| IR-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| IR-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| IR-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| IR-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| IR-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики реагування на інциденти та відповідних заходів управління доступом | | | | | | | | |
| IR-1(a)[2] | IR-1(a)[2]{1} | | | IR-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика індивідуальної участі | | | | | |
| IR-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики реагування на інциденти та пов'язаних з нею заходів реагування на інциденти | | | | | |
| IR-1(a)[2]{2} | | | IR-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика реагування на інциденти | | | | | |
| IR-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики реагування на інциденти та пов'язаних з нею заходів реагування на інциденти | | | | | |
| IR-1(a)[3] | IR-1(a)[3]{1} | | | IR-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику реагування на інциденти, яка: | | | | | | | |
| IR-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| IR-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| IR-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| IR-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| IR-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| IR-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| IR-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| IR-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| IR-1(a)[3](1)(b) | | | Відповідає: | | | | |
| IR-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| IR-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| IR-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| IR-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| IR-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| IR-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| IR-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| IR-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації політики реагування на інциденти та відповідних заходів управління доступом | | | | | | | |
| IR-1(a)[3]{2} | | | IR-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику реагування на інциденти, яка: | | | | | | | |
| IR-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| IR-1(a)[3]{2}(1)(а)[1] | | мету, | |
| IR-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| IR-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| IR-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| IR-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| IR-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| IR-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| IR-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| IR-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| IR-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| IR-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| IR-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| IR-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| IR-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| IR-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| IR-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики реагування на інциденти та пов'язаних з нею заходів реагування на інциденти; | | | | | | | |
| IR-1(b) | IR-1(b)[1] | визначає посадову особу для управління політикою та процедурами реагування на інциденти | | | | | | | | | | | |
| IR-1(b)[2] | призначає посаду для управління політикою та процедурами реагування на інциденти | | | | | | | | | | | |
| IR-1(с) | IR-1(с)[1] | IR-1(с)[1](1) | | IR-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики реагування на інциденти | | | | | | | |
| IR-1(с)[1](1)[2] | | переглядає поточну політику реагування на інциденти з визначеною організацією частотою | | | | | | | |
| IR-1(с)[1](2) | | R-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур реагування на інциденти | | | | | | | |
| IP-1(с)[1](2)[2] | | переглядає поточні процедури індивідуальної участі з визначеною організацією частотою | | | | | | | |
| IR-1(с)[2] | IR-1(с)[2](1) | | IR-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики реагування на інциденти | | | | | | | |
| IP-1(с)[2](1)[2] | | оновлює поточну політику реагування на інциденти з визначеною організацією частотою | | | | | | | |
| IR-1(с)[2](2) | | IR-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур реагування на інциденти | | | | | | | |
| IR-1(с)[2](2)[2] | | оновлює поточні процедури реагування на інциденти з визначеною організацією частотою | | | | | | | |
| IR-1(d) | переконується, що процедури реагування на інциденти реалізують політику та заходи реагування на інциденти | | | | | | | | | | | | |
| IR-1(e) | IR-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики реагування на інциденти | | | | | | | | | | |
| IR-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики реагування на інциденти | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури реагування на інциденти; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику реагування на інциденти; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IR-2 | НАВЧАННЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| IR-2[1] | IR-2[1][1] | Організація призначає ролі, за якими необхідно проводити навчання користувачів про систему реагування на інциденти | | |
| IR-2[1][2] | Організація призначає обов'язки, за якими необхідно проводити навчання користувачів про систему реагування на інциденти | | |
| IR-2[1][3] | Організація визначає період часу, коли необхідно брати на себе авторизовану роль або відповідальність за реагування інциденти; | | |
| IR-2[1][4] | Визначає частоту з якою необхідно проводити навчання користувачів про систему реагування на інциденти. | | |
| IR-2[2] | IR-2[2](a) | Організація забезпечує навчання користувачів про систему реагування на інциденти, відповідно до призначених ролей в рамках визначеного організацією період часу коли необхідно брати на себе: | | |
| IR-2[2](a){1} | | авторизовану роль |
| IR-2[2](a){2} | | відповідальність за реагування інциденти; |
| IR-2[2](b) | Забезпечити навчання користувачів про систему реагування на інциденти, відповідно до призначених ролей у разі внесення змін у системі | | |
| IR-2[2](c) | Забезпечити навчання користувачів про систему реагування на інциденти, відповідно до призначених ролей з визначеною організацією частотою надалі. | | |
| IR-2[3] | IR-2[3](a) | Забезпечити навчання користувачів про систему реагування на інциденти, відповідно до призначених обов'язків в рамках визначеного організацією період часу коли необхідно брати на себе: | | |
| IR-2[3](a){1} | авторизовану роль | |
| IR-2[3](a){2} | відповідальність за реагування інциденти; | |
| IR-2[3](b) | Забезпечити навчання користувачів про систему реагування на інциденти, відповідно до призначених обов'язків у разі внесення змін у системі | | |
| IR-2[3](c) | Забезпечити навчання користувачів про систему реагування на інциденти, відповідно до призначених обов'язків з визначеною організацією частотою надалі. | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються навчання реагування на інциденти; навчальна програма з реагування на інциденти; навчальні матеріали щодо реагування на інциденти; план безпеки; план реагування на інциденти; план безпеки; записи навчання реагування на інциденти; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який пройшов навчання з реагування на інциденти та виконував оперативні обов’язки; організаційний персонал, який відповідає за інформаційну безпеку]. | | | | |

|  |  |  |
| --- | --- | --- |
| IR-2(1) | НАВЧАННЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ - МОДЕЛЮВАННЯ ПОДІЙ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-2(1)[1] | Організація моделює події реагування на інциденти для забезпечення ефективного реагування персоналу в кризових ситуаціях. |
| IR-2(1)[2] | Організація впроваджує у процес навчання моделювання події реагування на інциденти для забезпечення ефективного реагування персоналу в кризових ситуаціях. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються навчання реагування на інциденти; Навчальна програма з реагування на інциденти; навчальні матеріали щодо реагування на інциденти; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який пройшов навчання з реагування на інциденти та відповідав за оперативні обов’язки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують змодельовані події для навчання реагування на інциденти]. | |

|  |  |  |
| --- | --- | --- |
| IR-2(2) | НАВЧАННЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ - АВТОМАТИЗОВАНІ НАВЧАЛЬНІ СЕРЕДОВИЩА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-2(2)[1] | Організація будує навчальне середовище реагування на інциденти |
| IR-2(2)[2] | Організація використовує автоматизовані механізми для побудови більш ретельного та реалістичного навчального середовища реагування на інциденти. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються навчання реагування на інциденти; Навчальна програма з реагування на інциденти; навчальні матеріали щодо реагування на інциденти; автоматизовані механізми, що підтримують навчання з реагування на інциденти; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який пройшов навчання з реагування на інциденти та відповідає за оперативні обов’язки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що забезпечують ретельне та реалістичне навчальне середовище реагування на аварії]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| IR-3 | ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IR-3[1] | організація визначає частоту з якою необхідно перевіряти спроможність системи реагувати на інциденти | |
| IR-3[2] | організація визначає тести для визначення ефективності реагування на інциденти | |
| IR-3[3] | IR-3[3][1] | Перевіряти спроможність системи реагувати на інциденти з визначеною організацією частотою за допомогою визначених організацією тестів для визначення ефективності реагування на інциденти |
| IR-3[3][2] | документувати результати тестування для визначення ефективності реагування на інциденти. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на аварії; політика планування на випадок непередбачених ситуацій; процедури, що стосуються тестування реагування на аварії; процедури, що стосуються тестування плану дій на випадок непередбачених ситуацій; матеріал для тестування реакції на аварії; результати випробувань реакції на аварії; план випробувань реагування на аварії; план реагування на аварії; резервний план; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за тестування реагування на аварії; організаційний персонал, який відповідає за інформаційну безпеку]. | | |

|  |  |  |
| --- | --- | --- |
| IR-3(1) | ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ - АВТОМАТИЧНЕ ТЕСТУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-3(1)[1] | Використовувати автоматизовані механізми для більш ретельного та ефективного тестування можливостей реагування на інциденти. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; політика планування на випадок непередбачених ситуацій; процедури, що стосуються тестування реагування на інциденти; процедури, що стосуються тестування плану дій на випадок непередбачених ситуацій; документація на тестування реагування на інциденти; результати випробувань реакції на інциденти; план випробувань реагування на інциденти; план реагування на інциденти; резервний план; план безпеки; автоматизовані механізми, що підтримують тести реагування на інциденти; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за тестування реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку]  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, які ретельніше та ефективніше перевіряють можливість реагування на інциденти]. | |

|  |  |  |
| --- | --- | --- |
| IR-3(2) | ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ - КООРДИНАЦІЯ З ПОВ'ЯЗАНИМИ ПЛАНАМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-3(2)[1] | Визначити організаційні елементи, що відповідають за плани пов'язані з тестування реагування на інциденти |
| IR-3(2)[2] | Координувати тестування реагування на інциденти з організаційними елементами, що відповідають за пов'язані плани. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; політика планування на випадок непередбачених ситуацій; процедури, що стосуються тестування реагування на інциденти; документація на тестування реакції на аварії план реагування на інциденти; плани безперервності бізнесу; плани на випадок непередбачених ситуацій; плани аварійного відновлення; плани безперервності операцій; кризові плани комунікацій; плани критичної інфраструктури; плани надзвичайних ситуацій для пасажирів; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за тестування реагування на інциденти; організаційний персонал, відповідальний за тестування організаційних планів, пов’язаних з тестуванням реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IR-3(3) | ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ - ПОСТІЙНЕ ПОКРАЩЕННЯ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| IR-3(3)[1] | Використовувати якісні дані за результатами тестування для: | | | |
| IR-3(3)[1](a) | визначення ефективності процесів реагування на інциденти | | |
| IR-3(3)[1](b) | постійного вдосконалення процесів реагування на інциденти, включаючи передову практику інформаційної безпеки | | |
| IR-3(3)[1](c) | IR-3(3)[1](c)[1] | впровадження показників реагування на інциденти які є: | |
| IR-3(3)[1](c)[1][1] | точними, |
| IR-3(3)[1](c)[1][2] | послідовними |
| IR-3(3)[1](c)[1][3] | відтворюваними |
| IR-3(3)[1](c)[2] | впровадження метрик реагування на інциденти які є: | |
| IR-3(3)[1](c)[2][1] | точними, |
| IR-3(3)[1](c)[2][2] | послідовними |
| IR-3(3)[1](c)[2][3] | відтворюваними |
| IR-3(3)[2] | Використовувати кількісні дані за результатами тестування для: | | | |
| IR-3(3)[2](a) | визначення ефективності процесів реагування на інциденти | | |
| IR-3(3)[2](b) | постійного вдосконалення процесів реагування на інциденти, включаючи передову практику інформаційної безпеки | | |
| IR-3(3)[2](c) | IR-3(3)[2](c)[1] | впровадження показників реагування на інциденти які є: | |
| IR-3(3)[2](c)[1][1] | точними, |
| IR-3(3)[2](c)[1][2] | послідовними |
| IR-3(3)[2](c)[1][3] | відтворюваними |
| IR-3(3)[2](c)[2] | впровадження метрик реагування на інциденти які є: | |
| IR-3(3)[2](c)[2][1] | точними, |
| IR-3(3)[2](c)[2][2] | послідовними |
| IR-3(3)[2](c)[2][3] | відтворюваними |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; політика планування на випадок непередбачених ситуацій; процедури, що стосуються тестування реагування на інциденти; документація на тестування реакції на аварії план реагування на інциденти; плани безперервності бізнесу; плани на випадок непередбачених ситуацій; плани аварійного відновлення; плани безперервності операцій; кризові плани комунікацій; плани критичної інфраструктури; плани надзвичайних ситуацій для пасажирів; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за тестування реагування на інциденти; організаційний персонал, відповідальний за тестування організаційних планів, пов’язаних з тестуванням реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку]. | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IR-4 | ОБРОБКА ІНЦИДЕНТУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IR-4(a) | Впровадити можливості обробки інцидентів безпеки та приватності, включаючи: | | |
| IR-4(a)[1] | підготовку, | |
| IR-4(a)[2] | виявлення | |
| IR-4(a)[3] | аналіз, | |
| IR-4(a)[4] | стримування, | |
| IR-4(a)[5] | ліквідацію | |
| IR-4(a)[6] | відновлення | |
| IR-4(b) | Координувати діяльність з обробки інцидентів зі заходами з забезпечення безперервності функціонування | | |
| IR-4(c) | Включати уроки, що отримані з поточних дій з обробки інцидентів та вносити відповідні зміни, в: | | |
| IR-4(c)[1] | процедури реагування на інциденти, | |
| IR-4(c)[2] | навчання та | |
| IR-4(c)[3] | тестування | |
| IR-4(d) | IR-4(d)[1] | Забезпечити можливість порівняти у всій організації: | |
| IR-4(d)[1][1] | Строгість діяльності по обробці інцидентів |
| IR-4(d)[1][2] | Інтенсивність діяльності по обробці інцидентів |
| IR-4(d)[1][3] | обсяг діяльності по обробці інцидентів |
| IR-4(d)[1][4] | результати діяльності по обробці інцидентів |
| IR-4(d)[2] | Забезпечити можливість передбачити у всій організації: | |
| IR-4(d)[2][1] | Строгість діяльності по обробці інцидентів |
| IR-4(d)[2][2] | Інтенсивність діяльності по обробці інцидентів |
| IR-4(d)[2][3] | обсяг діяльності по обробці інцидентів |
| IR-4(d)[2][4] | результати діяльності по обробці інцидентів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; політика планування на випадок непередбачених ситуацій; процедури, що стосуються врегулювання інцидентів; план реагування на інциденти; резервний план; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, відповідальний за планування на випадок непередбачених ситуацій; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Можливість організації обробки випадків] | | | |

|  |  |  |
| --- | --- | --- |
| IR-4(1) | ОБРОБКА ІНЦИДЕНТУ - АВТОМАТИЗОВАНІ ПРОЦЕСИ ОБРОБКИ ІНЦИДЕНТІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-4(1)[1] | Використовувати автоматизовані механізми для підтримки процесу обробки інцидентів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; автоматизовані механізми, що підтримують обробку інцидентів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують процес обробки інцидентів]. | |

|  |  |  |
| --- | --- | --- |
| IR- 4(2) | ОБРОБКА ІНЦИДЕНТУ - ДИНАМІЧНА РЕКОНФІГУРАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR- 4(2)[1] | організація визначає системні компоненти у яких необхідно включити динамічну реконфігурацію |
| IR- 4(2)[2] | Включити динамічну реконфігурацію у визначених організацією системних компонентах як частину здатності реагування на інциденти. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; автоматизовані механізми, що підтримують обробку інцидентів; перелік системних компонентів, що підлягають динамічному переконфігуруванню як частина можливості реагування на інциденти; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують динамічну реконфігурацію компонентів як частину реагування на інциденти] | |

|  |  |  |  |
| --- | --- | --- | --- |
| IR-4(3) | ОБРОБКА ІНЦИДЕНТУ - БЕЗПЕРЕРВНІСТЬ ОПЕРАЦІЙ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IR-4(3)[1] | організація визначає класи інцидентів | |
| IR-4(3)[2] | організація визначає дії, які необхідно вжити у відповідь згідно з класом інциденту | |
| IR-4(3)[3] | Ідентифікувати визначені організацією класи інцидентів та визначені організацією дії, які необхідно вжити у відповідь згідно з класом інциденту для: | |
| IR-4(3)[3][1] | забезпечення безперервності виконання організаційних завдань |
| IR-4(3)[3][2] | забезпечення безперервності виконання організаційних функцій. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; план реагування на інциденти; план безпеки; перелік класів інцидентів; перелік відповідних дій з реагування на події; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують безперервність операцій]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IR-4(4) | ОБРОБКА ІНЦИДЕНТУ - ІНФОРМАЦІЙНА КОРЕЛЯЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IR-4(4)[1] | Зіставляти інформацію про інцидент та про індивідуальне реагування на інцидент з метою: | |
| IR-4(4)[1][1] | досягнення загальноорганізаційного бачення на обізнаність про інциденти |
| IR-4(4)[1][2] | реагування на інцидент. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються обробки інцидентів; план реагування на інциденти; план безпеки; автоматизовані механізми, що підтримують кореляцію подій та інцидентів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; журнали кореляції управління інцидентами; журнали кореляції управління подіями; інформація про безпеку та журнали управління подіями; звіти про кореляцію управління інцидентами; звіти про кореляцію управління подіями; інформація про безпеку та звіти про управління подіями; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, з яким слід співвідносити інформацію про події та реагування на окремі події].  Перевірка: [ВИБРАТИ З: Організаційні процеси для співвіднесення інформації про події та індивідуальних реакцій на події; автоматизовані механізми, що підтримують та / або впроваджують співвідношення інформації про реакцію на події з окремими реакціями на події]. | | |

|  |  |  |
| --- | --- | --- |
| IR-4(5) | ОБРОБКА ІНЦИДЕНТУ - АВТОМАТИЧНЕ ВИМКНЕННЯ СИСТЕМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-4(5)[1] | організація визначає порушення безпеки за яких необхідно автоматичного вимикати систему |
| IR-4(5)[2] | розробити налаштовувані можливості для автоматичного вимикання системи, якщо виявлено визначені організацією порушення безпеки. |
| IR-4(5)[3] | Реалізувати налаштовувані можливості для автоматичного вимикання системи, якщо виявлено визначені організацією порушення безпеки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; автоматизовані механізми, що підтримують обробку інцидентів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, який відповідає за інформаційну безпеку; розробники системи].  Перевірка: [ВИБРАТИ З: Можливість організації обробки інциденти; автоматизовані механізми, що підтримують та / або реалізують автоматичне відключення інформаційної системи] | |

|  |  |  |
| --- | --- | --- |
| IR-4(6) | ОБРОБКА ІНЦИДЕНТУ - ВНУТРІШНІ ЗАГРОЗИ - ОСОБЛИВІ МОЖЛИВОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-4(6)[1] | Реалізувати можливість обробки інцидентів, пов'язаних з внутрішніми загрозами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; автоматизовані механізми, що підтримують обробку інцидентів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; план реагування на інциденти; план безпеки; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ ВІД: Можливість організації обробки випадків] | |

|  |  |  |  |
| --- | --- | --- | --- |
| IR-4(7) | ОБРОБКА ІНЦИДЕНТУ - ВНУТРІШНІ ЗАГРОЗИ - ВНУТРІШНЬООРГАНІЗАЦІЙНА КООРДИНАЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IR-4(7)[1] | IR-4(7)[1]{1} | організація визначає компоненти організації через яку координують здатність обробки інцидентів для внутрішніх загроз |
| IR-4(7)[1]{2} | організація визначає елементи організації через яку координують здатність обробки інцидентів для внутрішніх загроз |
| IR-4(7)[2] | IR-4(7)[2]{1} | Координувати здатність обробки інцидентів для внутрішніх загроз через визначені організацією компоненти організації. |
| IR-4(7)[2]{2} | Координувати здатність обробки інцидентів для внутрішніх загроз через визначені організацією елементи організації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал / елементи, з якими слід узгоджувати можливості поводження з інцидентами].  Перевірка: [ВИБРАТИ З: Організаційні процеси для координації обробки інцидентів]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IR-4(8) | ОБРОБКА ІНЦИДЕНТУ - КООРДИНАЦІЯ З ЗОВНІШНІМИ ОРГАНІЗАЦІЯМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IR-4(8)[1] | IR-4(8)[1][1] | організація визначає зовнішні організації з якими координують для зіставлення та поширення інформації, що визначається організацією. | |
| IR-4(8)[1][2] | організація визначає інформацію, яка необхідна для досягнення міжорганізаційного бачення на обізнаність про інциденти та більш ефективного реагування на інциденти. | |
| IR-4(8)[2] | IR-4(8)[2][1] | Координувати з визначеними організацією зовнішніми організаціями для зіставлення інформації, що визначається організацією, для: | |
| IR-4(8)[2][1][1] | досягнення міжорганізаційного бачення на обізнаність про інциденти |
| IR-4(8)[2][1][2] | більш ефективного реагування на інциденти. |
| IR-4(8)[2][2] | Координувати з визначеними організацією зовнішніми організаціями для поширення інформації, що визначається організацією, для: | |
| IR-4(8)[2][2][1] | досягнення міжорганізаційного бачення на обізнаність про інциденти |
| IR-4(8)[2][2][2] | більш ефективного реагування на інциденти. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються обробки інцидентів; перелік зовнішніх організацій; записи координації обробки подій із зовнішніми організаціями; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, який відповідає за інформаційну безпеку; персонал із зовнішніх організацій, з якими слід координувати / обмінюватися / співвідносити інформацію щодо реагування на події].  Перевірка: [ВИБРАТИ З: Організаційні процеси для узгодження інформації про обробку інцидентів із зовнішніми організаціями]. | | | |

|  |  |  |
| --- | --- | --- |
| IR-4(9) | ОБРОБКА ІНЦИДЕНТУ - ЗДАТНІСТЬ ДИНАМІЧНОГО РЕАГУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-4(9)[1] | організація визначає можливості динамічного реагування для ефективного реагування на інциденти безпеки. |
| IR-4(9)[2] | Використовувати визначені організацією можливості динамічного реагування для ефективного реагування на інциденти безпеки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються обробки інцидентів; автоматизовані механізми, що підтримують можливості динамічного реагування; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; план реагування на інциденти; план безпеки; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для можливості динамічного реагування; автоматизовані механізми, що підтримують та / або реалізують можливість динамічного реагування для організації] | |

|  |  |  |
| --- | --- | --- |
| IR-4(10) | ОБРОБКА ІНЦИДЕНТУ - КООРДИНАЦІЯ ЛАНЦЮГА ПОСТАЧАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-4(10)[1] | Координувати діяльність з обробки інцидентів, пов'язану з подіями ланцюжка постачання, з іншими організаціями, що беруть участь у ланцюжку постачання. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються координації ланцюгів постачання; договори придбання; угоди про рівень обслуговування; план реагування на інциденти; план безпеки; плани реагування на інциденти іншої організації, яка бере участь у діяльності ланцюга постачання; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обробку інцидентів; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за ланцюжки постачання]. | |

|  |  |  |
| --- | --- | --- |
| IR-5 | МОНІТОРИНГ ІНЦИДЕНТУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-5[1] | Відстежувати та документувати інциденти безпеки |
| IR-5[2] | Відстежувати та документувати інциденти приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З:: Політика реагування на інциденти; процедури, що стосуються моніторингу інцидентів; записи та документація щодо реагування на інциденти; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за моніторинг інцидентів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Можливість організації моніторингу інцидентів; автоматизовані механізми, що підтримують та / або реалізують відстеження та документування системних інцидентів]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| IR-5(1) | МОНІТОРИНГ ІНЦИДЕНТУ - АВТОМАТИЗОВАНЕ ВІДСТЕЖЕННЯ, ЗБІР ДАНИХ ТА АНАЛІЗ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IR-5(1)[1] | Використовувати автоматизовані механізми для: | |
| IR-5(1)[1] | відстеження інцидентів безпеки |
| IR-5(1)[1] | відстеження інцидентів приватності |
| IR-5(1)[1] | збору інформації про інциденти. |
| IR-5(1)[1] | аналізу інформації про інциденти |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються моніторингу інцидентів; автоматизовані механізми, що підтримують моніторинг інцидентів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; план реагування на інциденти; план безпеки; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за моніторинг інцидентів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що допомагають відстежувати інциденти безпеки та збирати та аналізувати інформацію про інциденти]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IR-6 | ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IR-6(a) | IR-6(a)[1] | організація визначає період часу впродовж якого персонал має повідомляти про підозрілі інциденти з безпеки та приватності відповідно до організаційної спроможності реагування на інциденти впродовж | |
| IR-6(a)[2] | IR-6(a)[2][1] | Вимагати від персоналу повідомляти про підозрілі інциденти з безпеки відповідно до організаційної спроможності реагування на інциденти впродовж визначеного організацією періоду часу |
| IR-6(a)[2][2] | Вимагати від персоналу повідомляти про підозрілі інциденти з приватності відповідно до організаційної спроможності реагування на інциденти впродовж визначеного організацією періоду часу |
| IR-6(b) | IR-6(b)[1] | організація визначає уповноважений орган до якого звітують про інциденти безпеки, приватності та ланцюжка постачання в | |
| IR-6(b)[2] | Звітувати в визначений організацією уповноважений орган про: | |
| IR-6(b)[2][1] | інциденти безпеки, |
| IR-6(b)[2][2] | приватності |
| IR-6(b)[2][3] | ланцюжка постачання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються повідомлення про інциденти; записи та документація про повідомлення про події; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за повідомлення про інциденти; організаційний персонал, який відповідає за інформаційну безпеку; персонал, який мав / повинен був повідомити про інциденти; персонал (органи влади), якому слід повідомляти інформацію про події].  Перевірка: [ВИБРАТИ З: Організаційні процеси для повідомлення про інциденти; автоматизовані механізми, що підтримують та / або впроваджують повідомлення про інциденти]. | | | |

|  |  |  |
| --- | --- | --- |
| IR-6(1) | ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ - АВТОМАТИЧНЕ ЗВІТУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-6(1)[1] | Використовувати автоматичні механізми звітування про інциденти безпеки |
| IR-6(1)[2] | Використовувати автоматичні механізми звітування про інциденти приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються повідомлення про інциденти; автоматизовані механізми підтримки повідомлення про події; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; план реагування на аварії; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за повідомлення про інциденти; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для повідомлення про інциденти; автоматизовані механізми, що підтримують та / або впроваджують звітування про інциденти безпеки]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IR-6(2) | ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ - ВРАЗЛИВІСТЬ, ПОВ'ЯЗАНА З ІНЦИДЕНТАМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IR-6(2)[1] | IR-6(2)[1]{1} | організація визначає персонал, яким необхідно повідомляти про вразливості системи, пов'язані з зареєстрованими інцидентами безпеки та приватності | |
| IR-6(2)[1]{2} | організація визначає ролі, яким необхідно повідомляти про вразливості системи, пов'язані з зареєстрованими інцидентами безпеки та приватності | |
| IR-6(2)[2] | IR-6(2)[2]{1} | Повідомляти визначений організацією персонал про вразливості системи, пов'язані з зареєстрованими інцидентами: | |
| IR-6(2)[2]{1}[1] | безпеки |
| IR-6(2)[2]{1}[2] | приватності |
| IR-6(2)[2]{2} | Повідомляти визначені організацією ролі про вразливості системи, пов'язані з зареєстрованими інцидентами: | |
| IR-6(2)[2]{1}[1] | безпеки |
| IR-6(2)[2]{1}[2] | приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються повідомлення про інциденти; план реагування на інциденти; план безпеки; звіти про інциденти безпеки та пов'язані з ними вразливості інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за повідомлення про інциденти; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; персонал, якому повідомляється про вразливості, пов'язані з інцидентами безпеки].  Перевірка: [ВИБРАТИ З:Організаційні процеси для повідомлення про інциденти; автоматизовані механізми, що підтримують та / або впроваджують повідомлення про вразливості, пов'язані з інцидентами безпеки]. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IR-6(3) | ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ - КООРДИНАЦІЯ ЛАНЦЮЖКА ПОСТАЧАННЯ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| IR-6(3)[1] | Надати інформацію про інциденти безпеки: | | | |
| IR-6(3)[1][1] | IR-6(3)[1][1]{1} | постачальнику продукту, які беруть участь у: | |
| IR-6(3)[1][1]{1}{1} | ланцюжку постачання систем |
| IR-6(3)[1][1]{1}{2} | компонентів системи, пов'язаних з інцидентом. |
| IR-6(3)[1][1]{2} | постачальнику послуги, які беруть участь у: | |
| IR-6(3)[1][1]{2}{1} | ланцюжку постачання систем |
| IR-6(3)[1][1]{2}{2} | компонентів системи, пов'язаних з інцидентом. |
| IR-6(3)[1][2] | іншим організаціям, які беруть участь у: | | |
| IR-6(3)[1][2]{1} | ланцюжку постачання систем | |
| IR-6(3)[1][2]{2} | компонентів системи, пов'язаних з інцидентом. | |
| IR-6(3)[2] | Надати інформацію про інциденти приватності: | | | |
| IR-6(3)[2][1] | IR-6(3)[2][1]{1} | постачальнику продукту, які беруть участь у: | |
| IR-6(3)[2][1]{1}{1} | ланцюжку постачання систем |
| IR-6(3)[2][1]{1}{2} | компонентів системи, пов'язаних з інцидентом. |
| IR-6(3)[2][1]{2} | постачальнику послуги, які беруть участь у: | |
| IR-6(3)[2][1]{2}{1} | ланцюжку постачання систем |
| IR-6(3)[2][1]{2}{2} | компонентів системи, пов'язаних з інцидентом. |
| IR-6(3)[2][2] | іншим організаціям, які беруть участь у: | | |
| IR-6(3)[2][2]{1} | ланцюжку постачання систем | |
| IR-6(3)[2][2]{2} | компонентів системи, пов'язаних з інцидентом. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються координації ланцюгів постачання; договори придбання; угоди про рівень обслуговування; план реагування на інциденти; план безпеки; плани іншої організації, яка бере участь у діяльності ланцюга постачання; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за повідомлення про інциденти; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за ланцюжки постачання].  Перевірка: [ВИБРАТИ З: Організаційні процеси для повідомлення про інциденти; автоматизовані механізми, що підтримують та / або впроваджують звіт про інформацію про події, що бере участь у ланцюгу постачання] | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IR-7 | ПІДТРИМКА РЕАГУВАННЯ НА ІНЦИДЕНТИ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| IR-7[1] | Надавати ресурси для підтримки реагування на інциденти, що є невіддільною частиною організаційних спроможностей реагування на інциденти, які являють собою: | | | |
| IR-7[1][1] | поради користувачам інформаційної системи для: | | |
| IR-7[1][1][1] | обробки звітності про: | |
| IR-7[1][1][1][1] | інциденти безпеки |
| IR-7[1][1][1][2] | інциденти приватності. |
| IR-7[1][1][2] | формування звітності про: | |
| IR-7[1][1][2][1] | інциденти безпеки |
| IR-7[1][1][2][2] | інциденти приватності. |
| IR-7[1][2] | допомогу користувачам інформаційної системи для обробки та формування звітності про інциденти безпеки та приватності. | | |
| IR-7[1][2][1] | обробки звітності про: | |
| IR-7[1][2][1][1] | інциденти безпеки |
| IR-7[1][2][1][2] | інциденти приватності. |
| IR-7[1][2][2] | формування звітності про: | |
| IR-7[1][2][2][1] | інциденти безпеки |
| IR-7[1][2][2][2] | інциденти приватності. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються допомоги у реагуванні на інциденти; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за допомогу та підтримку у справах подій; організаційний персонал, який має доступ до служби підтримки та реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для надання допомоги у реагуванні на інциденти; автоматизовані механізми підтримки та / або реалізації допомоги у реагуванні на інциденти]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IR-7(1) | ПІДТРИМКА РЕАГУВАННЯ НА ІНЦИДЕНТИ - АВТОМАТИЗАЦІЯ ПІДТРИМКИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ІНФОРМАЦІЇ ТА ПІДТРИМКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IR-7(1)[1] | Впровадити автоматизовані механізми для збільшення доступності пов'язаної з реагуванням на: | |
| IR-7(1)[1][1] | інциденти інформації |
| IR-7(1)[1][2] | інциденти підтримки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються допомоги у реагуванні на інциденти; автоматизовані механізми, що підтримують підтримку та допомогу у реагуванні на інциденти; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; план реагування на інциденти; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за підтримку та допомогу щодо реагування на події; організаційний персонал, який має доступ до служби підтримки та реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для надання допомоги у реагуванні на інциденти; автоматизовані механізми, що підтримують та / або впроваджують збільшення доступності інформації та підтримки реагування на інциденти]. | | |

|  |  |  |
| --- | --- | --- |
| IR-7(2) | Підтримка реагування на інциденти - Координація з зовнішніми постачальниками | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-7(2)(a) | Встановити прямі відносини кооперації між здатністю реагування на інциденти та зовнішніми постачальниками можливостей захисту системи. |
| IR-7(2)(b) | Визначити членів команди реагування на інциденти в організації для зовнішніх постачальників послуг. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на аварії; процедури, що стосуються допомоги у реагуванні на інциденти; план реагування на аварії; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за підтримку та допомогу щодо реагування на події; зовнішні постачальники можливостей захисту інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку] | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| IR-8 | ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| IR-8(a) | Розробити план реагування на інциденти, який: | | | | |
| IR-8(a)(1) | IR-8(a)(1)[1] | | Організація розробляє методичні рекомендації для реалізації спроможності реагування на інциденти; | |
| IR-8(a)(1)[2] | | Надає організації методичні рекомендації для реалізації спроможності реагування на інциденти; | |
| IR-8(a)(2) | IR-8(a)(2)[1] | | Описує структуру спроможності реагування на інциденти; | |
| IR-8(a)(2)[2] | | Описує організацію спроможності реагування на інциденти; | |
| IR-8(a)(3) | Надає високорівневий підхід до того, як здатність реагування на інциденти вписується в загальну практику організації | | | |
| IR-8(a)(4) | Відповідає унікальним вимогам організації, які пов'язані з: | | | |
| IR-8(a)(4)[1] | | завданням | |
| IR-8(a)(4)[2] | | розміром | |
| IR-8(a)(4)[3] | | структурою | |
| IR-8(a)(4)[4] | | функціями | |
| IR-8(a)(5) | Визначає підзвітні інциденти | | | |
| IR-8(a)(6) | Надає показники для вимірювання можливостей реагування на інциденти всередині організації | | | |
| IR-8(a)(7) | IR-8(a)(7)[1] | Визначає ресурси необхідні для ефективної підтримки та розвитку можливостей реагування на інциденти; | | |
| IR-8(a)(7)[2] | Визначає управлінську підтримку, необхідну для ефективної підтримки та розвитку можливостей реагування на інциденти; | | |
| IR-8(a)(8) | IR-8(a)(8)[1] | IR-8(a)(8)[1]{1} | | організація визначає персонал |
| IR-8(a)(8)[1]{2} | | організація визначає ролі |
| IR-8(a)(8)[2] | організація визначає частоту з якою необхідно розглядати та схвалювати визначений організацією персонал або ролі | | |
| IR-8(a)(8)[3] | організація розглядає, з визначеною організацією частотою, визначений організацією: | | |
| IR-8(a)(8)[3]{1} | | персонал |
| IR-8(a)(8)[3]{2} | | ролі |
| IR-8(a)(8)[4] | організація схвалює, з визначеною організацією частотою, визначений організацією: | | |
| IR-8(a)(8)[4]{1} | | персонал |
| IR-8(a)(8)[4]{2} | | ролі |
| IR-8(a)(9) | IR-8(a)(9)[1] | IR-8(a)(9)[1]{1} | | організація визначає персонал, відповідальний за реагування на інциденти |
| IR-8(a)(9)[1]{2} | | організація визначає ролями, відповідальний за реагування на інциденти |
| IR-8(a)(9)[2] | Явно визначає відповідальність за реагування на інциденти визначеним організацією: | | |
| IR-8(a)(9)[2]{1} | | персоналом |
| IR-8(a)(9)[2]{2} | | ролями |
| IR-8(b) | IR-8(b)[1] | IR-8(b)[1][1] | організація визначає персонал, який відповідає за конкретні дії, який визначається: | | |
| IR-8(b)[1][1]{1} | | за іменем та / або |
| IR-8(b)[1][1]{2} | | за ролями |
| IR-8(b)[1][2] | організація визначає організаційні елементи серед яких необхідно поширити копії плану реагування на інциденти | | |
| IR-8(b)[2] | Поширити копії плану реагування на інциденти серед: | | | |
| IR-8(b)[2][1] | визначеного організацією персоналу, який відповідає за конкретні дії, | | |
| IR-8(b)[2][2] | організаційними елементами | | |
| IR-8(c) | IR-8(c)[1] | IR-8(c)[1]{1} | IR-8(c)[1]{1}[1] | |  |
| IR-8(c)[1]{1}[2] | | Оновлювати план реагування на інциденти у разі організаційних змін |
| IR-8(c)[1]{2} | Оновлювати план реагування на інциденти у разі проблем, що виникають при: | | |
| IR-8(c)[1]{2}{1} | | реалізації |
| IR-8(c)[1]{2}{2} | | виконанні |
| IR-8(c)[1]{2}{3} | | тестуванні плану |
| IR-8(d) | IR-8(d)[1] | IR-8(d)[1][1] | організація визначає персонал, з реагування на інциденти, який визначається: | | |
| IR-8(d)[1][1]{1} | | за іменем та / або |
| IR-8(d)[1][1]{2} | | за ролями |
| IR-8(d)[1][2] | організація визначає організаційні елементи яким необхідно повідомляти про зміни плану реагування на інциденти | | |
| IR-8(d)[2] | Повідомляти про зміни плану реагування на інциденти: | | | |
| IR-8(d)[2][1] | визначений організацією персонал, з реагування на інциденти | | |
| IR-8(d)[2][2] | організаційні елементи | | |
| IR-8(e) | IR-8(e)[1] | Захистити план реагування на інциденти від несанкціонованого розкриття та зміни | | | |
| IR-8(e)[2] | Захистити план реагування на інциденти від несанкціонованого розкриття та зміни | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються планування реагування на інциденти; план реагування на інциденти; записи оглядів та затверджень плану реагування на інциденти; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за планування реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: План реагування на організаційні події та пов’язані з ними організаційні процеси]. | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IR-8(1) | ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ - ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| IR-8(1)[1] | Включити такі додаткові процеси в План реагування на інциденти для інцидентів, пов'язаних з персональними даними: | | |
| IR-8(1)[1](a) | IR-8(1)[1](a)[1] | процес визначення доцільності повідомлення наглядових організацій і |
| IR-8(1)[1](a)[2] | надання повідомлення наглядових організацій, якщо це доречно |
| IR-8(1)[1](b) | процес оцінки, стосовно постраждалих осіб, для визначення ступеня: | |
| IR-8(1)[1](b){1} | шкоди |
| IR-8(1)[1](b){2} | труднощів |
| IR-8(1)[1](b){3} | незручностей |
| IR-8(1)[1](b){4} | несправедливості |
| IR-8(1)[1](c) | IR-8(1)[1](c)[1] | організація визначає ролі, які забезпечують інформування користувачів організації про будь-які інциденти з приватністю |
| IR-8(1)[1](c)[2] | процес, що забезпечує оперативне інформування користувачів організації про будь-які інциденти з приватністю ролями, які визначаються організацією |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються планування реагування на інциденти; план реагування на інциденти; записи оглядів та затверджень плану реагування на інциденти; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за планування реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: План реагування на організаційні події та пов’язані з ними організаційні процеси]. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IR-9 | РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| IR-9[1] | Реагувати на витік інформації шляхом: | | | |
| IR-9[1](a) | Визначення конкретної інформації, пов'язаної з джерелом витоку у системі | | |
| IR-9[1](b) | IR-9[1](b)[1] | IR-9[1](b)[1]{1} | організація визначає персонал, який необхідно попереджати про витік інформації, використовуючи метод зв'язку, не пов'язаний з витоком |
| IR-9[1](b)[1]{2} | організація визначає ролі, які необхідно попереджати про витік інформації, використовуючи метод зв'язку, не пов'язаний з витоком |
| IR-9[1](b)[2] | IR-9[1](b)[2]{1} | Попередження визначеного організацією персоналу про витік інформації, використовуючи метод зв'язку, не пов'язаний з витоком |
| IR-9[1](b)[2]{2} | Попередження визначеного організацією ролей про витік інформації, використовуючи метод зв'язку, не пов'язаний з витоком |
| IR-9[1](c) | IR-9[1](c){1} | Ізолювання системи | |
| IR-9[1](c){2} | Ізолювання системної компоненти | |
| IR-9[1](d) | IR-9[1](d){1} | Видалення інформації з компонента системи | |
| IR-9[1](d){2} | Видалення інформації з системи | |
| IR-9[1](e) | IR-9[1](e){1} | Визначення іншої системи, які згодом могли б бути джерелом витоку інформації | |
| IR-9[1](e){2} | Визначення іншого компонента системи, які згодом могли б бути джерелом витоку інформації | |
| IR-9[1](f) | IR-9[1](f)[1] | організація визначає додаткові дії необхідні для реагування на витік інформації | |
| IR-9[1](f)[2] | Організація виконує такі додаткові дії. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються розливу інформації; план реагування на інциденти; записи попереджень / сповіщень про розлив інформації, список персоналу, який повинен отримувати попередження про розлив інформації; перелік дій, які слід виконати щодо розливу інформації; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для реагування на витік інформації; автоматизовані механізми, що підтримують та / або реалізують дії щодо реагування на витік інформації та пов'язані з ними комунікації]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| IR-9(1) | РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - ВІДПОВІДАЛЬНИЙ ПЕРСОНАЛ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IR-9(1)[1] | IR-9(1)[1]{1} | організація визначає персонал, відповідальний за реагування на витік інформації |
| IR-9(1)[1]{2} | організація визначає ролі відповідальні за реагування на витік інформації |
| IR-9(1)[2] | IR-9(1)[2]{1} | Призначити визначений організацією персонал відповідальний за реагування на витік інформації |
| IR-9(1)[2]{2} | Призначити визначені організацією ролі відповідальні за реагування на витік інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються розливу інформації; план реагування на інциденти; перелік персоналу, відповідального за реагування на витік інформації; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку] | | |

|  |  |  |
| --- | --- | --- |
| IR-9(2) | РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - ТРЕНУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-9(2)[1] | організація визначає частоту навчання з реагування на витік інформації |
| IR-9(2)[2] | Забезпечити навчання з реагування на витік інформації з визначеною організацією частотою. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються тренінгів щодо реагування на витік інформації; навчальна програма з питань реагування на витік інформації; навчальні матеріали щодо реагування на витік інформації; план реагування на інциденти; записи навчальних заходів щодо реагування на витік інформації; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за тренування з питань реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку]. | |

|  |  |  |
| --- | --- | --- |
| IR-9(3) | РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - РОБОТА ПІСЛЯ ВИТОКУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-9(3)[1] | організація визначає процедури з метою забезпечення спроможності персоналу організації, на який впливає витік інформації, продовжувати виконувати поставлені завдання, у той час, як постраждалі системи зазнають коригувальних дій. |
| IR-9(3)[2] | Реалізувати визначені організацією процедури, з метою забезпечення спроможності для персоналу організації, на який впливає витік інформації, продовжувати виконувати поставлені завдання, у той час, як постраждалі системи зазнають коригувальних дій. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; процедури, що стосуються розливу інформації; план реагування на інциденти; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для операцій після розливу] | |

|  |  |  |
| --- | --- | --- |
| IR-9(4) | РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - ВИКРИТТЯ НЕАВТОРИЗОВАНОГО ПЕРСОНАЛУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| IR-9(4)[1] | організація визначає механізми захисту |
| IR-9(4)[2] | Застосовуйте визначені організацією заходи (засоби) захисту для персоналу, що має доступ до інформації, яка не відповідає призначеним правам доступу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; процедури, що стосуються розливу інформації; план реагування на інциденти; гарантії безпеки щодо витоку інформації / впливу неавторизованого персоналу; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для роботи з інформацією, що потрапляє до несанкціонованого персоналу; автоматизовані механізми, що підтримують та / або впроваджують запобіжні заходи для персоналу, який потрапляє під дію інформації, яка не знаходиться в межах призначених дозволів доступу]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| IR-10 | ІНТЕГРОВАНА КОМАНДА АНАЛІЗУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| IR-10[1] | IR-10[1][1] | Визначити команду аналітиків криміналістів для обробки інцидентів в режимі реального часу. |
| IR-10[1][2] | Визначити аналітиків зловмисного коду для обробки інцидентів в режимі реального часу. |
| IR-10[1][3] | Визначити розробників інструментів для обробки інцидентів в режимі реального часу. |
| IR-10[1][4] | Визначити оперативного персоналу для обробки інцидентів в режимі реального часу. |
| IR-10[2] | Створити інтегровану команду для обробки інцидентів в режимі реального часу з: | |
| IR-10[2][1] | аналітиків криміналістів |
| IR-10[2][2] | аналітиків зловмисного коду |
| IR-10[2][3] | розробників інструментів |
| IR-10[2][4] | оперативного персоналу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика реагування на інциденти; процедури, що стосуються планування реагування на інциденти та інтеграції групи аналізу безпеки; план реагування на інциденти; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за реагування на інциденти та аналіз інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який бере участь у групах інтегрованого аналізу безпеки]. | | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ MA – ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| MA-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| MA-1(a) | MA-1(a)[1] | MA-1(a)[1](1) | | | Розробляє та документує політику технічного обслуговування, яка: | | | | | | | | |
| MA-1(a)[1](1)(a) | | Містить: | | | | | | |
| MA-1(a)[1](1)(a)[1] | | | | мету, | | |
| MA-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| MA-1(a)[1](1)(a)[3] | | | | ролі, | | |
| MA-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| MA-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| MA-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| MA-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| MA-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| MA-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| MA-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| MA-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| MA-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| MA-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| MA-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| MA-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| MA-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики технічного обслуговування та відповідних заходів управління доступом | | | | | | | | |
| MA-1(a)[2] | MA-1(a)[2]{1} | | | MA-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика індивідуальної участі | | | | | |
| MA-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики технічного обслуговування та пов'язаних з нею заходів технічного обслуговування | | | | | |
| MA-1(a)[2]{2} | | | MA-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика технічного обслуговування | | | | | |
| MA-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики технічного обслуговування та пов'язаних з нею заходів технічного обслуговування | | | | | |
| MA-1(a)[3] | MA-1(a)[3]{1} | | | MA-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику технічного обслуговування, яка: | | | | | | | |
| MA-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| MA-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| MA-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| MA-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| MA-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| MA-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| MA-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| MA-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| MA-1(a)[3](1)(b) | | | Відповідає: | | | | |
| MA-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| MA-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| MA-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| MA-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| MA-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| MA-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| MA-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| MA-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації політики технічного обслуговування та відповідних заходів управління доступом | | | | | | | |
| MA-1(a)[3]{2} | | | MA-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику технічного обслуговування, яка: | | | | | | | |
| MA-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| MA-1(a)[3]{2}(1)(а)[1] | | мету, | |
| MA-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| MA-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| MA-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| MA-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| MA-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| MA-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| MA-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| MA-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| MA-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| MA-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| MA-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| MA-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| MA-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| MA-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| MA-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики технічного обслуговування та пов'язаних з нею заходів технічного обслуговування | | | | | | | |
| MA-1(b) | MA-1(b)[1] | визначає посадову особу для управління політикою та процедурами технічного обслуговування | | | | | | | | | | | |
| MA-1(b)[2] | призначає посаду для управління політикою та процедурами технічного обслуговування | | | | | | | | | | | |
| MA-1(с) | MA-1(с)[1] | MA-1(с)[1](1) | | MA-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики технічного обслуговування | | | | | | | |
| MA-1(с)[1](1)[2] | | переглядає поточну політику технічного обслуговування з визначеною організацією частотою | | | | | | | |
| MA-1(с)[1](2) | | MA-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур технічного обслуговування | | | | | | | |
| MA-1(с)[1](2)[2] | | переглядає поточні процедури технічного обслуговування з визначеною організацією частотою | | | | | | | |
| MA-1(с)[2] | MA-1(с)[2](1) | | MA-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики технічного обслуговування | | | | | | | |
| MA-1(с)[2](1)[2] | | оновлює поточну політику технічного обслуговування з визначеною організацією частотою | | | | | | | |
| MA-1(с)[2](2) | | MA-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур технічного обслуговування | | | | | | | |
| MA-1(с)[2](2)[2] | | оновлює поточні процедури технічного обслуговування з визначеною організацією частотою | | | | | | | |
| MA-1(d) | переконується, що процедури технічного обслуговування реалізують політику та заходи технічного обслуговування | | | | | | | | | | | | |
| MA-1(e) | MA-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики технічного обслуговування | | | | | | | | | | |
| MA-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики технічного обслуговування | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури технічного обслуговування; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику технічного обслуговування; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| MA-2 | КОНТРОЛЬОВАНЕ ОБСЛУГОВУВАННЯ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | | | | |
| MA-2(a) | MA-2(a)[1] | MA-2(a)[1]{1} | | | Планувати записи з технічного обслуговування компонентів системи відповідно до: | | | | | | | | |
| MA-2(a)[1]{1}{1} | | | | вимог виробника | | | | |
| MA-2(a)[1]{1}{2} | | | | вимог постачальників | | | | |
| MA-2(a)[1]{1}{3} | | | | організаційних вимог | | | | |
| MA-2(a)[1]{2} | | | Планувати записи з ремонту компонентів системи відповідно до: | | | | | | | | |
| MA-2(a)[1]{2}{1} | | | | вимог виробника | | | | |
| MA-2(a)[1]{2}{2} | | | | вимог постачальників | | | | |
| MA-2(a)[1]{2}{3} | | | | організаційних вимог | | | | |
| MA-2(a)[1]{3} | | | Планувати записи з заміни компонентів системи відповідно до: | | | | | | | | |
| MA-2(a)[1]{3}{1} | | | | вимог виробника | | | | |
| MA-2(a)[1]{3}{2} | | | | вимог постачальників | | | | |
| MA-2(a)[1]{3}{3} | | | | організаційних вимог | | | | |
| MA-2(a)[2] | MA-2(a)[2]{1} | | | документувати записи з технічного обслуговування компонентів системи відповідно до: | | | | | | | | |
| MA-2(a)[2]{1}{1} | | | вимог виробника | | | | | |
| MA-2(a)[2]{1}{2} | | | вимог постачальників | | | | | |
| MA-2(a)[2]{1}{3} | | | організаційних вимог | | | | | |
| MA-2(a)[2]{2} | | | документувати записи з ремонту компонентів системи відповідно до: | | | | | | | | |
| MA-2(a)[2]{2}{1} | | | вимог виробника | | | | | |
| MA-2(a)[2]{2}{2} | | | вимог постачальників | | | | | |
| MA-2(a)[2]{2}{3} | | | організаційних вимог | | | | | |
| MA-2(a)[2]{3} | | | документувати записи з заміни компонентів системи відповідно до: | | | | | | | | |
| MA-2(a)[2]{3}{1} | | | вимог виробника | | | | | |
| MA-2(a)[2]{3}{2} | | | вимог постачальників | | | | | |
| MA-2(a)[2]{3}{3} | | | організаційних вимог | | | | | |
| MA-2(a)[3] | MA-2(a)[3]{1} | | | переглядати записи з технічного обслуговування компонентів системи відповідно до: | | | | | | | | |
| MA-2(a)[3]{1}{1} | | | вимог виробника | | | | | |
| MA-2(a)[3]{1}{2} | | | вимог постачальників | | | | | |
| MA-2(a)[3]{1}{3} | | | організаційних вимог | | | | | |
| MA-2(a)[3]{2} | | | переглядати записи з ремонту компонентів системи відповідно до: | | | | | | | | |
| MA-2(a)[3]{2}{1} | | | вимог виробника | | | | | |
| MA-2(a)[3]{2}{2} | | | вимог постачальників | | | | | |
| MA-2(a)[3]{2}{3} | | | організаційних вимог | | | | | |
| MA-2(a)[3]{3} | | | переглядати записи з заміни компонентів системи відповідно до: | | | | | | | | |
| MA-2(a)[3]{3}{1} | | | вимог виробника | | | | | |
| MA-2(a)[3]{3}{2} | | | вимог постачальників | | | | | |
| MA-2(a)[3]{3}{3} | | | організаційних вимог | | | | | |
| MA-2(b) | MA-2(b)[1] | Затвердити порядок моніторингу усіх заходів з технічного обслуговування, незалежно від того, виконуються вони на місці або віддалено, а також чи обслуговуються системи або системні компоненти на місці або переміщуються в інше місце | | | | | | | | | | | |
| MA-2(b)[2] | здійснювати моніторинг усіх заходів з технічного обслуговування, незалежно від того, виконуються вони на місці або віддалено, а також чи обслуговуються системи або системні компоненти на місці або переміщуються в інше місце | | | | | | | | | | | |
| MA-2(c) | MA-2(c)[1] | MA-2(c)[1]{1} | | організація визначає персонал явно схвалили видалення системи або компоненту системи з організаційного обладнання | | | | | | | | | |
| MA-2(c)[1]{2} | | організація визначає ролі явно схвалили видалення системи або компоненту системи з організаційного обладнання | | | | | | | | | |
| MA-2(c)[2] | MA-2(c)[2]{1} | | Вимагати, щоб визначені організацією персонал явно схвалили: | | | | | | | | | |
| MA-2(c)[2]{1}{1} | | | видалення системи з організаційного обладнання для: | | | | | | |
| MA-2(c)[2]{1}{1}{1} | | | технічного обслуговування поза об'єктами експлуатації | | | |
| MA-2(c)[2]{1}{1}{2} | | | ремонту поза об'єктами експлуатації | | | |
| MA-2(c)[2]{1}{1}{3} | | | чи заміни поза об'єктами експлуатації | | | |
| MA-2(c)[2]{1}{2} | | | видалення компоненту системи з організаційного обладнання для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації | | | | | | |
| MA-2(c)[2]{1}{2}{1} | | | | | технічного обслуговування поза об'єктами експлуатації | |
| MA-2(c)[2]{1}{2}{2} | | | | | ремонту поза об'єктами експлуатації | |
| MA-2(c)[2]{1}{2}{3} | | | | | чи заміни поза об'єктами експлуатації | |
| MA-2(c)[2]{2} | | Вимагати, щоб визначені організацією ролі явно схвалили: | | | | | | | | | |
| MA-2(c)[2]{1}{1} | | видалення системи з організаційного обладнання для: | | | | | | | |
| MA-2(c)[2]{1}{1}{1} | | | | | | | технічного обслуговування поза об'єктами експлуатації |
| MA-2(c)[2]{1}{1}{2} | | | | | | | ремонту поза об'єктами експлуатації |
| MA-2(c)[2]{1}{1}{3} | | | | | | | чи заміни поза об'єктами експлуатації |
| MA-2(c)[2]{1}{2} | | видалення компоненту системи з організаційного обладнання для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації | | | | | | | |
| MA-2(c)[2]{1}{2}{1} | | | | | технічного обслуговування поза об'єктами експлуатації | | |
| MA-2(c)[2]{1}{2}{2} | | | | | ремонту поза об'єктами експлуатації | | |
| MA-2(c)[2]{1}{2}{3} | | | | | чи заміни поза об'єктами експлуатації | | |
| MA-2(d) | Очищати обладнання з точки зору видалення всієї інформації з носіїв до вилучення обладнання організації для: | | | | | | | | | | | | |
| MA-2(d){1} | | технічного обслуговування поза об'єктами експлуатації; | | | | | | | | | | |
| MA-2(d){2} | | ремонту поза об'єктами експлуатації; | | | | | | | | | | |
| MA-2(d){3} | | заміни поза об'єктами експлуатації поза об'єктами експлуатації; | | | | | | | | | | |
| MA-2(e) | Перевірити всі потенційно порушені заходи захисту, щоб переконатися, що вони, як і раніше працюють належним чином після дій з: | | | | | | | | | | | | |
| MA-2(e){1} | | обслуговування, | | | | | | | | | | |
| MA-2(e){2} | | ремонту; | | | | | | | | | | |
| MA-2(e){3} | | заміни | | | | | | | | | | |
| MA-2(f) | MA-2(f)[1] | | організація визначає інформацію, пов'язану з технічним обслуговуванням, яку необхідно включити до записів з технічного обслуговування | | | | | | | | | | |
| MA-2(f)[2] | | Включати визначену організацією інформацію, пов'язану з технічним обслуговуванням до записів з технічного обслуговування | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються технічного обслуговування контрольованої інформаційної системи; записи технічного обслуговування; технічні характеристики виробника / постачальника; записи технічного обладнання; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за обробку засобів масової інформації; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для планування, виконання, документування, перегляду, затвердження та моніторингу технічного обслуговування та ремонту інформаційної системи; організаційні процеси обробки компонентів інформаційної системи; автоматизовані механізми, що підтримують та / або впроваджують контрольоване обслуговування; автоматизовані механізми, що здійснюють обробку компонентів інформаційної системи]. | | | | | | | | | | | | | |

|  |  |
| --- | --- |
| MA-2(1) | КОНТРОЛЬОВАНЕ ОБСЛУГОВУВАННЯ - ЗМІСТ ЗАПИСУ |
| [Вилучено: Включено до МА-2] | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| MA-2(2) | КОНТРОЛЬОВАНЕ ОБСЛУГОВУВАННЯ - АВТОМАТИЗОВАНА ТЕХНІЧНА ДІЯЛЬНІСТЬ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| MA-2(2)(a) | MA-2(2)(a)[1] | MA-2(2)(a)[1]{1} | Використовувати автоматизовані механізми для планування, дій по: | | |
| MA-2(2)(a)[1]{1}[1] | | обслуговуванню системи |
| MA-2(2)(a)[1]{1}[2] | | ремонту системи |
| MA-2(2)(a)[1]{1}[3] | | заміни системи |
| MA-2(2)(a)[1]{2} | Використовувати автоматизовані механізми для планування, дій по: | | |
| MA-2(2)(a)[1]{1}[1] | | обслуговуванню компонентів системи |
| MA-2(2)(a)[1]{1}[2] | | ремонту компонентів системи |
| MA-2(2)(a)[1]{1}[3] | | заміни компонентів системи |
| MA-2(2)(a)[2] | MA-2(2)(a)[2] | Використовувати автоматизовані механізми для проведення дій по: | | |
| MA-2(2)(a)[1]{1}[1] | | обслуговуванню системи |
| MA-2(2)(a)[1]{1}[2] | | ремонту системи |
| MA-2(2)(a)[1]{1}[3] | | заміни системи |
| MA-2(2)(a)[2] | Використовувати автоматизовані механізми для проведення дій по: | | |
| MA-2(2)(a)[1]{1}[1] | | обслуговуванню компонентів системи |
| MA-2(2)(a)[1]{1}[2] | | ремонту компонентів системи |
| MA-2(2)(a)[1]{1}[3] | | заміни компонентів системи |
| MA-2(2)(a)[3] | MA-2(2)(a)[3] | Використовувати автоматизовані механізми для документування дій по: | | |
| MA-2(2)(a)[1]{1}[1] | | обслуговуванню системи |
| MA-2(2)(a)[1]{1}[2] | | ремонту системи |
| MA-2(2)(a)[1]{1}[3] | | заміни системи |
| MA-2(2)(a)[3] | Використовувати автоматизовані механізми для документування дій по: | | |
| MA-2(2)(a)[1]{1}[1] | | обслуговуванню компонентів системи |
| MA-2(2)(a)[1]{1}[2] | | ремонту компонентів системи |
| MA-2(2)(a)[1]{1}[3] | | заміни компонентів системи |
| MA-2(2)(b) | MA-2(2)(b)[1] | Надавати оновлені, точні та повні записи про всі дії з технічного обслуговування:. | | | |
| MA-2(2)(b)[1][1] | | замовлених дій | |
| MA-2(2)(b)[1][2] | | запланованих дій | |
| MA-2(2)(b)[1][3] | | виконуваних дій | |
| MA-2(2)(b)[1][4] | | завершених дій | |
| MA-2(2)(b)[2] | Надавати оновлені, точні та повні записи про всі дії з ремонту: | | | |
| MA-2(2)(b)[2][1] | | замовлених дій | |
| MA-2(2)(b)[2][2] | | запланованих дій | |
| MA-2(2)(b)[2][3] | | виконуваних дій | |
| MA-2(2)(b)[2][4] | | завершених дій | |
| MA-2(2)(b)[3] | Надавати оновлені, точні та повні записи про всі дії з заміни: | | | |
| MA-2(2)(b)[3][1] | | замовлених дій | |
| MA-2(2)(b)[3][2] | | запланованих дій | |
| MA-2(2)(b)[3][3] | | виконуваних дій | |
| MA-2(2)(b)[3][4] | | завершених дій | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування контрольованої інформаційної системи; автоматизовані механізми, що підтримують діяльність з обслуговування інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи технічного обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або впроваджують контрольоване технічне обслуговування; автоматизовані механізми, що підтримують та / або впроваджують виготовлення записів про технічне обслуговування та ремонтні роботи]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| MA-3 | ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| MA-3(a) | використання засобів технічного обслуговування має бути: | |
| MA-3(a)[1] | Затверджено |
| MA-3(a)[2] | контрольовано |
| MA-3(a)[3] | відстежуватися |
| MA-3(b) | MA-3(b)[1] | затвердити інструменти технічного обслуговування |
| MA-3(b)[2] | організація визначає частоту з якою необхідно переглядати раніше затверджені інструменти технічного обслуговування |
| MA-3(b)[3] | Переглядати раніше затверджені інструменти технічного обслуговування з частотою, визначеною організацією |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються засобів обслуговування інформаційної системи; засоби технічного обслуговування інформаційної системи та відповідна документація; записи технічного обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для затвердження, контролю та моніторингу засобів обслуговування; автоматизовані механізми, що підтримують та / або впроваджують затвердження, контроль та / або моніторинг засобів технічного обслуговування]. | | |

|  |  |  |
| --- | --- | --- |
| MA-3(1) | ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ПЕРЕВІРКА ІНСТРУМЕНТІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MA-3(1){1} | Оглянути інструменти для технічного обслуговування, які доставлені на об'єкт обслуговуючим персоналом, на предмет неправильних модифікацій |
| MA-3(1){2} | Оглянути інструменти для технічного обслуговування, які доставлені на об'єкт обслуговуючим персоналом, на предмет несанкціонованих модифікацій. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються засобів обслуговування інформаційної системи; засоби технічного обслуговування інформаційної системи та відповідна документація; записи про перевірку інструменту технічного обслуговування; записи технічного обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для перевірки засобів технічного обслуговування; автоматизовані механізми, що підтримують та / або впроваджують перевірку засобів технічного обслуговування]. | |

|  |  |  |
| --- | --- | --- |
| MA-3(2) | ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ПЕРЕВІРКА НОСІЇВ ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MA-3(2)[1] | Перед використанням носіїв у системі перевірити носії, що містять діагностичні програми на наявність шкідливого коду |
| MA-3(2)[2] | Перед використанням носіїв у системі перевірити носії, що містять тестові програми на наявність шкідливого коду |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються засобів обслуговування інформаційної системи; засоби технічного обслуговування інформаційної системи та відповідна документація; записи технічного обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційний процес перевірки носія інформації на наявність шкідливого коду; автоматизовані механізми, що підтримують та / або здійснюють перевірку носіїв, що використовуються для технічного обслуговування]. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| MA-3(3) | ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОМУ ПЕРЕМІЩЕННЮ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| MA-3(3)[1] | Запобігти переміщенню обладнання для технічного обслуговування, що містить організаційну інформацію, шляхом: | | | | |
| MA-3(3)[1](a) | Перевірки відсутності організаційної інформації розміщеної на обладнанні; | | | |
| MA-3(3)[1](b) | MA-3(3)[1](b){1} | | очищення обладнання | |
| MA-3(3)[1](b){2} | | знищення обладнання | |
| MA-3(3)[1](c) | утримання обладнання на об'єкті | | | |
| MA-3(3)[1](d) | MA-3(3)[1](d)[1] | MA-3(3)[1](d)[1]{1} | | організація визначає персонал |
| MA-3(3)[1](d)[1]{2} | | організація визначає ролі |
| MA-3(3)[1](d)[2] | MA-3(3)[1](d)[2]{1} | | отримання дозволу від визначеного організацією персоналу, які явно дозволяють переміщення обладнання з об'єкта |
| MA-3(3)[1](d)[2]{2} | | отримання дозволу від визначених організацією ролей, які явно дозволяють переміщення обладнання з об'єкта |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються засобів обслуговування інформаційної системи; засоби технічного обслуговування інформаційної системи та відповідна документація; записи технічного обслуговування; записи санітарії обладнання(Санітарна обробка - це процес видалення конфіденційної інформації з документа або іншого повідомлення, щоб документ міг бути поширений серед ширшої аудиторії); записи санітарії засобів масової інформації; звільнення від вивезення обладнання; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за санітарію засобів масової інформації].  Перевірка: [ВИБРАТИ З: Організаційний процес запобігання несанкціонованому видаленню інформації; автоматизовані механізми, що підтримують санітарію засобів масової інформації або знищення обладнання; автоматизовані механізми, що підтримують перевірку дезінфекції засобів масової інформації]. | | | | | |

|  |  |  |
| --- | --- | --- |
| MA-3(4) | ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ОБМЕЖЕННЯ ВИКОРИСТАННЯ ІНСТРУМЕНТА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MA-3(4)[1] | Обмежити використання інструментів технічного обслуговування лише авторизованим персоналом. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються засобів обслуговування інформаційної системи; засоби технічного обслуговування інформаційної системи та відповідна документація; список персоналу, уповноваженого користуватися інструментами технічного обслуговування; записи використання технічного обслуговування; записи технічного обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційний процес для обмеження використання засобів технічного обслуговування; автоматизовані механізми, що підтримують та / або впроваджують обмежене використання засобів технічного обслуговування]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MA-4 | ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| MA-4(a) | MA-4(a)[1] | MA-4(a)[1][1] | Впровадити віддалені дії з обслуговування |
| MA-4(a)[1][2] | Впровадити віддалені дії з діагностики |
| MA-4(a)[2] | MA-4(a)[2][1] | відстежувати віддалені дії з обслуговування |
| MA-4(a)[2][2] | відстежувати віддалені дії з діагностики |
| MA-4(b) | Дозволити використання віддалених засобів технічного обслуговування лише: | | |
| MA-4(b)[1] | відповідно до організаційної політики | |
| MA-4(b)[2] | у разі, якщо це документально зафіксовано в плані безпеки системи | |
| MA-4(c) | MA-4(c)[1] | Використовувати сувору автентифікацію при встановленні віддалених технічних сеансів | |
| MA-4(c)[2] | Використовувати сувору автентифікацію при встановленні віддалених діагностичних сеансів | |
| MA-4(d) | MA-4(d)[1] | Вести облік віддалених дій з обслуговування | |
| MA-4(d)[2] | Вести облік віддалених дій з діагностики | |
| MA-4(e) | MA-4(e)[1] | Припинити сесії та мережеві з'єднання, коли завершено віддалене обслуговування | |
| MA-4(e)[2] | Припинити сесії та мережеві з'єднання, коли завершено віддалене обслуговування | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування нелокальної інформаційної системи; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи технічного обслуговування; діагностичні записи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для управління нелокальним обслуговуванням; автоматизовані механізми реалізації, підтримки та / або управління нелокальним технічним обслуговуванням; автоматизовані механізми для надійної автентифікації нелокальних діагностичних сеансів обслуговування; автоматизовані механізми припинення нелокальних сеансів технічного обслуговування та мережевих з'єднань]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MA-4(1) | ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - АУДИТ ТА ОГЛЯД | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| MA-4(1)(a) | MA-4(1)(a)[1] | організація визначає події аудиту для віддалених сеансів обслуговування та діагностики | |
| MA-4(1)(a)[2] | Проводити аудит визначені організацією події аудиту для віддалених сеансів: | |
| MA-4(1)(a)[2][1] | обслуговування |
| MA-4(1)(a)[2][2] | діагностики |
| MA-4(1)(b) | Здійснювати огляд записів про сеанси віддаленого: | | |
| MA-4(1)(b)[1] | обслуговування | |
| MA-4(1)(b)[2] | діагностики | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування нелокальної інформаційної системи; перелік аудиторських подій; налаштування конфігурації інформаційної системи та відповідна документація; записи технічного обслуговування; діагностичні записи; записи аудиту; огляди записів сеансів обслуговування та діагностики; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за аудит та перевірку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для аудиту та перегляду нелокального обслуговування; автоматизовані механізми, що підтримують та / або впроваджують аудит та огляд нелокального обслуговування]. | | | |

|  |  |
| --- | --- |
| MA-4(2) | ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - ДОКУМЕНТУВАННЯ ВІДДАЛЕНОГО ОБСЛУГОВУВАННЯ |
|  | [Вилучено: включено до MA-1 та МА-4] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| MA-4(3) | ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - ПОРІВНЯЛЬНА БЕЗПЕКА І ОЧИЩЕННЯ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| MA-4(3)(a) | Вимагати, щоб віддалені послуги з обслуговування виконувалися з системи, яка реалізує заходи безпеки, і які можна порівняти з заходами, реалізованими в системі, що обслуговується; | | | | |
| MA-4(3)(b) | MA-4(3)(b){1} | MA-4(3)(b){1}[1] | Необхідно: видалити компонент, який підлягає обслуговуванню, з системи до віддаленого обслуговування; | | |
| MA-4(3)(b){1}[2] | очистити компонент (від організаційної інформації) перед видаленням з організаційних об'єктів; | | |
| MA-4(3)(b){1}[3] | після того, як обслуговування виконано: | | |
| MA-4(3)(b){1}[3][1] | оглянути компонент (на предмет потенційно шкідливого програмного забезпечення) перед тим, як під'єднувати компонент до системи. | |
| MA-4(3)(b){1}[3][2] | очистити компонент (від потенційно шкідливого програмного забезпечення) перед тим, як під'єднувати компонент до системи. | |
| MA-4(3)(b){2} | MA-4(3)(b){2}[1] | Необхідно: видалити компонент, який підлягає обслуговуванню, з системи до діагностичних послуг; | | |
| MA-4(3)(b){2}[2] | очистити компонент (від організаційної інформації) перед видаленням з організаційних об'єктів; | | |
| MA-4(3)(b){2}[3] | після того, як обслуговування виконано: | | |
| MA-4(3)(b){2}[3][1] | | оглянути компонент (на предмет потенційно шкідливого програмного забезпечення) перед тим, як під'єднувати компонент до системи. |
| MA-4(3)(b){2}[3][2] | | очистити компонент (від потенційно шкідливого програмного забезпечення) перед тим, як під'єднувати компонент до системи. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування нелокальної інформаційної системи; контракти про надання послуг та / або угоди про рівень послуг; записи технічного обслуговування; протоколи перевірок; записи аудиту; записи санітарії обладнання; записи санітарії засобів масової інформації; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; постачальник технічного обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за санітарію засобів масової інформації; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для порівняльної безпеки та санітарії для нелокального обслуговування; організаційні процеси з видалення, санітарної обробки та перевірки компонентів, що обслуговуються через нелокальне технічне обслуговування; автоматизовані механізми підтримки та / або впровадження дезінфекції та інспекції компонентів]. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| MA-4(4) | ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - АВТЕНТИФІКАЦІЯ ТА РОЗПОДІЛ СЕСІЇ ОБСЛУГОВУВАННЯ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| MA-4(5)[1] | Захистити віддалені сеанси обслуговування за допомогою: | | | |
| MA-4(5)[1](a) | MA-4(5)[1](a)[1] | | організація визначає автентифікатори, які стійкі до відтворення |
| MA-4(5)[1](a)[2] | | використання визначених організацією автентифікаторів, які стійкі до відтворення |
| MA-4(5)[1](b) | відокремлення сеансів обслуговування від інших мережевих сеансів з системою шляхом: | | |
| MA-4(5)[1](b)[1] | фізично відокремленого шляху зв'язку; | |
| MA-4(5)[1](b)[2] | логічно розділеного шляху зв'язку на основі шифрування | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування нелокальної інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи технічного обслуговування; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; мережеві інженери; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для захисту нелокальних сеансів технічного обслуговування; автоматизовані механізми, що реалізують стійкі до відтворення автентифікатори; автоматизовані механізми, що реалізують логічно розділені / зашифровані шляхи зв'язку]. | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| MA-4(5) | ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - СХВАЛЕННЯ ТА ПОВІДОМЛЕННЯ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| MA-4(5)(a) | MA-4(5)(a)[1] | MA-4(5)(a)[1]{1} | організація визначає персонал | | |
| MA-4(5)(a)[1]{2} | організація визначає ролі | | |
| MA-4(5)(a)[2] | MA-4(5)(a)[2]{1} | вимагати схвалення кожного віддаленого сеансу технічного обслуговування персоналом, що визначила організація | | |
| MA-4(5)(a)[2]{2} | вимагати схвалення кожного віддаленого сеансу технічного обслуговування роллю, що визначила організація | | |
| MA-4(5)(b) | MA-4(5)(b)[1] | MA-4(5)(b)[1]{1} | організація визначає персонал | | |
| MA-4(5)(b)[1]{2} | організація визначає ролі | | |
| MA-4(5)(b)[2] | MA-4(5)(b)[2]{1} | повідомити персонал, що визначила організація про: | | |
| MA-4(5)(b)[2]{1}[1] | дату запланованого віддаленого обслуговування | |
| MA-4(5)(b)[2]{1}[2] | час запланованого віддаленого обслуговування | |
| MA-4(5)(b)[2]{2} | повідомити ролі, що визначила організація про дату та час запланованого віддаленого обслуговування | | |
| MA-4(5)(b)[2]{2}[1] | | дату запланованого віддаленого обслуговування |
| MA-4(5)(b)[2]{2}[2] | | час запланованого віддаленого обслуговування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування локальної інформаційної системи; план безпеки; повідомлення, що підтримують нелокальні сеанси технічного обслуговування; записи технічного обслуговування; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; організаційний персонал, який відповідає за повідомлення; організаційний персонал, що відповідає за затвердження; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для затвердження та повідомлення персоналу щодо нелокального технічного обслуговування; автоматизовані механізми, що підтримують повідомлення та затвердження нелокального технічного обслуговування]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| MA-4(6) | ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - КРИПТОГРАФІЧНИЙ ЗАХИСТ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| MA-4(6)[1] | Запровадити криптографічні механізми для захисту цілісності: | |
| MA-4(6)[1][1] | віддаленого обслуговування |
| MA-4(6)[1][2] | діагностичних комунікацій |
| MA-4(6)[2] | Запровадити криптографічні механізми для захисту конфіденційності | |
| MA-4(6)[2][1] | віддаленого обслуговування |
| MA-4(6)[2][2] | та діагностичних комунікацій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування локальної інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; криптографічні механізми, що захищають нелокальну діяльність з технічного обслуговування; записи технічного обслуговування; діагностичні записи; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; мережеві інженери; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Криптографічні механізми захисту нелокального технічного обслуговування та діагностичних комунікацій]. | | |

|  |  |  |
| --- | --- | --- |
| MA-4(7) | ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - ПЕРЕВІРКА ВІДДАЛЕНОГО РОЗ’ЄДНАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MA-4(7)[1] | Реалізувати перевірку віддаленого роз’єднання у разі припинення віддалених сеансів обслуговування |
| MA-4(7)[2] | Реалізувати перевірку віддаленого роз’єднання у разі припинення віддалених сеансів діагностики |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування локальної інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; криптографічні механізми, що захищають нелокальну діяльність з технічного обслуговування; записи технічного обслуговування; діагностичні записи; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; мережеві інженери; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MA-5 | ТЕХНІЧНИЙ ПЕРСОНАЛ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| MA-5(a) | MA-5(a)[1] | Встановити процедуру авторизації технічного персоналу та | |
| MA-5(a)[2] | MA-5(a)[2]{1} | вести перелік авторизованих організацій технічного обслуговування |
| MA-5(a)[2]{2} | вести перелік авторизованого персоналу технічного обслуговування |
| MA-5(b) | MA-5(b)[1] | Перевіряти, що персонал, який не супроводжується має необхідні дозволи на доступ | |
| MA-5(b)[2] | Перевіряти, що персонал, який виконує технічне обслуговування в системі, має необхідні дозволи на доступ | |
| MA-5(c) | для нагляду за персоналом з технічного обслуговування, який не має необхідних дозволів на доступ потрібно визначити персонал організації з: | | |
| MA-5(c)[1] | необхідними повноваженнями щодо доступу та | |
| MA-5(c)[2] | технічною компетенцією | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговуючого персоналу; договори про надання послуг; угоди про рівень обслуговування; список уповноваженого персоналу; записи технічного обслуговування; записи контролю доступу; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для уповноваження та управління обслуговуючим персоналом; автоматизовані механізми, що підтримують та / або впроваджують дозвіл обслуговуючого персоналу]. | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| MA-5(1) | ТЕХНІЧНИЙ ПЕРСОНАЛ - ОСОБИ БЕЗ НАЛЕЖНОГО ДОСТУПУ | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | | |
| MA-5(1)(a) | MA-5(1)(a)[1] | | Реалізувати процедури залучення персоналу з технічного обслуговування, який: | | | | | | | | |
| MA-5(1)(a)[1]{1} | не має відповідних дозволів (допуску) | | | | | | | |
| MA-5(1)(a)[1]{2} | не є громадянами України | | | | | | | |
| MA-5(1)(a)[2] | | MA-5(1)(a)[2](1) | MA-5(1)(a)[2](1){1} | | процедури залучення персоналу з технічного обслуговування, який не має відповідних дозволів (допуску) включають такі вимоги: | | | | | |
| MA-5(1)(a)[2](1){1}[1] | Обслуговуючий персонал, що не має необхідних прав доступу, повинен | | | | |
| MA-5(1)(a)[2](1){1}[1][1] | | супроводжуватися та бути під наглядом уповноваженого організацією персоналу, з необхідним рівнем допуску | | |
| MA-5(1)(a)[2](1){1}[1][2] | | мати відповідну технічну кваліфікацію для виконання технічного обслуговування та діагностичних заходів в системі | | |
| MA-5(1)(a)[2](1){1}[2] | Обслуговуючий персонал, що не має необхідного, рівня допуску, повинен: | | | | |
| MA-5(1)(a)[2](1){1}[2][1] | | супроводжуватися та бути під наглядом уповноваженого організацією персоналу, з необхідним рівнем допуску | | |
| MA-5(1)(a)[2](1){1}[2][2] | | мати відповідну технічну кваліфікацію для виконання технічного обслуговування та діагностичних заходів в системі | | |
| MA-5(1)(a)[2](1){1}[3] | Обслуговуючий персонал, що не має офіційного затвердженого доступу повинен: | | | | |
| MA-5(1)(a)[2](1){1}[3][1] | | супроводжуватися та бути під наглядом уповноваженого організацією персоналу, з необхідним рівнем допуску | | |
| MA-5(1)(a)[2](1){1}[3][2] | | мати відповідну технічну кваліфікацію для виконання технічного обслуговування та діагностичних заходів в системі | | |
| MA-5(1)(a)[2](1){2} | | процедури залучення персоналу з технічного обслуговування, який не є громадянами України включають такі вимоги: | | | | | |
| MA-5(1)(a)[2](1){2}[1] | Обслуговуючий персонал, що не має необхідних прав доступу, повинен | | | | |
| MA-5(1)(a)[2](1){2}[1][1] | | супроводжуватися та бути під наглядом уповноваженого організацією персоналу, з необхідним рівнем допуску | | |
| MA-5(1)(a)[2](1){2}[1][2] | | мати відповідну технічну кваліфікацію для виконання технічного обслуговування та діагностичних заходів в системі | | |
| MA-5(1)(a)[2](1){2}[2] | Обслуговуючий персонал, що не має необхідного, рівня допуску, повинен: | | | | |
| MA-5(1)(a)[2](1){2}[2][1] | | супроводжуватися та бути під наглядом уповноваженого організацією персоналу, з необхідним рівнем допуску | | |
| MA-5(1)(a)[2](1){2}[2][2] | | мати відповідну технічну кваліфікацію для виконання технічного обслуговування та діагностичних заходів в системі | | |
| MA-5(1)(a)[2](1){2}[3] | Обслуговуючий персонал, що не має офіційного затвердженого доступу повинен: | | | | |
| MA-5(1)(a)[2](1){2}[3][1] | | супроводжуватися та бути під наглядом уповноваженого організацією персоналу, з необхідним рівнем допуску | | |
| MA-5(1)(a)[2](1){2}[3][2] | | мати відповідну технічну кваліфікацію для виконання технічного обслуговування та діагностичних заходів в системі | | |
| MA-5(1)(a)[2](2) | MA-5(1)(a)[2](2){1} | | Перед тим, як розпочати технічне обслуговування персоналом, який: | | | | | |
| MA-5(1)(a)[2](2){1}{1} | не має необхідних прав допуску, упевнитися, що | | | | |
| MA-5(1)(a)[2](2){1}[1] | | всі компоненти енергонезалежного зберігання інформації в системі очищуються, | | |
| MA-5(1)(a)[2](2){1}{1}[2] | | MA-5(1)(a)[2](2){1}{1}[2]{1} | всі енергонезалежні носії видаляються; | |
| MA-5(1)(a)[2](2){1}{1}[2]{2} | або фізично відключаються від системи та надійно захищаються | |
| MA-5(1)(a)[2](2){1}{2} | не має рівня допуску, упевнитися, що | | | | |
| MA-5(1)(a)[2](2){1}{2}[1] | | всі компоненти енергонезалежного зберігання інформації в системі очищуються, | | |
| MA-5(1)(a)[2](2){1}{2}[2] | | MA-5(1)(a)[2](2){1}{2}[2]{1} | | всі енергонезалежні носії видаляються; |
| MA-5(1)(a)[2](2){1}{2}[2]{2} | | або фізично відключаються від системи та надійно захищаються |
| MA-5(1)(b) | | MA-5(1)(b)[1] | | | Розробити альтернативні заходи безпеки, якщо компонент системи не може бути: | | | | | | |
| MA-5(1)(b)[1]{1} | | | очищено | | | |
| MA-5(1)(b)[1]{2} | | | вилучено | | | |
| MA-5(1)(b)[1]{3} | | | відключено від системи | | | |
| MA-5(1)(b)[2] | | | впровадити альтернативні заходи безпеки, якщо компонент системи не може бути: | | | | | | |
| MA-5(1)(b)[1]{1} | | | очищено | | | |
| MA-5(1)(b)[1]{2} | | | вилучено | | | |
| MA-5(1)(b)[1]{3} | | | відключено від системи | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговуючого персоналу; політика захисту засобів масової інформації інформаційної системи; політика щодо фізичного та екологічного захисту; план безпеки; перелік обслуговуючого персоналу, що вимагає супроводу / нагляду; записи технічного обслуговування; записи контролю доступу; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; організаційний персонал, який відповідає за забезпечення персоналу; організаційний персонал, який відповідає за фізичний контроль доступу; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за санітарію засобів масової інформації; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для управління обслуговуючим персоналом без відповідного доступу; автоматизовані механізми, що підтримують та / або впроваджують альтернативні гарантії безпеки; автоматизовані механізми підтримки та / або впровадження дезінфекції компонентів зберігання інформації]. | | | | | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MA-5(2) | ТЕХНІЧНИЙ ПЕРСОНАЛ - ОФОРМЛЕННЯ ДОПУСКУ ДЛЯ СИСТЕМ, ЩО ОБРОБЛЯЮТЬ ІНФОРМАЦІЮ З ОБМЕЖЕНИМ ДОСТУПОМ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| MA-5(2)[1] | Переконатися, що персонал, який виконує технічне обслуговування та діагностику в системі, яка: | | |
| MA-5(2)[1][1] | MA-5(2)[1][1]{1} | Обробляє таємну інформацію |
| MA-5(2)[1][1]{2} | зберігає таємну інформацію |
| MA-5(2)[1][1]{3} | передає таємну інформацію, |
| MA-5(2)[1][2] | має рівень допуску на доступ для:. | |
| MA-5(2)[1][2][1] | принаймні найвищого рівня секретності |
| MA-5(2)[1][2][2] | всієї інформації в системі |
| MA-5(2)[1][3] | має офіційне схвалення на доступ для: | |
| MA-5(2)[1][3][1] | принаймні найвищого рівня секретності |
| MA-5(2)[1][3][2] | всієї інформації в системі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговуючого персоналу; кадровий облік; записи технічного обслуговування; записи контролю доступу; облікові дані доступу; дозволи на доступ; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; організаційний персонал, який відповідає за забезпечення персоналу; організаційний персонал, який відповідає за фізичний контроль доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для управління дозволами безпеки для обслуговуючого персоналу]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| MA-5(3) | ТЕХНІЧНИЙ ПЕРСОНАЛ - ВИМОГИ ДО ГРОМАДЯНСТВА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| MA-5(3)[1] | Переконатися, що працівники, які виконують технічне обслуговування та діагностичні заходи з | |
| MA-5(3)[1]{1} | Обробки є громадянами України. |
| MA-5(3)[1]{2} | зберігання є громадянами України. |
| MA-5(3)[1]{3} | передачі таємної інформації, є громадянами України. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговуючого персоналу; кадровий облік; записи технічного обслуговування; записи контролю доступу; облікові дані доступу; дозволи на доступ; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи; організаційний персонал, який відповідає за забезпечення персоналу; організаційний персонал, який відповідає за інформаційну безпеку]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MA-5(4) | ТЕХНІЧНИЙ ПЕРСОНАЛ - ІНОЗЕМНІ ГРОМАДЯНИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| MA-5(4)(a) | MA-5(4)(a)[1] | Переконайтеся, що іноземні громадяни з відповідним рівнем допуску залучаються для проведення технічного обслуговування в системах, що обробляють інформацію з обмеженим доступом тільки тоді, коли: | |
| MA-5(4)(a)[1]{1} | ці системи спільно належать та експлуатуються урядами України та закордонних союзників, |
| MA-5(4)(a)[1]{2} | належать та експлуатуються виключно іноземними союзними урядами |
| MA-5(4)(a)[2] | Переконайтеся, що іноземні громадяни з відповідним рівнем допуску залучаються для проведення діагностичних робіт в системах, що обробляють інформацію з обмеженим доступом тільки тоді, коли: | |
| MA-5(4)(a)[2]{1} | ці системи спільно належать та експлуатуються урядами України та закордонних союзників, |
| MA-5(4)(a)[2]{2} | або належать та експлуатуються виключно іноземними союзними урядами |
| MA-5(4)(b) | MA-5(4)(b)[1] | MA-5(4)(b)[1][1] | Переконайтеся, що схвалення, що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування систем, що обробляють інформацію з обмеженим доступом повністю задокументувати у Меморандумі про угоду. |
| MA-5(4)(b)[1][2] | Переконайтеся, що згоди що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування систем, що обробляють інформацію з обмеженим доступом повністю задокументувати у Меморандумі про угоду. |
| MA-5(4)(b)[1][3] | Переконайтеся, додаткові умови експлуатації, що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування систем, що обробляють інформацію з обмеженим доступом повністю задокументувати у Меморандумі про угоду. |
| MA-5(4)(b)[2] | MA-5(4)(b)[2][1] | Переконайтеся, що схвалення, що стосуються залучення іноземних громадян для проведення робіт з діагностики систем, що обробляють інформацію з обмеженим доступом повністю задокументувати у Меморандумі про угоду. |
| MA-5(4)(b)[2][2] | Переконайтеся, що згоди що стосуються залучення іноземних громадян для проведення робіт з діагностики систем, що обробляють інформацію з обмеженим доступом повністю задокументувати у Меморандумі про угоду. |
| MA-5(4)(b)[2][3] | Переконайтеся, додаткові умови експлуатації, що стосуються залучення іноземних громадян для проведення робіт з діагностики систем, що обробляють інформацію з обмеженим доступом повністю задокументувати у Меморандумі про угоду. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговуючого персоналу; політика захисту засобів масової інформації інформаційної системи; політика та процедури контролю доступу; політика та процедури фізичного та екологічного захисту; меморандум про угоду; записи технічного обслуговування; записи контролю доступу; облікові дані доступу; дозволи на доступ; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за обслуговування інформаційної системи, організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, який керує меморандумами про угоди; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для управління іноземним національним обслуговуючим персоналом]. | | | |

|  |  |  |
| --- | --- | --- |
| MA-5(5) | ТЕХНІЧНИЙ ПЕРСОНАЛ - НЕСИСТЕМНЕ ОБСЛУГОВУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MA-5(5)[1] | Переконатися, що персонал, який не супроводжується, що здійснює ремонтні роботи, не пов'язаний безпосередньо з системою, але знаходиться фізично близько від системи, має необхідні дозволи на доступ. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговуючого персоналу; політика захисту засобів масової інформації інформаційної системи; політика та процедури контролю доступу; політика та процедури фізичного та екологічного захисту; записи технічного обслуговування; записи контролю доступу; дозволи на доступ; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, який відповідає за забезпечення персоналу; організаційний персонал, який відповідає за фізичний контроль доступу; організаційний персонал, який відповідає за інформаційну безпеку]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| MA-6 | СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| MA-6[1] | організація визначає компоненти системи у разі відмови яких необхідно надати (один або кілька): | |
| MA-6[1]{1} | технічну підтримку |
| MA-6[1]{2} | запасні частини |
| MA-6[2] | організація визначає період часу за який у разі відмови визначених компонентів системи необхідно надати (один або кілька): | |
| MA-6[2]{1} | технічну підтримку |
| MA-6[2]{2} | запасні частини |
| MA-6[3] | у разі відмови для визначених організацією компонентів системи в межах визначеного організацією періоду часу. (один або кілька): | |
| MA-6[3]{1} | Отримати технічну підтримку |
| MA-6[3]{2} | запасні частини |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування інформаційної системи; договори про надання послуг; угоди про рівень обслуговування; інвентаризація та наявність запасних частин; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, який відповідає за придбання; організаційний персонал, відповідальний за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для забезпечення своєчасного обслуговування]. | | |

|  |  |  |
| --- | --- | --- |
| MA-6(1) | СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ - ПРОФІЛАКТИЧНЕ ОБСЛУГОВУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MA-6(1)[1] | організація визначає компоненти системи яким необхідно здійснювати профілактичне обслуговування |
| MA-6(1)[2] | організація визначає часові інтервали з якими необхідно здійснювати профілактичне обслуговування визначеним організацією компонентам системи |
| MA-6(1)[3] | Здійснювати профілактичне обслуговування визначених організацією компонентів системи у визначені організацією часові інтервали. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування інформаційної системи; договори про надання послуг; угоди про рівень обслуговування; план безпеки; записи технічного обслуговування; перелік компонентів системи, що вимагають профілактичного обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для профілактичного обслуговування; автоматизовані механізми підтримки та / або впровадження профілактичного обслуговування]. | |

|  |  |  |
| --- | --- | --- |
| MA-6(2) | СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ - ПЛАНОВЕ ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MA-6(2)[1] | організація визначає системні компоненти яким необхідно здійснювати планове технічне обслуговування |
| MA-6(2)[2] | організація визначає часові інтервали з якими необхідно здійснювати планове технічне обслуговування |
| MA-6(2)[3] | Здійснювати планове технічне обслуговування визначених організацією системних компонентів у визначені організацією часові інтервали. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування інформаційної системи; договори про надання послуг; угоди про рівень обслуговування; план безпеки; записи технічного обслуговування; перелік системних компонентів, що вимагають інтелектуального обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для інтелектуального обслуговування; автоматизовані механізми, що підтримують та / або впроваджують прогнозне обслуговування]. | |

|  |  |  |
| --- | --- | --- |
| MA-6(3) | СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ - АВТОМАТИЗОВАНА ПІДТРИМКА ПЛАНОВОГО ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MA-6(3)[1] | Визначити автоматизовані механізми для передачі даних планового технічного обслуговування до комп'ютеризованої системи управління обслуговуванням |
| MA-6(3)[2] | Використовувати автоматизовані механізми для передачі даних планового технічного обслуговування до комп'ютеризованої системи управління обслуговуванням. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування інформаційної системи; договори про надання послуг; угоди про рівень обслуговування; план безпеки; записи технічного обслуговування; перелік системних компонентів, що вимагають технічного обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують передачу прогнозних даних технічного обслуговування в комп’ютеризовану систему управління технічним обслуговуванням; операції системи управління комп'ютерним обслуговуванням]. | |

|  |  |  |
| --- | --- | --- |
| MA-6(4) | СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ - ВІДПОВІДНЕ ПОСТАЧАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MA-6(4)[1] | організація визначає критичні компоненти системи |
| MA-6(4)[2] | організація визначає гарантії безпеки які необхідні, щоб забезпечити відповідне постачання визначених організацією критичних компонентів системи |
| MA-6(4)[3] | впровадити визначені організацією гарантії безпеки, щоб забезпечити відповідне постачання визначених організацією критичних компонентів системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика обслуговування інформаційної системи; процедури, що стосуються обслуговування інформаційної системи; договори про надання послуг; угоди про рівень обслуговування; план безпеки; записи технічного обслуговування; перелік системних компонентів, що вимагають технічного обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за обслуговування інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що реалізують передачу прогнозних даних технічного обслуговування в комп’ютеризовану систему управління технічним обслуговуванням; операції системи управління комп'ютерним обслуговуванням]. | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ MP – ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| MP-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ ЩОДО ЗАХИСТУ НОСІЇВ ІНФОРМАЦІЇ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| MP-1(a) | MP-1(a)[1] | MP-1(a)[1](1) | | | Розробляє та документує політику захисту носіїв інформації, яка: | | | | | | | | |
| MP-1(a)[1](1)(a) | | Містить: | | | | | | |
| MP-1(a)[1](1)(a)[1] | | | | мету, | | |
| MP-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| MP-1(a)[1](1)(a)[3] | | | | ролі, | | |
| MP-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| MP-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| MP-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| MP-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| MP-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| MP-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| MP-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| MP-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| MP-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| MP-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| MP-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| MP-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| MP-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики захисту носіїв інформації та відповідних заходів управління доступом | | | | | | | | |
| MP-1(a)[2] | MP-1(a)[2]{1} | | | MP-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика індивідуальної участі | | | | | |
| MP-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики захисту носіїв інформації та пов'язаних з нею заходів захисту носіїв інформації | | | | | |
| MP-1(a)[2]{2} | | | MP-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика захисту носіїв інформації | | | | | |
| MP-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики захисту носіїв інформації та пов'язаних з нею заходів захисту носіїв інформації | | | | | |
| MP-1(a)[3] | MP-1(a)[3]{1} | | | MP-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику захисту носіїв інформації, яка: | | | | | | | |
| MP-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| MP-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| MP-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| MP-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| MP-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| MP-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| MP-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| MP-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| MP-1(a)[3](1)(b) | | | Відповідає: | | | | |
| MP-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| MP-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| MP-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| MP-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| MP-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| MP-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| MP-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| MP-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації політики захисту носіїв інформації та відповідних заходів управління доступом | | | | | | | |
| MP-1(a)[3]{2} | | | MP-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику захисту носіїв інформації, яка: | | | | | | | |
| MP-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| MP-1(a)[3]{2}(1)(а)[1] | | мету, | |
| MP-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| MP-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| MP-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| MP-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| MP-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| MP-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| MP-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| MP-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| MP-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| MP-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| MP-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| MP-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| MP-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| MP-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| MP-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики захисту носіїв інформації та пов'язаних з нею заходів захисту носіїв інформації | | | | | | | |
| MP-1(b) | MP-1(b)[1] | визначає посадову особу для управління політикою та процедурами захисту носіїв інформації | | | | | | | | | | | |
| MP-1(b)[2] | призначає посаду для управління політикою та процедурами захисту носіїв інформації | | | | | | | | | | | |
| MP-1(с) | MP-1(с)[1] | MP-1(с)[1](1) | | MP-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики захисту носіїв інформації | | | | | | | |
| MP-1(с)[1](1)[2] | | переглядає поточну політику захисту носіїв інформації з визначеною організацією частотою | | | | | | | |
| MP-1(с)[1](2) | | MP-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур захисту носіїв інформації | | | | | | | |
| MP-1(с)[1](2)[2] | | переглядає поточні процедури захисту носіїв інформації з визначеною організацією частотою | | | | | | | |
| MP-1(с)[2] | MP-1(с)[2](1) | | MP-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики захисту носіїв інформації | | | | | | | |
| MP-1(с)[2](1)[2] | | оновлює поточну політику захисту носіїв інформації з визначеною організацією частотою | | | | | | | |
| MP-1(с)[2](2) | | MP-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур захисту носіїв інформації | | | | | | | |
| MP-1(с)[2](2)[2] | | оновлює поточні процедури захисту носіїв інформації з визначеною організацією частотою | | | | | | | |
| MP-1(d) | переконується, що процедури захисту носіїв інформації реалізують політику та заходи захисту носіїв інформації | | | | | | | | | | | | |
| MP-1(e) | MP-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики захисту носіїв інформації | | | | | | | | | | |
| MP-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики захисту носіїв інформації | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури захисту носіїв інформації; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику захисту носіїв інформації; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MP-2 | ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| MP-2[1] | MP-2[1]{1} | організація визначає типи цифрових носіїв інформації до яких необхідно обмежити доступ, та / або | |
| MP-2[1]{2} | організація визначає типи нецифрових носіїв інформації до яких необхідно обмежити доступ | |
| MP-2[2] | MP-2[2]{1} | організація визначає персонал, який обмежує доступ до визначених організацією типів цифрових та / або нецифрових носіїв інформації | |
| MP-2[2]{2} | організація визначає ролі, які обмежують доступ до визначених організацією типів цифрових та / або нецифрових носіїв інформації | |
| MP-2[3] | MP-2[3]{1} | Обмежити доступ до визначених організацією типів цифрових носіїв інформації визначеним організацією: | |
| MP-2[3]{1}{1} | персоналом |
| MP-2[3]{1}{2} | Ролями, та / або: |
| MP-2[3]{2} | Обмежити доступ до визначених організацією типів нецифрових носіїв інформації визначеним організацією персоналом або ролями | |
| MP-2[3]{2}{1} | персоналом |
| MP-2[3]{2}{2} | ролями |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту засобів носіїв інформації інформаційної системи; процедури, що стосуються обмежень доступу до носіїв інформації; політика та процедури контролю доступу; політика та процедури фізичного та екологічного захисту; засоби зберігання носіїв; записи контролю доступу; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за захист засобів носіїв інформації в інформаційній системі; організаційний персонал, відповідальний за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для обмеження інформаційних засобів; автоматизовані механізми, що підтримують та / або запроваджують обмеження доступу до носіїв інформації]. | | | |

|  |  |
| --- | --- |
| MP-2(1) | ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ - АВТОМАТИЗОВАНИЙ ОБМЕЖЕННИЙ ДОСТУП |
|  | [Вилучено: Включено до MP-4(2)] |

|  |  |
| --- | --- |
| MP-2(2) | ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ |
|  | [Вилучено: Включено до SC-28(1)] |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MP-3 | МАРКУВАННЯ НОСІЇВ ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| MP-3(a) | Наносити на носії інформації маркування, що вказують на: | | |
| MP-3(a)[1] | обмеження поширення, | |
| MP-3(a)[2] | обмеження обробки, а також | |
| MP-3(a)[3] | застереження безпеки (якщо такі є) інформації | |
| MP-3(a)[4] | відповідні мітки безпеки (якщо такі є) інформації | |
| MP-3(b) | MP-3(b)[1] | MP-3(b)[1][1] | організація визначає типи системних носіїв які необхідно звільнити від маркування, якщо носії залишаються в межах визначених організацією контрольованих зон |
| MP-3(b)[1][2] | організація визначає контрольовані зони в межах яких нема потреби в маркуванні системних носіїв |
| MP-3(b)[2] | Звільнити визначені організацією типи системних носіїв від маркування, якщо носії залишаються в межах визначених організацією контрольованих зон | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються маркування носіїв інформації; політика та процедури фізичного та екологічного захисту; план безпеки; перелік носіїв інформаційної системи, що позначають атрибути безпеки; визначені контрольовані зони; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за захист та маркування системних носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для маркування носіїв інформації; автоматизовані механізми, що підтримують та / або впроваджують маркування носіїв інформації]. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| MP-4 | ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| MP-4(a) | MP-4(a)[1] | MP-4(a)[1]{1} | | організація визначає типи цифрових носіїв інформації до яких необхідно обмежити доступ, та / або | |
| MP-4(a)[1]{2} | | організація визначає типи нецифрових носіїв інформації до яких необхідно обмежити доступ | |
| MP-4(a)[2] | організація визначає контрольовані зони в межах яких нема потреби в маркуванні системних носіїв | | | |
| MP-4(a)[3] | MP-4(a)[3][1] | Фізично контролювати визначені організацією типи: | | |
| MP-4(a)[3][1]{1} | | цифрових носіїв інформації в межах визначених організацією контрольованих зон, та / або: |
| MP-4(a)[3][1]{2} | | нецифрових носіїв інформації в межах визначених організацією контрольованих зон |
| MP-4(a)[3][2] | безпечно зберігати визначені організацією типи цифрових та / або нецифрових носіїв інформації в межах визначених організацією контрольованих зон | | |
| MP-4(a)[3][2]{1} | | цифрових носіїв інформації в межах визначених організацією контрольованих зон, та / або: |
| MP-4(a)[3][2]{2} | | нецифрових носіїв інформації в межах визначених організацією контрольованих зон |
| MP-4(b) | MP-4(b){1} | Захищати системні носії до того часу, як носії знищуються, з використанням: | | | |
| MP-4(b){1}[1] | | затвердженого обладнання, | |
| MP-4(b){1}[2] | | Затверджених методів | |
| MP-4(b){1}[3] | | затверджених процедур | |
| MP-4(b){2} | Захищати системні носії до того часу, як носії очищаються, з використанням: | | | |
| MP-4(b){2}[1] | | затвердженого обладнання, | |
| MP-4(b){2}[2] | | Затверджених методів | |
| MP-4(b){2}[3] | | затверджених процедур | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються зберігання носіїв; політика та процедури фізичного та екологічного захисту; політика та процедури контролю доступу; план безпеки; носії інформаційної системи; визначені контрольовані зони; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за захист та зберігання носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для зберігання носіїв інформації; автоматизовані механізми, що підтримують та / або впроваджують безпечне зберігання носіїв інформації / захист носіїв інформації]. | | | | | |

|  |  |
| --- | --- |
| MP-4(1) | ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ |
|  | [Вилучено: Включено до SC-28(1)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| MP-4(2) | ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ - АВТОМАТИЗОВАНИЙ ОБМЕЖЕНИЙ ДОСТУП | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| MP-4(2)[1] | Впровадити автоматизовані механізми для: | |
| MP-4(2)[1][1] | обмеження доступу до зон зберігання носіїв інформації |
| MP-4(2)[1][2] | аудиту спроб доступу та доступу, який надано. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються зберігання носіїв; політика та процедури контролю доступу; політика та процедури фізичного та екологічного захисту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; засоби зберігання носіїв; пристрої контролю доступу; записи контролю доступу; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за захист та зберігання носіїв інформації; організаційний персонал, відповідальний за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що обмежують доступ до областей зберігання носіїв; автоматизовані механізми, що перевіряють спроби доступу та доступ, наданий зонам зберігання носіїв]. | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| MP-5 | ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| MP-5(a) | MP-5(a)[1] | MP-5(a)[1][1] | організація визначає типи системних носіїв які необхідно: | | |
| MP-5(a)[1][1] | захищати під час транспортування за межами контрольованих зон | |
| MP-5(a)[1][1] | контролювати під час транспортування за межами контрольованих зон | |
| MP-5(a)[1][2] | організація визначає заходи безпеки для визначених організацією типів системних носіїв під час транспортування за межами контрольованих зон для їх: | | |
| MP-5(a)[1][2][1] | | Захисту |
| MP-5(a)[1][2][2] | | контролю |
| MP-5(a)[2] | MP-5(a)[2][1] | Захищати визначені організацією типи системних носіїв під час транспортування за межами контрольованих зон, використовуючи визначені організацією заходи безпеки | | |
| MP-5(a)[2][2] | контролювати визначені організацією типи системних носіїв під час транспортування за межами контрольованих зон, використовуючи визначені організацією заходи безпеки | | |
| MP-5(b) | MP-5(b)[1] | Підтримувати підзвітність під час транспортування системних носіїв за межами контрольованих зон; | | | |
| MP-5(c) | Документувати дії, пов'язані з транспортуванням системних носіїв | | | | |
| MP-5(d) | Обмежити діяльність уповноваженого персоналу, пов'язану з транспортуванням системних носіїв. | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту засобів носіїв інформації інформаційної системи; процедури, що стосуються зберігання носіїв; політика та процедури фізичного та екологічного захисту; політика та процедури контролю доступу; план безпеки; носії інформаційної системи; визначені контрольовані зони; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за захист та зберігання засобів інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для зберігання носіїв інформації; автоматизовані механізми, що підтримують та / або впроваджують носій / захист медіа]. | | | | | |

|  |  |
| --- | --- |
| MP-5(1) | ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗАХИСТ ПОЗА КОНТРОЛЬОВАНИМИ ЗОНАМИ |
|  | [Вилучено: Включено до MP-5]. |

|  |  |
| --- | --- |
| MP-5(2) | ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - ДОКУМЕНТУВАННЯ ДІЙ |
|  | [Вилучено: Включено до MP-5]. |

|  |  |  |
| --- | --- | --- |
| MP-5(3) | ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗБЕРІГАЧІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MP-5(3)[1] | визначити зберігачів інформації під час транспортування системних носіїв за межі контрольованих зон. |
| MP-5(3)[2] | Наймати визначених зберігачів інформації під час транспортування системних носіїв за межі контрольованих зон. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються транспорту носіїв інформації; політика та процедури фізичного та екологічного захисту; транспортні записи носіїв інформаційні системи; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за транспортну відповідальність інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку]. | |

|  |  |
| --- | --- |
| MP-5(4) | ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ |
|  | [Вилучено: Включено до SC-28(1)]. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| MP-6 | ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| MP-6(a) | MP-6(a)[1] | організація визначає системні носії, які необхідно Очищувати перед: | | |
| MP-6(a)[1]{1} | утилізацією, | |
| MP-6(a)[1]{2} | випуском за межі організаційного контролю, | |
| MP-6(a)[1]{3} | повторним використанням | |
| MP-6(a)[2] | MP-6(a)[2][1] | організація визначає методи очищення визначених організацією системних носіїв | |
| MP-6(a)[2][2] | організація визначає процедури очищення визначених організацією системних носіїв | |
| MP-6(a)[3] | Очищувати визначені організацією системні носії перед: | | |
| MP-6(a)[3]{1} | утилізацією, визначеними організацією: | |
| MP-6(a)[3]{1}[1] | методами очищення |
| MP-6(a)[3]{1}[2] | процедурами очищення |
| MP-6(a)[3]{2} | випуском за межі організаційного контролю, визначеними організацією: | |
| MP-6(a)[3]{2}[1] | методами очищення |
| MP-6(a)[3]{2}[2] | процедурами очищення |
| MP-6(a)[3]{3} | або перед повторним використанням, визначеними організацією: | |
| MP-6(a)[3]{3}[1] | методами очищення |
| MP-6(a)[3]{3}[2] | процедурами очищення |
| MP-6(b) | Використовувати механізми очищення зі: | | | |
| MP-6(b)[1] | стійкістю що відповідає: | | |
| MP-6(b)[1]{1} | категорії безпеки або | |
| MP-6(b)[1]{2} | рівню секретності інформації | |
| MP-6(b)[2] | цілісністю, що відповідає: | | |
| MP-6(b)[2]{1} | категорії безпеки або | |
| MP-6(b)[2]{2} | рівню секретності інформації | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються санітарії та утилізації носіїв інформації; застосовними державними стандартами та політикою, що стосуються санітарії носіїв інформації; записи санітарії носіїв інформації; записи аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за санітарію носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для санітарії засобів масової інформації; автоматизовані механізми підтримки та / або впровадження санітарії носіїв інформації]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| MP-6(1) | ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ПЕРЕГЛЯДАТИ, ЗАТВЕРДЖЕННЯ, ВІДСТЕЖЕННЯ, ДОКУМЕНТУВАННЯ ТА ПЕРЕВІРКА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| MP-6(1)[1] | очищення носіїв інформації необхідно: | |
| MP-6(1)[1][1] | Переглядати, |
| MP-6(1)[1][2] | затверджувати, |
| MP-6(1)[1][3] | відстежувати, |
| MP-6(1)[1][4] | документувати |
| MP-6(1)[1][5] | перевіряти |
| MP-6(1)[2] | дії по утилізації носіїв інформації: | |
| MP-6(1)[2][1] | Переглядати, |
| MP-6(1)[2][2] | затверджувати, |
| MP-6(1)[2][3] | відстежувати, |
| MP-6(1)[2][4] | документувати |
| MP-6(1)[2][5] | перевіряти |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються санітарії та утилізації носіїв інформації; записи про санітарію та утилізацію носіїв інформації; переглядати записи щодо заходів щодо санітарії та утилізації носіїв інформації; погодження заходів щодо санітарії та утилізації носіїв інформації; відстеження записів; записи перевірки; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за санітарію та утилізацію носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для санітарії носіїв інформації; автоматизовані механізми підтримки та / або впровадження санітарії носіїв інформації]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| MP-6(2) | ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ПЕРЕВІРКА ОБЛАДНАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| MP-6(2)[1] | MP-6(2)[1][1] | організація визначає частоту з якою необхідно перевіряти обладнання для очищення, щоб переконатися в досягненні запланованого очищення |
| MP-6(2)[1][2] | організація визначає частоту з якою необхідно перевіряти процедури для очищення, щоб переконатися в досягненні запланованого очищення |
| MP-6(2)[2] | MP-6(2)[2][1] | Перевіряти обладнання для очищення з визначеною організацією частотою, щоб переконатися в досягненні запланованого очищення. |
| MP-6(2)[2][2] | Перевіряти процедури для очищення з визначеною організацією частотою, щоб переконатися в досягненні запланованого очищення. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються санітарії та утилізації носіїв інформації; процедури, що стосуються випробувань засобів санітарії носіїв інформації; результати тестування обладнання та процедур санітарії носіїв інформації; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за санітарію носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для санітарії носіїв інформації; автоматизовані механізми підтримки та / або впровадження санітарії носіїв інформації]. | | |

|  |  |  |
| --- | --- | --- |
| MP-6(3) | ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - НЕРУЙНІВНІ МЕТОДИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MP-6(3)[1] | організація визначає умови, які вимагають очищення портативних запам'ятовувальних пристроїв |
| MP-6(3)[2] | Застосовувати методи неруйнівного очищення до портативних запам'ятовувальних пристроїв перед підключенням таких пристроїв до системи при визначених організацією умовах, що вимагають очищення портативних запам'ятовувальних пристроїв. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються санітарії та утилізації носіїв інформації; перелік обставин, що вимагають санітарії портативних пристроїв зберігання; записи санітарії носіїв інформації; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за санітарію носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для санітарії носіїв портативних пристроїв зберігання; автоматизовані механізми підтримки та / або впровадження санітарії носіїв інформації]. | |

|  |  |
| --- | --- |
| MP-6(4) | ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - КЕРОВАНА НЕСЕКРЕТНА ІНФОРМАЦІЯ |
|  | [Вилучено: Включено до MP-6]. |

|  |  |
| --- | --- |
| MP-6(5) | ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - СЕКРЕТНА ІНФОРМАЦІЯ |
|  | [Вилучено: Включено до MP-6]. |

|  |  |
| --- | --- |
| MP-6(6) | ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ЗНИЩЕННЯ НОСІЇВ ІНФОРМАЦІЇ |
|  | [Вилучено: Включено до MP-6] |

|  |  |  |
| --- | --- | --- |
| MP-6(7) | ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ПОДВІЙНА АВТОРИЗАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MP-6(7)[1] | організація визначає системні носії для яких необхідно здійснювати подвійну авторизацію для очищення |
| MP-6(7)[2] | Здійснювати подвійну авторизацію для очищення визначених організацією системних носіїв |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються санітарії та утилізації носіїв інформації; перелік носіїв інформації інформаційної системи, що потребують подвійного дозволу на санітарну обробку; записи авторизації; записи санітарії носіїв інформації; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за санітарію носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси, що вимагають подвійного дозволу на санітарію носіїв інформації; автоматизовані механізми підтримки та / або впровадження санітарії носіїв інформації; автоматизовані механізми, що підтримують та / або реалізують подвійну авторизацію]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MP-6(8) | ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ВІДДАЛЕНЕ ОЧИЩЕННЯ АБО СТИРАННЯ ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| MP-6(8)[1] | організація визначає систему для якої необхідно забезпечити: | | |
| MP-6(8)[1]{1} | віддалену можливість очищення інформації | |
| MP-6(8)[1]{2} | віддалену можливість стирання інформації | |
| MP-6(8)[1]{3} | за визначених організацією умов | |
| MP-6(8)[2] | організація визначає компоненти системи для яких необхідно забезпечити: | | |
| MP-6(8)[2]{1} | віддалену можливість очищення інформації | |
| MP-6(8)[2]{2} | віддалену можливість стирання інформації | |
| MP-6(8)[2]{3} | за визначених організацією умов | |
| MP-6(8)[3] | організація визначає умови за яких необхідно забезпечити віддалену можливість очищення або стирання інформації | | |
| MP-6(8)[3]{1} | Забезпечити віддалену можливість очищення інформації з визначених організацією: | |
| MP-6(8)[3]{1}{1} | систем |
| MP-6(8)[3]{1}{2} | компонентів системи |
| MP-6(8)[3]{1}{3} | за визначених організацією умов |
| MP-6(8)[3]{2} | Забезпечити віддалену можливість стирання інформації з визначених організацією: | |
| MP-6(8)[3]{2}{1} | систем |
| MP-6(8)[3]{2}{2} | компонентів системи |
| MP-6(8)[3]{2}{3} | за визначених організацією умов |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються санітарії та утилізації носіїв інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи санітарії носіїв інформації; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за санітарію носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси очищення / витирання середовища; автоматизовані механізми, що підтримують та / або реалізують можливості продувки / протирання]. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| MP-6(9) | ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ЗНИЩЕННЯ ПЕРСОНАЛЬНОЇ ІДЕНТИФІКАЦІЙНОЇ ІНФОРМАЦІЇ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| MP-6(9)[1] | Сприяти знищенню персональної ідентифікаційної інформації у разі: | | | | |
| MP-6(9)[1](a) | де-ідентифікації персональної ідентифікаційної інформації | | | |
| MP-6(9)[1](b) | завчасного аналізу носіїв інформації для: | | | |
| MP-6(9)[1](b)[1] | активного пошуку персональної ідентифікаційної інформації та | | |
| MP-6(9)[1](b)[2] | видалення персональної ідентифікаційної інформації | | |
| MP-6(9)[1](c) | перевірки засобів масової інформації: | | | |
| MP-6(9)[1](c){1} | в момент їх архівування для | | |
| MP-6(9)[1](c){1}[1] | пошуку персональної ідентифікаційної інформації | |
| MP-6(9)[1](c){1}[2] | видалення персональної ідентифікаційної інформації | |
| MP-6(9)[1](c){2} | в момент їх утилізації для | | |
| MP-6(9)[1](c){2}[1] | | пошуку персональної ідентифікаційної інформації |
| MP-6(9)[1](c){2}[2] | | видалення персональної ідентифікаційної інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються санітарії та утилізації носіїв інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи санітарії носіїв інформації; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за санітарію носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси пошуку / видалення середовища; автоматизовані механізми, що підтримують та / або реалізують можливості пошуку / видалення]. | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| MP-7 | ВИКОРИСТАННЯ НОСІЇВ ІНФОРМАЦІЇ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| MP-7(a) | MP-7(a)[1] | MP-7(a)[1][1] | організація визначає типи системних носіїв, використання яких необхідно обмежити або заборонити на визначені організацією системи або компоненти системи | |
| MP-7(a)[1][2] | MP-7(a)[1][2]{1} | організація визначає системи на яких необхідно обмежити або заборонити використання визначених організацією типів системних носіїв |
| MP-7(a)[1][2]{2} | організація визначає компоненти системи на яких необхідно обмежити або заборонити використання визначених організацією типів системних носіїв |
| MP-7(a)[1][3] | організація визначає заходи безпеки, які використовують для обмеження або заборони використання визначених організацією типів системних носіїв на визначених організацією системах або компонентах системи. | |
| MP-7(a)[2] | MP-7(a)[2]{1} | обмежити використання визначених організацією типів системних носіїв на: | |
| MP-7(a)[2]{1}{1} | визначених організацією системах використовуючи визначені організацією заходи безпеки |
| MP-7(a)[2]{1}{2} | визначених організацією компонентах системи, використовуючи визначені організацією заходи безпеки |
| MP-7(a)[2]{1} | заборонити використання визначених організацією типів системних носіїв на: | |
| MP-7(a)[2]{1}{1} | визначених організацією системах використовуючи визначені організацією заходи безпеки |
| MP-7(a)[2]{1}{2} | визначених організацією компонентах системи, використовуючи визначені організацією заходи безпеки |
| MP-7(b) | Заборонити використання портативних пристроїв зберігання в системах організації, якщо такі пристрої не мають визначеного власника | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту портативних пристроїв зберігання інформації інформаційної системи; політика використання системи; процедури, що стосуються обмежень використання портативних пристроїв зберігання; план безпеки; правила поведінки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за використання портативних пристроїв зберігання інформації в інформаційній системі; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для використання портативних пристроїв зберігання інформації; автоматизовані механізми, що обмежують або забороняють використання портативних пристроїв зберігання інформаційної системи на інформаційних системах або компонентах системи]. | | | | |

|  |  |
| --- | --- |
| MP-7(1) | ВИКОРИСТАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗАБОРОНА ВИКОРИСТАННЯ БЕЗ ВИЗНАЧЕНОГО ВЛАСНИКА |
|  | [Вилучено: Включено до MP-7] |

|  |  |  |
| --- | --- | --- |
| MP-7(2) | Використання носіїв інформації Заборона використання стійких до очищення носіїв інформації | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MP-7(2)[1] | Заборонити використання в організаційних системах засобів, що не піддаються очищенню |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи, політика використання системи; процедури, що стосуються обмежень використання носіїв інформації; правила поведінки; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за використання носіїв інформації в інформаційній системі; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для використання носіїв інформації; автоматизовані механізми, що забороняють використання носіїв інформації в інформаційних системах або компонентах системи]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| MP-8 | ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| MP-8(a) | MP-8(a)[1] | організація визначає процес зниження категорії безпеки носіїв інформації який включає використання механізмів зниження грифа таємності носіїв інформації за: | | |
| MP-8(a)[1][1] | стійкістю, що відповідає: | |
| MP-8(a)[1][1]{1} | категорії безпеки |
| MP-8(a)[1][1]{2} | рівню секретності інформації |
| MP-8(a)[1][2] | цілісністю, що відповідає: категорії безпеки або рівню секретності інформації | |
| MP-8(a)[1][2]{1} | категорії безпеки |
| MP-8(a)[1][2]{2} | рівню секретності інформації |
| MP-8(a)[2] | Встановити визначений організацією процес зниження категорії безпеки носіїв інформації, який включає використання механізмів зниження грифа таємності носіїв інформації за: | | |
| MP-8(a)[2][1] | стійкістю, що відповідає: | |
| MP-8(a)[2][1]{1} | категорії безпеки |
| MP-8(a)[2][1]{2} | рівню секретності інформації |
| MP-8(a)[2][2] | цілісністю, що відповідає: категорії безпеки або рівню секретності інформації | |
| MP-8(a)[2][2]{1} | категорії безпеки |
| MP-8(a)[2][2]{2} | рівню секретності інформації |
| MP-8(b) | Забезпечити, що процес зниження категорії безпеки носія відповідає: | | | |
| MP-8(b)[1] | MP-8(b)[1]{1} | категорії безпеки | |
| MP-8(b)[1]{2} | рівню секретності інформації, яку потрібно видалити | |
| MP-8(b)[2] | рівню доступу потенційних одержувачів до інформації з меншим рівнем секретності | | |
| MP-8(c) | організація визначає системні носії, що вимагають зниження категорії безпеки | | | |
| MP-8(d) | Знижувати категорію безпеки визначеного носія за допомогою встановленого процесу | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються зниження рівня носіїв інформації; документація щодо категоризації системи; список носіїв інформації, що вимагають зниження рівня; записи про зниження рейтингу носіїв; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за зменшення рівня носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі].  Перевірка: [ВИБРАТИ З: Організаційні процеси для зниження рівня носіїв; автоматизовані механізми підтримки та / або впровадження зниження рівня зниження носіїв]. | | | | |

|  |  |  |
| --- | --- | --- |
| MP-8(1) | ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - ДОКУМЕНТУВАННЯ ПРОЦЕСУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MP-8(1)[1] | Документувати дії зі зниження категорії безпеки носіїв інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються зниження категорії безпеки носіїв; список носіїв інформації, що вимагають зниження категорії безпеки носіїв; записи про зниження категорії безпеки носіїв; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за зниження категорії безпеки носіїв; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для зниження категорії безпеки носіїв; автоматизовані механізми підтримки та / або впровадження зниження категорії безпеки носіїв]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| MP-8(2) | ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - ПЕРЕВІРКА ОБЛАДНАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| MP-8(2)[1] | організація визначає частоту з якою необхідно перевіряти обладнання та процедури заниження категорії безпеки | |
| MP-8(2)[2] | MP-8(2)[2][1] | Перевіряти обладнання та процедури заниження категорії безпеки з визначеною організацією частотою, щоб переконатися у досягненні запланованих заходів щодо зниження. |
| MP-8(2)[2][2] | Перевіряти обладнання та процедури заниження категорії безпеки з визначеною організацією частотою, щоб переконатися у досягненні запланованих заходів щодо зниження. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика захисту носіїв інформації інформаційної системи; процедури, що стосуються зниження категорії безпеки носіїв; процедури, що стосуються випробувань обладнання, що знижує категорії безпеки носіїв; результати тестування обладнання та процедур, що знижують категорії безпеки носіїв; записи аудиту: інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, який відповідає за зниження категорії безпеки носіїв; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для зниження категорії безпеки носіїв; автоматизовані механізми підтримки та / або впровадження зниження категорії безпеки носіїв; автоматизовані механізми, що підтримують та / або впроваджують випробування для зниження категорії безпеки носіїв]. | | |

|  |  |  |
| --- | --- | --- |
| MP-8(3) | ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - КРИТИЧНА ІНФОРМАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MP-8(3)[1] | Організація визначає критичну інформацію за наявності якої на носії інформації, знижують категорію безпеки носіїв до рівня публічного доступу. |
| MP-8(3)[2] | Знижувати категорію безпеки носіїв, що містять визначену організацією критичну інформацію до рівня публічного доступу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика захисту носіїв інформації інформаційної системи; політика авторизації доступу; процедури, що стосуються зниження категорії безпеки носіїв, що містять критичну несекретну інформацію; застосовними державними та організаційними стандартами та політикою щодо захисту критичної несекретної інформації; зниження категорії безпеки носіїв; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за зниження категорії безпеки носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для зниження категорії безпеки носіїв; автоматизовані механізми підтримки та / або впровадження зниження категорії безпеки носіїв]. | |

|  |  |  |
| --- | --- | --- |
| MP-8(4) | ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - ТАЄМНА ІНФОРМАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| MP-8(4)[1] | Знижувати категорію безпеки носіїв, що містять таємну інформацію, до категорії безпеки для осіб без необхідних дозволів на доступ. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика захисту носіїв інформації інформаційної системи; політика авторизації доступу; процедури розв’язання питання зниження категорії безпеки носіїв інформації, що містять секретну інформацію; процедури, що стосуються обробки секретної інформації; Стандарти та політика щодо захисту секретної інформації; зниження категорії безпеки носіїв; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за зниження категорії безпеки носіїв інформації; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для зниження категорії безпеки носіїв; автоматизовані механізми підтримки та / або впровадження зниження категорії безпеки носіїв]. | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ PA – АВТОРИЗАЦІЯ ПРИВАТНОСТІ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PA-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ АВТОРИЗАЦІЇ ПРИВАТНОСТІ | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| PA-1(a) | PA-1(a)[1] | PA-1(a)[1](1) | | | Розробляє та документує політику авторизації приватності, яка: | | | | | | | | |
| PA-1(a)[1](1)(a) | | Містить: | | | | | | |
| PA-1(a)[1](1)(a)[1] | | | | мету, | | |
| PA-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| PA-1(a)[1](1)(a)[3] | | | | ролі, | | |
| PA-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| PA-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| PA-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| PA-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| PA-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| PA-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| PA-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| PA-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| PA-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| PA-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| PA-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| PA-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| PA-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики авторизації приватності та відповідних заходів управління доступом | | | | | | | | |
| PA-1(a)[2] | PA-1(a)[2]{1} | | | PA-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика авторизації приватності | | | | | |
| PA-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики авторизації приватності та пов'язаних з нею заходів авторизації приватності | | | | | |
| PA-1(a)[2]{2} | | | PA-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика авторизації приватності | | | | | |
| PA-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики авторизації приватності та пов'язаних з нею заходів авторизації приватності | | | | | |
| PA-1(a)[3] | PA-1(a)[3]{1} | | | PA-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику авторизації приватності, яка: | | | | | | | |
| PA-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| PA-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| PA-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| PA-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| PA-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| PA-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| PA-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| PA-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| PA-1(a)[3](1)(b) | | | Відповідає: | | | | |
| PA-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| PA-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| PA-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| PA-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| PA-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| PA-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| PA-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| PA-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації політики авторизації приватності та відповідних заходів управління доступом | | | | | | | |
| PA-1(a)[3]{2} | | | PA-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику авторизації приватності, яка: | | | | | | | |
| PA-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| PA-1(a)[3]{2}(1)(а)[1] | | мету, | |
| PA-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| PA-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| PA-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| PA-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| PA-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| PA-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| PA-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| PA-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| PA-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| PA-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| PA-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| PA-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| PA-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| PA-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| PA-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики авторизації приватності та пов'язаних з нею заходів авторизації приватності | | | | | | | |
| PA-1(b) | PA-1(b)[1] | визначає посадову особу для управління політикою та процедурами авторизації приватності | | | | | | | | | | | |
| PA-1(b)[2] | призначає посаду для управління політикою та процедурами авторизації приватності | | | | | | | | | | | |
| PA-1(с) | PA-1(с)[1] | PA-1(с)[1](1) | | PA-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики авторизації приватності | | | | | | | |
| PA-1(с)[1](1)[2] | | переглядає поточну політику авторизації приватності з визначеною організацією частотою | | | | | | | |
| PA-1(с)[1](2) | | PA-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур авторизації приватності | | | | | | | |
| PA-1(с)[1](2)[2] | | переглядає поточні процедури авторизації приватності з визначеною організацією частотою | | | | | | | |
| PA-1(с)[2] | PA-1(с)[2](1) | | PA-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики авторизації приватності | | | | | | | |
| PA-1(с)[2](1)[2] | | оновлює поточну політику авторизації приватності з визначеною організацією частотою | | | | | | | |
| PA-1(с)[2](2) | | PA-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур авторизації приватності | | | | | | | |
| PA-1(с)[2](2)[2] | | оновлює поточні процедури авторизації приватності з визначеною організацією частотою | | | | | | | |
| PA-1(d) | переконується, що процедури авторизації приватності реалізують політику та заходи авторизації приватності | | | | | | | | | | | | |
| PA-1(e) | PA-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики авторизації приватності | | | | | | | | | | |
| PA-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики авторизації приватності | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури авторизації приватності; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику авторизації приватності; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PA-2 | ПОВНОВАЖЕННЯ НА ЗБІР ПЕРСОНАЛЬНИХ ДАНИХ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PA-2[1] | Визначати уповноважений орган, який буде мати право~~,~~ як в цілому, так і для підтримки конкретної програми або системи: | |
| PA-2[1][1] | збирати персональні дані |
| PA-2[1][2] | використовувати персональні дані |
| PA-2[1][3] | обслуговувати персональні дані |
| PA-2[1][4] | розповсюджуватися персональні дані |
| PA-2[2] | надати уповноваженому органу повноваження~~,~~ як в цілому, так і для підтримки конкретної програми або системи: | |
| PA-2[2][1] | збирати персональні дані |
| PA-2[2][2] | використовувати персональні дані |
| PA-2[2][3] | обслуговувати персональні дані |
| PA-2[2][4] | розповсюджуватися персональні дані |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PA-3 | СПЕЦИФІКАЦІЯ МЕТИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PA-3[1] | Визначити та задокументувати мету (цілі), для якої | |
| PA-3[1][1] | Збирається персональні дані в повідомленнях про приватність |
| PA-3[1][2] | використовується персональні дані в повідомленнях про приватність |
| PA-3[1][3] | підтримується персональні дані в повідомленнях про приватність |
| PA-3[1][4] | розповсюджуються персональні дані в повідомленнях про приватність |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PA-3(1) | СПЕЦИФІКАЦІЯ МЕТИ - ОБМЕЖЕННЯ ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ (ПД) | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PA-3(1)[1] | Обмежити використання ПД лише для дозволених цілей, відповідно до: | |
| PA-3(1)[1]{1} | чинного законодавства |
| PA-3(1)[1]{2} | Чинних правил |
| PA-3(1)[1]{3} | публічних повідомлень |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PA-3(2) | СПЕЦИФІКАЦІЯ МЕТИ - АВТОМАТИЗАЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PA-3(2)[1] | Використовувати автоматизовані механізми для підтримки: | |
| PA-3(2)[1][1] | управлінського обліку політик авторизації, що стосуються ПД. |
| PA-3(2)[1][2] | управлінського обліку процедур авторизації, що стосуються ПД. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політика управління управлінського обліку політик авторизації; план безпеки; проєктна документація інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи чи записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за управління розташуванням інформації; організаційний персонал, що працює, використовує та / або підтримує інформаційну систему].  Перевірка: [ВИБРАТИ З: Організаційні процеси, що керують управлінським обліком політик авторизації] | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| РА-4 | ОБМІН ПЕРСОНАЛЬНИМИ ДАНИМИ З СТОРОННІМИ ОРГАНІЗАЦІЯМИ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| РА-4(a) | РА-4(a)[1] | Розробити, задокументувати рекомендації для обміну ПД зі сторонніми організаціями тільки: | | | |
| РА-4(a)[1][1] | для дозволених цілей, | | |
| РА-4(a)[1][2] | РА-4(a)[1][2]{1} | | відповідно до чинного законодавства, |
| РА-4(a)[1][2]{2} | | для цілей, які сумісні з дозволеними цілями |
| РА-4(a)[2] | РА-4(a)[2][1] | РА-4(a)[2][1]{1} | | організація визначає персонал серед якого поширюють рекомендації для обміну ПД зі сторонніми організаціями |
| РА-4(a)[2][1]{2} | | організація визначає ролі серед яких поширюють рекомендації для обміну ПД зі сторонніми організаціями |
| РА-4(a)[2][2] | поширити рекомендації для обміну ПД з сторонніми організаціями серед: | | |
| РА-4(a)[2][2]{1} | | визначеного організацією персоналу |
| РА-4(a)[2][2]{2} | | визначеного організацією ролей |
| РА-4(b) | Оцінити запропоновані нові випадки обміну ПД із зовнішніми сторонами для оцінки того: | | | | |
| РА-4(b)(1) | Чи є дозволеним спільне використання | | | |
| РА-4(b)(2) | РА-4(b)(2){1} | | Чи потребує цей обмін додаткового публічного повідомлення | |
| РА-4(b)(2){2} | | Чи потребує цей обмін нового публічного повідомлення | |
| РА-4(c) | Укласти угоду про обмін ПД зі сторонніми організаціями, яка зокрема: | | | | |
| РА-4(c)[1] | Описує ПД, що є предметом угоди | | | |
| РА-4(c)[2] | Перераховує цілі, для яких можуть бути використані ПД | | | |
| РА-4(c)[3] | Включає вимоги безпеки, які відповідають інформації, що підлягає обміну | | | |
| РА-4(d) | РА-4(d)[1] | Проводити моніторинг дозволеного спільного використання ПД зі сторонніми організаціями | | | |
| РА-4(d)[2] | Проводити аудит дозволеного спільного використання ПД зі сторонніми організаціями | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика контролю доступу; стратегія управління персональними даними; процедури, що стосуються персональних даних, інші відповідні документи або записи].  Співбесіда: [ВИБІР: Системні / мережеві адміністратори; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи].  Перевірка [ВИБІР: Автоматизовані механізми, що реалізують збір дозволу обробку своїх персональних даних]. | | | | | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ PE -** [**ФІЗИЧНИЙ ЗАХИСТ ТА ЗАХИСТ РОБОЧОГО СЕРЕДОВИЩА**](#_РЕ-1_Політика_та)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| РЕ-1 | ПОЛІТИКА ТА ПРОЦЕДУРИ ФІЗИЧНОГО ЗАХИСТУ ТА ЗАХИСТУ РОБОЧОГО СЕРЕДОВИЩА | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | | | | | | | | | | | |
| PE-1(a) | PE-1(a)[1] | PE-1(a)[1](1) | | | Розробляє та документує політику та процедури фізичного захисту та захисту робочого середовища , яка: | | | | | | | | |
| PE-1(a)[1](1)(a) | | Містить: | | | | | | |
| PE-1(a)[1](1)(a)[1] | | | | мету, | | |
| PE-1(a)[1](1)(a)[2] | | | | сферу застосування, | | |
| PE-1(a)[1](1)(a)[3] | | | | ролі, | | |
| PE-1(a)[1](1)(a)[4] | | | | обов'язки, | | |
| PE-1(a)[1](1)(a)[5] | | | | відповідальність керівництва, | | |
| PE-1(a)[1](1)(a)[6] | | | | координацію між організаційними підрозділами | | |
| PE-1(a)[1](1)(a)[7] | | | | систему контролю відповідності (compliances); | | |
| PE-1(a)[1](1)(b) | | Відповідає: | | | | | | |
| PE-1(a)[1](1)(b)[1] | | | | чинному законодавству, | | |
| PE-1(a)[1](1)(b)[2] | | | | чинним нормативним документам, | | |
| PE-1(a)[1](1)(b)[3] | | | | чинним директивам, | | |
| PE-1(a)[1](1)(b)[4] | | | | чинним нормам, | | |
| PE-1(a)[1](1)(b)[5] | | | | чинним політикам, | | |
| PE-1(a)[1](1)(b)[6] | | | | чинним стандартам | | |
| PE-1(a)[1](1)(b)[7] | | | | чинним керівним документам | | |
| PE-1(a)[1](2) | | | розробляє, документує процедури, що сприяють реалізації політики в галузі фізичного захисту та захисту робочого середовища та відповідних заходів управління доступом | | | | | | | | |
| PE-1(a)[2] | PE-1(a)[2]{1} | | | PE-1(a)[2]{1}[1] | | | визначає персонал серед якого має бути поширена політика індивідуальної участі | | | | | |
| PE-1(a)[2]{1}[2] | | | визначає персонал серед якого мають бути поширені процедури, що спрямовані на реалізацію політики в галузі фізичного захисту та захисту робочого середовища та пов'язаних з нею заходів в галузі фізичного захисту та захисту робочого середовища | | | | | |
| PE-1(a)[2]{2} | | | PE-1(a)[2]{2}[1] | | | визначає посадових осіб серед яких має бути поширена політика в галузі фізичного захисту та захисту робочого середовища | | | | | |
| PE-1(a)[2]{2}[2] | | | визначає посадових осіб серед яких мають бути поширені процедури, що спрямовані на реалізацію політики в галузі фізичного захисту та захисту робочого середовища та пов'язаних з нею заходів в галузі фізичного захисту та захисту робочого середовища | | | | | |
| PE-1(a)[3] | PE-1(a)[3]{1} | | | PE-1(a)[3]{1}(1) | поширює серед визначеного організацією персоналу політику в галузі фізичного захисту та захисту робочого середовища, яка: | | | | | | | |
| PE-1(a)[3]{1}(1)(a) | | | Містить: | | | | |
| PE-1(a)[3]{1}(1)(a)[1] | | | | мету, |
| PE-1(a)[3]{1}(1)(a)[2] | | | | сферу застосування, |
| PE-1(a)[3]{1}(1)(a)[3] | | | | ролі, |
| PE-1(a)[3]{1}(1)(a)[4] | | | | обов'язки, |
| PE-1(a)[3]{1}(1)(a)[5] | | | | зобов'язання керівництва, |
| PE-1(a)[3]{1}(1)(a)[6] | | | | координацію між організаційними підрозділами |
| PE-1(a)[3]{1}(1)(a)[7] | | | | систему контролю відповідності (compliances); |
| PE-1(a)[3](1)(b) | | | Відповідає: | | | | |
| PE-1(a)[3]{1}(1)(b)[1] | | | | чинному законодавству |
| PE-1(a)[3]{1}(1)(b)[2] | | | | чинним нормативним документам, |
| PE-1(a)[3]{1}(1)(b)[3] | | | | чинним директивам, |
| PE-1(a)[3]{1}(1)(b)[4] | | | | чинним нормам, |
| PE-1(a)[3]{1}(1)(b)[5] | | | | чинним політикам, |
| PE-1(a)[3]{1}(1)(b)[6] | | | | чинним стандартам |
| PE-1(a)[3]{1}(1)(b)[7] | | | | чинним керівним документам |
| PE-1(a)[3]{1}(2) | поширює серед визначених організацією персоналу процедури, що сприяють реалізації політики в галузі фізичного захисту та захисту робочого середовища та відповідних заходів управління доступом | | | | | | | |
| PE-1(a)[3]{2} | | | PE-1(a)[3]{2}(1) | поширює серед визначених організацією ролей політику в галузі фізичного захисту та захисту робочого середовища, яка: | | | | | | | |
| PE-1(a)[3]{2}(1)(а) | | | | Містить: | | | |
| PE-1(a)[3]{2}(1)(а)[1] | | мету, | |
| PE-1(a)[3]{2}(1)(а)[2] | | сферу застосування, | |
| PE-1(a)[3]{2}(1)(а)[3] | | ролі, | |
| PE-1(a)[3]{2}(1)(а)[4] | | обов'язки, | |
| PE-1(a)[3]{2}(1)(а)[5] | | відповідальність керівництва, | |
| PE-1(a)[3]{2}(1)(а)[6] | | координацію між організаційними підрозділами | |
| PE-1(a)[3]{2}(1)(а)[7] | | систему контролю відповідності (compliances); | |
| PE-1(a)[3]{2}(1)(b) | | | | Відповідає: | | | |
| PE-1(a)[3]{2}(1)(b) | | чинному законодавству | |
| PE-1(a)[3]{2}(1)(b) | | чинним нормативним документам, | |
| PE-1(a)[3]{2}(1)(b) | | чинним директивам, | |
| PE-1(a)[3]{2}(1)(b) | | чинним нормам, | |
| PE-1(a)[3]{2}(1)(b) | | чинним політикам, | |
| PE-1(a)[3]{2}(1)(b) | | чинним стандартам | |
| PE-1(a)[3]{2}(1)(b) | | чинним керівним документам | |
| PE-1(a)[3]{2}(2) | поширює серед визначених організацією ролей процедури, що сприяють реалізації політики в галузі фізичного захисту та захисту робочого середовища та пов'язаних з нею заходів фізичного захисту та захисту робочого середовища | | | | | | | |
| PE-1(b) | PE-1(b)[1] | визначає посадову особу для управління політикою та процедурами фізичного захисту та захисту робочого середовища | | | | | | | | | | | |
| PE-1(b)[2] | призначає посаду для управління політикою та процедурами фізичного захисту та захисту робочого середовища | | | | | | | | | | | |
| PE-1(с) | PE-1(с)[1] | PE-1(с)[1](1) | | PE-1(с)[1](1)[1] | | визначає частоту перегляду поточної політики в галузі фізичного захисту та захисту робочого середовища | | | | | | | |
| PA-1(с)[1](1)[2] | | переглядає поточну політику в галузі фізичного захисту та захисту робочого середовища з визначеною організацією частотою | | | | | | | |
| PE-1(с)[1](2) | | PE-1(с)[1](2)[1] | | визначає частоту перегляду поточних процедур фізичного захисту та захисту робочого середовища | | | | | | | |
| PE-1(с)[1](2)[2] | | переглядає поточні процедури фізичного захисту та захисту робочого середовища з визначеною організацією частотою | | | | | | | |
| PE-1(с)[2] | PE-1(с)[2](1) | | PE-1(с)[2](1)[1] | | визначає частоту оновлення поточної політики в галузі фізичного захисту та захисту робочого середовища | | | | | | | |
| PE-1(с)[2](1)[2] | | оновлює поточну політику в галузі фізичного захисту та захисту робочого середовища з визначеною організацією частотою | | | | | | | |
| PE-1(с)[2](2) | | PE-1(с)[2](2)[1] | | визначає частоту оновлення поточних процедур авторизації приватності | | | | | | | |
| PE-1(с)[2](2)[2] | | оновлює поточні процедури фізичного захисту та захисту робочого середовища з визначеною організацією частотою | | | | | | | |
| PE-1(d) | переконується, що процедури фізичного захисту та захисту робочого середовища реалізують політику та заходи фізичного захисту та захисту робочого середовища | | | | | | | | | | | | |
| PE-1(e) | PE-1(e)[1] | | розробляє та задокументовує процедури відновлення у разі порушень політики в галузі фізичного захисту та захисту робочого середовища | | | | | | | | | | |
| PE-1(e)[2] | | впроваджує процедури відновлення у разі порушень політики в галузі фізичного захисту та захисту робочого середовища | | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політики та процедури фізичного захисту та захисту робочого середовища; інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Персонал відповідальний за політику фізичного захисту та захисту робочого середовища; персонал, відповідальний за інформаційну безпеку]. | | | | | | | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| РЕ-2 | АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| РЕ-2(a) | РЕ-2(a)[1] | Розробити, перелік осіб, які мають право авторизованого доступу до об'єкта, де знаходиться система | |
| РЕ-2(a)[2] | затвердити перелік осіб, які мають право авторизованого доступу до об'єкта, де знаходиться система | |
| РЕ-2(a)[3] | вести перелік осіб, які мають право авторизованого доступу до об'єкта, де знаходиться система | |
| РЕ-2(b) | Надати повноваження для доступу до об'єкта для визначених раніше осіб | | |
| РЕ-2(c) | РЕ-2(c)[1] | організація визначає частоту з якою переглядають список доступу, в якому закріплений перелік персоналу або ролей, яким дозволений санкціонований доступ до об’єкта | |
| РЕ-2(c)[2] | Переглядати список доступу, в якому закріплений перелік: | |
| РЕ-2(c)[2]{1} | персоналу, якому дозволений санкціонований доступ до об’єкта з визначеною організацією частотою |
| РЕ-2(c)[2]{2} | ролей, яким дозволений санкціонований доступ до об’єкта з визначеною організацією частотою |
| РЕ-2(d) | Видалити персонал зі списку доступу до об'єкта, коли такий доступ більше не потрібний | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються дозволів фізичного доступу; план безпеки; список доступу уповноваженого персоналу; авторизаційні дані; огляди списків фізичного доступу; записи про припинення фізичного доступу та відповідна документація; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за дозвіл на фізичний доступ; організаційний персонал з фізичним доступом до об'єкта інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для дозволів фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують дозволи фізичного доступу]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-2(1) | АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ - ДОСТУП НА ОСНОВІ ПОСАДИ АБО РОЛІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-2(1)[1] | Авторизувати фізичний доступ до об'єкта, де знаходиться система на основі: | |
| РЕ-2(1)[1]{1} | ролі |
| РЕ-2(1)[1]{2} | посади |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються дозволів фізичного доступу; журнали або записи фізичного контролю доступу; перелік посад / ролей та відповідних дозволів фізичного доступу; точки входу та виходу інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за дозвіл фізичного доступу; організаційний персонал з фізичним доступом до об'єкта інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для дозволів фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують дозволи фізичного доступу]. | | |

|  |  |  |
| --- | --- | --- |
| РЕ-2(2) | АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ - ДВІ ФОРМИ ІДЕНТИФІКАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-2(2)[1] | організація визначає список прийнятних форм ідентифікації |
| РЕ-2(2)[2] | Вимагати дві форми ідентифікації від визначеного організацією списку прийнятних форм ідентифікації для доступу відвідувачів до об'єкта, де знаходиться система. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються дозволів фізичного доступу; перелік прийнятних форм ідентифікації для доступу відвідувачів до закладу, де знаходиться інформаційна система; доступ до форм авторизації; облікові дані доступу; журнали або записи фізичного контролю доступу; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за дозвіл на фізичний доступ; організаційний персонал з фізичним доступом до об'єкта інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для дозволів фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують дозволи фізичного доступу]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-2(3) | АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ - ОБМЕЖЕННЯ ДОСТУПУ БЕЗ СУПРОВОДУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-2(3)[1] | визначені організацією повноваження при наявності яких персоналу необхідне супровід при доступі до об’єкта, де розміщується інформаційна система | |
| РЕ-2(3)[2] | Заборонити доступ без супроводу до об'єкта, де розміщується інформаційна система, для персоналу, що має одне або кілька з наступного: | |
| РЕ-2(3)[2]{1} | рівень допуску для всієї інформації, що міститься в системі; |
| РЕ-2(3)[2]{2} | авторизація офіційного доступу до всієї інформації, що міститься в системі; |
| РЕ-2(3)[2]{3} | необхідність доступу до всієї інформації, що міститься в системі; |
| РЕ-2(3)[2]{4} | визначені організацією повноваження |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються дозволів фізичного доступу; список доступу уповноваженого персоналу; дозволи безпеки; дозволи на доступ; облікові дані доступу; журнали або записи контролю фізичного доступу; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за дозвіл на фізичний доступ; організаційний персонал з фізичним доступом до об'єкта інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для дозволів фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують дозволи фізичного доступу]. | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| РЕ-3 | КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | | | |
| РЕ-3(a) | РЕ-3(a)[1] | | РЕ-3(a)[1][1] | | організація визначає точки входу до об'єкта, де знаходиться система | | | | | | | |
| РЕ-3(a)[1][2] | | організація визначає точки виходу до об'єкта, де знаходиться система | | | | | | | |
| РЕ-3(a)[2] | | Забезпечити авторизацію фізичного доступу за адресою визначених організацією точок входу до об'єкта, де знаходиться система шляхом: | | | | | | | | | |
| РЕ-3(a)[2](1) | | Перевірки індивідуального дозволу доступу до об'єкта | | | | | | | |
| РЕ-3(a)[2](2) | | РЕ-3(a)[2](2)[1] | | | РЕ-3(a)[2](2)[1]{1} | | | | організація визначає, фізичні системи контролю доступу |
| РЕ-3(a)[2](2)[2]{2} | | | | організація визначає, пристрої контролю доступу |
| РЕ-3(a)[2](2)[2] | | | Управління входом на об'єкт за допомогою (вибрати один або кілька): | | | | |
| РЕ-3(a)[2](2)[2]{1} | | | | визначені  організацією, фізичні системи контролю доступу |
| РЕ-3(a)[2](2)[2]{2} | | | | визначені організацією, фізичні пристрої контролю доступу |
| РЕ-3(a)[2](2)[2]{3} | | | | охорона |
| РЕ-3(a)[2](2)[3] | | | Управління виходом на об'єкт за допомогою (вибрати один або кілька): | | | | |
| РЕ-3(a)[2](2) [3]{1} | | | | визначені організацією, фізичні системи контролю доступу |
| РЕ-3(a)[2](2)[3]{2} | | | | визначені організацією, фізичні пристрої контролю доступу |
| РЕ-3(a)[2](2)[3]{3} | | | | охорона |
| РЕ-3(a)[3] | | Забезпечити авторизацію фізичного доступу за адресою визначених організацією точок виходу з об'єкта, де знаходиться система шляхом: | | | | | | | | | |
| РЕ-3(a)[3](1) | | | Перевірки індивідуального дозволу доступу до об'єкта | | | | | | |
| РЕ-3(a)[3](2) | | | РЕ-3(a)[3](2)[1] | | | РЕ-3(a)[3](2)[1]{1} | | | організація визначає, фізичні системи контролю доступу |
| РЕ-3(a)[3](2)[2]{2} | | | організація визначає, пристрої контролю доступу |
| РЕ-3(a)[3](2)[2] | | | Управління входом на об'єкт за допомогою (вибрати один або кілька): | | | |
| РЕ-3(a)[3](2)[2]{1} | | | визначені організацією, фізичні системи контролю доступу |
| РЕ-3(a)[3](2)[2]{2} | | | визначені організацією, фізичні пристрої контролю доступу |
| РЕ-3(a)[3](2)[2]{3} | | | охорона |
| РЕ-3(a)[3](2)[3] | | | Управління виходом на об'єкт за допомогою (вибрати один або кілька): | | | |
| РЕ-3(a)[3](2) [3]{1} | | | визначені організацією, фізичні системи контролю доступу |
| РЕ-3(a)[3](2)[3]{2} | | | визначені організацією, фізичні пристрої контролю доступу |
| РЕ-3(a)[3](2)[3]{3} | | | охорона |
| РЕ-3(b) | | РЕ-3(b)[1] | | РЕ-3(b)[1][1] | | | організація визначає точки входу на яких необхідно вести журнали контролю фізичного доступу | | | | | |
| РЕ-3(b)[1][2] | | | організація визначає точки виходу на яких необхідно вести журнали контролю фізичного доступу | | | | | |
| РЕ-3(b)[2] | | РЕ-3(b)[2][1] | | | Вести журнали контролю фізичного доступу для визначеної організацією точки входу | | | | | |
| РЕ-3(b)[2][2] | | | Вести журнали контролю фізичного доступу для визначеної організацією точки виходу | | | | | |
| РЕ-3(c) | | РЕ-3(c)[1] | | організація визначає заходи захисту для контролю доступу в зони всередині об'єкта, позначені як загальнодоступний | | | | | | | | |
| РЕ-3(c)[2] | | Забезпечити визначені організацією заходи захисту для контролю доступу в зони всередині об'єкта, позначені як загальнодоступний | | | | | | | | |
| РЕ-3(d) | | РЕ-3(d)[1] | | визначені організацією умови, що вимагають супроводу відвідувачів і моніторингу | | | | | | | | |
| РЕ-3(d)[2] | | РЕ-3(d)[2][1] | | | Супроводжувати відвідувачів за визначених організацією умов, що вимагають: | | | | | |
| РЕ-3(d)[2][1][1] | | | супроводу відвідувачів | | |
| РЕ-3(d)[2][1][2] | | | моніторингу | | |
| РЕ-3(d)[2][2] | | | контролювати активність відвідувачів визначені організацією умови, що вимагають супроводу відвідувачів і моніторингу | | | | | |
| РЕ-3(d)[2][2][1] | | | супроводу відвідувачів | | |
| РЕ-3(d)[2][2][2] | | | моніторингу | | |
| РЕ-3(e) | | Забезпечити захист: | | | | | | | | | | |
| РЕ-3(e)[1] | | ключів, | | | | | | | | |
| РЕ-3(e)[2] | | кодів доступу | | | | | | | | |
| РЕ-3(e)[3] | | інших пристроїв фізичного доступу | | | | | | | | |
| РЕ-3(f) | | РЕ-3(f)[1] | | РЕ-3(f)[1][1] | | | організація визначає пристрої фізичного доступу щодо яких необхідно проводити інвентаризацію | | | | | |
| РЕ-3(f)[1][2] | | | організація визначає частоту з якою необхідно проводити інвентаризацію пристроїв фізичного доступу | | | | | |
| РЕ-3(f)[2] | | Проводити інвентаризацію визначених організацією пристроїв фізичного доступу з визначеною організацією частотою | | | | | | | | |
| РЕ-3(g) | | РЕ-3(g)[1] | | РЕ-3(g)[1][1] | | | організація визначає частоту з якою необхідно здійснювати зміну кодів доступу | | | | | |
| РЕ-3(g)[1][2] | | | організація визначає частоту з якою необхідно здійснювати зміну ключів | | | | | |
| РЕ-3(g)[2] | | РЕ-3(g)[2][1] | | | Здійснювати зміну кодів з визначеною організацією частотою коли: | | | | | |
| РЕ-3(g)[2][1]{1} | | | | ключі втрачені, | |
| РЕ-3(g)[2][1]{2} | | | | комбінації скомпрометовані | |
| РЕ-3(g)[2][1]{3} | | | | фізичні особи переведені | |
| РЕ-3(g)[2][1]{4} | | | | фізичні особи звільнені. | |
| РЕ-3(g)[2][2] | | | Здійснювати зміну ключів з визначеною організацією частотою коли: ключі втрачені, комбінації скомпрометовані або фізичні особи переведені або звільнені. | | | | | |
| РЕ-3(g)[2][2]{1} | | | ключі втрачені, | | |
| РЕ-3(g)[2][2]{2} | | | комбінації скомпрометовані | | |
| РЕ-3(g)[2][2]{3} | | | фізичні особи переведені | | |
| РЕ-3(g)[2][2]{4} | | | фізичні особи звільнені. | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; журнали або записи контролю фізичного доступу; пристрої фізичного контролю доступу; дозволи на доступ; облікові дані доступу; точки входу та виходу інформаційної системи; перелік територій в установі, що містять концентрації компонентів інформаційної системи або компонентів інформаційної системи, що потребують додаткового фізичного захисту; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за фізичний дозвіл на доступ; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для контролю фізичного доступу до інформаційної системи / компонентів; автоматизовані механізми, що підтримують та / або впроваджують фізичний контроль доступу до об'єктів, що містять компоненти інформаційної системи]. | | | | | | | | | | | | |

|  |  |  |
| --- | --- | --- |
| РЕ-3(1) | КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ДОСТУП ДО СИСТЕМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-3(1)[1] | організація визнає фізичні приміщення, що містять один або більше компонентів системи, до яких необхідно застосовувати авторизацію фізичного доступу до системи на додаток до керування фізичного доступу до об’єкта |
| РЕ-3(1)[2] | Застосовувати авторизацію фізичного доступу до системи на додаток до керування фізичного доступу до об’єкта в визначених організацією фізичних приміщеннях, що містять один або більше компонентів системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; журнали або записи контролю фізичного доступу; пристрої контролю фізичного доступу; дозволи на доступ; облікові дані доступу; точки входу та виходу інформаційної системи; перелік територій в установі, що містять концентрації компонентів інформаційної системи або компонентів інформаційної системи, що потребують додаткового фізичного захисту; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за фізичний дозвіл на доступ; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для контролю фізичного доступу до інформаційної системи / компонентів; автоматизовані механізми, що підтримують та / або впроваджують контроль фізичного доступу до об'єктів, що містять компоненти інформаційної системи]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| РЕ-3(2) | КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - МЕЖІ ОБ’ЄКТУ ТА СИСТЕМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| РЕ-3(2)[1] | РЕ-3(2)[1]{1} | організація визнає частоту з якою необхідно здійснювати перевірку безпеки на фізичній межі об'єкта для: | |
| РЕ-3(2)[1]{1}{1} | видалення інформації |
| РЕ-3(2)[1]{1}{2} | вилучення компонентів системи |
| РЕ-3(2)[1]{2} | організація визнає частоту з якою необхідно здійснювати перевірку безпеки на фізичній межі системи для: | |
| РЕ-3(2)[1]{2}{1} | видалення інформації |
| РЕ-3(2)[1]{2}{2} | вилучення компонентів системи |
| РЕ-3(2)[2] | РЕ-3(2)[2]{1} | Здійснювати перевірку безпеки з визначеною організацією частотою на фізичній межі об'єкта для: | |
| РЕ-3(2)[2]{1}{1} | видалення інформації |
| РЕ-3(2)[2]{1}{2} | вилучення компонентів системи |
| РЕ-3(2)[2]{2} | Здійснювати перевірку безпеки з визначеною організацією частотою на фізичній межі системи для видалення інформації або вилучення компонентів системи | |
| РЕ-3(2)[2]{2}{1} | видалення інформації |
| РЕ-3(2)[2]{2}{2} | вилучення компонентів системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; журнали або записи контролю фізичного доступу; записи перевірок безпеки; звіти про аудит безпеки; звіти про перевірку безпеки; документація з планування об'єкта; точки входу та виходу інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за фізичний контроль доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для контролю фізичного доступу до об'єкта та / або інформаційної системи; автоматизовані механізми, що підтримують та / або впроваджують контроль фізичного доступу до об'єкта або інформаційної системи; автоматизовані механізми, що підтримують та / або впроваджують перевірки безпеки на предмет несанкціонованого розповсюдження інформації]. | | | |

|  |  |  |
| --- | --- | --- |
| РЕ-3(3) | КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - БЕЗПЕРЕРВНА ОХОРОНА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-3(3)[1] | організація визначає фізичні точки доступу до яких необхідно забезпечити цілодобову безперервну охорону для контролю доступу до об'єкта, де знаходиться система |
| РЕ-3(3)[2] | Забезпечити цілодобову безперервну охорону для контролю доступу визначені організацією фізичні точки доступу до об'єкта, де знаходиться система |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; журнали або записи контролю фізичного доступу; пристрої контролю фізичного доступу; записи спостереження за об'єктами; документація з планування об'єкта; точки входу та виходу інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для контролю фізичного доступу до об'єкта, де знаходиться інформаційна система; автоматизовані механізми, що підтримують та / або впроваджують контроль фізичного доступу до об'єкта, де знаходиться інформаційна система]. | |

|  |  |  |
| --- | --- | --- |
| РЕ-3(4) | КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - КОРПУСИ ПОСИЛЕНОГО ЗАХИСТУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-3(4)[1] | організація визначає компоненти системи для яких необхідно використовувати фізичні корпуси посиленого захисту для захисту |
| РЕ-3(4)[2] | Використовувати фізичні корпуси посиленого захисту для захисту визначених організацією компонентів системи від несанкціонованого фізичного доступу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; план безпеки; перелік компонентів інформаційної системи, що потребують захисту через корпуси посиленого захисту; фізичні корпуси посиленого захисту; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: корпуси посиленого захисту]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| РЕ-3(5) | КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ЗАХИСТ ВІД ЗЛОМУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| РЕ-3(5)[1] | РЕ-3(5)[1][1] | організація визначає заходи захисту для: | |
| РЕ-3(5)[1][1]{1} | Виявлення фізичної підробки або підміни визначених організацією апаратних компонентів всередині системи. та/або |
| РЕ-3(5)[1][1]{2} | запобігання фізичної підробки або підміни визначених організацією апаратних компонентів всередині системи. |
| РЕ-3(5)[1][2] | організація визначає апаратні компоненти до яких необхідно застосовувати визначені організацією заходи захисту для: | |
| РЕ-3(5)[1][2]{1} | Виявлення фізичної підробки або підміни всередині системи. та/або |
| РЕ-3(5)[1][2]{2} | запобігання фізичної підробки або підміни всередині системи |
| РЕ-3(5)[1] | РЕ-3(5)[1]{1} | Застосовувати визначені організацією заходи захисту для виявлення фізичної підробки визначених організацією апаратних компонентів всередині системи | |
| РЕ-3(5)[1]{2} | Застосовувати визначені організацією заходи захисту для запобігання фізичної підміни визначених організацією апаратних компонентів всередині системи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; перелік гарантій безпеки для виявлення / запобігання фізичним фальсифікаціям чи змінам апаратних компонентів інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за фізичний контроль доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для виявлення / запобігання фізичному втручанню чи зміні апаратних компонентів інформаційної системи; автоматизовані механізми / гарантії безпеки, що підтримують та / або реалізують виявлення / запобігання фізичному втручанню / чергуванню апаратних компонентів інформаційної системи]. | | | |

|  |  |
| --- | --- |
| РЕ-3(6) | КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ТЕСТУВАННЯ НА МОЖЛИВІСТЬ ПРОНИКНЕННЯ |
|  | [Вилучено: включено до CA-8]. |

|  |  |  |
| --- | --- | --- |
| РЕ-3(7) | КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ФІЗИЧНІ ПЕРЕШКОДИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-3(7)[1] | Обмежити доступ за допомогою фізичних перешкод |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; перелік фізичних перешкод для обмеження доступу; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за фізичний контроль доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для виявлення / запобігання фізичному втручанню; автоматизовані механізми / гарантії безпеки, що підтримують та / або реалізують виявлення / запобігання фізичному втручанню до компонентів інформаційної системи]. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| РЕ-4 | КОНТРОЛЬ ДОСТУПУ ДО ДЖЕРЕЛ ТА ЛІНІЙ ЕЛЕКТРОЖИВЛЕННЯ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| РЕ-4[1] | РЕ-4[1][1] | організація визначає системи розподілу живлення доступ до яких підлягає контролю у рамках організаційних можливостей | | | |
| РЕ-4[1][2] | організація визначає системи постачання живлення доступ до яких підлягає контролю у рамках організаційних можливостей | | | |
| РЕ-4[1][3] | РЕ-4[1][3][1] | | організація встановлює заходи захисту за допомогою яких контролюють фізичний доступ до | |
| РЕ-4[1][3][1][1] | визначених організацією систем розподілу живлення у рамках організаційних можливостей |
| РЕ-4[1][3][1][2] | визначених організацією систем постачання живлення у рамках організаційних можливостей |
| РЕ-4[1][3][2] | | організація встановлює засоби захисту за допомогою яких контролюють фізичний доступ до: | |
| РЕ-4[1][3][2] | визначених організацією систем розподілу живлення у рамках організаційних можливостей |
| РЕ-4[1][3][2] | визначених організацією систем постачання живлення у рамках організаційних можливостей |
| РЕ-4[2] | РЕ-4[2][1] | Контролювати фізичний доступ до визначених організацією систем розподілу живлення у рамках організаційних можливостей, використовуючи встановлені організацією:. | | | |
| РЕ-4[2][1][1] | заходи захисту | | |
| РЕ-4[2][1][2] | засоби захисту | | |
| РЕ-4[2][2] | Контролювати фізичний доступ до визначених організацією систем постачання живлення у рамках організаційних можливостей, використовуючи встановлені організацією заходи та засоби захисту. | | | |
| РЕ-4[2][2][1] | заходи захисту | | |
| РЕ-4[2][2][2] | засоби захисту | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю доступу до середовища передачі; проєктна документація інформаційної системи; комунікаційні та електричні схеми об'єкта; перелік засобів фізичної безпеки, що застосовуються до ліній розподілу та передачі інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для контролю доступу до ліній розподілу та передачі; автоматизовані механізми / гарантії безпеки, що підтримують та / або впроваджують контроль доступу до ліній розподілу та передачі]. | | | | | |

|  |  |  |
| --- | --- | --- |
| РЕ-5 | КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-5[1] | організація визначає пристрої для виведення інформації над якими необхідний контроль над фізичним доступом до вихідних даних |
| РЕ-5[2] | Керувати фізичним доступом до вихідних даних з визначених організацією пристроїв для виведення інформації, для запобігання несанкціонованого отримання користувачами вихідних даних. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю доступу до носія виведення; фактичні відображення від компонентів інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для контролю доступу до пристроїв виведення; автоматизовані механізми, що підтримують та / або впроваджують контроль доступу до вихідних пристроїв]. | |

|  |  |  |
| --- | --- | --- |
| РЕ-5(1) | КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ - ДОСТУП ДО ВИХІДНИХ ДАНИХ УПОВНОВАЖЕНИМИ ОСОБАМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-5(1)[1] | Забезпечити, щоб тільки авторизовані особи отримували доступ до вихідних пристроїв |
| РЕ-5(1)[2] | перевіряти, що тільки авторизовані особи отримують доступ до вихідних пристроїв |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; перелік пристроїв виведення та супутніх виходів, що вимагають контролю фізичного доступу; журнали або записи контролю фізичного доступу для областей, що містять пристрої виведення та відповідні виходи; інші відповідні документи або записи].  Співбесіда: [ВИБІР З:Організаційний персонал, який відповідає за фізичний контроль доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З:Організаційні процеси для контролю доступу до вихідних пристроїв; автоматизовані механізми, що підтримують та / або впроваджують контроль доступу до вихідних пристроїв]. | |

|  |  |  |
| --- | --- | --- |
| РЕ-5(2) | КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ - ДОСТУП ДО ВИХІДНИХ ДАНИХ ФІЗИЧНИМИ ОСОБАМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-5(2)[1] | Пов'язувати дані про цифрову ідентичність з підтвердженням отримання даних від вихідних пристроїв |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік пристроїв виведення та супутніх виходів, що вимагають контролю фізичного доступу; журнали або записи контролю фізичного доступу для областей, що містять пристрої виведення та відповідні виходи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР З:Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи].  Перевірка: [ВИБІР З:Організаційні процеси для контролю доступу до вихідних пристроїв; автоматизовані механізми, що підтримують та / або впроваджують контроль доступу до вихідних пристроїв]. | |

|  |  |  |
| --- | --- | --- |
| РЕ-5(3) | КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ - МАРКУВАННЯ ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-5(3)[1] | організація визначає пристрої виведення інформації, яким необхідно забезпечити маркування, що вказує на мітку безпеки інформації, яку дозволено виводити з пристрою |
| РЕ-5(3)[2] | Забезпечити маркування визначених організацією пристроїв виведення інформації, що вказує на мітку безпеки інформації, яку дозволено виводити з пристрою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; маркування безпеки для типів інформації, дозволених як вихідні з пристроїв виведення інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР З:Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З:Організаційні процеси для маркування пристроїв виведення]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| РЕ-6 | МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| РЕ-6(a) | Проводити моніторинг фізичного доступу до об'єкта, де знаходиться система, з метою | | | |
| РЕ-6(a)[1] | виявлення на інциденти фізичної безпеки; | | |
| РЕ-6(a)[2] | реагування на інциденти фізичної безпеки; | | |
| РЕ-6(b) | РЕ-6(b)[1] | РЕ-6(b)[1]{1} | | організація визначає події на предмет наявності яких слід переглядати журнали фізичного доступу |
| РЕ-6(b)[1]{2} | | організація визначає потенційні ознаки подій на предмет наявності яких слід переглядати журнали фізичного доступу |
| РЕ-6(b)[2] | організація визначає частоту з якою необхідно переглядати журнали фізичного доступу на предмет наявності: | | |
| РЕ-6(b)[1]{1} | визначених організацією подій | |
| РЕ-6(b)[1]{2} | потенційних ознак подій | |
| РЕ-6(b)[3] | Переглядати журнали фізичного доступу з визначеною організацією частотою на предмет наявності визначених організацією подій або потенційних ознак подій | | |
| РЕ-6(c) | РЕ-6(c)[1] | Узгоджувати результати перегляду з організаційними можливостями реагування на інциденти | | |
| РЕ-6(c)[2] | Узгоджувати результати розслідувань з організаційними можливостями реагування на інциденти | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу фізичного доступу; план безпеки; журнали або записи фізичного доступу; записи моніторингу фізичного доступу; огляди журналу фізичного доступу; інші відповідні документи або записи].  Співбесіда: [ВИБІР З:Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, відповідальний за реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З:Організаційні процеси для моніторингу фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують моніторинг фізичного доступу; автоматизовані механізми, що підтримують та / або здійснюють перегляд фізичних журналів доступу]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-6(1) | МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - ОХОРОННА СИГНАЛІЗАЦІЯ ТА ОБЛАДНАННЯ ДЛЯ СПОСТЕРЕЖЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-6(1)[1] | Здійснювати моніторинг фізичного доступу до об'єкта, де розміщується система, використовуючи: | |
| РЕ-6(1)[1][1] | засоби сигналізації |
| РЕ-6(1)[1][2] | обладнання для спостереження |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу фізичного доступу; план безпеки; журнали або записи фізичного доступу; записи моніторингу фізичного доступу; огляди журналу фізичного доступу; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, відповідальний за реагування на інциденти; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для моніторингу фізичних сигналізацій про вторгнення та обладнання спостереження; автоматизовані механізми, що підтримують та / або впроваджують фізичний моніторинг доступу; автоматизовані механізми, що підтримують та / або впроваджують сигналізацію про фізичне вторгнення та обладнання спостереження]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-6(2) | МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - АВТОМАТИЧНЕ РОЗПІЗНАВАННЯ ВТОРГНЕНЬ ТА ВІДПОВІДНА РЕАКЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-6(2)[1] | РЕ-6(2)[1]{1} | організація визначає класи вторгнень задля розпізнавання яких необхідно впровадити автоматизовані механізми |
| РЕ-6(2)[1]{2} | організація визначає типи вторгнень задля розпізнавання яких необхідно впровадити автоматизовані механізми |
| РЕ-6(2)[2] | організація визначає відповідні реакції, які ініціюють при розпізнаванні визначених організацією класів або типів вторгнень | |
| РЕ-6(2)[3] | РЕ-6(2)[3]{1} | Впровадити автоматизовані механізми для розпізнавання визначених організацією класів вторгнень та ініціювання визначених організацією відповідних реакцій |
| РЕ-6(2)[3]{2} | Впровадити автоматизовані механізми для розпізнавання визначених організацією типів вторгнень та ініціювання визначених організацією відповідних реакцій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу фізичного доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; список дій відповіді, які слід розпочати, коли розпізнаються конкретні класи / типи вторгнень; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для моніторингу фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують моніторинг фізичного доступу; автоматизовані механізми, що підтримують та / або реалізують розпізнавання класів / типів вторгнень та ініціювання відповіді]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-6(3) | МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - ВІДЕОСПОСТЕРЕЖЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-6(3)[1] | РЕ-6(3)[1][1] | організація визначає зони в яких необхідно впровадити відеоспостереження |
| РЕ-6(3)[1][2] | організація визначає період часу впродовж якого необхідно зберігати відеозаписи |
| РЕ-6(3)[2] | РЕ-6(3)[2][1] | впровадити відеоспостереження визначених організацією зон |
| РЕ-6(3)[2][2] | зберігати відеозаписи впродовж визначеного організацією періоду часу. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу фізичного доступу; обладнання відеоспостереження, що використовується для спостереження за робочими зонами; відеозаписи операційних районів, де застосовується відеоспостереження; журнали або записи обладнання відеоспостереження; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для моніторингу фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують моніторинг фізичного доступу; автоматизовані механізми підтримки та / або впровадження відеоспостереження]. | | |

|  |  |  |
| --- | --- | --- |
| РЕ-6(4) | МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ ДО СИСТЕМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-6(4)[1] | організація визначає фізичні приміщення, що містять один або більше компонентів системи, які потребують здійснення моніторингу фізичного доступу до системи на додаток до моніторингу фізичного доступу до об'єкта |
| РЕ-6(4)[2] | здійснювати моніторинг фізичного доступу до системи на додаток до моніторингу фізичного доступу до об'єкта в визначені організацією фізичні приміщення, що містять один або більше компонентів системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу фізичного доступу; журнали або записи фізичного контролю доступу; пристрої фізичного контролю доступу; дозволи на доступ; облікові дані доступу; перелік територій на об'єкті, що містять концентрації компонентів інформаційної системи або компоненти інформаційної системи, що вимагають додаткового моніторингу фізичного доступу; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, який відповідає за контроль фізичного доступу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З:Організаційні процеси для моніторингу фізичного доступу до інформаційної системи; автоматизовані механізми, що підтримують та / або впроваджують моніторинг фізичного доступу до областей, що містять компоненти інформаційної системи]. | |

|  |  |
| --- | --- |
| РЕ-7 | КОНТРОЛЬ ВІДВІДУВАЧІВ |
|  | [Вилучено: Включено до РЕ-2 і РЕ-3]. |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-8 | РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-8(a) | РЕ-8(a)[1] | організація визначає період часу впродовж якого необхідно вести реєстр доступу відвідувачів до об'єкта, де знаходиться система. |
| РЕ-8(a)[2] | вести реєстр доступу відвідувачів до об'єкта, де знаходиться система, впродовж визначеного організацією періоду часу |
| РЕ-8(b) | РЕ-8(b)[1] | організація визначає частоту з якою необхідно Переглядати реєстр доступу відвідувачів |
| РЕ-8(b)[2] | Переглядати реєстр доступу відвідувачів з визначеною організацією частота |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються записів про доступ відвідувачів; план безпеки; журнали або записи контролю доступу відвідувачів; огляд доступу відвідувачів або огляди журналів; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за записи відвідувачів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для ведення та перегляду записів про доступ відвідувачів; автоматизовані механізми, що підтримують та / або впроваджують обслуговування та перегляд записів доступу відвідувачів]. | | |

|  |  |  |
| --- | --- | --- |
| РЕ-8(1) | РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ - АВТОМАТИЗОВАНЕ ВЕДЕННЯ ТА ПЕРЕГЛЯД РЕЄСТРУ ВІДВІДУВАЧІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-8(1)[1] | Впровадити автоматизовані механізми для ведення реєстру відвідувачів |
| РЕ-8(1)[2] | Впровадити автоматизовані механізми для перегляду (аналізу) реєстру відвідувачів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються записів про доступ відвідувачів; автоматизовані механізми, що підтримують управління записами доступу відвідувачів; журнали або записи контролю доступу відвідувачів; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за ведення запису відвідувачів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Організаційні процеси для ведення та перегляду записів про доступ відвідувачів; автоматизовані механізми, що підтримують та / або впроваджують обслуговування та перегляд записів доступу відвідувачів]. | |

|  |  |
| --- | --- |
| РЕ-8(2) | Реєстр доступу відвідувачів - Реєстр фізичного доступу |
|  | [Вилучено: включено до РЕ-2]. |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-9 | ЕНЕРГЕТИЧНЕ ОБЛАДНАННЯ ТА КАБЕЛІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-9[1] | Захищати енергетичне обладнання системи від: | |
| РЕ-9[1][1] | пошкоджень |
| РЕ-9[1][2] | руйнувань |
| РЕ-9[2] | Захищати силові кабелі системи від: | |
| РЕ-9[2][1] | пошкоджень |
| РЕ-9[2][2] | руйнувань |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються захисту енергетичного обладнання / кабелів; об'єкти, в яких розміщується енергетичне обладнання / кабелі; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за захист енергетичного обладнання / кабелів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують захист енергетичного обладнання / кабелів]. | | |

|  |  |  |
| --- | --- | --- |
| РЕ-9(1) | ЕНЕРГЕТИЧНЕ ОБЛАДНАННЯ ТА КАБЕЛІ - РЕЗЕРВНІ КАБЕЛІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-9(1)[1] | організація визначає відстань, на яку повинні бути відокремлені резервні силові кабельні системи |
| РЕ-9(1)[2] | Використовувати резервні силові кабельні системи, які фізично відокремлені на відстань визначена організацією відстань |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються захисту енергетичного обладнання / кабелів; об'єкти, в яких розміщується енергетичне обладнання / кабелі; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за захист енергетичного обладнання / кабелів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують захист енергетичного обладнання / кабелів]. | |

|  |  |  |
| --- | --- | --- |
| РЕ-9(2) | ЕНЕРГЕТИЧНЕ ОБЛАДНАННЯ ТА КАБЕЛІ - АВТОМАТИЧНЕ КЕРУВАННЯ НАПРУГОЮ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-9(2)[1] | організація визначає критичні компоненти системи для яких необхідно впровадити механізми автоматичного керування напругою |
| РЕ-9(2)[2] | Впровадити механізми автоматичного керування напругою для визначених організацією критичних компонентів системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю напруги; план безпеки; перелік важливих компонентів інформаційної системи, що вимагають автоматичного регулювання напруги; автоматичні механізми регулювання напруги та відповідні конфігурації; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за захисту робочого середовища компонентів інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують автоматичне регулювання напруги]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| РЕ-10 | АВАРІЙНЕ ВІДКЛЮЧЕННЯ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| РЕ-10(a) | РЕ-10(a){1} | Забезпечити можливість відключення системи від живлення у надзвичайних ситуаціях | | |
| РЕ-10(a){2} | Забезпечити можливість відключення окремих компонентів системи від живлення у надзвичайних ситуаціях | | |
| РЕ-10(b) | РЕ-10(b)[1] | РЕ-10(b)[1]{1} | організація визначає місця розташування в системі в яких буде встановлено: | |
| РЕ-10(b)[1]{1}{1} | перемикачі |
| РЕ-10(b)[1]{1}{2} | пристрої аварійного відключення |
| РЕ-10(b)[1]{2} | організація визначає місця розташування в компоненті системи | |
| РЕ-10(b)[1]{2}{1} | перемикачі |
| РЕ-10(b)[1]{2}{2} | пристрої  аварійного відключення |
| РЕ-10(b)[2] | РЕ-10(b)[2]{1} | Встановити перемикачі в визначені організацією місця розташування в: | |
| РЕ-10(b)[2]{1}{1} | системі для забезпечення безпечного та легкого доступу персоналу |
| РЕ-10(b)[2]{1}{2} | компоненті системи для забезпечення безпечного та легкого доступу персоналу |
| РЕ-10(b)[2]{1} | Встановити пристрої аварійного відключення в визначені організацією місця розташування в: | |
| РЕ-10(b)[2]{1}{1} | системі для забезпечення безпечного та легкого доступу персоналу |
| РЕ-10(b)[2]{1}{2} | компоненті системи для забезпечення безпечного та легкого доступу персоналу |
| РЕ-10(c) | Захищати механізми (систему) аварійного відключення живлення від несанкціонованої активації | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються аварійного відключення джерела живлення; план безпеки; аварійне відключення управління або перемикачів; місця розміщення аварійних вимикачів та пристроїв; запобіжні заходи, що захищають можливість аварійного відключення живлення від несанкціонованої активації; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за аварійне відключення живлення (як впровадження, так і можливості використання); організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують аварійне відключення живлення]. | | | | |

|  |  |
| --- | --- |
| РЕ-10(1) | Аварійне відключення - Випадкова і несанкціонована активація |
|  | [Виключено: включено до РЕ-10]. |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-11 | АВАРІЙНЕ ЕНЕРГОЗАБЕЗПЕЧЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-11[1] | Впровадити тимчасове джерело безперебійного живлення для забезпечення (один або кілька): | |
| РЕ-11[1]{1} | впорядкованого виключення системи у разі втрати первинного джерела живлення. |
| РЕ-11[1]{2} | перехід системи на довгострокову альтернативну систему живлення у разі втрати первинного джерела живлення. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури вирішення надзвичайних ситуацій; джерело безперебійного живлення; документація на джерело безперебійного живлення; записи випробувань джерела безперебійного живлення; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за аварійне живлення та / або планування; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують джерело безперебійного живлення; джерело безперебійного живлення]. | | |

|  |  |  |
| --- | --- | --- |
| РЕ-11(1) | АВАРІЙНЕ ЕНЕРГОЗАБЕЗПЕЧЕННЯ - ДОВГОСТРОКОВЕ АЛЬТЕРНАТИВНЕ ДЖЕРЕЛО ЖИВЛЕННЯ - МІНІМАЛЬНІ ЕКСПЛУАТАЦІЙНІ МОЖЛИВОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-11(1)[1] | Забезпечити для системи наявність довгострокового альтернативного джерела живлення, яке може підтримувати мінімально необхідну експлуатаційну спроможність у разі тривалої втрати первинного джерела живлення. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури вирішення надзвичайних ситуацій; змінне джерело живлення; документація про альтернативне джерело живлення; записи про випробування джерел живлення; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за аварійне живлення та / або планування; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують альтернативне джерело живлення; альтернативне джерело живлення]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| РЕ-11(2) | АВАРІЙНЕ ЕНЕРГОЗАБЕЗПЕЧЕННЯ - ДОВГОСТРОКОВЕ АЛЬТЕРНАТИВНЕ ДЖЕРЕЛО ЖИВЛЕННЯ – АВТОНОМНЕ ЖИВЛЕННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| РЕ-11(2)[1] | Забезпечити для системи наявність довгострокового альтернативного джерела живлення, яке: | | |
| РЕ-11(2)[1](a) | є автономним | |
| РЕ-11(2)[1](b) | не залежить від зовнішнього постачання енергії | |
| РЕ-11(2)[1](c) | у разі тривалої втрати первинного джерела живлення, здатне підтримувати: | |
| РЕ-11(2)[1](c){1} | мінімально необхідні операційні можливості; |
| РЕ-11(2)[1](c){2} | повнe експлуатаційнe здатність |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури вирішення надзвичайних ситуацій; змінне джерело живлення; документація про альтернативне джерело живлення; записи про випробування джерел живлення; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за аварійне живлення та / або планування; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують альтернативне джерело живлення; альтернативне джерело живлення]. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| РЕ-12 | АВАРІЙНЕ ОСВІТЛЕННЯ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| РЕ-12[1] | Використовувати системи автоматичного аварійного освітлення, які: | | | |
| РЕ-12[1][1] | РЕ-12[1][1]{1} | | активуються в разі відключення електроживлення |
| РЕ-12[1][1]{2} | | активуються в разі збою електроживлення |
| РЕ-12[1][2] | РЕ-12[1][2][1] | | охоплюють аварійні виходи. |
| РЕ-12[1][2][2] | | охоплюють маршрути евакуації всередині об'єкта. |
| РЕ-12[2] | підтримувати системи автоматичного аварійного освітлення, які: | | | |
| РЕ-12[2][1] | | РЕ-12[2][1]{1} | активуються в разі відключення електроживлення |
| РЕ-12[2][1]{2} | активуються в разі збою електроживлення |
| РЕ-12[2][2] | | РЕ-12[2][2][1] | охоплюють аварійні виходи. |
| РЕ-12[2][2][2] | охоплюють маршрути евакуації всередині об'єкта. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються аварійного освітлення; документація на аварійне освітлення; протоколи випробувань аварійного освітлення; аварійні виходи та шляхи евакуації; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за аварійне освітлення та / або планування; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують можливість аварійного освітлення]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-12(1) | АВАРІЙНЕ ОСВІТЛЕННЯ - ОСНОВНІ ЗАДАЧІ ТА ФУНКЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-12[1] | Визначити всі зони, які підтримують: виконання основних задач та функцій | |
| РЕ-12[1][1] | виконання основних задач |
| РЕ-12[1][2] | виконання основних функцій |
| РЕ-12[2] | Забезпечити аварійне освітлення для всіх зон, які підтримують: | |
| РЕ-12[2][1] | виконання основних задач |
| РЕ-12[2][2] | виконання основних функцій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються аварійного освітлення; документація на аварійне освітлення; протоколи випробувань аварійного освітлення; аварійні виходи та шляхи евакуації; райони / місця в межах установи, що підтримують основні місії та ділові функції;інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за аварійне освітлення та / або планування; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують можливість аварійного освітлення]. | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| РЕ-13 | ПРОТИПОЖЕЖНИЙ ЗАХИСТ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| РЕ-13[1] | РЕ-13[1][1] | Використовувати: | | | |
| РЕ-13[1][1][1] | пристрої: | | |
| РЕ-13[1][1][1][1] | | пожежогасіння |
| РЕ-13[1][1][1][2] | | виявлення пожежі |
| РЕ-13[1][1][2] | cистеми: | | |
| РЕ-13[1][1][2][1] | пожежогасіння | |
| РЕ-13[1][1][2][2] | виявлення пожежі | |
| РЕ-13[1][2] | підтримувати у працездатному стані: | | | |
| РЕ-13[1][2][1] | пристрої | | |
| РЕ-13[1][2][1][1] | пожежогасіння | |
| РЕ-13[1][2][1][2] | виявлення пожежі | |
| РЕ-13[1][2][2] | системи: | | |
| РЕ-13[1][2][2][1] | пожежогасіння | |
| РЕ-13[1][2][2][2] | виявлення пожежі | |
| РЕ-13[2] | Забезпечити роботу систем протипожежного захисту незалежним джерелом живлення. | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються протипожежного захисту; прилади / системи пожежогасіння та виявлення пожежі; пристрої / системи документації щодо придушення та виявлення пожежі; протоколи випробувань приладів / систем гасіння та виявлення пожежі; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за прилади / системи виявлення та гасіння пожежі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують пристрої / системи пожежогасіння / виявлення]. | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| РЕ-13(1) | ПРОТИПОЖЕЖНИЙ ЗАХИСТ - ПРИСТРОЇ ТА СИСТЕМИ ВИЯВЛЕННЯ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| РЕ-13(1)[1] | РЕ-13(1)[1][1] | РЕ-13(1)[1][1]{1} | | організація визначає персонал, якому необхідно повідомляти у випадку виявлення пожежі | | |
| РЕ-13(1)[1][1]{2} | | організація визначає посадові особи, яким необхідно повідомляти у випадку виявлення пожежі | | |
| РЕ-13(1)[1][2] | організація визначає аварійну команду яким необхідно повідомляти у випадку виявлення пожежі | | | | |
| РЕ-13(1)[2] | РЕ-13(1)[2]{1} | Використовувати такі пристрої для виявлення пожежі в системі, які активуються автоматично та повідомляють у випадку пожежі: | | | | |
| РЕ-13(1)[2]{1}[1] | РЕ-13(1)[2]{1}[1]{1} | | визначений організацією персонал | |
| РЕ-13(1)[2]{1}[1]{2} | | визначені організацією посадові особи | |
| РЕ-13(1)[2]{1}[2] | визначену організацією аварійну команду | | | |
| РЕ-13(1)[2]{2} | Використовувати такі системи для виявлення пожежі в системі, які активуються автоматично та повідомляють у випадку пожежі: | | | | |
| РЕ-13(1)[2]{2}[1] | РЕ-13(1)[2]{2}[1]{1} | | | визначений організацією персонал |
| РЕ-13(1)[2]{2}[1]{2} | | | визначені організацією посадові особи |
| РЕ-13(1)[2]{2}[2] | визначену організацією аварійну команду | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються протипожежного захисту; заклад, в якому розміщена інформаційна система; угоди про рівень сигналізації; протоколи випробувань приладів / систем гасіння та виявлення пожежі; пристрої / системи документації щодо придушення та виявлення пожежі; оповіщення / повідомлення про пожежні події; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за прилади / системи виявлення та гасіння пожежі; організаційний персонал, відповідальний за повідомлення відповідного персоналу, ролей та аварійну команду; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або впроваджують пристрої / системи виявлення пожежі; активація пристроїв / систем виявлення пожежі (змодельовані); автоматизовані повідомлення]. | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| РЕ-13(2) | ПРОТИПОЖЕЖНИЙ ЗАХИСТ - ПРИСТРОЇ ТА СИСТЕМИ АВТОМАТИЧНОГО ПОЖЕЖОГАСІННЯ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| РЕ-13(2)(a) | РЕ-13(2)(a)[1] | РЕ-13(2)(a)  [1][1] | РЕ-13(2)(a)  [1][1]{1} | організація визначає персонал, якому необхідно повідомляти про будь-яку активацію |
| РЕ-13(2)(a)  [1][1]{2} | організація визначає посадові особи, яким необхідно повідомляти про будь-яку активацію |
| РЕ-13(2)(a)  [1][2] | організація визначає аварійну команду яким необхідно повідомляти про будь-яку активацію | |
| РЕ-13(2)(a)[2] | Використовувати такі пристрої пожежогасіння для системи, які забезпечують автоматичне сповіщення про будь-яку активацію: | | |
| РЕ-13(2)(a)  [2][1] | РЕ-13(2)(a)  [2][1]{1} | визначений організацією персонал |
| РЕ-13(2)(a)  [2][1]{2} | визначені організацією посадові особи |
| РЕ-13(2)(a)  [2][2] | визначену організацією аварійну команду | |
| РЕ-13(2)(a)[2] | Використовувати такі системи пожежогасіння для системи, які забезпечують автоматичне сповіщення про будь-яку активацію: | | |
| РЕ-13(2)(a)  [2][1] | РЕ-13(2)(a)  [2][1]{1} | визначений організацією персонал |
| РЕ-13(2)(a)  [2][1]{2} | визначені організацією посадові особи |
| РЕ-13(2)(a)  [2][2] | визначену організацією аварійну команду | |
| РЕ-13(2)(b) | РЕ-13(2)(b)[1] | Впровадити системи автоматичного гасіння пожежі, коли об’єкт не укомплектований відповідним персоналом на постійній основі. | | |
| РЕ-13(2)(b)[2] | Впровадити засоби автоматичного гасіння пожежі, коли об’єкт не укомплектований відповідним персоналом на постійній основі. | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються протипожежного захисту; пристрої / системи документації щодо придушення та виявлення пожежі; заклад, в якому розміщена інформаційна система; угоди про рівень сигналізації; протоколи випробувань приладів / систем гасіння та виявлення пожежі; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Організаційний персонал, відповідальний за прилади / системи виявлення та гасіння пожежі; організаційний персонал, відповідальний за автоматичне сповіщення про будь-яке спрацьовування приладів / систем протипожежного захисту для відповідного персоналу, ролей та аварійних служб; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР З: Автоматизовані механізми, що підтримують та / або реалізують пристрої / системи пожежогасіння; активація приладів / систем пожежогасіння (змодельовані); автоматизовані повідомлення]. | | | | |

|  |  |
| --- | --- |
| РЕ-13(3) | ПРОТИПОЖЕЖНИЙ ЗАХИСТ - АВТОМАТИЧНЕ ПОЖЕЖОГАСІННЯ |
|  | [Виключено: включено до РЕ-13 (2)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-13(4) | ПРОТИПОЖЕЖНИЙ ЗАХИСТ - ПЕРЕВІРКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-13(4)[1] | РЕ-13(4)[1][1] | організація визначає частоту з якою об’єкт проходить перевірки пожежної безпеки |
| РЕ-13(4)[1][2] | організація визначає час, за який на об’єкті повинні усуватися виявлені під час перевірки пожежної безпеки недоліки. |
| РЕ-13(4)[2] | РЕ-13(4)[2][1] | переконатися, що об’єкт проходить перевірки пожежної безпеки з визначеною організацією частотою |
| РЕ-13(4)[2][2] | переконатися, що на об’єкті усуваються виявлені недоліки в межах визначеного організацією часу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються протипожежного захисту; план безпеки; заклад, в якому розміщена інформаційна система; плани інспекції; результати перевірки; перевіряти звіти; протоколи випробувань приладів / систем гасіння та виявлення пожежі; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за планування, затвердження та виконання пожежних інспекцій; організаційний персонал, який відповідає за інформаційну безпеку]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| РЕ-14 | КОНТРОЛЬ ТЕМПЕРАТУРИ ТА ВОЛОГОСТІ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| РЕ-14(a) | РЕ-14(a)[1] | організація визначає рівень: | |
| РЕ-14(a)[1][1] | температури в приміщенні, де знаходиться система |
| РЕ-14(a)[1][2] | вологості в приміщенні, де знаходиться система |
| РЕ-14(a)[2] | РЕ-14(a)[2][1] | Підтримувати температуру в приміщенні, де знаходиться система в рамках визначеного організацією рівня |
| РЕ-14(a)[2][2] | Підтримувати вологість в приміщенні, де знаходиться система в рамках визначеного організацією рівня |
| РЕ-14(b) | РЕ-14(b)[1] | організація визначає частотою, з якою необхідно контролювати рівні: | |
| РЕ-14(b)[1][1] | температури |
| РЕ-14(b)[1][2] | вологості |
| РЕ-14(b)[2] | Контролювати, з визначеною організацією частотою, рівні: | |
| РЕ-14(b)[2][1] | температури |
| РЕ-14(b)[2][2] | вологості |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю температури та вологості; план безпеки; регулювання температури та вологості; заклад, в якому розміщена інформаційна система; документація щодо контролю температури та вологості; записи температури та вологості; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за захист робочого середовища; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або впроваджують технічне обслуговування та моніторинг рівня температури та вологості]. | | | |

|  |  |  |
| --- | --- | --- |
| РЕ-14(1) | КОНТРОЛЬ ТЕМПЕРАТУРИ ТА ВОЛОГОСТІ - АВТОМАТИЧНИЙ КОНТРОЛЬ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-14(1)[1] | Впровадити автоматичне регулювання температури на об'єкті для запобігання потенційно шкідливих для інформаційної системи коливань |
| РЕ-14(1)[2] | Впровадити автоматичне регулювання вологості на об'єкті для запобігання потенційно шкідливих для інформаційної системи коливань |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю температури та вологості; заклад, в якому розміщена інформаційна система; автоматизовані механізми для температури та вологості; регулювання температури та вологості; документація щодо температури та вологості; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за контроль за робочим середовищем інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують рівні температури та вологості]. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| РЕ-14(2) | КОНТРОЛЬ ТЕМПЕРАТУРИ ТА ВОЛОГОСТІ - МОНІТОРИНГ ЗА ДОПОМОГОЮ СИГНАЛІЗАЦІЙ ТА СПОВІЩЕНЬ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| РЕ-14(2)[1] | РЕ-14(2)[1]{1} | організація визначає персонал, який необхідно сповістити про потенційно небезпечні зміни для персоналу або обладнання щодо температури та вологості | | | |
| РЕ-14(2)[1]{2} | організація визначає ролі, які необхідно сповістити про потенційно небезпечні зміни для персоналу або обладнання щодо температури та вологості | | | |
| РЕ-14(2)[2] | РЕ-14(2)[2][1] | Впровадити моніторинг температури з використанням засобів: | | | |
| РЕ-14(2)[2][1]{1} | сигналізації до визначеного організацією: | | |
| РЕ-14(2)[2][1]{1}{1} | персоналу про потенційно небезпечні зміни для: | |
| РЕ-14(2)[2][1]{1}{1}{1} | персоналу |
| РЕ-14(2)[2][1]{1}{1}{2} | обладнання |
| РЕ-14(2)[2][1]{1}{2} | ролей про потенційно небезпечні зміни для: | |
| РЕ-14(2)[2][1]{1}{2}{1} | персоналу |
| РЕ-14(2)[2][1]{1}{2}{2} | обладнання |
| РЕ-14(2)[2][1]{2} | сповіщення до визначеного організацією: | | |
| РЕ-14(2)[2][1]{2}{1} | персоналу про потенційно небезпечні зміни для: | |
| РЕ-14(2)[2][1]{2}{1}{1} | персоналу |
| РЕ-14(2)[2][1]{2}{1}{2} | обладнання |
| РЕ-14(2)[2][1]{2}{2} | ролей про потенційно небезпечні зміни для: | |
| РЕ-14(2)[2][1]{2}{2}{1} | персоналу |
| РЕ-14(2)[2][1]{2}{2}{2} | обладнання |
| РЕ-14(2)[2][2] | Впровадити моніторинг вологості з використанням засобів сигналізації або сповіщення до визначеного організацією персоналу або ролей про потенційно небезпечні зміни для персоналу або обладнання | | | |
| РЕ-14(2)[2][2]{1} | сигналізації до визначеного організацією: | | |
| РЕ-14(2)[2][2]{1}{1} | персоналу про потенційно небезпечні зміни для: | |
| РЕ-14(2)[2][2]{1}{1}{1} | персоналу |
| РЕ-14(2)[2][2]{1}{1}{2} | обладнання |
| РЕ-14(2)[2][2]{1}{2} | ролей про потенційно небезпечні зміни для: | |
| РЕ-14(2)[2][2]{1}{2}{1} | персоналу |
| РЕ-14(2)[2][2]{1}{2}{2} | обладнання |
| РЕ-14(2)[2][2]{2} | сповіщення до визначеного організацією: | | |
| РЕ-14(2)[2][2]{2}{1} | персоналу про потенційно небезпечні зміни для: | |
| РЕ-14(2)[2][2]{2}{1}{1} | персоналу |
| РЕ-14(2)[2][2]{2}{1}{2} | обладнання |
| РЕ-14(2)[2][2]{2}{2} | ролей про потенційно небезпечні зміни для: | |
| РЕ-14(2)[2][2]{2}{2}{1} | персоналу |
| РЕ-14(2)[2][2]{2}{2}{2} | обладнання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу температури та вологості; заклад, в якому розміщена інформаційна система; журнали або записи контролю за температурою та вологістю; записи змін температури та рівня вологості, які генерують сигнали тривоги або сповіщення; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за контроль робочого середовища інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або впроваджують моніторинг температури та вологості]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-15 | ЗАХИСТ ВІД ПОШКОДЖЕННЯ ВОДОЮ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-15[1] | Забезпечити захист інформаційної системи від пошкоджень, що виникають у разі витоку води, використовуючи: | |
| РЕ-15[1]{1} | відповідні ізоляційні клапани. |
| РЕ-15[1]{2} | відповідні запірні клапани. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються захисту від водної шкоди; заклад, в якому розміщена інформаційна система; ведучі запірні клапани; список ключового персоналу, що знає місце розташування та процедури активації головних запірних клапанів для сантехнічної системи; основна документація запірного клапана; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за контроль робочого середовища інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Основні водозапірні клапани; організаційний процес активації головного відключення води]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| РЕ-15(1) | ЗАХИСТ ВІД ПОШКОДЖЕННЯ ВОДОЮ - АВТОМАТИЧНА ПІДТРИМКА | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| РЕ-15(1)[1] | РЕ-15(1)[1]{1} | організація визначає персонал, який повинні сповістити у разі виявлення води поблизу  інформаційної системи | |
| РЕ-15(1)[1]{2} | організація визначає ролі, які повинні сповістити у разі виявлення води поблизу інформаційної системи | |
| РЕ-15(1)[2] | РЕ-15(1)[2][1] | Впровадити автоматизовані механізми виявлення води поблизу інформаційної системи | |
| РЕ-15(1)[2][2] | Впровадити автоматизовані механізми оповіщення про виявлену воду поблизу інформаційної системи визначеного організацією: | |
| РЕ-15(1)[2][2]{1} | персоналу |
| РЕ-15(1)[2][2]{2} | ролей |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються захисту від водної шкоди; заклад, в якому розміщена інформаційна система; автоматизовані механізми для запірних клапанів; автоматизовані механізми, що визначають наявність води поблизу інформаційної системи; попередження / повідомлення про виявлення води в об'єкті інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за контроль робочого середовища інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Автоматизовані механізми, що підтримують та / або реалізують можливість виявлення води та попередження для інформаційної системи]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| РЕ-16 | ДОСТАВЛЕННЯ І ВИДАЛЕННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| РЕ-16[1] | організація визначає типи компонентів інформаційної системи, що входять та виходять з об'єкта, для проведення: | | |
| РЕ-16[1][1] | авторизації, | |
| РЕ-16[1][2] | моніторингу | |
| РЕ-16[1][3] | контролю | |
| РЕ-16[1][4] | ведення обліку цих елементів | |
| РЕ-16[2] | Проводити для визначених організацією типів компонентів інформаційної системи, що: | | |
| РЕ-16[2][1] | входять до об'єкта: | |
| РЕ-16[2][1][1] | авторизацію |
| РЕ-16[2][1][2] | моніторинг |
| РЕ-16[2][1][3] | контроль |
| РЕ-16[2][2] | виходять з об'єкта: | |
| РЕ-16[2][2][1] | авторизацію |
| РЕ-16[2][2][2] | моніторинг |
| РЕ-16[2][2][3] | контроль |
| РЕ-16[2][3] | вести облік цих елементів | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБРАТИ З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються доставлення та вивезення компонентів інформаційної системи з об'єкта; план безпеки; заклад, в якому розміщена інформаційна система; записи предметів, що входять і виходять з об'єкта; інші відповідні документи або записи].  Співбесіда: [ВИБРАТИ З: Організаційний персонал, відповідальний за контроль за компонентами інформаційної системи, що входять і виходять із закладу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційний процес авторизації, моніторингу та контролю елементів, пов’язаних з інформаційною системою, що входять і виходять із об’єкта; автоматизовані механізми, що підтримують та / або впроваджують санкціонування, моніторинг та контроль елементів, пов’язаних з інформаційною системою, що входять і виходять з об’єкта]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-17 | АЛЬТЕРНАТИВНЕ РОБОЧЕ МІСЦЕ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-17(a) | РЕ-17(a)[1] | організація визначає альтернативні робочі місця, які дозволені для використання співробітниками |
| РЕ-17(a)[2] | Визначити та задокументувати визначені організацією альтернативні робочі місця, які дозволені для використання співробітниками |
| РЕ-17(b) | РЕ-17(b)[1] | організація визначає заходи захисту на альтернативних робочих місцях |
| РЕ-17(b)[2] | Впровадити визначені організацією заходи захисту на альтернативних робочих місцях |
| РЕ-17(c) | Оцінити ефективність заходів захисту на альтернативних робочих місцях | |
| РЕ-17(d) | Надати співробітникам засоби комунікації з персоналом служби інформаційної безпеки у разі інцидентів безпеки | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються альтернативних місць роботи персоналу організації; план безпеки; перелік засобів контролю, необхідних для альтернативних робочих місць; оцінки засобів контролю на альтернативних робочих місцях; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З:Організаційний персонал, що схвалює використання альтернативних робочих місць; організаційний персонал, що використовує альтернативні робочі місця; організаційний персонал, що оцінює контроль на альтернативних робочих місцях; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для безпеки на альтернативних робочих місцях; автоматизовані механізми, що підтримують альтернативні робочі місця; засоби контролю, що застосовуються на альтернативних робочих місцях; засоби зв'язку між персоналом на місцях альтернативних робіт та персоналом охорони]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| РЕ-18 | РОЗТАШУВАННЯ КОМПОНЕНТІВ СИСТЕМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| РЕ-18[1] | РЕ-18[1][1] | організація визначає фізичні небезпеки, які можуть заподіяти шкоду об’єкту | |
| РЕ-18[1][2] | організація визначає екологічні небезпеки, які можуть заподіяти шкоду об’єкту | |
| РЕ-18[2] | РЕ-18[2][1] | Встановити компоненти інформаційної системи на об'єкті, з метою: | |
| РЕ-18[2][1][1] | мінімізації потенційної шкоди від визначеної організацією фізичної небезпеки |
| РЕ-18[2][1][2] | мінімізації можливості несанкціонованого доступу |
| РЕ-18[2][2] | Встановити компоненти інформаційної системи на об'єкті, з метою: | |
| РЕ-18[2][2][1] | мінімізації потенційної шкоди від визначеної організацією екологічної небезпеки |
| РЕ-18[2][2][2] | мінімізації можливості несанкціонованого доступу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються позиціювання компонентів інформаційної системи; документація, що забезпечує розташування компонентів інформаційної системи всередині об'єкта; розташування компонентів інформаційної системи в межах об’єкта; перелік фізичних та екологічних небезпек, що можуть призвести до пошкодження компонентів інформаційної системи всередині об'єкта; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, відповідальний за розміщення компонентів інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для позиціювання компонентів інформаційної системи]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-18(1) | РОЗТАШУВАННЯ КОМПОНЕНТІВ СИСТЕМИ - МІСЦЕ РОЗМІЩЕННЯ ОБ’ЄКТА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-18(1)(a) | РЕ-18(1)(a)[1] | Планувати розташування інформаційної системи, враховуючи фізичні ризики. |
| РЕ-18(1)(a)[2] | Планувати розташування інформаційної системи, враховуючи екологічні ризики. |
| РЕ-18(1)(b) | РЕ-18(1)(b)[1] | Для чинних об'єктів враховувати фізичні ризики в організаційній стратегії управління ризиками |
| РЕ-18(1)(b)[2] | Для чинних об'єктів враховувати екологічні ризики в організаційній стратегії управління ризиками |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Фізичної та екологічної політики; документи фізичного планування ділянки; організаційна оцінка ризику, план на випадок непередбачених ситуацій; документація щодо стратегії зменшення ризику; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за вибір місця для об’єкта, в якому розміщена інформаційна система; організаційний персонал, відповідальний за зменшення ризиків; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для планування розташування]. | | |

|  |  |  |
| --- | --- | --- |
| РЕ-19 | ВИТІК ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РЕ-19[1] | Забезпечити захист від витоку інформації шляхом випромінювання електромагнітних сигналів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Фізичної та екологічної політики; процедури, що стосуються витоку інформації внаслідок випромінювання електромагнітних сигналів; механізми захисту інформаційної системи від електронного випромінювання сигналів; заклад, в якому розміщена інформаційна система; записи з тестів на випромінювання електромагнітних сигналів; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, відповідальний за екологічний контроль за інформаційною системою; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та / або реалізують захист від витоку інформації внаслідок випромінювання електромагнітних сигналів]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| РЕ-19(1) | ВИТІК ІНФОРМАЦІЇ - НАЦІОНАЛЬНІ ПОЛІТИКИ ТА ПРОЦЕДУРИ ЩОДО ПЕМВН | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| РЕ-19(1)[1] | Забезпечити, відповідно до національних політик та процедур захисту, від побічних електромагнітних випромінювань на основі: | | |
| РЕ-19(1)[1]{1} | категорії безпеки | |
| РЕ-19(1)[1]{1}[1] | захист інформаційної системи, |
| РЕ-19(1)[1]{1}[2] | захист передачі даних |
| РЕ-19(1)[1]{1}[3] | захист мережі |
| РЕ-19(1)[1]{2} | класифікації інформації | |
| РЕ-19(1)[1]{2}[1] | захист інформаційної системи, |
| РЕ-19(1)[1]{2}[2] | захист передачі даних |
| РЕ-19(1)[1]{2}[3] | захист мережі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Фізичної та екологічної політики; процедури, що стосуються витоку інформації, що відповідає національним викидам та політиці та процедурам побічних електромагнітних випромінювань; проєктна документація на компоненти інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація, інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, відповідальний за екологічний контроль за інформаційною системою; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Компоненти інформаційної системи на відповідність національним викидам та політиці та процедурам побічних електромагнітних випромінювань]. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| РЕ-20 | МОНІТОРИНГ ТА ВІДСТЕЖЕННЯ АКТИВІВ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| РЕ-20[1] | РЕ-20[1][1] | організація визначає активи переміщення та місця розташування яких необхідно відстежувати | | | |
| РЕ-20[1][2] | організація визначає контрольовані зони в яких необхідно | | | |
| РЕ-20[1][2][1] | | Моніторити: | |
| РЕ-20[1][2][1][1] | місця розташування визначених організацією активів |
| РЕ-20[1][2][1][2] | переміщення визначених організацією активів |
| РЕ-20[1][2][2] | | Відстежувати: | |
| РЕ-20[1][2][2][1] | місця розташування визначених організацією активів |
| РЕ-20[1][2][2][2] | переміщення визначених організацією активів |
| РЕ-20[1][3] | організація визначає технології визначення місця розташування для: | | | |
| РЕ-20[1][3][1] | | Моніторингу: | |
| РЕ-20[1][3][1][1] | місця розташування визначених організацією активів |
| РЕ-20[1][3][1][2] | переміщення визначених організацією активів |
| РЕ-20[1][3][2] | | Відстеження: | |
| РЕ-20[1][3][2][1] | місця розташування визначених організацією активів |
| РЕ-20[1][3][2][2] | переміщення визначених організацією активів |
| РЕ-20[2] | Використовувати визначені організацією технології визначення місця розташування для: | | | | |
| РЕ-20[2][1] | | Моніторингу: | | |
| РЕ-20[2][1][1] | місця розташування визначених організацією активів у визначені організацією контрольовані зони | |
| РЕ-20[2][1][2] | переміщення визначених організацією активів у визначені організацією контрольовані зони | |
| РЕ-20[2][2] | | Відстеження: | | |
| РЕ-20[2][2][1] | місця розташування визначених організацією активів у визначені організацією контрольовані зони | |
| РЕ-20[2][2][2] | переміщення визначених організацією активів у визначені організацією контрольовані зони | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Фізичної та екологічної політики; процедури, що стосуються моніторингу та відстеження активів; технології розміщення активів та пов'язана з ними конфігураційна документація; перелік організаційних активів, що вимагають відстеження та моніторингу; записи про моніторинг та відстеження активів; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за моніторинг та відстеження активів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для відстеження та моніторингу активів; автоматизовані механізми підтримки та / або реалізації відстеження та моніторингу активів]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| РЕ-21 | ЗАХИСТ ВІД ЕЛЕКТРОМАГНІТНОГО ІМПУЛЬСУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| РЕ-21[1] | РЕ-21[1][1] | Організація визначає системи, яким необхідне захист від пошкодження електромагнітним імпульсом |
| РЕ-21[1][2] | Організація визначає заходи захисту проти пошкодження електромагнітним імпульсом для визначених організацією систем |
| РЕ-21[2] | Використовувати визначені організацією заходи захисту проти пошкодження електромагнітним імпульсом для визначених організацією систем | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються захисту від пошкодження електромагнітним імпульсом; заходи захисту проти пошкодження електромагнітним імпульсом та пов'язана з ними конфігураційна документація; перелік організаційних систем, яким необхідний захист від пошкодження електромагнітним імпульсом; записи про проведені заходи захисту проти пошкодження електромагнітним імпульсом; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за захист від пошкодження електромагнітним імпульсом; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для захисту від пошкодження електромагнітним імпульсом; автоматизовані механізми підтримки та / або реалізації захисту від пошкодження електромагнітним імпульсом]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| РЕ-22 | МАРКУВАННЯ КОМПОНЕНТІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| РЕ-22[1] | організація визначає апаратні компоненти, що вказують: | | |
| РЕ-22[1]{1} | рівень впливу інформації, яка дозволена для:. | |
| РЕ-22[1]{1}{1} | Обробки з використанням апаратних компонентів |
| РЕ-22[1]{1}{2} | зберігання з використанням апаратних компонентів |
| РЕ-22[1]{1}{3} | передачі з використанням апаратних компонентів |
| РЕ-22[1]{2} | класифікацію інформації, яка дозволена для: | |
| РЕ-22[1]{2}{1} | Обробки з використанням апаратних компонентів |
| РЕ-22[1]{2}{2} | зберігання з використанням апаратних компонентів |
| РЕ-22[1]{2}{3} | передачі з використанням апаратних компонентів |
| РЕ-22[2] | Позначати визначені організацією апаратні компоненти, що вказують: | | |
| РЕ-22[2]{1} | рівень впливу інформації, яка дозволена для:. | |
| РЕ-22[2]{1}{1} | Обробки з використанням апаратних компонентів |
| РЕ-22[2]{1}{2} | зберігання з використанням апаратних компонентів |
| РЕ-22[2]{1}{3} | передачі з використанням апаратних компонентів |
| РЕ-22[2]{2} | класифікацію інформації, яка дозволена для: | |
| РЕ-22[2]{2}{1} | Обробки з використанням апаратних компонентів |
| РЕ-22[2]{2}{2} | зберігання з використанням апаратних компонентів |
| РЕ-22[2]{2}{3} | передачі з використанням апаратних компонентів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються з маркування компонентів; перелік організаційних апаратних компонентів, які підлягають маркуванню; записи про проведене маркування компонентів; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за маркування компонентів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для маркування компонентів; автоматизовані механізми підтримки та / або реалізації маркування компонентів]. | | | |