

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 3

Додаток А

Методика оцінювання груп заходів захисту класів PL, PM, PS, RA, SA, SC та SI

Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Київ 2021

Додаток А

В додатку А тому 3 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: PL, PM, PS, RA, SA, SC та SI на наступних сторінках:

[XIV. КЛАС ЗАХОДІВ ЗАХИСТУ PL – ПЛАНУВАННЯ БЕЗПЕКИ 467](#_Toc89270132)

[XV. КЛАС ЗАХОДІВ ЗАХИСТУ PM – МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 484](#_Toc89270133)

[XVI. КЛАС ЗАХОДІВ ЗАХИСТУ PS – КАДРОВА БЕЗПЕКА 538](#_Toc89270134)

[XVII. КЛАС ЗАХОДІВ ЗАХИСТУ RA – ОЦІНКА РИЗИКУ 560](#_Toc89270135)

[XVIII. КЛАС ЗАХОДІВ ЗАХИСТУ SA – ПРИДБАННЯ СИСТЕМИ ТА ПОСЛУГ 583](#_Toc89270136)

[XIX. КЛАС ЗАХОДІВ ЗАХИСТУ SC – ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА КОМУНІКАЦІЙ 746](#_Toc89270137)

[XX. КЛАС ЗАХОДІВ ЗАХИСТУ SI – ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ 826](#_Toc89270138)

1. **КЛАС ЗАХОДІВ ЗАХИСТУ PL – ПЛАНУВАННЯ БЕЗПЕКИ**

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PL-2 | ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| PL-2(a) | розробити план захисту інформації та персональних даних для інформаційної системи, який: | | | |
| PL-2(a)(1) | узгоджується з архітектурою підприємства організації | | |
| PL-2(a)(2) | ясно визначає межу акредитації інформаційної системи | | |
| PL-2(a)(3) | описує оперативний контекст інформаційної системи з точки зору: | | |
| PL-2(a)(3)[1] | завдань | |
| PL-2(a)(3)[2] | процесів | |
| PL-2(a)(4) | забезпечує категоріювання інформаційної системи, включаючи відповідне обґрунтування | | |
| PL-2(a)(5) | PL-2(a)(5)[1] | описує робоче середовище інформаційної системи | |
| PL-2(a)(5)[2] | описує відносини з іншими інформаційними системами | |
| PL-2(a)(5)[3] | описує з'єднання з іншими інформаційними системами | |
| PL-2(a)(6) | надає огляд вимог безпеки та приватності інформаційної системи | | |
| PL-2(a)(7) | визначає будь-які відповідні перекриття, якщо вони застосовуються | | |
| PL-2(a)(8) | PL-2(a)(8){1} | описує чинні заходи щодо забезпечення безпеки та приватності, включаючи обґрунтування рішень щодо налаштування | |
| PL-2(a)(8){2} | описує заплановані заходи щодо забезпечення безпеки та приватності, включаючи обґрунтування рішень щодо налаштування | |
| PL-2(a)(9) | PL-2(a)(9)[1] | PL-2(a)(9)[1]{1} | організація уповноважує посадову особу, яка розглядає та затверджує план захисту інформації та персональних даних для інформаційної системи |
| PL-2(a)(9)[1]{2} | організація призначає представника, який розглядає та затверджує план захисту інформації та персональних даних для інформаційної системи |
| PL-2(a)(9)[2] | розглядається та затверджується: | |
| PL-2(a)(9)[2]{1} | уповноваженою посадовою особою до початку здійснення плану |
| PL-2(a)(9)[2]{2} | призначеним представником до початку здійснення плану |
| PL-2(b) | PL-2(b)[1] | організація визначає персонал, серед якого необхідно: | | |
| PL-2(b)[1][1] | поширювати копії планів захисту інформації та персональних даних | |
| PL-2(b)[1][2] | повідомляти про подальші зміни планів | |
| PL-2(b)[2] | організація визначає ролі, серед яких необхідно: | | |
| PL-2(b)[2][1] | поширювати копії планів захисту інформації та персональних даних | |
| PL-2(b)[2][2] | повідомляти про подальші зміни планів | |
| PL-2(b)[3] | поширити копії планів захисту інформації та персональних даних серед: | | |
| PL-2(b)[3]{1} | визначеного організацією персоналу | |
| PL-2(b)[3]{2} | визначених організацією ролей | |
| PL-2(b)[4] | Повідомляти про подальші зміни планів захисту інформації серед: | | |
| PL-2(b)[4]{1} | визначеного організацією персоналу | |
| PL-2(b)[4]{2} | визначених організацією ролей | |
| PL-2(c) | PL-2(c)[1] | організація визначає частоту, з якою необхідно переглядати плани захисту інформації та персональних даних | | |
| PL-2(c)[2] | переглядати плани захисту інформації та персональних даних з визначеною організацією частотою | | |
| PL-2(d) | оновлювати плани захисту інформації та персональних даних для врахування: | | | |
| PL-2(d){1} | PL-2(d){1}[1] | змін в інформаційній системі | |
| PL-2(d){1}[2] | змін в робочому середовищі | |
| PL-2(d){2} | проблем, виявлених в ході: | | |
| PL-2(d){2}{1} | реалізації заходів безпеки та приватності | |
| PL-2(d){2}{2} | оцінки заходів безпеки та приватності | |
| PL-2(e) | забезпечити захист планів захисту інформації та персональних даних від: | | | |
| PL-2(e)[1] | несанкціонованого розкриття | | |
| PL-2(e)[2] | несанкціонованих змін | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика планування безпеки; процедури, що стосуються розробки та реалізації плану безпеки; процедури, що стосуються огляду та оновлення планів безпеки; документація з архітектури підприємства; план безпеки інформаційної системи; записи оглядів та оновлень планів безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування безпеки та виконання плану; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану безпеки; автоматизовані механізми, що підтримують план безпеки інформаційної системи]. | | | | |

|  |  |
| --- | --- |
| PL-2(1) | ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ - КОНЦЕПЦІЯ ЕКСПЛУАТАЦІЇ |
|  | [Вилучено: включено до PL-7] |

|  |  |
| --- | --- |
| PL-2(2) | ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ - ФУНКЦІОНАЛЬНА АРХІТЕКТУРА |
|  | [Вилучено: включено до PL-8]. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| PL-2(3) | ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ - ПЛАНУВАННЯ ТА КООРДИНАЦІЯ З ІНШИМИ ОРГАНІЗАЦІЙНИМИ СТРУКТУРАМИ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| PL-2(3)[1] | PL-2(3)[1]{1} | організація визначає окремих осіб, з якими необхідно співпрацювати при: | | | |
| PL-2(3)[1]{1}[1] | плануванні діяльності, що: | | |
| PL-2(3)[1]{1}[1][1] | стосується безпеки та приватності | |
| PL-2(3)[1]{1}[1][2] | яка впливає на інформаційну систему | |
| PL-2(3)[1]{1}[2] | координуванні діяльності, що: | | |
| PL-2(3)[1]{1}[2][1] | стосується безпеки та приватності | |
| PL-2(3)[1]{1}[2][2] | яка впливає на інформаційну систему | |
| PL-2(3)[1]{2} | організація визначає окремі групи, з якими необхідно співпрацювати при: | | | |
| PL-2(3)[1]{2}[1] | плануванні діяльності, що: | | |
| PL-2(3)[1]{2}[1][1] | стосується безпеки та приватності | |
| PL-2(3)[1]{2}[1][2] | яка впливає на інформаційну систему | |
| PL-2(3)[1]{2}[2] | координуванні діяльності, що: | | |
| PL-2(3)[1]{2}[2][1] | | стосується безпеки та приватності |
| PL-2(3)[1]{2}[2][2] | | яка впливає на інформаційну систему |
| PL-2(3)[2] | PL-2(3)[2][1] | планувати діяльність, що стосується безпеки та приватності, та яка впливає на інформаційну систему у співпраці з: | | | |
| PL-2(3)[2][1]{1} | визначеними організацією окремими особами перед проведенням таких заходів, для зменшення впливу на інші організаційні структури | | |
| PL-2(3)[2][1]{2} | визначеними організацією окремими групами перед проведенням таких заходів, для зменшення впливу на інші організаційні структури | | |
| PL-2(3)[2][2] | координувати діяльність, що стосується безпеки та приватності, та яка впливає на інформаційну систему у співпраці з [Призначення: визначеними організацією окремими особами або групами] перед проведенням таких заходів, для зменшення впливу на інші організаційні структури | | | |
| PL-2(3)[2][2]{1} | визначеними організацією окремими особами перед проведенням таких заходів, для зменшення впливу на інші організаційні структури | | |
| PL-2(3)[2][2]{2} | визначеними організацією окремими групами перед проведенням таких заходів, для зменшення впливу на інші організаційні структури | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: політика планування безпеки; політика контролю доступу; політика планування на випадок непередбачених ситуацій; процедури, що стосуються планування діяльності в галузі безпеки інформаційної системи; план безпеки інформаційної системи; план дій на випадок непередбачених ситуацій для інформаційної системи; проєктна документація інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: організаційний персонал, який відповідає за планування безпеки та виконання плану; організаційні особи чи групи, з якими планується та координується діяльність, яка пов’язана з безпекою; організаційний персонал, який відповідає за інформаційну безпеку]. | | | | | |

|  |  |
| --- | --- |
| PL-3 | ОНОВЛЕННЯ ПЛАНІВ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ |
|  | [Вилучено: включено до PL-2] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| PL-4 | ПРАВИЛА ПОВЕДІНКИ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| PL-4(a) | PL-4(a)[1] | створити правила, які описують для осіб, які потребують доступу до інформаційної системи: | | | |
| PL-4(a)[1][1] | обов'язки щодо: | | |
| PL-4(a)[1][1][1] | | інформації |
| PL-4(a)[1][1][2] | | використання інформаційної системи |
| PL-4(a)[1][1][3] | | безпеки |
| PL-4(a)[1][1][4] | | приватності |
| PL-4(a)[1][2] | очікувану поведінку щодо: | | |
| PL-4(a)[1][2][1] | | інформації |
| PL-4(a)[1][2][2] | | використання інформаційної системи |
| PL-4(a)[1][2][3] | | безпеки |
| PL-4(a)[1][2][4] | | приватності |
| PL-4(a)[2] | надати особам, які потребують доступу до інформаційної системи, правила, які описують їх: | | | |
| PL-4(a)[2][1] | обов'язки щодо: | | |
| PL-4(a)[2][1][1] | | інформації |
| PL-4(a)[2][1][2] | | використання інформаційної системи |
| PL-4(a)[2][1][3] | | безпеки |
| PL-4(a)[2][1][4] | | приватності |
| PL-4(a)[2][2] | очікувану поведінку щодо: | | |
| PL-4(a)[2][2][1] | | інформації |
| PL-4(a)[2][2][2] | | використання інформаційної системи |
| PL-4(a)[2][2][3] | | безпеки |
| PL-4(a)[2][2][4] | | приватності |
| PL-4(b) | перш ніж дозволяти доступ до інформації та інформаційної системи, отримати документальне підтвердження від осіб, які потребують доступу до інформаційної системи, про те, що вони: | | | | |
| PL-4(b)[1] | прочитали правила поведінки | | | |
| PL-4(b)[2] | зрозуміли правила поведінки | | | |
| PL-4(b)[3] | погодилися дотримуватися правил поведінки | | | |
| PL-4(c) | PL-4(c)[1] | організація визначає частоту з якою необхідно: | | | |
| PL-4(c)[1][1] | | переглядати правила поведінки | |
| PL-4(c)[1][2] | | оновлювати правила поведінки | |
| PL-4(c)[2] | PL-4(c)[2][1] | | переглядати правила поведінки з визначеною організацією частотою | |
| PL-4(c)[2][2] | | оновлювати правила поведінки з визначеною організацією частотою | |
| PL-4(d) | PL-4(d)[1] | організація визначає частоту, з якою необхідно перечитати та повторно підписати правила особами, які підписали попередню версію правил поведінки | | | |
| PL-4(d)[2] | Вимагати від осіб, які підписали попередню версію правил поведінки, перечитати та повторно підписати правила (один або декілька): | | | |
| PL-4(d)[2][1] | | з визначеною організацією частотою | |
| PL-4(d)[2][2] | | коли правила переглядаються чи оновлюються | |
| PL-4(d)[2][3] | | коли правила переглядаються чи оновлюються | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР Політику планування безпеки; процедури, що стосуються правил поведінки користувачів інформаційної системи; правила поведінки; підписані ознайомлення з правилами; записи щодо правил поведінки, перегляди та оновлення; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за встановлення, перегляд та оновлення правил поведінки; організаційний персонал, який є уповноваженими користувачами інформаційної системи та має підписані та звільнені правила поведінки; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для встановлення, перегляду, розповсюдження та оновлення правил поведінки; автоматизовані механізми, що підтримують та, або впроваджують встановлення, перегляд, розповсюдження та оновлення правил поведінки]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PL-4(1) | ПРАВИЛА ПОВЕДІНКИ - ОБМЕЖЕННЯ НА СОЦІАЛЬНІ МЕДІА ТА МЕРЕЖУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PL-4(1)[1] | включити до правил поведінки чіткі обмеження на: | |
| PL-4(1)[1][1] | використання соціальних мереж (сайтів) та |
| PL-4(1)[1][2] | розміщення організаційної інформації на публічних ресурсах (вебсайтах). |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика планування безпеки; процедури, що стосуються правил поведінки користувачів інформаційної системи; правила поведінки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за встановлення, перегляд та оновлення правил поведінки; організаційний персонал, який є уповноваженими користувачами інформаційної системи та має підписані правила поведінки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для встановлення правил поведінки; автоматизовані механізми підтримки та, або реалізації встановлення правил поведінки]. | | |

|  |  |
| --- | --- |
| PL-5 | ОЦІНКА ВПЛИВУ НА ПРИВАТНІСТЬ |
|  | [Вилучено: включено до RА-8]. |

|  |  |
| --- | --- |
| PL-6 | ПЛАНУВАННЯ ДІЯЛЬНОСТІ, ПОВ'ЯЗАНОЇ З БЕЗПЕКОЮ |
|  | [Вилучено: включено до PL-2] |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PL-7 | КОНЦЕПЦІЯ ЕКСПЛУАТАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PL-7(a) | розробити концепцію експлуатації інформаційної системи, яка описує, як організація має намір керувати системою з точки зору забезпечення безпеки та приватності інформації | | |
| PL-7(b) | PL-7(b)[1] | організація визначає частоту: | |
| PL-7(b)[1][1] | перегляду концепції експлуатації |
| PL-7(b)[1][2] | оновлення концепції експлуатації |
| PL-7(b)[2] | PL-7(b)[2][1] | переглядати концепцію експлуатації з визначеною організацією частотою |
| PL-7(b)[2][2] | оновлювати концепцію експлуатації з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика планування безпеки; процедури, що стосуються розробки концепції експлуатації; процедури, що стосуються огляду та оновлення системи концепції експлуатації; захист концепції експлуатації для інформаційної системи; план безпеки інформаційної системи; записи про огляди та оновлення концепції експлуатації; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування безпеки та виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду та оновлення системи безпеки концепції експлуатації; автоматизовані механізми, що підтримують та, або впроваджують розробку, огляд та оновлення системи безпеки концепції експлуатації]. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| PL-8 | АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| PL-8(a) | розробити архітектуру безпеки та приватності для інформаційної системи, яка: | | | | |
| PL-8(a)(1) | характеризує: | | | |
| PL-8(a)(1)[1] | методологію, яку слід вживати для забезпечення: | | |
| PL-8(a)(1)[1][1] | | конфіденційності інформації, яка циркулює в системі |
| PL-8(a)(1)[1][2] | | цілісності інформації, яка циркулює в системі |
| PL-8(a)(1)[1][3] | | доступності інформації, яка циркулює в системі |
| PL-8(a)(1)[2] | вимоги, які слід вживати для забезпечення: | | |
| PL-8(a)(1)[2][1] | | конфіденційності інформації, яка циркулює в системі |
| PL-8(a)(1)[2][2] | | цілісності інформації, яка циркулює в системі |
| PL-8(a)(1)[2][3] | | доступності інформації, яка циркулює в системі |
| PL-8(a)(1)[3] | підходи, які слід вживати для забезпечення: | | |
| PL-8(a)(1)[3][1] | | конфіденційності інформації, яка циркулює в системі |
| PL-8(a)(1)[3][2] | | цілісності інформації, яка циркулює в системі |
| PL-8(a)(1)[3][3] | | доступності інформації, яка циркулює в системі |
| PL-8(a)(2) | характеризує: | | | |
| PL-8(a)(2)[1] | | методологію обробки персональних даних | |
| PL-8(a)(2)[2] | | вимоги до обробки персональних даних | |
| PL-8(a)(2)[3] | | підхід до обробки персональних даних | |
| PL-8(a)(3) | характеризує, як архітектури безпеки та приватності інтегруються в архітектуру підприємства | | | |
| PL-8(a)(4) | характеризує: | | | |
| PL-8(a)(4)[1] | будь-які припущення, що пов'язані з безпекою та приватністю, щодо зовнішніх служб та | | |
| PL-8(a)(4)[2] | залежності від зовнішніх служб | | |
| PL-8(b) | PL-8(b)[1] | організація визначає частоту | | | |
| PL-8(b)[1][1] | перегляду архітектури безпеки та приватності | | |
| PL-8(b)[1][2] | оновлення архітектури безпеки та приватності | | |
| PL-8(b)[2] | PL-8(b)[2][1] | переглядати архітектуру безпеки та приватності з визначеною організацією частотою, щоб відображати оновлення в архітектурі підприємства | | |
| PL-8(b)[2][2] | оновлювати архітектуру безпеки та приватності з визначеною організацією частотою, щоб відображати оновлення в архітектурі підприємства | | |
| PL-8(c) | відображати зміни щодо планової архітектури безпеки та приватності в політиках безпеки та приватності | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика планування безпеки; процедури, що стосуються розвитку архітектури інформаційної безпеки; процедури, що стосуються огляду та оновлення архітектури інформаційної безпеки; документація з архітектури підприємства; документація архітектури інформаційної безпеки; план безпеки інформаційної системи; захист концепції експлуатації для інформаційної системи; записи оглядів та оновлень архітектури інформаційної безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування безпеки та виконання плану; організаційний персонал, відповідальний за розробку архітектури інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду та оновлення архітектури інформаційної безпеки; автоматизовані механізми, що підтримують та, або впроваджують розробку, огляд та оновлення архітектури інформаційної безпеки]. | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| PL-8(1) | АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ - «ГЛИБОКА ОБОРОНА» | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| PL-8(1)[1] | спроєктувати архітектуру безпеки та приватності для інформаційної системи, використовуючи підхід «глибокої оборони», що: | | | | | |
| PL-8(1)[1](a) | PL-8(1)[1](a)[1] | PL-8(1)[1](a)[1][1] | | організація визначає заходи захисту | |
| PL-8(1)[1](a)[1][2] | | організація визначає місця | |
| PL-8(1)[1](a)[1][3] | | організація визначає архітектурні рівні | |
| PL-8(1)[1](a)[2] | призначає визначені організацією заходи захисту для: | | | |
| PL-8(1)[1](a)[2][1] | | | визначених організацією місць |
| PL-8(1)[1](a)[2][2] | | | визначених організацією архітектурних рівнів |
| PL-8(1)[1](b) | забезпечує, щоб призначені заходи захисту діяли: | | | | |
| PL-8(1)[1](b)[1] | | скоординовано | | |
| PL-8(1)[1](b)[2] | | на взаємодоповнюючій основі | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика планування безпеки; процедури, що стосуються розвитку архітектури інформаційної безпеки; документація з архітектури підприємства; документація архітектури інформаційної безпеки; план безпеки інформаційної системи; захист концепції експлуатації для інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування безпеки та виконання плану; організаційний персонал, відповідальний за розробку архітектури інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для проєктування архітектури інформаційної безпеки; автоматизовані механізми, що підтримують та, або реалізують дизайн архітектури інформаційної безпеки]. | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PL-8(2) | АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ - РІЗНОМАНІТНІСТЬ ПОСТАЧАЛЬНИКІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PL-8(2)[1] | PL-8(2)[1][1] | організація визначає заходи захисту, призначені для визначених організацією місць та архітектурних рівнів |
| PL-8(2)[1][2] | організація визначає місця |
| PL-8(2)[1][3] | організація визначає архітектурні рівні |
| PL-8(2)[2] | забезпечити, щоб визначені організацією заходи захисту, призначені для: | |
| PL-8(2)[2][1] | визначених організацією місць, були отримані від різних постачальників |
| PL-8(2)[2][2] | визначених організацією архітектурних рівнів, були отримані від різних постачальників |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика планування безпеки; процедури, що стосуються розвитку архітектури інформаційної безпеки; документація з архітектури підприємства; документація архітектури інформаційної безпеки; план безпеки інформаційної системи; захист концепції експлуатації для інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування безпеки та виконання плану; організаційний персонал, відповідальний за розробку архітектури інформаційної безпеки; організаційний персонал, який відповідає за придбання; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для отримання гарантій захисту інформації від різних постачальників]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PL-9 | ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PL-9[1] | PL-9[1][1] | | організація визначає заходи захисту |
| PL-9[1][2] | | організація визначає пов'язані з заходами захисту процеси |
| PL-9[2] | централізовано управляти: | | |
| PL-9[2][1] | визначеними організацією організаційними заходами захисту | |
| PL-9[2][2] | визначеними організацією процесами, пов'язаними з організаційними заходами захисту | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика планування безпеки; процедури, що стосуються розробки та реалізації плану безпеки; план безпеки інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування безпеки та виконання плану; організаційний персонал, відповідальний за планування, реалізацію центрального управління контролем безпеки та супутніми процесами; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для централізованого управління системами контролю безпеки та пов'язаними з ними процесами; автоматизовані механізми, що підтримують та, або впроваджують централізоване управління контролем безпеки та супутніми процесами]. | | | |

|  |  |  |
| --- | --- | --- |
| PL-10 | ВИБІР БАЗОВОГО ПРОФІЛЮ БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PL-10[1] | вибрати базовий профіль безпеки для інформаційної системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика планування безпеки; процедури, що стосуються розробки та реалізації плану безпеки; план безпеки інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування безпеки та виконання плану; організаційний персонал, відповідальний за планування, реалізацію центрального управління контролем безпеки та супутніми процесами; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для централізованого управління системами контролю безпеки та пов'язаними з ними процесами; автоматизовані механізми, що підтримують та, або впроваджують централізоване управління контролем безпеки та супутніми процесами]. | |

|  |  |  |
| --- | --- | --- |
| PL-11 | НАЛАШТУВАННЯ БАЗОВОГО ПРОФІЛЮ БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PL-11[1] | налаштувати обраний базовий профіль безпеки, застосовуючи вказані дії для налаштування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика планування безпеки; процедури, що стосуються розробки та реалізації плану безпеки; план безпеки інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування безпеки та виконання плану; організаційний персонал, відповідальний за планування, реалізацію центрального управління контролем безпеки та супутніми процесами; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для централізованого управління системами контролю безпеки та пов'язаними з ними процесами; автоматизовані механізми, що підтримують та, або впроваджують централізоване управління контролем безпеки та супутніми процесами]. | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ PM – МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| РM-1 | ПРОГРАМА (КОНЦЕПЦІЯ) ІНФОРМАЦІЙНОЇ БЕЗПЕКИ | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | |
| РM-1(a) | РM-1(a)[1] | розробляє на організаційному рівні програму (концепцію) з інформаційної безпеки, яка: | | | | | | | | |
| РM-1(a)[1](1) | РM-1(a)[1](1)[1] | | містить огляд вимог до програми (концепції) безпеки | | | | | |
| РM-1(a)[1](1)[2] | | описує заходи управління програмою інформаційної безпеки | | | | | |
| РM-1(a)[1](1)[3] | | описує загальні заходи безпеки, які: | | | | | |
| РM-1(a)[1](1)[3]{1} | | | | | використовуються для виконання вимог до програми (концепції) безпеки |
| РM-1(a)[1](1)[3]{2} | | | | | плануються для виконання вимог до програми (концепції) безпеки |
| РM-1(a)[1](2) | містить: | | | | | | | |
| РM-1(a)[1](2)[1] | | визначення: | | | | | |
| РM-1(a)[1](2)[1][1] | | | | | ролей |
| РM-1(a)[1](2)[1][2] | | | | | обов'язків |
| РM-1(a)[1](2)[1][3] | | | | | відповідальності керівництва |
| РM-1(a)[1](2)[1][4] | | | | | заходи з координації діяльності організаційних структур та |
| РM-1(a)[1](2)[1][5] | | | | | забезпечення відповідності вимогам законодавства та іншим нормативним документам |
| РM-1(a)[1](2)[2] | | розподіл: | | | | | |
| РM-1(a)[1](2)[2][1] | | | | ролей | |
| РM-1(a)[1](2)[2][2] | | | | обов'язків | |
| РM-1(a)[1](2)[2][3] | | | | відповідальності керівництва | |
| РM-1(a)[1](2)[2][4] | | | | заходи з координації діяльності організаційних структур та | |
| РM-1(a)[1](2)[2][5] | | | | забезпечення відповідності вимогам законодавства та іншим нормативним документам | |
| РM-1(a)[1](3) | відображає координацію між організаційними елементами, що відповідають за інформаційну безпеку | | | | | | | |
| РM-1(a)[1](4) | затверджена вищою посадовою особою, яка відповідає за: | | | | | | | |
| РM-1(a)[1](4)[1] | | | управління ризиками, пов'язаними з організаційними операціями, включаючи: | | | | |
| РM-1(a)[1](4)[1][1] | | | завдання (місію) організації | |
| РM-1(a)[1](4)[1][2] | | | функції організації | |
| РM-1(a)[1](4)[1][3] | | | імідж організації | |
| РM-1(a)[1](4)[1][4] | | | репутацію організації, | |
| РM-1(a)[1](4)[2] | | | організаційні активи | | | | |
| РM-1(a)[1](4)[3] | | | фізичних осіб | | | | |
| РM-1(a)[1](4)[4] | | | інші організації | | | | |
| РM-1(a)[1](4)[5] | | | державу | | | | |
| РM-1(a)[2] | поширює на організаційному рівні програму (концепцію) з інформаційної безпеки, яка: | | | | | | | | |
| РM-1(a)[2](1) | РM-1(a)[2](1)[1] | | | | містить огляд вимог до програми (концепції) безпеки | | | |
| РM-1(a)[2](1)[2] | | | | описує заходи управління програмою інформаційної безпеки | | | |
| РM-1(a)[2](1)[3] | | | | описує загальні заходи безпеки, які: | | | |
| РM-1(a)[2](1)[3]{1} | використовуються для виконання вимог до програми (концепції) безпеки | | |
| РM-1(a)[2](1)[3]{2} | плануються для виконання вимог до програми (концепції) безпеки | | |
| РM-1(a)[2](2) | містить: | | | | | | | |
| РM-1(a)[2](2)[1] | | | | визначення: | | | |
| РM-1(a)[2](2)[1][1] | ролей | | |
| РM-1(a)[2](2)[1][2] | обов'язків | | |
| РM-1(a)[2](2)[1][3] | відповідальності керівництва | | |
| РM-1(a)[2](2)[1][4] | заходи з координації діяльності організаційних структур та | | |
| РM-1(a)[2](2)[1][5] | забезпечення відповідності вимогам законодавства та іншим нормативним документам | | |
| РM-1(a)[2](2)[2] | | | | розподіл: | | | |
| РM-1(a)[2](2)[2][1] | ролей | | |
| РM-1(a)[2](2)[2][2] | обов'язків | | |
| РM-1(a)[2](2)[2][3] | відповідальності керівництва | | |
| РM-1(a)[2](2)[2][4] | заходи з координації діяльності організаційних структур та | | |
| РM-1(a)[2](2)[2][5] | забезпечення відповідності вимогам законодавства та іншим нормативним документам | | |
| РM-1(a)[2](3) | відображає координацію між організаційними елементами, що відповідають за інформаційну безпеку | | | | | | | |
| РM-1(a)[2](4) | затверджена вищою посадовою особою яка відповідає та підзвітна за: | | | | | | | |
| РM-1(a)[2](4)[1] | | | | управління ризиками, пов'язаними з організаційними операціями, включаючи: | | | |
| РM-1(a)[2](4)[1][1] | завдання (місію) організації | | |
| РM-1(a)[2](4)[1][2] | функції організації | | |
| РM-1(a)[2](4)[1][3] | імідж організації | | |
| РM-1(a)[2](4)[1][4] | репутацію організації, | | |
| РM-1(a)[2](4)[2] | | | | організаційні активи | | | |
| РM-1(a)[2](4)[3] | | | | фізичних осіб | | | |
| РM-1(a)[2](4)[4] | | | | інші організації | | | |
| РM-1(a)[2](4)[5] | | | | державу | | | |
| РM-1(b) | РM-1(b)[1] | організація визначає частоту перегляду програми (концепції) інформаційної безпеки | | | | | | | | |
| РM-1(b)[2] | переглядати програму (концепцію) інформаційної безпеки з визначеною організацією частотою | | | | | | | | |
| РM-1(c) | оновлювати програму (концепцію) інформаційної безпеки. у разі: | | | | | | | | | |
| РM-1(c)[1] | організаційних змін, виявлених під час: | | | | | | | | |
| РM-1(c)[1][1] | | виконання програми | | | | | | |
| РM-1(c)[1][2] | | контрольних оцінок | | | | | | |
| РM-1(c)[2] | організаційних завдань, виявлених під час: | | | | | | | | |
| РM-1(c)[2][1] | | виконання програми | | | | | | |
| РM-1(c)[2][2] | | контрольних оцінок | | | | | | |
| РM-1(d) | забезпечити захист програми (концепції) інформаційної безпеки від: | | | | | | | | | |
| РM-1(d)[1] | несанкціонованого розкриття | | | | | | | | |
| РM-1(d)[2] | несанкціонованої зміни | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PM-2 | РОЛІ ПРОГРАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| PM-2(a) | призначити старшу посадову особу служби інформаційної безпеки, яка наділена відповідними: | | | |
| PM-2(a)[1] | завданнями для здійснення: | | |
| PM-2(a)[1][1] | | координації програми (концепції) інформаційної безпеки |
| PM-2(a)[1][2] | | розробки програми (концепції) інформаційної безпеки |
| PM-2(a)[1][3] | | впровадження програми (концепції) інформаційної безпеки |
| PM-2(a)[1][4] | | підтримки програми (концепції) інформаційної безпеки |
| PM-2(a)[2] | ресурсами для здійснення: | | |
| PM-2(a)[2][1] | | координації програми (концепції) інформаційної безпеки |
| PM-2(a)[2][2] | | розробки програми (концепції) інформаційної безпеки |
| PM-2(a)[2][3] | | впровадження програми (концепції) інформаційної безпеки |
| PM-2(a)[2][4] | | підтримки програми (концепції) інформаційної безпеки |
| PM-2(b) | призначити старшу посадову особу з управління ризиками для узгодження процедур управління інформаційною безпекою із процесами: | | | |
| PM-2(b)[1] | стратегічного планування | | |
| PM-2(b)[2] | оперативного планування | | |
| PM-2(b)[3] | бюджетного планування | | |
| PM-2(c) | призначити відповідального за виконання ризиків (функцій) для: | | | |
| PM-2(c)[1] | перегляду: | | |
| PM-2(c)[1][1] | ризиків з точки зору організації | |
| PM-2(c)[1][2] | забезпечення послідовності наскрізного управління ризиками в організації | |
| PM-2(c)[2] | аналізу | | |
| PM-2(c)[2][1] | ризиків з точки зору організації | |
| PM-2(c)[2][2] | забезпечення послідовності наскрізного управління ризиками в організації | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; старший працівник інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку] | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PM-3 | РЕСУРСИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРИВАТНОСТІ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PM-3(a) | PM-3(a)[1] | включити ресурси, необхідні для реалізації програми інформаційної безпеки та приватності, в процесі: | |
| PM-3(a)[1][1] | планування капіталовкладень та |
| PM-3(a)[1][2] | запитів на інвестиції та |
| PM-3(a)[2] | задокументувати всі винятки з цієї вимоги | |
| PM-3(b) | підготувати документацію, необхідну для вирішення завдань програми інформаційної безпеки та приватності: | | |
| PM-3(b)[1] | у процесі планування фінансування відповідно до чинних: | |
| PM-3(b)[1][1] | законів |
| PM-3(b)[1][2] | виконавчих наказів |
| PM-3(b)[1][3] | директив |
| PM-3(b)[1][4] | політик, |
| PM-3(b)[1][5] | правил |
| PM-3(b)[1][6] | стандартів |
| PM-3(b)[2] | запитів на інвестування відповідно до чинних: законів, виконавчих наказів, директив, політик, правил, стандартів | |
| PM-3(b)[2][1] | законів |
| PM-3(b)[2][2] | виконавчих наказів |
| PM-3(b)[2][3] | директив |
| PM-3(b)[2][4] | політик |
| PM-3(b)[2][5] | правил |
| PM-3(b)[2][6] | стандартів |
| PM-3(c) | Забезпечити доступ до ресурсів, призначених для вирішення завдань із захисту: | | |
| PM-3(c)[1] | інформації | |
| PM-3(c)[2] | приватності | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; приклади для планування капіталу та інвестицій; процедури планування капіталу та інвестицій; документація про винятки з вимог капітального планування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм інформаційної безпеки; організаційний персонал, відповідальний за планування капіталу та інвестиції; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для планування капіталу та інвестицій; автоматизовані механізми, що підтримують процес планування реалізації програми інформаційної безпеки та приватності]. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PМ-4 | ПЛАН ДІЙ ТА ЕТАПИ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| PМ-4(a) | PМ-4(a)[1] | запровадити процес для забезпечення того, щоб плани дій програм безпеки та приватності та пов'язаних організаційних систем: | | |
| PМ-4(a)[1][1] | PМ-4(a)[1][1][1] | розроблялися |
| PМ-4(a)[1][1][2] | підтримувалися |
| PМ-4(a)[1][2] | задокументовані корегувальні заходи захисту адекватно реагували на ризики для: | |
| PМ-4(a)[1][2][1] | організаційних операцій |
| PМ-4(a)[1][2][2] | організаційних активів |
| PМ-4(a)[1][2][3] | фізичних осіб |
| PМ-4(a)[1][2][4] | інших організацій |
| PМ-4(a)[1][2][5] | держави |
| PМ-4(a)[1][3] | оприлюднювалися відповідно до встановлених вимог до звітності | |
| PМ-4(a)[2] | запровадити процес для забезпечення того, щоб етапи програм безпеки та приватності та пов'язаних організаційних систем: | | |
| PМ-4(a)[1][1] | PМ-4(a)[1][1][1] | розроблялися |
| PМ-4(a)[1][1][2] | підтримувалися |
| PМ-4(a)[1][2] | задокументовані корегувальні заходи захисту адекватно реагували на ризики для: | |
| PМ-4(a)[1][2][1] | організаційних операцій |
| PМ-4(a)[1][2][2] | організаційних активів |
| PМ-4(a)[1][2][3] | фізичних осіб |
| PМ-4(a)[1][2][4] | інших організацій |
| PМ-4(a)[1][2][5] | держави |
| PМ-4(a)[1][3] | оприлюднювалися відповідно до встановлених вимог до звітності | |
| PМ-4(b) | PМ-4(b)[1] | переглядати плани дій для узгодженості з: | | |
| PМ-4(b)[1][1] | організаційною стратегією управління ризиками | |
| PМ-4(b)[1][2] | організаційними пріоритетами щодо дій з реагування на ризики | |
| PМ-4(b)[2] | переглядати етапи для узгодженості з: | | |
| PМ-4(b)[2][1] | організаційною стратегією управління ризиками | |
| PМ-4(b)[2][2] | організаційними пріоритетами щодо дій з реагування на ризики | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; плани дій та етапи; процедури, що стосуються планів дій та етапів розробки та обслуговування; процедури, що стосуються планів дій та звітування про етапи; процедури перегляду планів дій та етапів для узгодження зі стратегією управління ризиками та пріоритетами реагування на ризик; результати оцінки ризику, пов'язані з планами дій та етапами; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за розробку, підтримку, перегляд та звітування про плани дій та етапи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки плану дій та етапів, огляду, супроводу, звітності; автоматизовані механізми, що підтримують плани дій та етапи]. | | | | |

|  |  |  |
| --- | --- | --- |
| PM-5 | ІНВЕНТАРИЗАЦІЯ СИСТЕМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-5[1] | розробити процедуру інвентаризації організаційних інформаційних систем |
| PM-5[2] | забезпечити проведення процедури інвентаризації організаційних інформаційних систем |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; інвентаризація інформаційної системи; процедури, що стосуються розробки та обслуговування інвентаризації інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за розробку та ведення інвентаризації інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси з розробки та обслуговування інвентаризації інформаційної системи; автоматизовані механізми підтримки інвентаризації інформаційної системи]. | |

|  |  |  |
| --- | --- | --- |
| РМ-6 | ПОКАЗНИКИ ПРОДУКТИВНОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| РМ-6[1] | розробити вимірювання показників продуктивності забезпечення безпеки інформації та приватності |
| РМ-6[2] | відстежувати результати вимірювань показників продуктивності забезпечення безпеки інформації та приватності |
| РМ-6[3] | звітувати про результати вимірювань показників продуктивності забезпечення безпеки інформації та приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; заходи інформаційної безпеки; процедури, що стосуються розробки, моніторингу та звітності про заходи інформаційної безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та несе відповідальність за виконання плану; організаційний персонал, відповідальний за розробку, моніторинг та звітування про заходи інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, моніторингу та звітування про заходи інформаційної безпеки; автоматизовані механізми, що підтримують розробку, моніторинг та звітування про заходи інформаційної безпеки]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PM-7 | АРХІТЕКТУРА ПІДПРИЄМСТВА | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PM-7[1] | розробити корпоративну архітектуру з урахуванням: | | |
| PM-7[1][1] | вимог програми інформаційної безпеки та приватності | |
| PM-7[1][2] | результуючого ризику для: | |
| PM-7[1][2][1] | організаційних операцій |
| PM-7[1][2][2] | організаційних активів |
| PM-7[1][2][3] | фізичних осіб |
| PM-7[1][2][4] | інших організацій |
| PM-7[1][2][5] | держави |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; документація з архітектури підприємства; процедури, що стосуються розвитку архітектури підприємства; результати оцінки ризиків архітектури підприємства; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за розробку архітектури підприємства; організаційний персонал, відповідальний за оцінку ризиків архітектури підприємства; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розвитку архітектури підприємства; автоматизовані механізми підтримки архітектури підприємства та її розвитку]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PM-8 | ПЛАН ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PM-8[1] | визначити завдання інформаційної безпеки та приватності при: | |
| PM-8[1][1] | розробці документації |
| PM-8[1][2] | оновленні плану захисту критичної інфраструктури та ключових ресурсів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; план захисту критичної інфраструктури та ключових ресурсів; процедури, що стосуються розробки, документації та оновлення критичної інфраструктури та плану захисту ключових ресурсів; Національний план захисту інфраструктури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та несе відповідальність за виконання плану; організаційний персонал, відповідальний за розробку, документування та оновлення критичної інфраструктури та плану захисту ключових ресурсів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, документування та оновлення критичної інфраструктури та плану захисту ключових ресурсів; автоматизовані механізми, що підтримують розробку, документацію та оновлення критичної інфраструктури та плану захисту ключових ресурсів]. | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| PM-9 | СТРАТЕГІЯ УПРАВЛІННЯ РИЗИКАМИ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| PM-9(a) | розробити комплексну стратегію управління: | | | | | |
| PM-9(a)(1) | ризиками безпеки для: | | | | |
| PM-9(a)(1)[1] | пов'язаних з експлуатацією | | | |
| PM-9(a)(1)[1][1] | | організаційних операцій | |
| PM-9(a)(1)[1][2] | | організаційних активів | |
| PM-9(a)(1)[1][3] | | фізичних осіб | |
| PM-9(a)(1)[1][4] | | інших організацій та | |
| PM-9(a)(1)[1][5] | | держави | |
| PM-9(a)(1)[2] | пов'язаних з використанням організаційних систем | | | |
| PM-9(a)(1)[2][1] | | організаційних операцій | |
| PM-9(a)(1)[2][2] | | організаційних активів | |
| PM-9(a)(1)[2][3] | | фізичних осіб | |
| PM-9(a)(1)[2][4] | | інших організацій та | |
| PM-9(a)(1)[2][5] | | держави | |
| PM-9(a)(2) | ризиками приватності для фізичних осіб, які можуть виникати внаслідок: | | | | |
| PM-9(a)(2)[1] | | збирання персональних даних | | |
| PM-9(a)(2)[2] | | обміну персональними даними | | |
| PM-9(a)(2)[3] | | зберігання персональних даних | | |
| PM-9(a)(2)[4] | | передачі персональних даних | | |
| PM-9(a)(2)[5] | | використання персональних даних | | |
| PM-9(a)(2)[6] | | розпорядження персональними даними | | |
| PM-9(a)(3) | ризиками ланцюга постачання, пов'язаних з: | | | | |
| PM-9(a)(3)[1] | | розробкою: | | |
| PM-9(a)(3)[1][1] | | інформаційних систем |
| PM-9(a)(3)[1][2] | | компонентів інформаційної системи |
| PM-9(a)(3)[1][3] | | системних послуг |
| PM-9(a)(3)[2] | | придбанням: | | |
| PM-9(a)(3)[2][1] | | інформаційних систем |
| PM-9(a)(3)[2][2] | | компонентів інформаційної системи |
| PM-9(a)(3)[2][3] | | системних послуг |
| PM-9(a)(3)[3] | | обслуговуванням: | | |
| PM-9(a)(3)[3][1] | | інформаційних систем |
| PM-9(a)(3)[3][2] | | компонентів інформаційної системи |
| PM-9(a)(3)[3][3] | | системних послуг |
| PM-9(a)(3)[4] | | утилізацією: | | |
| PM-9(a)(3)[4][1] | | інформаційних систем |
| PM-9(a)(3)[4][2] | | компонентів інформаційної системи |
| PM-9(a)(3)[4][3] | | системних послуг |
| PM-9(b) | реалізувати стратегію управління ризиками в масштабах організації | | | | | |
| PM-9(c) | PM-9(c)[1] | організація визначає частоту: | | | | |
| PM-9(c)[1][1] | | перегляду стратегії управління ризиками | | |
| PM-9(c)[1][2] | | оновлення стратегії управління ризиками | | |
| PM-9(c)[2] | переглядати стратегію управління ризиками: | | | | |
| PM-9(c)[2]{1} | | з визначеною організацією частотою | | |
| PM-9(c)[2]{2} | | якщо потрібно, у разі організаційних змін | | |
| PM-9(c)[3] | оновлювати стратегію управління ризиками: | | | | |
| PM-9(c)[3]{1} | | з визначеною організацією частотою | | |
| PM-9(c)[3]{2} | | якщо потрібно, у разі організаційних змін | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; стратегія управління ризиками; процедури, що стосуються розробки, впровадження, перегляду та оновлення стратегії управління ризиками; результати оцінки ризику, що стосуються стратегії управління ризиками; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за розробку, впровадження, перегляд та оновлення стратегії управління ризиками; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, впровадження, перегляду та оновлення стратегії управління ризиками; автоматизовані механізми, що підтримують розробку, впровадження, перегляд та оновлення стратегії управління ризиками]. | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PM-10 | ПРОЦЕС АКРЕДИТАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PM-10(a) | PM-10(a)[1] | управляти станом безпеки та приватності інформаційних систем організації через процедури акредитації; |
| PM-10(a)[2] | управляти станом безпеки та приватності середовищ, в яких інформаційні системи експлуатуються через процедури акредитації; |
| PM-10(b) | призначити окремих осіб для виконання певних: | |
| PM-10(b)[1] | ролей в рамках організаційного процесу управління ризиками |
| PM-10(b)[2] | обов'язків в рамках організаційного процесу управління ризиками |
| PM-10(c) | інтегрувати процеси акредитації в загальноорганізаційну програму управління ризиками | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються управління (тобто документації, відстеження та звітування) процесу авторизації безпеки; документи дозволу безпеки; списки або інша документація про ролі та обов'язки процесу авторизації безпеки; результати оцінки ризиків, що стосуються процесу санкціонування безпеки та загальноорганізаційної програми управління ризиками; стратегія управління організаційними ризиками; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за управління процесом авторизації безпеки; уповноважені посадові особи; власники системи, старший працівник інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для авторизації безпеки; автоматизовані механізми, що підтримують процес авторизації безпеки]. | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PM-11 | ВИЗНАЧЕННЯ ЗАВДАНЬ ТА ПРОЦЕСІВ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| PM-11(a) | визначити: | | | | | | |
| PM-11(a)[1] | PM-11(a)[1][1] | організаційні завдання з урахуванням інформаційної безпеки та приватності та | | | | |
| PM-11(a)[1][2] | організаційні завдання з урахуванням ризиків, пов'язаних з: | | | | |
| PM-11(a)[1][2][1] | | організаційними операціями | | |
| PM-11(a)[1][2][2] | | організаційними активами | | |
| PM-11(a)[1][2][3] | | фізичними особами | | |
| PM-11(a)[1][2][4] | | іншими організаціями | | |
| PM-11(a)[1][2][5] | | державою | | |
| PM-11(a)[2] | PM-11(a)[2][1] | організаційні процеси з урахуванням інформаційної безпеки та приватності та ризиків, пов'язаних з: | | | | |
| PM-11(a)[2][2] | організаційні процеси з урахуванням ризиків, пов'язаних з: | | | | |
| PM-11(a)[2][2][1] | | організаційними операціями | | |
| PM-11(a)[2][2][2] | | організаційними активами | | |
| PM-11(a)[2][2][3] | | фізичними особами | | |
| PM-11(a)[2][2][4] | | іншими організаціями | | |
| PM-11(a)[2][2][5] | | державою | | |
| PM-11(b) | PM-11(b)[1] | визначити процеси захисту інформації, які випливають із: | | | | | |
| PM-11(b)[1][1] | | завдань | | | |
| PM-11(b)[1][2] | | процесів | | | |
| PM-11(b)[2] | визначити процеси захисту персональних даних, які випливають із: | | | | | |
| PM-11(b)[2][1] | | завдань | | | |
| PM-11(b)[2][2] | | процесів | | | |
| PM-11(c) | PM-11(c)[1] | організація визначає частоту з якою необхідно | | | | | |
| PM-11(c)[1][1] | | переглядати: | | | |
| PM-11(c)[1][1][1] | | | завдання |
| PM-11(c)[1][1][2] | | | процеси |
| PM-11(c)[1][2] | | перевіряти: | | | |
| PM-11(c)[1][2][1] | | | завдання |
| PM-11(c)[1][2][2] | | | процеси |
| PM-11(c)[2] | PM-11(c)[2][1] | | переглядати з визначеною організацією частотою: | | | |
| PM-11(c)[2][1][1] | | завдання, доки не буде досягнуто допустимого рівня захисту персональних даних | |
| PM-11(c)[2][1][2] | | процеси, доки не буде досягнуто допустимого рівня захисту персональних даних | |
| PM-11(c)[2][2] | | перевіряти з визначеною організацією частотою: | | | |
| PM-11(c)[2][2][1] | | завдання, доки не буде досягнуто допустимого рівня захисту персональних даних | |
| PM-11(c)[2][2][2] | | процеси, доки не буде досягнуто допустимого рівня захисту персональних даних | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми захисту інформації; стратегія управління ризиками; процедури визначення потреб у захисті місії, бізнесу; результати оцінки ризику, що стосуються визначення потреб місії, бізнесу у захисті; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за місію, процеси; організаційний персонал, відповідальний за визначення потреб у захисті інформації для місій, процесів; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення місії, процесів та їхніх потреб у захисті інформації]. | | | | | | | |

|  |  |  |
| --- | --- | --- |
| PM-12 | ПРОГРАМА ІНСАЙДЕРСЬКОЇ ЗАГРОЗИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-12[1] | розробити програму інсайдерської загрози, яка передбачає наявність команди з обробки інцидентів, пов'язаних із внутрішньою дисципліною |
| PM-12[2] | сформувати команду з обробки інцидентів, пов'язаних із внутрішньою дисципліною |
| PM-12[3] | впровадити програму інсайдерської загрози, яка передбачає наявність команди з обробки інцидентів, пов'язаних із внутрішньою дисципліною |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми захисту інформації; документація програми інсайдерських загроз; процедури програми внутрішньої загрози; результати оцінки ризику, що стосуються інсайдерських загроз; перелік або інша документація групи з питань взаємодії із загрозами внутрішньої дисципліни; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за програму інсайдерських загроз; члени команди з обробки інцидентів із внутрішніх загроз; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБРАТИ З: Організаційні процеси для реалізації програми внутрішньої загрози та міждисциплінарної групи з обробки інцидентів; автоматизовані механізми, що підтримують та, або впроваджують програму інсайдерських загроз та команду з обробки інцидентів із внутрішньою загрозою]. | |

|  |  |  |
| --- | --- | --- |
| PM-13 | БЕЗПЕКА ТА ПРИВАТНІСТЬ СПІВРОБІТНИКІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-13[1] | створити програму розвитку та вдосконалення співробітників з питань безпеки та приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; документація щодо розробки та вдосконалення співробітників з питань інформаційної безпеки; процедури розробки та вдосконалення співробітників з питань інформаційної безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за програму розвитку та вдосконалення співробітників з питань інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для впровадження програми розвитку та вдосконалення співробітників з питань інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації програми розвитку та вдосконалення співробітників з питань інформаційної безпеки]. | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PM-14 | ТЕСТУВАННЯ, НАВЧАННЯ ТА МОНІТОРИНГ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| PM-14(a) | PM-14(a)[1] | розробити процес забезпечення організаційних планів проведення: | | | | | |
| PM-14(a)[1][1] | | тестування безпеки та приватності | | | |
| PM-14(a)[1][2] | | навчання діяльності, пов'язаної з інформаційними системами організації | | | |
| PM-14(a)[1][3] | | моніторингу діяльності, пов'язаної з інформаційними системами організації | | | |
| PM-14(a)[2] | впровадити процес забезпечення організаційних планів проведення: | | | | | |
| PM-14(a)[2][1] | | тестування безпеки та приватності, який: | | | |
| PM-14(a)[2][1](1) | | PM-14(a)[2][1](1)[1] | є розробленим |
| PM-14(a)[2][1](1)[2] | підтримується постійно |
| PM-14(a)[2][1](2) | | виконується своєчасно | |
| PM-14(a)[2][2] | | навчання діяльності, пов'язаної з інформаційними системами організації, яка: | | | |
| PM-14(a)[2][2](1) | | PM-14(a)[2][2](1)[1] | є розробленим |
| PM-14(a)[2][2](1)[2] | підтримується постійно |
| PM-14(a)[2][2](2) | | виконується своєчасно | |
| PM-14(a)[2][3] | | моніторингу діяльності, пов'язаної з інформаційними системами організації, який: | | | |
| PM-14(a)[2][3](1) | | PM-14(a)[2][3](1)[1] | є розробленим |
| PM-14(a)[2][3](1)[2] | підтримується постійно |
| PM-14(a)[2][3](2) | | виконується своєчасно | |
| PM-14(b) | PM-14(b)[1] | | для узгодженості з організаційною стратегією управління ризиками перевіряти плани: | | | | |
| PM-14(b)[1][1] | | тестування | | |
| PM-14(b)[1][2] | | навчання | | |
| PM-14(b)[1][3] | | моніторингу | | |
| PM-14(b)[2] | | для узгодженості з загальноорганізаційними пріоритетами дій щодо реагування на ризик перевіряти плани: | | | | |
| PM-14(b)[2][1] | | тестування, | | |
| PM-14(b)[2][2] | | навчання | | |
| PM-14(b)[2][3] | | моніторингу | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; плани проведення тестування, навчання та моніторингу безпеки; організаційні процедури, що стосуються розробки та підтримки планів проведення тестування, навчання та моніторингу безпеки; стратегія управління ризиками; процедури перегляду планів проведення тестування, навчання та моніторингу безпеки на відповідність стратегії управління ризиками та пріоритетам реагування на ризик; результати оцінки ризику, пов’язані з проведенням перевірок безпеки, навчання та моніторингу; докази того, що плани проведення заходів з тестування, навчання та моніторингу безпеки виконуються своєчасно; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за розробку та підтримку планів проведення тестування, навчання та моніторингу безпеки; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки та підтримки планів проведення тестування, навчання та моніторингу безпеки; автоматизовані механізми, що підтримують розробку та підтримку планів проведення тестування, навчання та моніторингу безпеки]. | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PM-15 | КОНТАКТИ З ГРУПАМИ ТА АСОЦІАЦІЯМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PM-15[1] | створити контакти між обраними групами та асоціаціями зі спільнотами безпеки та приватності для: | | |
| PM-15[1](a) | PM-15[1](a)[1] | сприяння постійному навчанню персоналу в галузі безпеки та приватності |
| PM-15[1](a)[2] | сприяння постійній підготовці персоналу в галузі безпеки та приватності |
| PM-15[1](b) | підтримки ознайомленості з: | |
| PM-15[1](b)[1] | рекомендованими практиками безпеки та приватності |
| PM-15[1](b)[2] | техніками |
| PM-15[1](b)[3] | технологіями |
| PM-15[1](c) | розповсюдження поточної інформації про стан безпеки та приватності, включаючи: | |
| PM-15[1](c)[1] | загрози |
| PM-15[1](c)[2] | вразливості |
| PM-15[1](c)[3] | інциденти |
| PM-15[2] | інституціоналізувати контакти між обраними групами та асоціаціями з спільнотами безпеки та приватності для: | | |
| PM-15[2](a) | PM-15[2](a)[1] | сприяння постійному навчанню персоналу в галузі безпеки та приватності |
| PM-15[2](a)[2] | сприяння постійній підготовці персоналу в галузі безпеки та приватності |
| PM-15[2](b) | підтримки ознайомленості з: | |
| PM-15[2](b)[1] | рекомендованими практиками безпеки та приватності |
| PM-15[2](b)[2] | техніками |
| PM-15[2](b)[3] | технологіями |
| PM-15[1](c) | розповсюдження поточної інформації про стан безпеки та приватності, включаючи: | |
| PM-15[1](c)[1] | загрози |
| PM-15[1](c)[2] | вразливості |
| PM-15[1](c)[3] | інциденти |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми захисту інформації; стратегія управління ризиками; процедури контактів з групами безпеки та асоціаціями; докази встановленого та інституціоналізованого контакту з групами безпеки та асоціаціями; списки або інша документація про контакти та, або членство в групах безпеки та асоціаціях; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за встановлення та організацію контактів з групами безпеки та асоціаціями; організаційний персонал, який відповідає за інформаційну безпеку; персонал із вибраних груп та асоціацій, з якими організація встановила та інституціоналізувала контакти].  Перевірка: [ВИБІР: Організаційні процеси для встановлення та інституціоналізації контактів із групами безпеки та асоціаціями; автоматизовані механізми, що підтримують контакти з групами безпеки та асоціаціями]. | | | |

|  |  |  |
| --- | --- | --- |
| PM-16 | ПРОГРАМА ІНФОРМУВАННЯ ПРО ЗАГРОЗИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-16[1] | створити програму поінформованості про загрози, яка містить можливості спільного обміну інформацією між організаціями. |
| PM-16[2] | запровадити програму поінформованості про загрози, яка містить можливості спільного обміну інформацією між організаціями. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми захисту інформації; документація програми інформування про загрози; процедури для програми інформування про загрози; результати оцінки ризику, що стосуються інформування про загрози; перелік чи інша документація щодо можливості організації обміну інформацією між організаціями; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за програму інформування про загрози; організаційний персонал, відповідальний за можливості міжорганізаційного обміну інформацією; організаційний персонал, який відповідає за інформаційну безпеку; персонал, з яким організація передає інформацію про інформування про загрози].  Перевірка: [ВИБІР: Організаційні процеси для реалізації програми інформування про загрози; Організаційні процеси для впровадження міжорганізаційної можливості обміну інформацією; автоматизовані механізми підтримки та, або реалізації програми інформування про загрози; автоматизовані механізми, що підтримують та, або реалізують можливості міжорганізаційного обміну інформацією]. | |

|  |  |  |
| --- | --- | --- |
| PM-16(1) | ПРОГРАМА ІНФОРМУВАННЯ ПРО ЗАГРОЗИ - АВТОМАТИЗОВАНІ ЗАСОБИ ДЛЯ ОБМІНУ ІНФОРМАЦІЄЮ ПРО ЗАГРОЗИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-16(1)[1] | використовувати автоматизовані засоби, з метою максимізації ефективності обміну інформацією про виявлені загрози |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми захисту інформації; документація програми інформування про загрози; процедури для програми інформування про загрози; результати оцінки ризику, що стосуються інформування про загрози; перелік чи інша документація щодо можливості організації обміну інформацією між організаціями; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за програму інформування про загрози; організаційний персонал, відповідальний за можливості міжорганізаційного обміну інформацією; організаційний персонал, який відповідає за інформаційну безпеку; персонал, з яким організація передає інформацію про інформування про загрози].  Перевірка: [ВИБІР: Організаційні процеси для реалізації програми інформування про загрози; автоматизовані механізми підтримки та, або реалізації програми інформування про загрози; автоматизовані механізми, що підтримують та, або реалізують можливості міжорганізаційного обміну інформацією; автоматизовані засоби для максимізації ефективності обміну інформацією про виявлені загрози]. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| PM-17 | ЗАХИСТ ПУБЛІЧНОЇ ІНФОРМАЦІЇ НА ЗОВНІШНІХ СИСТЕМАХ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| PM-17(a) | PM-17(a)[1] | розробити політику для забезпечення того, щоб вимоги здійснювалися відповідно до чинного законодавства щодо захисту публічної інформації, яка: | | | |
| PM-17(a)[1]{1} | | обробляється по зовнішніх системах | |
| PM-17(a)[1]{2} | | зберігається по зовнішніх системах | |
| PM-17(a)[1]{3} | | передається по зовнішніх системах | |
| PM-17(a)[2] | розробити процедури для забезпечення того, щоб вимоги здійснювалися відповідно до чинного законодавства, щодо захисту публічної інформації, яка: | | | |
| PM-17(a)[2]{1} | | обробляється по зовнішніх системах | |
| PM-17(a)[2]{2} | | зберігається по зовнішніх системах | |
| PM-17(a)[2]{3} | | передається по зовнішніх системах | |
| PM-17(b) | PM-17(b)[1] | | організація визначає частоту, з якою необхідно оновлювати: | | |
| PM-17(b)[1][1] | | політику |
| PM-17(b)[1][2] | | процедури |
| PM-17(b)[2] | | оновлювати з визначеною організацією частотою: | | |
| PM-17(b)[2][1] | | політику |
| PM-17(b)[2][2] | | процедури |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми захисту інформації; документація програми інформування про загрози; процедури для програми інформування про загрози; результати оцінки ризику, що стосуються інформування про загрози; перелік чи інша документація щодо можливості організації обміну інформацією між організаціями; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, відповідальний за програму інформування про загрози; організаційний персонал, відповідальний за можливості міжорганізаційного обміну інформацією; організаційний персонал, який відповідає за інформаційну безпеку; персонал, з яким організація передає інформацію про інформування про загрози].  Перевірка: [ВИБІР: Організаційні процеси для реалізації програми інформування про загрози; автоматизовані механізми підтримки та, або реалізації програми інформування про загрози; автоматизовані механізми, що підтримують та, або реалізують можливості міжорганізаційного обміну інформацією; автоматизовані засоби для максимізації ефективності обміну інформацією про виявлені загрози]. | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PM-18 | ПРОГРАМА (КОНЦЕПЦІЯ) ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | |
| PM-18(a) | PM-18(a)[1] | розробити загальноорганізаційну програму (концепцію) забезпечення приватності, яка: | | | | | | | |
| PM-18(a)[1](1) | | PM-18(a)[1](1)[1] | | включає опис структури програми забезпечення приватності, призначеної для реалізації програми забезпечення приватності | | | |
| PM-18(a)[1](1)[2] | | включає опис структури програми забезпечення ресурсів, призначених для реалізації програми забезпечення приватності | | | |
| PM-18(a)[1](2) | | містить: | | | | | |
| PM-18(a)[1][2][1] | | огляд вимог до забезпечення приватності та | | | |
| PM-18(a)[1][2][2] | | опис засобів управління програмою забезпечення приватності та загальних заходів захисту, встановлених або запланованих для задоволення цих вимог | | | |
| PM-18(a)[1][2][3] | | опис загальних заходів захисту: | | | |
| PM-18(a)[1][2][4] | | PM-18(a)[1][2][4]{1} | | встановлених для задоволення цих вимог | |
| PM-18(a)[1][2][4]{2} | | запланованих для задоволення цих вимог | |
| PM-18(a)[1](3) | | PM-18(a)[1](3)[1] | | визначає обов’язки посадової особи щодо приватності | | | |
| PM-18(a)[1](3)[2] | | визначає обов’язки з питань забезпечення приватності інших: | | | |
| PM-18(a)[1](3)[2][1] | | посадових осіб | |
| PM-18(a)[1](3)[2][2] | | персоналу | |
| PM-18(a)[1](4) | | описує: | | | | | |
| PM-18(a)[1](4)[1] | | зобов'язання керівництва | | | |
| PM-18(a)[1](4)[2] | | стратегічні цілі | | | |
| PM-18(a)[1](4)[3] | | завдання програми забезпечення приватності | | | |
| PM-18(a)[1](5) | | відображає координацію між організаційними структурами, відповідальними за різні аспекти приватності | | | | | |
| PM-18(a)[1](6) | | затверджена високопосадовцем, який є відповідальним (та підзвітним) за управління ризиками приватності, що виникають при здійсненні організаційних операцій, включаючи: | | | | | |
| PM-18(a)[1](6)[1] | | завдання | | | |
| PM-18(a)[1](6)[2] | | функції | | | |
| PM-18(a)[1](6)[3] | | імідж та | | | |
| PM-18(a)[1](6)[4] | | репутацію | | | |
| PM-18(a)[1](6)[5] | | організаційні активи | | | |
| PM-18(a)[1](6)[6] | | фізичних осіб | | | |
| PM-18(a)[1](6)[7] | | інші організації та нації | | | |
| PM-18(a)[2] | поширити загальноорганізаційну програму (концепцію) забезпечення приватності, яка: | | | | | | | |
| PM-18(a)[2](1) | | PM-18(a)[2](1)[1] | | включає опис структури програми забезпечення приватності, призначеної для реалізації програми забезпечення приватності | | | |
| PM-18(a)[2](1)[2] | | включає опис структури програми забезпечення ресурсів, призначених для реалізації програми забезпечення приватності | | | |
| PM-18(a)[2](2) | | містить: | | | | | |
| PM-18(a)[2][2][1] | | огляд вимог до забезпечення приватності та | | | |
| PM-18(a)[2][2][2] | | опис засобів управління програмою забезпечення приватності та загальних заходів захисту, встановлених або запланованих для задоволення цих вимог | | | |
| PM-18(a)[2][2][3] | | опис загальних заходів захисту: | | | |
| PM-18(a)[2][2][4] | | PM-18(a)[2][2][4]{1} | | | встановлених для задоволення цих вимог |
| PM-18(a)[2][2][4]{2} | | | запланованих для задоволення цих вимог |
| PM-18(a)[2](3) | | PM-18(a)[2](3)[1] | | визначає обов’язки посадової особи щодо приватності, | | | |
| PM-18(a)[2](3)[2] | | визначає обов’язки з питань забезпечення приватності інших: | | | |
| PM-18(a)[2](3)[2][1] | | | посадових осіб |
| PM-18(a)[2](3)[2][2] | | | персоналу |
| PM-18(a)[2](4) | | описує: | | | | | |
| PM-18(a)[2](4)[1] | | зобов'язання керівництва | | | |
| PM-18(a)[2](4)[2] | | стратегічні цілі | | | |
|  | |  | | PM-18(a)[2](4)[3] | | завдання програми забезпечення приватності | | |
| PM-18(a)[2](5) | | відображає координацію між організаційними структурами, відповідальними за різні аспекти приватності | | | | |
| PM-18(a)[2](6) | | затверджена високопосадовцем, який є відповідальним (та підзвітним) за управління ризиками приватності, що виникають при здійсненні організаційних операцій, включаючи: | | | | |
| PM-18(a)[2](6)[1] | | завдання | | |
| PM-18(a)[2](6)[2] | | функції | | |
| PM-18(a)[2](6)[3] | | імідж та | | |
| PM-18(a)[2](6)[4] | | репутацію | | |
| PM-18(a)[2](6)[5] | | організаційні активи | | |
| PM-18(a)[2](6)[6] | | фізичних осіб | | |
| PM-18(a)[2](6)[7] | | інші організації та нації | | |
| PM-18(b) | оновлювати програму у разі: | | | | | | | | |
| PM-18(b)[1] | | змін законодавства | | | | | | |
| PM-18(b)[2] | | організаційних змін | | | | | | |
| PM-18(b)[3] | | організаційних проблем, що були виявлені в ході: | | | | | | |
| PM-18(b)[3]{1} | | реалізації програми | | | | |
| PM-18(b)[3]{2} | | оцінки заходів приватності | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| PM-19 | РОЛІ ПРОГРАМИ ПРИВАТНОСТІ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| PM-19[1] | призначити старшу посадову особу з питань забезпечення приватності з: | | | | | |
| PM-19[1][1] | повноваженнями для: | | | | |
| PM-19[1][1][1] | координації відповідних вимог забезпечення: | | | |
| PM-19[1][1][1][1] | | | приватності в рамках програми забезпечення приватності всієї організації |
| PM-19[1][1][1][2] | | | управління ризиками приватності в рамках програми забезпечення приватності всієї організації |
| PM-19[1][1][2] | розробки відповідних вимог забезпечення: | | | |
| PM-19[1][1][2][1] | | приватності в рамках програми забезпечення приватності всієї організації | |
| PM-19[1][1][2][2] | | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | |
| PM-19[1][1][3] | реалізації відповідних вимог забезпечення: | | | |
| PM-19[1][1][3][1] | | приватності в рамках програми забезпечення приватності всієї організації | |
| PM-19[1][1][3][2] | | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | |
| PM-19[1][2] | завданням для: | | | | |
| PM-19[1][2][1] | координації відповідних вимог забезпечення: | | | |
| PM-19[1][2][1][1] | приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][2][1][2] | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][2][2] | розробки відповідних вимог забезпечення: | | | |
| PM-19[1][2][2][1] | приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][2][2][2] | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][2][3] | реалізації відповідних вимог забезпечення: | | | |
| PM-19[1][2][3][1] | приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][2][3][2] | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][3] | підзвітністю для: | | | | |
| PM-19[1][3][1] | координації відповідних вимог забезпечення: | | | |
| PM-19[1][3][1][1] | приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][3][1][2] | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][3][2] | розробки відповідних вимог забезпечення: | | | |
| PM-19[1][3][2][1] | приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][3][2][2] | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][3][3] | реалізації відповідних вимог забезпечення: | | | |
| PM-19[1][3][3][1] | приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][3][3][2] | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][4] | ресурсами для: | | | | |
| PM-19[1][4][1] | координації відповідних вимог забезпечення: | | | |
| PM-19[1][4][1][1] | приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][4][1][2] | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][4][2] | розробки відповідних вимог забезпечення: | | | |
| PM-19[1][4][2][1] | приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][4][2][2] | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][4][3] | реалізації відповідних вимог забезпечення: | | | |
| PM-19[1][4][3][1] | приватності в рамках програми забезпечення приватності всієї організації | | |
| PM-19[1][4][3][2] | управління ризиками приватності в рамках програми забезпечення приватності всієї організації | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | | | | |

|  |  |  |
| --- | --- | --- |
| PM-20 | СИСТЕМА ЗАПИСІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-20(a) | вносити записи у державні реєстри з урахуванням необхідних процесів нагляду для систем, що містять персональні дані; |
| PM-20(b) | зберігати відповідні звіти |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PM-21 | ПОШИРЕННЯ ІНФОРМАЦІЇ ПРО ПРОГРАМУ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| PM-21(a) | забезпечити громадськості | | | |
| PM-21(a)[1] | доступ до інформації про діяльність щодо забезпечення приватності в організації | | |
| PM-21(a)[2] | можливість комунікації з уповноваженою посадовою особою з питань забезпечення приватності | | |
| PM-21(b) | оприлюднити організаційну політику забезпечення приватності: | | | |
| PM-21(b){1} | | на сайті організації | |
| PM-21(b){2} | | або іншим чином | |
| PM-21(c) | використовувати, з метою забезпечення можливості громадськості(один або кілька): | | | |
| PM-21(c){1} | | надавати зворотний зв'язок за допомогою: | |
| PM-21(c){1}{1} | публічних адрес електронної пошти та, або |
| PM-21(c){1}{2} | телефонних ліній |
| PM-21(c){2} | | поставити прямі питання щодо правил приватності за допомогою: | |
| PM-21(c){2}{1} | публічних адрес електронної пошти та, або |
| PM-21(c){2}{2} | телефонних ліній |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | | |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PM-22 | ОБЛІК РОЗКРИТТЯ ПЕРСОНАЛЬНИХ ДАНИХ | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | |
| PM-22(a) | PM-22(a)[1] | розробити облік подій з розкриття персональних даних, що зберігається в кожній системі, в тому числі: | | | | | | |
| PM-22(a)[1](1) | | PM-22(a)[1](1)[1] | дата кожного розкриття запису | | | |
| PM-22(a)[1](1)[2] | характер кожного розкриття запису | | | |
| PM-22(a)[1](1)[3] | мета кожного розкриття запису | | | |
| PM-22(a)[1](2) | | PM-22(a)[1](2)[1] | дані особи, щодо яких було зроблено розкриття даних: | | | |
| PM-22(a)[1](2)[1][1] | | ім'я особи | |
| PM-22(a)[1](2)[1][2] | | адреса особи або | |
| PM-22(a)[1](2)[2] | дані організації, щодо яких було зроблено розкриття даних: | | | |
| PM-22(a)[1](2)[2][1] | | | назва організації |
| PM-22(a)[1](2)[2][2] | | | адреса організації |
| PM-22(a)[2] | вести облік подій з розкриття персональних даних, що зберігаються в кожній системі, в тому числі: | | | | | | |
| PM-22(a)[2](1) | | PM-22(a)[2](1)[1] | дата кожного розкриття запису | | | |
| PM-22(a)[2](1)[2] | характер кожного розкриття запису | | | |
| PM-22(a)[2](1)[3] | мета кожного розкриття запису | | | |
| PM-22(a)[2](2) | | PM-22(a)[2](2)[1] | дані особи, щодо яких було зроблено розкриття даних: | | | |
| PM-22(a)[2](2)[1][1] | ім'я особи | | |
| PM-22(a)[2](2)[1][2] | адреса особи або | | |
| PM-22(a)[21](2)[2] | дані організації, щодо яких було зроблено розкриття даних: | | | |
| PM-22(a)[2](2)[2][1] | назва організації | | |
| PM-22(a)[2](2)[2][2] | адреса організації | | |
| PM-22(b) | зберігати облік розкриття персональних даних протягом: | | | | | | | |
| PM-22(b){1} | | терміну дії запису | | | | | |
| PM-22(b){2} | | п'яти років після розкриття інформації | | | | | |
| PM-22(c) | здійснювати облік розкриття персональних даних доступним особі, зазначеній в записі за запитом | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PM-23 | УПРАВЛІННЯ ЯКІСТЮ ПЕРСОНАЛЬНИХ ДАНИХ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PM-23[1] | надавати рекомендації, що забезпечують: | |
| PM-23[1][1] | якість персональних даних протягом життєвого циклу персональних даних |
| PM-23[1][2] | корисність персональних даних протягом життєвого циклу персональних даних |
| PM-23[1][3] | об'єктивність персональних даних протягом життєвого циклу персональних даних |
| PM-23[1][4] | цілісність персональних даних протягом життєвого циклу персональних даних |
| PM-23[1][5] | визначення збитків персональних даних протягом життєвого циклу персональних даних. |
| PM-23[1][6] | деідентифікацію персональних даних протягом життєвого циклу персональних даних |
| PM-23[2] | надавати рекомендації, що максимізують: | |
| PM-23[1][1] | якість персональних даних протягом життєвого циклу персональних даних |
| PM-23[1][2] | корисність персональних даних протягом життєвого циклу персональних даних |
| PM-23[1][3] | об'єктивність персональних даних протягом життєвого циклу персональних даних |
| PM-23[1][4] | цілісність персональних даних протягом життєвого циклу персональних даних |
| PM-23[1][5] | визначення збитків персональних даних протягом життєвого циклу персональних даних |
| PM-23[1][6] | деідентифікацію персональних даних протягом життєвого циклу персональних даних. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | |

|  |  |  |
| --- | --- | --- |
| PM-23(1) | УПРАВЛІННЯ ЯКІСТЮ ПЕРСОНАЛЬНИХ ДАНИХ - АВТОМАТИЗАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-23(1)[1] | видавати технічні рекомендації для підтримки автоматизованої оцінки якості персональних даних протягом всього життєвого циклу персональних даних |
| PM-23(1)[2] | видавати технічну документацію для підтримки автоматизованої оцінки якості персональних даних протягом всього життєвого циклу персональних даних |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | |

|  |  |  |
| --- | --- | --- |
| PM-23(2) | УПРАВЛІННЯ ЯКІСТЮ ПЕРСОНАЛЬНИХ ДАНИХ - МАРКУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-23(2)[1] | видавати рекомендації щодо моделювання персональних даних для підтримки маркування персональних даних |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PM-23(3) | УПРАВЛІННЯ ЯКІСТЮ ПЕРСОНАЛЬНИХ ДАНИХ - ОНОВЛЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PM-23(3)[1] | розробити метод, за допомогою якого оновлюються персональні дані | | |
| PM-23(3)[2] | визначити частоту оновлень персональних даних за допомогою методу | | |
| PM-23(3)[3] | під час управління персональними даними: | | |
| PM-23(3)[3][1] | розробити процедури для: | |
| PM-23(3)[3][1][1] | ідентифікації методу, за допомогою якого оновлюються персональні дані |
| PM-23(3)[3][1][2] | фіксації методу, за допомогою якого оновлюються персональні дані |
| PM-23(3)[3][1][3] | Визначення частоти таких оновлень |
| PM-23(3)[3][2] | впровадити механізми для: | |
| PM-23(3)[3][2][1] | ідентифікації методу, за допомогою якого оновлюються персональні дані |
| PM-23(3)[3][2][2] | фіксації методу, за допомогою якого оновлюються персональні дані |
| PM-23(3)[3][2][3] | визначення частоти таких оновлень |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PM-24 | КОМІСІЯ З УПРАВЛІННЯ ДАНИМИ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| PM-24(a) | розробити устав (положення) комісії з управління персональними даними | | | | | | |
| PM-24(b) | PM-24(b)[1] | організація визначає ролі, з яких складається комісія з управління персональними даними | | | | | |
| PM-24(b)[2] | створити комісію з управління персональними даними, що складається з визначених організацією ролей та мають такі обов'язки: | | | | | |
| PM-24(b)[2](1) | PM-24(b)[2](1)[1] | розробляти рекомендації, які підтримують: | | | |
| PM-24(b)[2][1][1] | | моделювання персональних даних протягом життєвого циклу інформації | |
| PM-24(b)[2][1][2] | | якість персональних даних протягом життєвого циклу інформації | |
| PM-24(b)[2][1][3] | | цілісність персональних даних протягом життєвого циклу інформації | |
| PM-24(b)[2][1][4] | | деідентіфікацію персональних даних протягом життєвого циклу інформації | |
| PM-24(b)[2](1)[2] | впроваджувати рекомендації, які підтримують: | | | |
| PM-24(b)[2][2][1] | моделювання персональних даних протягом життєвого циклу інформації | | |
| PM-24(b)[2][2][2] | якість персональних даних протягом життєвого циклу інформації | | |
| PM-24(b)[2][2][3] | цілісність персональних даних протягом життєвого циклу інформації | | |
| PM-24(b)[2][2][4] | деідентіфікацію персональних даних протягом життєвого циклу інформації | | |
| PM-24(b)[2](2) | PM-24(b)[2](2)[1] | перевіряти додатки для: | | | |
| PM-24(b)[2](2)[1][1] | | | публікації даних поза організацією |
| PM-24(b)[2](2)[1][2] | | | архівування додатків |
| PM-24(b)[2](2)[1][3] | | | архівування персональних даних |
| PM-24(b)[2](2)[1][4] | | | проведення моніторингу |
| PM-24(b)[2](2)[2] | стверджувати додатки для: | | | |
| PM-24(b)[2](2)[2][1] | | | публікації даних поза організацією, |
| PM-24(b)[2](2)[2][2] | | | архівування додатків |
| PM-24(b)[2](2)[2][3] | | | архівування персональних даних |
| PM-24(b)[2](2)[2][4] | | | проведення моніторингу |
| PM-24(c) | PM-24(c)[1] | включити вимоги до взаємодії персоналу з комісією з управління персональними даними в області (та, або): | | | | | |
| PM-24(c)[1]{1} | | безпеки та приватності | | | |
| PM-24(c)[1]{2} | | навчання на основі ролей. | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | | | | | |

|  |  |  |
| --- | --- | --- |
| PM-25 | КОМІСІЯ З ПИТАНЬ ЦІЛІСНОСТІ ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-25[1] | створити комісію з питань цілісності даних для спостереження за угодами організації щодо дотримання вимог безпеки та приватності під час обміну даними між системами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | |

|  |  |  |
| --- | --- | --- |
| PM-25(1) | КОМІСІЯ З ПИТАНЬ ЦІЛІСНОСТІ ДАНИХ - ПУБЛІКАЦІЯ УГОД НА ВЕБСАЙТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-25(1)[1] | публікувати угоди про відповідність на загальнодоступному вебсайті організації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| PM-26 | МІНІМІЗАЦІЯ ПЕРСОНАЛЬНИХ ДАНИХ, ЩО ВИКОРИСТОВУЮТЬСЯ ПІД ЧАС ТЕСТУВАННЯ, НАВЧАННЯ ТА ДОСЛІДЖЕНЬ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| PM-26(a) | PM-26(a)[1] | розробити: | | | |
| PM-26(a)[1][1] | | політики, спрямовані на врегулювання питань використання персональних даних для: | |
| PM-26(a)[1][1][1] | внутрішнього тестування |
| PM-26(a)[1][1][2] | навчання |
| PM-26(a)[1][1][3] | досліджень |
| PM-26(a)[1][2] | | процедури, спрямовані врегулювання питань використання персональних даних для: | |
| PM-26(a)[1][2][1] | внутрішнього тестування |
| PM-26(a)[1][2][2] | навчання |
| PM-26(a)[1][2][3] | досліджень |
| PM-26(a)[2] | впровадити: | | | |
| PM-26(a)[1][1] | | політики, спрямовані врегулювання питань використання персональних даних для: | |
| PM-26(a)[1][1][1] | внутрішнього тестування |
| PM-26(a)[1][1][2] | навчання |
| PM-26(a)[1][1][3] | досліджень |
| PM-26(a)[1][2] | | процедури, спрямовані врегулювання питань використання персональних даних для: | |
| PM-26(a)[1][2][1] | внутрішнього тестування |
| PM-26(a)[1][2][2] | навчання |
| PM-26(a)[1][2][3] | досліджень |
| PM-26(b) | PM-26(b)[1] | визначити заходи щодо: | | | |
| PM-26(b)[1]{1} | | обмеження кількості персональних даних, які використовується для | |
| PM-26(b)[1]{1}[1] | внутрішнього тестування |
| PM-26(b)[1]{1}[2] | навчання |
| PM-26(b)[1]{1}[3] | досліджень |
| PM-26(b)[1]{2} | | зведення до мінімуму кількості персональних даних, які використовується для | |
| PM-26(b)[1]{2}[1] | внутрішнього тестування |
| PM-26(b)[1]{2}[2] | навчання |
| PM-26(b)[1]{2}[3] | досліджень |
| PM-26(b)[2] | вжити заходи щодо: | | | |
| PM-26(b)[2]{1} | | обмеження кількості персональних даних, які використовується для | |
| PM-26(b)[2]{1}[1] | внутрішнього тестування |
| PM-26(b)[2]{1}[2] | навчання |
| PM-26(b)[2]{1}[3] | досліджень |
| PM-26(b)[2]{2} | | зведення до мінімуму кількості персональних даних, які використовується для | |
| PM-26(b)[2]{2}[1] | внутрішнього тестування |
| PM-26(b)[2]{2}[2] | навчання |
| PM-26(b)[2]{2}[3] | досліджень |
| PM-26(c) | надавати дозвіл на використання персональних даних, коли така інформація вимагається для: | | | | |
| PM-26(c)[1] | | внутрішнього тестування | | |
| PM-26(c)[2] | | навчання | | |
| PM-26(c)[3] | | досліджень | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PM-27 | ІНДИВІДУАЛЬНИЙ КОНТРОЛЬ ДОСТУПУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PM-27(a) | публікувати: | | |
| PM-27(a)(1) | політику, що регулює, яким чином особи можуть запитувати доступ до записів, які зберігаються в системі | |
| PM-27(a)(2) | процедури доступу до персональних даних | |
| PM-27(b) | переконатися, що опубліковані | | |
| PM-27(b)[1] | правила доступу відповідають: | |
| PM-27(b)[1][1] | вимогам чинного законодавства, а також |
| PM-27(b)[1][2] | нормативним вимогам щодо обробки запитів про надання персональних даних |
| PM-27(b)[2] | процедури доступу відповідають | |
| PM-27(b)[2][1] | вимогам чинного законодавства, а також |
| PM-27(b)[2][2] | нормативним вимогам щодо обробки запитів про надання персональних даних |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PM-28 | УПРАВЛІННЯ СКАРГАМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи організація: | | | |
| PM-28[1] | визначає процес: | | |
| PM-28[1][1] | отримання скарг | |
| PM-28[1][2] | реагування на: | |
| PM-28[1][2]{1} | скарги від фізичних осіб щодо організаційної практики забезпечення приватності |
| PM-28[1][2]{2} | проблеми від фізичних осіб щодо організаційної практики забезпечення приватності |
| PM-28[1][2]{3} | запитання від фізичних осіб щодо організаційної практики забезпечення приватності |
| PM-28[2] | впроваджує процес отримання та реагування на скарги, проблеми або запитання від фізичних осіб щодо організаційної практики забезпечення приватності, який включає: | | |
| PM-28[2](a) | PM-28[2](a)[1] | механізми, які легко використовувати та |
| PM-28[2](a)[2] | механізми, які є легкодоступними для громадськості |
| PM-28[2](b) | всю інформацію, необхідну для успішного подання скарг | |
| PM-28[2](c) | PM-28[2](c)[1] | механізми відстеження, що забезпечують отримання всіх скарг |
| PM-28[2](c)[2] | механізми відстеження, що забезпечують вчасний та належний розгляд скарг |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PM-29 | ІНВЕНТАРИЗАЦІЯ ПЕРСОНАЛЬНИХ ДАНИХ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| PM-29(a) | PM-29(a)[1] | організація визначає частоту, з якою необхідно: | | | | | |
| PM-29(a)[1][1] | Встановити інвентаризацію всіх програм і систем, які: | | | | |
| PM-29(a)[1][1]{1} | | створюють персональні дані | | |
| PM-29(a)[1][1]{2} | | збирають персональні дані | | |
| PM-29(a)[1][1]{3} | | використовують персональні дані | | |
| PM-29(a)[1][1]{4} | | обробляють персональні дані | | |
| PM-29(a)[1][1]{5} | | зберігають персональні дані | | |
| PM-29(a)[1][1]{6} | | підтримують персональні дані | | |
| PM-29(a)[1][1]{7} | | поширюють персональні дані | | |
| PM-29(a)[1][1]{8} | | розкривають персональні дані | | |
| PM-29(a)[1][1]{9} | | розпоряджаються персональними даними | | |
| PM-29(a)[1][2] | підтримувати інвентаризацію всіх програм і систем, які: | | | | |
| PM-29(a)[1][2]{1} | | | створюють персональні дані | |
| PM-29(a)[1][2]{2} | | | збирають персональні дані | |
| PM-29(a)[1][2]{3} | | | використовують персональні дані | |
| PM-29(a)[1][2]{4} | | | обробляють персональні дані | |
| PM-29(a)[1][2]{5} | | | зберігають персональні дані | |
| PM-29(a)[1][2]{6} | | | підтримують персональні дані | |
| PM-29(a)[1][2]{7} | | | поширюють персональні дані | |
| PM-29(a)[1][2]{8} | | | розкривають персональні дані | |
| PM-29(a)[1][2]{9} | | | розпоряджаються персональними даними; | |
| PM-29(a)[1][3] | оновлювати інвентаризацію всіх програм і систем, які: | | | | |
| PM-29(a)[1][3]{1} | | | створюють персональні дані | |
| PM-29(a)[1][3]{2} | | | збирають персональні дані | |
| PM-29(a)[1][3]{3} | | | використовують персональні дані | |
| PM-29(a)[1][3]{4} | | | обробляють персональні дані | |
| PM-29(a)[1][3]{5} | | | зберігають персональні дані | |
| PM-29(a)[1][3]{6} | | | підтримують персональні дані | |
| PM-29(a)[1][3]{7} | | | поширюють персональні дані | |
| PM-29(a)[1][3]{8} | | | розкривають персональні дані | |
| PM-29(a)[1][3]{9} | | | розпоряджаються персональними даними | |
| PM-29(a)[2] | PM-29(a)[2][1] | Встановити, з визначеною організацією частотою інвентаризацію всіх: | | | | |
| PM-29(a)[2][1][1] | програм, які: | | | |
| PM-29(a)[2][1][1]{1} | | | створюють персональні дані |
| PM-29(a)[2][1][1]{2} | | | збирають персональні дані |
| PM-29(a)[2][1][1]{3} | | | використовують персональні дані |
| PM-29(a)[2][1][1]{4} | | | обробляють персональні дані |
| PM-29(a)[2][1][1]{5} | | | зберігають персональні дані |
| PM-29(a)[2][1][1]{6} | | | підтримують персональні дані |
| PM-29(a)[2][1][1]{7} | | | поширюють персональні дані |
| PM-29(a)[2][1][1]{8} | | | розкривають персональні дані |
| PM-29(a)[2][1][1]{9} | | | розпоряджаються персональними даними; |
| PM-29(a)[2][1][2] | систем, які: | | | |
| PM-29(a)[2][1][2]{1} | | | створюють персональні дані |
| PM-29(a)[2][1][2]{2} | | | збирають персональні дані |
| PM-29(a)[2][1][2]{3} | | | використовують персональні дані |
| PM-29(a)[2][1][2]{4} | | | обробляють персональні дані |
| PM-29(a)[2][1][2]{5} | | | зберігають персональні дані |
| PM-29(a)[2][1][2]{6} | | | підтримують персональні дані |
| PM-29(a)[2][1][2]{7} | | | поширюють персональні дані |
| PM-29(a)[2][1][2]{8} | | | розкривають персональні дані |
| PM-29(a)[2][1][2]{9} | | | розпоряджаються персональними даними; |
| PM-29(a)[2][2] | підтримувати з визначеною організацією частотою інвентаризацію всіх | | | | |
| PM-29(a)[2][2][1] | програм, які: | | | |
| PM-29(a)[2][2][1]{1} | | | створюють персональні дані |
| PM-29(a)[2][2][1]{2} | | | збирають персональні дані |
| PM-29(a)[2][2][1]{3} | | | використовують персональні дані |
| PM-29(a)[2][2][1]{4} | | | обробляють персональні дані |
| PM-29(a)[2][2][1]{5} | | | зберігають персональні дані |
| PM-29(a)[2][2][1]{6} | | | підтримують персональні дані |
| PM-29(a)[2][2][1]{7} | | | поширюють персональні дані |
| PM-29(a)[2][2][1]{8} | | | розкривають персональні дані |
| PM-29(a)[2][2][1]{9} | | | розпоряджаються персональними даними |
| PM-29(a)[2][2][2] | систем, які: | | | |
| PM-29(a)[2][2][2]{1} | | | створюють персональні дані |
| PM-29(a)[2][2][2]{2} | | | збирають персональні дані |
| PM-29(a)[2][2][2]{3} | | | використовують персональні дані |
| PM-29(a)[2][2][2]{4} | | | обробляють персональні дані |
| PM-29(a)[2][2][2]{5} | | | зберігають персональні дані |
| PM-29(a)[2][2][2]{6} | | | підтримують персональні дані |
| PM-29(a)[2][2][2]{7} | | | поширюють персональні дані |
| PM-29(a)[2][2][2]{8} | | | розкривають персональні дані |
| PM-29(a)[2][2][2]{9} | | | розпоряджаються персональними даними |
| PM-29(a)[2][3] | оновлювати з визначеною організацією частотою інвентаризацію всіх: | | | | |
| PM-29(a)[2][3][1] | програм, які: | | | |
| PM-29(a)[2][3][1]{1} | | | створюють персональні дані |
| PM-29(a)[2][3][1]{2} | | | збирають персональні дані |
| PM-29(a)[2][3][1]{3} | | | використовують персональні дані |
| PM-29(a)[2][3][1]{4} | | | обробляють персональні дані |
| PM-29(a)[2][3][1]{5} | | | зберігають персональні дані |
| PM-29(a)[2][3][1]{6} | | | підтримують персональні дані |
| PM-29(a)[2][3][1]{7} | | | поширюють персональні дані |
| PM-29(a)[2][3][1]{8} | | | розкривають персональні дані |
| PM-29(a)[2][3][1]{9} | | | розпоряджаються персональними даними |
| PM-29(a)[2][3][2] | систем, які: | | | |
| PM-29(a)[2][3][2]{1} | | | створюють персональні дані |
| PM-29(a)[2][3][2]{2} | | | збирають персональні дані |
| PM-29(a)[2][3][2]{3} | | | використовують персональні дані |
| PM-29(a)[2][3][2]{4} | | | обробляють персональні дані |
| PM-29(a)[2][3][2]{5} | | | зберігають персональні дані |
| PM-29(a)[2][3][2]{6} | | | підтримують персональні дані |
| PM-29(a)[2][3][2]{7} | | | поширюють персональні дані |
| PM-29(a)[2][3][2]{8} | | | розкривають персональні дані |
| PM-29(a)[2][3][2]{9} | | | розпоряджаються персональними даними |
| PM-29(b) | PM-29(b)[1] | PM-29(b)[1][1] | призначити: | | | | |
| PM-29(b)[1][1][1] | старшого спеціаліста з питань приватності | | | |
| PM-29(b)[1][1][2] | старшого спеціаліста з питань інформаційної безпеки | | | |
| PM-29(b)[1][1] | організація визначає частоту, з якою необхідно надавати оновлення інвентаризації персональних даних | | | | |
| PM-29(b)[1][1][1] | старшому спеціалісту з питань приватності | | | |
| PM-29(b)[1][1][2] | старшому спеціалісту з питань інформаційної безпеки | | | |
| PM-29(b)[2] | надавати, з визначеною організацією частотою, оновлення інвентаризації персональних даних: | | | | | |
| PM-29(b)[2][1] | старшому спеціалісту з питань приватності | | | | |
| PM-29(b)[2][2] | старшому спеціалісту з питань інформаційної безпеки | | | | |
| PM-29(c) | використовувати інвентарний опис персональних даних для підтримки встановлення вимог інформаційної безпеки та приватності для: | | | | | | |
| PM-29(c){1} | всіх нових систем, що містять персональні дані | | | | | |
| PM-29(c){2} | всіх модифікованих систем, що містять персональні дані | | | | | |
| PM-29(d) | PM-29(d)[1] | організація визначає частоту з якою необхідно переглядати інвентарний опис персональних даних | | | | | |
| PM-29(d)[2] | переглядати інвентарний опис персональних даних з визначеною організацією частотою | | | | | |
| PM-29(e) | Забезпечити: | | | | | | |
| PM-29(e)[1] | актуальність персональних даних | | | | | |
| PM-29(e)[2] | повноту персональних даних | | | | | |
| PM-29(f) | зводити до мінімуму обсяг персональних даних, необхідних для правильного виконання визначених організаційних функцій. | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | | | | | |

|  |  |  |
| --- | --- | --- |
| PM-29(1) | ІНВЕНТАРИЗАЦІЯ ПЕРСОНАЛЬНИХ ДАНИХ - АВТОМАТИЧНА ПІДТРИМКА | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PM-29(1)[1] | впровадити автоматизовані механізми для визначення, чи зберігаються персональні дані в електронному вигляді |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PM-30 | ЗВІТ ПРО ПРИВАТНІСТЬ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PM-30[1] | розробити звіти про забезпечення приватності для: | | |
| PM-30[1](a) | наглядових органів для підтвердження виконання вимог підзвітності відповідно до вимог забезпечення: | |
| PM-30[1](a)[1] | приватності |
| PM-30[1](a)[2] | законодавчої бази |
| PM-30[1](a)[3] | нормативної бази |
| PM-30[1](b) | PM-30[1](b)[1] | організація призначає посадових осіб відповідальних за моніторинг виконання та відповідності чинному законодавству програми забезпечення приватності |
| PM-30[1](b)[2] | організація призначає персонал відповідальний за моніторинг виконання та відповідності чинному законодавству програми забезпечення приватності. |
| PM-30[2] | поширити звіти про забезпечення приватності для: | | |
| PM-30[1](a) | наглядових органів для підтвердження виконання вимог підзвітності відповідно до вимог забезпечення: | |
| PM-30[1](a)[1] | приватності |
| PM-30[1](a)[2] | законодавчої бази |
| PM-30[1](a)[3] | нормативної бази |
| PM-30[1](b) | PM-30[1](b)[1] | організація призначає посадових осіб відповідальних за моніторинг виконання та відповідності чинному законодавству програми забезпечення приватності |
| PM-30[1](b)[2] | організація призначає персонал відповідальний за моніторинг виконання та відповідності чинному законодавству програми забезпечення приватності |
| PM-30[3] | оновлювати звіти про забезпечення приватності для: | | |
| PM-30[1](a) | наглядових органів для підтвердження виконання вимог підзвітності відповідно до вимог забезпечення: | |
| PM-30[1](a)[1] | приватності |
| PM-30[1](a)[2] | законодавчої бази |
| PM-30[1](a)[3] | нормативної бази |
| PM-30[1](b) | PM-30[1](b)[1] | організація призначає посадових осіб відповідальних за моніторинг виконання та відповідності чинному законодавству програми забезпечення приватності |
| PM-30[1](b)[2] | організація призначає персонал, відповідальний за моніторинг виконання та відповідності чинному законодавству програми забезпечення приватності. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PM-31 | ПЛАН УПРАВЛІННЯ РИЗИКОМ ЛАНЦЮГА ПОСТАЧАННЯ | | | | |
|  | МЕТА ОЦІНКИ:  визначте, чи організація: | | | | |
| PM-31(a) | розробляє план управління ризиками ланцюга постачання, пов'язаного з: | | | |
| PM-31(a)[1] | розробкою | | |
| PM-31(a)[1][1] | систем | |
| PM-31(a)[1][2] | компонентів системи | |
| PM-31(a)[1][3] | системних послуг | |
| PM-31(a)[2] | придбанням | | |
| PM-31(a)[2][1] | систем | |
| PM-31(a)[2][2] | компонентів системи | |
| PM-31(a)[2][3] | системних послуг | |
| PM-31(a)[3] | обслуговуванням | | |
| PM-31(a)[3][1] | систем | |
| PM-31(a)[3][2] | компонентів системи | |
| PM-31(a)[3][3] | системних послуг | |
| PM-31(a)[4] | утилізацією | | |
| PM-31(a)[4][1] | систем | |
| PM-31(a)[4][2] | компонентів системи | |
| PM-31(a)[4][3] | системних послуг | |
| PM-31(b) | реалізувати план управління ризиками ланцюга постачання послідовно та наскрізно по всій організації | | | |
| PM-31(c) | PM-31(c)[1] | організація визначає частоту з якою необхідно: | | |
| PM-31(c)[1][1] | переглядати план управління ризиком ланцюга постачання | |
| PM-31(c)[1][2] | оновлювати план управління ризиком ланцюга постачання | |
| PM-31(c)[2] | PM-31(c)[2][1] | Переглядати план управління ризиком ланцюга постачання: | |
| PM-31(c)[2][1]{1} | з визначеною організацією частотою |
| PM-31(c)[2][1]{2} | якщо потрібно, у разі організаційних змін |
| PM-31(c)[2][2] | оновлювати план управління ризиком ланцюга постачання з визначеною організацією частотою або, якщо потрібно, у разі організаційних змін | |
| PM-31(c)[2][2]{1} | з визначеною організацією частотою |
| PM-31(c)[2][2]{2} | якщо потрібно, у разі організаційних змін |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PM-32 | ВИЗНАЧЕННЯ РИЗИКІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PM-32(a) | визначити припущення, що впливають на: | |
| PM-32(a)[1] | оцінку ризиків |
| PM-32(a)[2] | реагування на ризики |
| PM-32(a)[3] | моніторинг ризиків |
| PM-32(b) | визначити обмеження, що впливають на: | |
| PM-32(b)[1] | оцінку ризиків |
| PM-32(b)[2] | реагування на ризики |
| PM-32(b)[3] | моніторинг ризиків |
| PM-32(c) | визначити допустимий рівень ризиків | |
| PM-32(d) | PM-32(d)[1] | визначити пріоритети, що розглядаються організацією для управління ризиками |
| PM-32(d)[2] | визначити компроміси, що розглядаються організацією для управління ризиками |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки]. | | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ PS – КАДРОВА БЕЗПЕКА**

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PS-2 | ВИЗНАЧЕННЯ ПОСАДОВОГО РИЗИКУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PS-2(a) | визначити ризики для всіх посад організації | | |
| PS-2(b) | встановити критерії відбору осіб, які заміщують ці посади | | |
| PS-2(c) | PS-2(c)[1] | організація визначає частоту, з якою необхідно | |
| PS-2(c)[1][1] | переглядати посадові ризики |
| PS-2(c)[1][2] | оновлювати посадові ризики |
| PS-2(c)[2] | PS-2(c)[2][1] | переглядати посадові ризики з визначеною організацією частотою |
| PS-2(c)[2][2] | оновлювати посадові ризики з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються категоризації посади; відповідні кодекси федеральних нормативних актів; перелік позначень ризиків для організаційних посад; план безпеки; записи оглядів та оновлення позначень ризиків позицій; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за забезпечення персоналу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для призначення, перегляду та оновлення позначень ризиків позицій; організаційні процеси для встановлення критеріїв скринінгу]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PS-3 | ПЕРЕВІРКА ПЕРСОНАЛУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PS-3(a) | перевіряти окремих осіб перед дозволом на доступ до інформаційної системи | | |
| PS-3(b) | PS-3(b)[1] | PS-3(b)[1][1] | організація визначає умови, що вимагають перегляду окремих осіб для дозволу на доступ, та, |
| PS-3(b)[1][2] | організація визначає необхідну частоту повторного перегляду |
| PS-3(b)[2] | PS-3(b)[2][1] | переглядати окремих осіб відповідно до визначених організацією умов, що вимагають перегляду, та, |
| PS-3(b)[2][2] | переглядати окремих осіб, якщо це визначено необхідною частотою повторного перегляду |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються скринінгу персоналу; записи про перевірений персонал; план безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за забезпечення персоналу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для перевірки персоналу]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PS-3(1) | ПЕРЕВІРКА ПЕРСОНАЛУ - ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PS-3(1)[1] | переконатися, що особи, які звертаються до інформаційної системи, що: | | |
| PS-3(1)[1][1] | PS-3(1)[1][1]{1} | обробляє інформацію з обмеженим доступом |
| PS-3(1)[1][1]{2} | зберігає інформацію з обмеженим доступом |
| PS-3(1)[1][1]{3} | передає інформацію з обмеженим доступом |
| PS-3(1)[1][2] | PS-3(1)[1][2][1] | є перевіреними на доступ до найвищої категорії критичності інформації, до якої вони мають доступ в інформаційній системі. |
| PS-3(1)[1][2][2] | є вповноваженими на доступ до найвищої категорії критичності інформації, до якої вони мають доступ в інформаційній системі. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються скринінгу персоналу; записи про перевірений персонал; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для перевірки та навчання персоналу для доступу до секретної інформації]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PS-3(2) | ПЕРЕВІРКА ПЕРСОНАЛУ - ІНСТРУКТАЖ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PS-3(2)[1] | переконатися, що особи, які звертаються до системи: | |
| PS-3(2)[1]{1} | обробки типів інформації з обмеженим доступом, які вимагають офіційного вповноваження, є офіційно проінструктованими про всі відповідні типи інформації, до якої вони мають доступ в системі |
| PS-3(2)[1]{2} | зберігання типів інформації з обмеженим доступом, які вимагають офіційного вповноваження, є офіційно проінструктованими про всі відповідні типи інформації, до якої вони мають доступ в системі |
| PS-3(2)[1]{3} | передачі типів інформації з обмеженим доступом, які вимагають офіційного вповноваження, є офіційно проінструктованими про всі відповідні типи інформації, до якої вони мають доступ в системі. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються скринінгу персоналу; записи про перевірений персонал; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для формальної обробки всіх відповідних типів інформації, до якої має доступ персонал]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PS-3(3) | ПЕРЕВІРКА ПЕРСОНАЛУ - ІНФОРМАЦІЯ, ЩО ПОТРЕБУЄ ДОДАТКОВИХ ЗАХОДІВ ЗАХИСТУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PS-3(3){1} | переконатися, що особи, які звертаються до ІС, і які зберігають інформацію, що потребує додаткових заходів захисту: | | |
| PS-3(3){1}(a) | мають дійсний дозвіл на доступ, який відповідає: | |
| PS-3(3){1}(a)[1] | законам |
| PS-3(3){1}(a)[2] | наказам |
| PS-3(3){1}(a)[3] | настановам |
| PS-3(3){1}(a)[4] | директивам тощо |
| PS-3(3){1}(b) | PS-3(3){1}(b)[1] | організація визначає додаткові критерії відбору персоналу |
| PS-3(3){1}(b)[2] | задовольняють визначеним організацією додатковим критеріям відбору персоналу |
| PS-3(3){2} | переконатися, що особи, які звертаються до ІС, і які обробляють інформацію, що потребує додаткових заходів захисту: | | |
| PS-3(3){2}(a) | мають дійсний дозвіл на доступ, який відповідає: | |
| PS-3(3){2}(a)[1] | законам |
| PS-3(3){2}(a)[2] | наказам |
| PS-3(3){2}(a)[3] | настановам |
| PS-3(3){2}(a)[4] | директивам тощо |
| PS-3(3){2}(b) | PS-3(3){2}(b)[1] | організація визначає додаткові критерії відбору персоналу |
| PS-3(3){2}(b)[2] | задовольняють визначеним організацією додатковим критеріям відбору персоналу |
| PS-3(3){3} | переконатися, що особи, які звертаються до ІС, які передають інформацію, що потребує додаткових заходів захисту: | | |
| PS-3(3){2}(a) | мають дійсний дозвіл на доступ, який відповідає: | |
| PS-3(3){2}(a)[1] | законам |
| PS-3(3){2}(a)[2] | наказам |
| PS-3(3){2}(a)[3] | настановам |
| PS-3(3){2}(a)[4] | директивам тощо |
| PS-3(3){2}(b) | PS-3(3){2}(b)[1] | організація визначає додаткові критерії відбору персоналу |
| PS-3(3){2}(b)[2] | задовольняють визначеним організацією додатковим критеріям відбору персоналу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; політика контролю доступу, процедури, що стосуються перевірки персоналу; записи про перевірений персонал; критерії скринінгу; записи дозволів на доступ; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для забезпечення дійсних дозволів на доступ до інформації, що вимагає особливого захисту; організаційний процес для додаткового відбору персоналу для інформації, що вимагає особливого захисту]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| PS-3(4) | ПЕРЕВІРКА ПЕРСОНАЛУ - ВИМОГИ ДО ГРОМАДЯН | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PS-3(4)[1] | PS-3(4)[1][1] | організація визначає вимоги до громадян щодо доступу до системи обробки, зберігання або передачі визначених організацією типів інформації |
| PS-3(4)[1][2] | організація визначає типи інформації, щодо яких існують вимоги до громадян для доступу |
| PS-3(4)[2] | переконатися, що особи, які звертаються до системи: | |
| PS-3(4)[2]{1} | обробки визначених організацією типів інформації, задовольняють визначеним організацією вимогам до громадян |
| PS-3(4)[2]{2} | зберігання визначених організацією типів інформації, задовольняють визначеним організацією вимогам до громадян |
| PS-3(4)[2]{3} | передачі визначених організацією типів інформації, задовольняють визначеним організацією вимогам до громадян |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; політика контролю доступу, процедури, що стосуються перевірки персоналу; записи про перевірений персонал; критерії скринінгу; записи дозволів на доступ; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для забезпечення дійсних дозволів на доступ до інформації, що вимагає особливого захисту; організаційний процес для додаткового відбору персоналу для інформації, що вимагає особливого захисту]. | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| PS-4 | ЗВІЛЬНЕННЯ ПЕРСОНАЛУ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| PS-4[1] | при припиненні особою індивідуальної трудової діяльності в організації необхідно: | | | | |
| PS-4[1](a) | PS-4[1](a)[1] | організація визначає період часу, за який необхідно відключити доступ до системи в мережах | | |
| PS-4[1](a)[2] | відключити доступ до системи в межах визначеного організацією періоду часу | | |
| PS-4[1](b) | PS-4[1](b){1} | завершити всі: | | |
| PS-4[1](b){1}[1] | | засоби автентифікації |
| PS-4[1](b){1}[2] | | облікові дані, пов'язані з цією особою |
| PS-4[1](b){2} | скасувати всі: | | |
| PS-4[1](b){2}[1] | | засоби автентифікації |
| PS-4[1](b){2}[2] | | облікові дані, пов'язані з цією особою |
| PS-4[1](c) | PS-4[1](c)[1] | організація визначає теми інформаційної безпеки, які необхідно обговорювати при звільненні | | |
| PS-4[1](c)[2] | провести співбесіди при звільненні, які включають обговорення визначених організацією тем інформаційної безпеки | | |
| PS-4[1](d) | отримати всі, пов'язані з безпекою, організаційні системні властивості | | | |
| PS-4[1](e) | зберігати доступ до: | | | |
| PS-4[1](e)[1] | організаційної інформації, яку раніше контролювала звільнена особа | | |
| PS-4[1](e)[2] | організаційних систем, які раніше контролювала звільнена особа | | |
| PS-4[1](f) | PS-4[1](f)[1] | PS-4[1](f)[1]{1} | організація визначає персонал, який необхідно повідомляти про звільнення співробітника | |
| PS-4[1](f)[1]{2} | організація визначає ролі, які необхідно повідомляти про звільнення співробітника | |
| PS-4[1](f)[2] | PS-4[1](f)[2][1] | організація визначає періоду часу, за який необхідно повідомляти про звільнення співробітника персонал або ролі | |
| PS-4[1](f)[3] | PS-4[1](f)[3]{1} | повідомити визначені організацією персонал протягом визначеного організацією періоду часу про звільнення співробітника | |
| PS-4[1](f)[3]{2} | повідомити визначені організацією ролі протягом визначеного організацією періоду часу про звільнення співробітника | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються звільнення персоналу; записи про припинення роботи персоналу; перелік рахунків інформаційної системи; записи припинених або анульованих автентифікаторів, посвідчень; записи виїзних співбесід; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, відповідальний за управління рахунками; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси припинення персоналу; автоматизовані механізми, що підтримують та, або впроваджують повідомлення про припинення роботи персоналу; автоматизовані механізми відключення доступу до інформаційної системи, скасування автентифікаторів]. | | | | | |

|  |  |  |
| --- | --- | --- |
| PS-4(1) | ЗВІЛЬНЕННЯ ПЕРСОНАЛУ - ВИМОГИ ПІСЛЯ ЗАКІНЧЕННЯ ТРУДОВОЇ ДІЯЛЬНОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PS-4(1)(a) | повідомити звільненим особам про чинні, юридично обов'язкові вимоги, що діють після закінчення трудової діяльності, які стосуються захисту інформації, що стала їм відома під час виконання службових обов’язків |
| PS-4(1)(b) | вимагати від звільнених осіб підписати підтвердження вимог після закінчення трудової діяльності в рамках процесу звільнення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються звільнення персоналу; підписані бланки підтвердження після працевлаштування; перелік застосовних, юридично обов’язкових вимог після працевлаштування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси, що відповідають вимогам після працевлаштування]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| PS-4(2) | ЗВІЛЬНЕННЯ ПЕРСОНАЛУ - АВТОМАТИЗОВАНЕ СПОВІЩЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| PS-4(2)[1] | PS-4(2)[1]{1} | організація визначає персонал, який необхідно повідомляти про звільнення особи |
| PS-4(2)[1]{2} | організація визначає ролі, які необхідно повідомляти про звільнення особи |
| PS-4(2)[2] | впровадити автоматизовані механізми для повідомлення після звільнення особи, визначеного організацією: | |
| PS-4(2)[2]{1} | персоналу |
| PS-4(2)[2]{2} | ролей |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються звільнення персоналу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи про припинення персоналу; автоматизовані повідомлення про звільнення працівників; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за забезпечення персоналу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси звільнення персоналу; автоматизовані механізми, що підтримують та, або впроваджують повідомлення про припинення персоналу]. | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PS-5 | ПЕРЕВЕДЕННЯ ПЕРСОНАЛУ | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | |
| PS-5(a) | PS-5(a){1} | коли особи перепризначаються: | | | | | | | |
| PS-5(a){1}[1] | переглядати поточну оперативну потребу в поточних дозволах: | | | | | | |
| PS-5(a){1}[1][1] | | | Логічного доступу до: | | | |
| PS-5(a){1}[1][1][1] | | | систем |
| PS-5(a){1}[1][1][2] | | | об'єктів |
| PS-5(a){1}[1][2] | | | фізичного доступу до: | | | |
| PS-5(a){1}[1][2][1] | | | систем |
| PS-5(a){1}[1][2][2] | | | об'єктів |
| PS-5(a){1}[2] | підтверджувати поточну оперативну потребу в поточних дозволах: | | | | | | |
| PS-5(a){1}[2][1] | | | логічного доступу до: | | | |
| PS-5(a){1}[2][1][1] | | систем | |
| PS-5(a){1}[2][1][2] | | об'єктів | |
| PS-5(a){1}[2][2] | | | фізичного доступу до: | | | |
| PS-5(a){1}[2][2][1] | | систем | |
| PS-5(a){1}[2][2][2] | | об'єктів | |
| PS-5(a){2} | коли особи переводяться на інші посади в організації: | | | | | | | |
| PS-5(a){2}[1] | переглядати поточну оперативну потребу в поточних дозволах: | | | | | | |
| PS-5(a){2}[1][1] | | | Логічного доступу до: | | | |
| PS-5(a){1}[1][1][1] | | систем | |
| PS-5(a){1}[1][1][2] | | об'єктів | |
| PS-5(a){2}[1][2] | | | фізичного доступу до: | | | |
| PS-5(a){1}[1][2][1] | | систем | |
| PS-5(a){1}[1][2][2] | | об'єктів | |
| PS-5(a){2}[2] | підтверджувати поточну оперативну потребу в поточних дозволах: | | | | | | |
| PS-5(a){2}[2][1] | | | Логічного доступу до: | | | |
| PS-5(a){2}[2][1][1] | | систем | |
| PS-5(a){2}[2][1][2] | | об'єктів | |
| PS-5(a){2}[2][2] | | | фізичного доступу до: | | | |
| PS-5(a){2}[2][2][1] | | систем | |
| PS-5(a){2}[2][2][2] | | об'єктів | |
| PS-5(b) | PS-5(b)[1] | організація визначає дії щодо: | | | | | | | |
| PS-5(b)[1]{1} | | переведення | | | | | |
| PS-5(b)[1]{2} | | перепризначення | | | | | |
| PS-5(b)[2] | організація визначає часовий період після формальної дії переказу, в межах якого необхідно ініціювати визначені організацією дії щодо: | | | | | | | |
| PS-5(b)[2]{1} | | переведення | | | | | |
| PS-5(b)[2]{2} | | перепризначення | | | | | |
| PS-5(b)[3] | ініціювати визначені організацією дії щодо: | | | | | | | |
| PS-5(b)[3]{1} | | переведення, в межах визначеного організацією часового періоду після формальної дії переказ? | | | | | |
| PS-5(b)[3]{2} | | перепризначення, в межах визначеного організацією часового періоду після формальної дії переказу. | | | | | |
| PS-5(c) | змінювати авторизацію доступу, якщо це необхідно, щоб відповідати будь-яким змінам операційної потреби через: | | | | | | | | |
| PS-5(c)[1] | перепризначення | | | | | | | |
| PS-5(c)[2] | переведення | | | | | | | |
| PS-5(d) | PS-5(d)[1] | PS-5(d)[1][1] | | | PS-5(d)[1][1]{1} | | організація визначає персонал, який необхідно повідомляти про переведення персоналу | | |
| PS-5(d)[1][1]{2} | | організація визначає посадові особи, яких необхідно повідомляти про переведення персоналу | | |
| PS-5(d)[1][2] | | | організація визначає період часу, в рамках якого необхідно повідомляти про переведення персоналу визначених організацією осіб | | | | |
| PS-5(d)[2] | повідомляти про переведення персоналу, визначений організацією: | | | | | | | |
| PS-5(d)[2][1] | | | персонал, в рамках визначеного організацією період часу | | | | |
| PS-5(d)[2][2] | | | посадових осіб, в рамках визначеного організацією період часу | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються переведення персоналу; план безпеки; записи про дії з переведення персоналу; перелік дозволів на доступ до інформаційної системи та об'єкта; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за забезпечення персоналу, організаційний персонал, який відповідає за управління рахунками; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для переведення персоналу; автоматизовані механізми, що підтримують та, або впроваджують повідомлення про переведення персоналу; автоматизовані механізми відключення доступу до інформаційної системи, скасування автентифікаторів]. | | | | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| PS-6 | УГОДИ ПРО ДОСТУП | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| PS-6(a) | PS-6(a)[1] | розробити угоди про доступ до інформаційних систем організації | | | |
| PS-6(a)[2] | оформити угоди про доступ до інформаційних систем організації | | | |
| PS-6(b) | PS-6(b)[1] | організація визначає частоту перегляду та оновлення угоди про доступ | | | |
| PS-6(b)[2] | PS-6(b)[2][1] | переглядати угоди про доступ з визначеною організацією частотою | | |
| PS-6(b)[2][2] | оновлювати угоди про доступ з визначеною організацією частотою | | |
| PS-6(c) | PS-6(c)[1] | Переконатися, що особи, які потребують доступу до організаційної інформації: | | | |
| PS-6(c)[1](1) | підписали відповідні угоди про доступ перед тим, як отримати доступ | | |
| PS-6(c)[1](2) | PS-6(c)[1](2)[1] | організація визначає частоту, з якою необхідно повторно підписали угоди про доступ для підтримки доступу до інформаційних систем організації | |
| PS-6(c)[1](2)[2] | повторно підписали угоди про доступ для підтримки доступу до інформаційних систем організації, коли угоди про доступ були: | |
| PS-6(c)[1](2)[2]{1} | оновлені |
| PS-6(c)[1](2)[2]{2} | з визначеною організацією частотою |
| PS-6(c)[2] | переконатися, що особи, які потребують доступу до організаційних систем: | | | |
| PS-6(c)[2](1) | підписали відповідні угоди про доступ перед тим, як отримати доступ | | |
| PS-6(c)[2](2) | PS-6(c)[2](2)[1] | організація визначає частоту, з якою необхідно повторно підписали угоди про доступ для підтримки доступу до інформаційних систем організації | |
| PS-6(c)[2](2)[2] | повторно підписали угоди про доступ для підтримки доступу до інформаційних систем організації, коли угоди про доступ були: | |
| PS-6(c)[2](2)[2]{1} | оновлені |
| PS-6(c)[2](2)[2]{2} | з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються угод про доступ до організаційної інформації та інформаційних систем; план безпеки; угоди про доступ; записи оглядів та оновлень угоди про доступ; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, який підписав, відмовившийся від угоди про доступ; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для угод про доступ; автоматизовані механізми, що підтримують договори про доступ]. | | | | | |

|  |  |
| --- | --- |
| PS-6(1) | УГОДИ ПРО ДОСТУП - ІНФОРМАЦІЯ, ЩО ВИМАГАЄ СПЕЦІАЛЬНОГО ЗАХИСТУ |
|  | [Виключено: включено до PS-3] |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PS-6(2) | УГОДИ ПРО ДОСТУП - ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, ЩО ВИМАГАЄ СПЕЦІАЛЬНОГО ЗАХИСТУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| PS-6(2)[1] | переконатися, що доступ до інформації з обмеженим доступом, що вимагає спеціального захисту, надається лише особам, які: | | |
| PS-6(2)[1](a) | мають дійсний дозвіл на доступ, який відповідає вимогам чинного законодавства | |
| PS-6(2)[1](b) | задовільняють відповідним критеріям безпеки щодо персоналу | |
| PS-6(2)[1](c) | угоду про нерозголошення: | |
| PS-6(2)[1](c)[1] | прочитали, |
| PS-6(2)[1](c)[2] | зрозуміли |
| PS-6(2)[1](c)[3] | підписали |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються угод про доступ до організаційної інформації та інформаційних систем; угоди про доступ; дозволи на доступ; критерії безпеки персоналу; підписані угоди про нерозголошення інформації; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, який підписав угоди про нерозголошення інформації; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси доступу до секретної інформації, що потребує особливого захисту]. | | | |

|  |  |  |
| --- | --- | --- |
| PS-6(3) | УГОДИ ПРО ДОСТУП - ВИМОГИ ПІСЛЯ ЗАКІНЧЕННЯ ТРУДОВОЇ ДІЯЛЬНОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| PS-6(3)(a) | повідомити особам про чинні, юридично обов'язкові вимоги після закінчення трудової діяльності щодо захисту організаційної інформації |
| PS-6(3)(b) | вимагати від осіб підписання підтвердження вимог, якщо це необхідно, як частину надання першого доступу до інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються угод про доступ до організаційної інформації та інформаційних систем; підписані бланки підтвердження після працевлаштування; угоди про доступ; перелік чинних, юридично обов’язкових вимог після працевлаштування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, який підписав угоди про доступ, що включають вимоги після закінчення роботи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси, що відповідають вимогам після працевлаштування; автоматизовані механізми, що підтримують повідомлення та індивідуальні підтвердження вимог після закінчення роботи]. | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PS-7 | БЕЗПЕКА ЗОВНІШНЬОГО ПЕРСОНАЛУ | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | |
| PS-7(a) | встановити вимоги щодо безпеки персоналу, включаючи: | | | | | | | | | |
| PS-7(a)[1] | | ролі щодо безпеки для зовнішніх постачальників послуг | | | | | | | |
| PS-7(a)[2] | | обов'язки щодо безпеки для зовнішніх постачальників послуг | | | | | | | |
| PS-7(b) | вимагати від зовнішніх постачальників дотримання: | | | | | | | | | |
| PS-7(b)[1] | | правил кадрової безпеки, встановлених організацією | | | | | | | |
| PS-7(b)[2] | | процедур кадрової безпеки, встановлених організацією | | | | | | | |
| PS-7(c) | вимагати безпечного ставлення персоналу до документів | | | | | | | | | |
| PS-7(d) | PS-7(d)[1] | PS-7(d)[1][1] | | PS-7(d)[1][1]{1} | організація визначає персонал, якому повинен повідомляти зовнішній постачальник про будь-які: | | | | | |
| PS-7(d)[1][1]{1}{1} | переведення зовнішнього персоналу, який: | | | | |
| PS-7(d)[1][1]{1}{1}{1} | | | володіє організаційними повноваженнями | |
| PS-7(d)[1][1]{1}{1}{2} | | | має системні привілеї | |
| PS-7(d)[1][1]{1}{2} | звільнення зовнішнього персоналу, який: | | | | |
| PS-7(d)[1][1]{1}{2}{1} | | | володіє організаційними повноваженнями | |
| PS-7(d)[1][1]{1}{2}{2} | | | має системні привілеї | |
| PS-7(d)[1][2] | | PS-7(d)[1][2]{2} | організація визначає ролі, яким повинен повідомляти зовнішній постачальник про будь-які: | | | | | |
| PS-7(d)[1][2]{2}{1} | | переведення зовнішнього персоналу, який: | | | |
| PS-7(d)[1][2]{2}{1}{1} | | | володіє організаційними повноваженнями |
| PS-7(d)[1][2]{2}{1}{2} | | | має системні привілеї |
| PS-7(d)[1][2]{2}{2} | | звільнення зовнішнього персоналу, який: | | | |
| PS-7(d)[1][2]{2}{2}{1} | | | володіє організаційними повноваженнями |
| PS-7(d)[1][2]{2}{2}{2} | | | має системні привілеї |
| PS-7(d)[1][3] | | організація визначає термін, у який зовнішні постачальники повинні повідомляти про будь-які переведення або звільнення зовнішнього персоналу, який володіє організаційними повноваженнями або має системні привілеї в межах визначеного організацією терміну | | | | | | |
| PS-7(d)[2] | вимагати від зовнішніх постачальників повідомляти визначені організацією: | | | | | | | | |
| PS-7(d)[2]{1} | | персонал щодо будь-яких: | | | | | | |
| PS-7(d)[2]{1}{1} | переведень зовнішнього персоналу, який: | | | | | |
| PS-7(d)[2]{1}{1}{1} | | | володіє організаційними повноваженнями в межах визначеного організацією терміну | | |
| PS-7(d)[2]{1}{1}{2} | | | має системні привілеї в межах визначеного організацією терміну | | |
| PS-7(d)[2]{1}{2} | звільнення зовнішнього персоналу, який: | | | | | |
| PS-7(d)[2]{1}{2}{1} | | | володіє організаційними повноваженнями в межах визначеного організацією терміну | | |
| PS-7(d)[2]{1}{2}{2} | | | має системні привілеї в межах визначеного організацією терміну | | |
| PS-7(d)[2]{2} | | ролі щодо будь-яких переведень або звільнення зовнішнього персоналу, який володіє організаційними повноваженнями або має системні привілеї в межах визначеного організацією терміну | | | | | | |
| PS-7(d)[2]{2}{1} | переведень зовнішнього персоналу, який: | | | | | |
| PS-7(d)[2]{2}{1}{1} | | | володіє організаційними повноваженнями в межах визначеного організацією терміну | | |
| PS-7(d)[2]{2}{1}{2} | | | має системні привілеї в межах визначеного організацією терміну | | |
| PS-7(d)[2]{2}{2} | звільнення зовнішнього персоналу, який: | | | | | |
| PS-7(d)[2]{2}{2}{1} | | | володіє організаційними повноваженнями в межах визначеного організацією терміну | | |
| PS-7(d)[2]{2}{2}{2} | | | має системні привілеї в межах визначеного організацією терміну | | |
| PS-7(e) | Контролювати відповідність постачальника | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР : Політика безпеки персоналу; процедури, що стосуються безпеки сторонніх кадрів; перелік вимог до безпеки персоналу; документи на придбання; угоди про рівень обслуговування; процес моніторингу дотримання; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за безпеку персоналу; сторонні провайдери; адміністратори системи, мережі; організаційний персонал, відповідальний за управління обліковими записами; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для управління та моніторингу безпеки сторонніх кадрів; автоматизовані механізми, що підтримують та, або впроваджують моніторинг дотримання вимог провайдера]. | | | | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PS-8 | КАДРОВІ САНКЦІЇ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| PS-8(a) | використовувати формальний процес санкцій для осіб, які не дотримуються встановлених: | | | |
| PS-8(a)[1] | правил інформаційної безпеки | | |
| PS-8(a)[2] | процедур інформаційної безпеки | | |
| PS-8(b) | PS-8(b)[1] | PS-8(b)[1]{1} | організація визначає персонал, який необхідно повідомляти, коли починається офіційний процес накладання санкцій працівникам, визначаючи особу та причину санкції. | |
| PS-8(b)[1]{2} | організація визначає ролі, які необхідно повідомляти, коли починається офіційний процес накладання санкцій працівникам, визначаючи особу та причину санкції. | |
| PS-8(b)[2] | організація визначає періоду часу, коли починається офіційний процес накладання санкцій працівникам, визначаючи особу та причину санкції. | | |
| PS-8(b)[3] | повідомляти визначений організацією: | | |
| PS-8(b)[3]{1} | персонал в межах визначеного організацією періоду часу, коли починається офіційний процес накладання санкцій працівникам, визначаючи: | |
| PS-8(b)[3]{1}[1] | особу |
| PS-8(b)[3]{1}[2] | причину санкції |
| PS-8(b)[3]{2} | ролі в межах визначеного організацією періоду часу, коли починається офіційний процес накладання санкцій працівникам, визначаючи; | |
| PS-8(b)[3]{2}[1] | особу |
| PS-8(b)[3]{2}[2] | причину санкції |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика безпеки персоналу; процедури, що стосуються кадрових санкцій; правила поведінки; записи формальних санкцій; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за безпеку персоналу; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для управління кадровими санкціями; автоматизовані механізми підтримки та, або реалізації повідомлень]. | | | | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ RA – ОЦІНКА РИЗИКУ**

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RA-2 | КАТЕГОРІЮВАННЯ БЕЗПЕКИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| RA-2(a) | RA-2(a)[1] | здійснити категоріювання інформаційної системи | |
| RA-2(a)[2] | здійснити категоріювання інформації, яку інформаційна система: | |
| RA-2(a)[2][1] | обробляє |
| RA-2(a)[2][2] | зберігає |
| RA-2(a)[2][3] | передає |
| RA-2(b) | задокументувати результати категоріювання безпеки, включаючи обґрунтування, в плані захисту інформаційної системи | | |
| RA-2(c) | RA-2(c){1} | підтвердити, що посадова особа: | |
| RA-2(c){1}[1] | переглядає рішення про категоріювання безпеки |
| RA-2(c){1}[2] | затверджує рішення про категоріювання безпеки |
| RA-2(c){2} | підтвердити, що уповноважений офіційний представник: | |
| RA-2(c){2}[1] | переглядає рішення про категоріювання безпеки |
| RA-2(c){2}[2] | затверджує рішення про категоріювання безпеки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; політика та процедури планування безпеки; процедури, що стосуються категоризації безпеки організаційної інформації та інформаційних систем; план безпеки; документація щодо категоризації безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за категоризацію безпеки та несе відповідальність за оцінку ризиків; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для категоріювання безпеки]. | | | |

|  |  |  |
| --- | --- | --- |
| RA-2(1) | КАТЕГОРІЮВАННЯ БЕЗПЕКИ - КАТЕГОРІЮВАННЯ ДРУГОГО РІВНЮ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| RA-2(1)[1] | провести категоріювання другого рівня для інформаційних систем організації з метою отримання додаткової деталізації рівнів критичності інформаційної системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; політика та процедури планування безпеки; процедури, що стосуються категоризації безпеки організаційної інформації та інформаційних систем; план безпеки; документація щодо категоризації безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за категоризацію безпеки та несе відповідальність за оцінку ризиків; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для категоріювання безпеки]. | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| RA-3 | ОЦІНКА РИЗИКУ | | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | | | | | |
| RA-3(a) | проводити оцінку ризику, включаючи: | | | | | | | | | | | | | |
| RA-3(a)[1] | вірогідність шкоди від: | | | | | | | | | | | | |
| RA-3(a)(1) | | RA-3(a)(1){1} | | | несанкціонованого доступу до: | | | | | | | |
| RA-3(a)(1){1}[1] | | інформаційної системи | | | | | |
| RA-3(a)(1){1}[2] | | Інформації, яку вона: | | | | | |
| RA-3(a)(1){1}[2][1] | | | | | обробляє |
| RA-3(a)(1){1}[2][2] | | | | | зберігає та |
| RA-3(a)(1){1}[2][3] | | | | | передає |
| RA-3(a)(1){1}[3] | | а також будь-якої пов'язаної інформації; | | | | | |
| RA-3(a)(1){2} | | | використання: | | | | | | | |
| RA-3(a)(1){2}[1] | | інформаційної системи | | | | | |
| RA-3(a)(1){2}[2] | | Інформації, яку вона: | | | | | |
| RA-3(a)(1){2}[2][1] | | | | | обробляє |
| RA-3(a)(1){2}[2][2] | | | | | зберігає та |
| RA-3(a)(1){2}[2][3] | | | | | передає |
| RA-3(a)(1){2}[3] | | а також будь-якої пов'язаної інформації; | | | | | |
| RA-3(a)(1){3} | | | розголошення, | | | | | | | |
| RA-3(a)(1){3}[1] | | | інформаційної системи | | | | |
| RA-3(a)(1){3}[2] | | | інформації, яку вона: | | | | |
| RA-3(a)(1){3}[2][1] | | | | обробляє |
| RA-3(a)(1){3}[2][2] | | | | зберігає та |
| RA-3(a)(1){3}[2][3] | | | | передає |
| RA-3(a)(1){3}[3] | | | а також будь-якої пов'язаної інформації | | | | |
| RA-3(a)(1){4} | | | руйнування | | | | | | | |
| RA-3(a)(1){4}[1] | | | інформаційної системи | | | | |
| RA-3(a)(1){4}[2] | | | інформації, яку вона: | | | | |
| RA-3(a)(1){4}[2][1] | | | | обробляє |
| RA-3(a)(1){4}[2][2] | | | | зберігає та |
| RA-3(a)(1){4}[2][3] | | | | передає |
| RA-3(a)(1){4}[3] | | | а також будь-якої пов'язаної інформації | | | | |
| RA-3(a)(1){5} | | | модифікації | | | | | | | |
| RA-3(a)(1){5}[1] | | | інформаційної системи | | | | |
| RA-3(a)(1){5}[2] | | | інформації, яку вона: | | | | |
| RA-3(a)(1){5}[2][1] | | | | обробляє |
| RA-3(a)(1){5}[2][2] | | | | зберігає та |
| RA-3(a)(1){5}[2][3] | | | | передає |
| RA-3(a)(1){5}[3] | | | а також будь-якої пов'язаної інформації | | | | |
| RA-3(a)(1){6} | | | знищення, | | | | | | | |
| RA-3(a)(1){6}[1] | | | інформаційної системи | | | | |
| RA-3(a)(1){6}[2] | | | інформації, яку вона: | | | | |
| RA-3(a)(1){6}[2][1] | | | | обробляє |
| RA-3(a)(1){6}[2][2] | | | | зберігає та |
| RA-3(a)(1){6}[2][3] | | | | передає |
| RA-3(a)(1){6}[3] | | | а також будь-якої пов'язаної інформації | | | | |
| RA-3(a)[1](2) | | проблем, пов'язаних з приватністю фізичних осіб, що виникають у результаті обробки персональних даних | | | | | | | | | | |
| RA-3(a)[2] | величину шкоди від: | | | | | | | | | | | | |
|  | RA-3(a)[2](1) | | RA-3(a)[2](1){1} | | | несанкціонованого доступу до: | | | | | | | |
| RA-3(a)[2](1){1}[1] | | | | інформаційної системи | | | |
| RA-3(a)[2](1){1}[2] | | | | Інформації, яку вона: | | | |
| RA-3(a)[2](1){1}[2][1] | | | обробляє |
| RA-3(a)[2](1){1}[2][2] | | | зберігає та |
| RA-3(a)[2](1){1}[2][3] | | | передає |
| RA-3(a)[2](1){1}[3] | | | | а також будь-якої пов'язаної інформації | | | |
| RA-3(a)[2](1){2} | | | використання: | | | | | | | |
| RA-3(a)[2](1){2}[1] | | | | інформаційної системи | | | |
| RA-3(a)[2](1){2}[2] | | | | Інформації, яку вона: | | | |
| RA-3(a)[2](1){2}[2][1] | | | обробляє |
| RA-3(a)[2](1){2}[2][2] | | | зберігає та |
| RA-3(a)[2](1){2}[2][3] | | | передає |
| RA-3(a)[2](1){2}[3] | | | | а також будь-якої пов'язаної інформації | | | |
| RA-3(a)[2](1){3} | | | розголошення | | | | | | | |
| RA-3(a)[2](1){3}[1] | | | | інформаційної системи | | | |
| RA-3(a)[2](1){3}[2] | | | | інформації, яку вона: | | | |
| RA-3(a)[2](1){3}[2][1] | | | обробляє |
| RA-3(a)[2](1){3}[2][2] | | | зберігає та |
| RA-3(a)[2](1){3}[2][3] | | | передає |
| RA-3(a)[2](1){3}[3] | | | | а також будь-якої пов'язаної інформації | | | |
| RA-3(a)[2](1){4} | | | руйнування | | | | | | | |
| RA-3(a)[2](1){4}[1] | | | | інформаційної системи | | | |
| RA-3(a)[2](1){4}[2] | | | | інформації, яку вона: | | | |
| RA-3(a)[2](1){4}[2][1] | | | обробляє |
| RA-3(a)[2](1){4}[2][2] | | | зберігає та |
| RA-3(a)[2](1){4}[2][3] | | | передає |
| RA-3(a)[2](1){4}[3] | | | | а також будь-якої пов'язаної інформації | | | |
| RA-3(a)[2](1){5} | | | модифікації | | | | | | | |
| RA-3(a)[2](1){5}[1] | | | | інформаційної системи | | | |
| RA-3(a)[2](1){5}[2] | | | | інформації, яку вона: | | | |
| RA-3(a)[2](1){5}[2][1] | | | обробляє |
| RA-3(a)[2](1){5}[2][2] | | | зберігає та |
| RA-3(a)[2](1){5}[2][3] | | | передає |
| RA-3(a)[2](1){5}[3] | | | | а також будь-якої пов'язаної інформації | | | |
| RA-3(a)[2](1){6} | | | знищення | | | | | | | |
| RA-3(a)[2](1){6}[1] | | | | | інформаційної системи | | |
| RA-3(a)[2](1){6}[2] | | | | | інформації, яку вона: | | |
| RA-3(a)[2](1){6}[2][1] | | обробляє |
| RA-3(a)[2](1){6}[2][2] | | зберігає та |
| RA-3(a)[2](1){6}[2][3] | | передає |
| RA-3(a)[2](1){6}[3] | | | | | а також будь-якої пов'язаної інформації | | |
| RA-3(a)[2](2) | | проблем, пов'язаних з приватністю фізичних осіб, що виникають у результаті обробки персональних даних | | | | | | | | | | |
| RA-3(b) | інтегрувати результати оцінки ризику та рішення з управління ризиками на рівні організації та завдань, процесів з оцінкою ризиків на рівні інформаційної системи | | | | | | | | | | | | | |
| RA-3(c) | RA-3(c)[1] | | організація визначає документ, у якому задокументовують результати оцінки ризику (один з наступного): | | | | | | | | | | | |
| RA-3(c)[1]{1} | | | плани безпеки та приватності | | | | | | | | |
| RA-3(c)[1]{2} | | | звіт про оцінку ризику | | | | | | | | |
| RA-3(c)[2] | | задокументувати результати оцінки ризику у визначений організацією документ: | | | | | | | | | | | |
| RA-3(c)[2]{1} | | | плани безпеки та приватності | | | | | | | | |
| RA-3(c)[2]{2} | | | звіт про оцінку ризику | | | | | | | | |
| RA-3(d) | RA-3(d)[1] | | організація визначає частоту перегляду результатів оцінки ризиків | | | | | | | | | | | |
| RA-3(d)[2] | | переглядати результати оцінки ризиків з визначеною організацією частотою | | | | | | | | | | | |
| RA-3(e) | RA-3(e)[1] | | RA-3(e)[1]{1} | | організація визначає персонал, серед якого мають поширювати результати оцінки ризику | | | | | | | | | |
| RA-3(e)[1]{2} | | організація визначає посадових осіб, серед яких мають поширювати результати оцінки ризику | | | | | | | | | |
| RA-3(e)[2] | | поширити результати оцінки ризику серед визначеного організацією: | | | | | | | | | | | |
| RA-3(e)[2]{1} | | персоналу | | | | | | | | | |
| RA-3(e)[2]{2} | | посадових осіб | | | | | | | | | |
| RA-3(f) | RA-3(f)[1] | | організація визначає частоту з якою необхідно оновлювати оцінку ризику | | | | | | | | | | | |
| RA-3(f)[2] | | оновлювати оцінку ризику: | | | | | | | | | | | |
| RA-3(f)[2]{1} | | з визначеною організацією частотою або | | | | | | | | | |
| RA-3(f)[2]{2} | | коли є суттєві зміни в: | | | | | | | | | |
| RA-3(f)[2]{2}{1} | | | інформаційній системі | | | | | | |
| RA-3(f)[2]{2}{2} | | | робочому середовищі інформаційній системі | | | | | | |
| RA-3(f)[2]{2}{3} | | | інших умовах, які можуть вплинути на: | | | | | | |
| RA-3(f)[2]{2}{3}{1} | | | | | стан безпеки | |
| RA-3(f)[2]{2}{3}{2} | | | | | приватність інформаційної системи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; політика та процедури планування безпеки; процедури, що стосуються організаційних оцінок ризику; план безпеки; оцінка ризику; результати оцінки ризику; огляди оцінки ризику; оновлення оцінки ризику; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за оцінку ризиків; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для оцінки ризиків; автоматизовані механізми підтримки та, або для проведення, документування, перегляду, розповсюдження та оновлення оцінки ризику]. | | | | | | | | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RA-3(1) | ОЦІНКА РИЗИКУ - ОЦІНКА РИЗИКУ ЛАНЦЮГА ПОСТАЧАННЯ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| RA-3(1)(a) | RA-3(1)(a)[1] | RA-3(1)(a)[1][1] | організація визначає системи, що можуть впливати на ризики ланцюга постачання | |
| RA-3(1)(a)[1][2] | організація визначає компоненти системи, що можуть впливати на ризики ланцюга постачання | |
| RA-3(1)(a)[1][3] | організація визначає системні служби, що можуть впливати на ризики ланцюга постачання | |
| RA-3(1)(a)[2] | оцінити ризики ланцюга постачання, пов'язані з: | | |
| RA-3(1)(a)[2][1] | визначеними організацією системами | |
| RA-3(1)(a)[2][2] | компонентами системи | |
| RA-3(1)(a)[2][3] | системними службами | |
| RA-3(1)(b) | RA-3(1)(b)[1] | організація визначає частоту, з якою необхідно оновлювати оцінку ризику ланцюга постачання | | |
| RA-3(1)(b)[2] | оновлювати оцінку ризику ланцюга постачання з: | | |
| RA-3(1)(b)[2]{1} | | визначеною організацією частотою |
| RA-3(1)(b)[2]{2} | | коли відбуваються значні зміни у відповідному ланцюгу постачання |
| RA-3(1)(b)[2]{3} | | коли є зміни в інформаційній системі |
| RA-3(1)(b)[2]{4} | | зміни в робочому середовищі |
| RA-3(1)(b)[2]{5} | | зміни в інших умовах можуть вимагати змін в ланцюгу постачання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; політика та процедури планування безпеки; процедури, що стосуються організаційних оцінок ризику; план безпеки; оцінка ризику; результати оцінки ризику; огляди оцінки ризику; оновлення оцінки ризику; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за оцінку ризиків; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для оцінки ризиків; автоматизовані механізми підтримки та, або для проведення, документування, перегляду, розповсюдження та оновлення оцінки ризику]. | | | | |

|  |  |
| --- | --- |
| RA-4 | ОНОВЛЕННЯ ОЦІНКИ РИЗИКУ |
|  | [Вилучено: включено до RА-3]. |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| RA-5 | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | |
| RA-5(a) | RA-5(a)[1] | організація визначає (один або кілька): | | | | | | | | |
| RA-5(a)[1]{1} | | | частоту сканування на наявність вразливостей в інформаційній системі та інстальованих додатках | | | | | |
| RA-5(a)[1]{2} | | | процес випадкового сканування на наявність вразливостей в інформаційній системі та інстальованих додатках | | | | | |
| RA-5(a)[2] | сканувати на наявність вразливостей в: | | | | | | | | |
| RA-5(a)[2][1] | | інформаційній системі з: | | | | | | |
| RA-5(a)[2][1][1] | | | RA-5(a)[2][1][1]{1} | | визначеною організацією частотою (та, або) | |
| RA-5(a)[2][1][1]{2} | | випадково відповідно до визначеного організацією процесу | |
| RA-5(a)[2][1][2] | | | коли виявляються нові вразливості, які потенційно впливають на інформаційну систему | | | |
| RA-5(a)[2][2] | | інстальованих додатках з визначеною організацією частотою та, або випадково відповідно до визначеного організацією процесу і коли виявляються нові вразливості, які потенційно впливають на інформаційну систему | | | | | | |
| RA-5(b) | використовувати: | | | | | | | | | |
| RA-5(b)[1] | | інструменти сканування вразливості, які: | | | | | | | |
| RA-5(b)[1][1] | | | полегшують сумісність між інструментами та | | | | |
| RA-5(b)[1][2] | | | автоматизують частини процесу управління вразливостями, використовуючи стандарти для: | | | | |
| RA-5(b)[1][2](1) | | RA-5(b)[1][2](1)[1] | | обліку платформ |
| RA-5(b)[1][2](1)[2] | | обліку недоліків програмного забезпечення |
| RA-5(b)[1][2](1)[3] | | обліку неправильних конфігурацій |
| RA-5(b)[1][2](2) | | RA-5(b)[1][2](2)[1] | | форматування контрольних списків тестування |
| RA-5(b)[1][2](2)[2] | | форматування процедур тестування |
| RA-5(b)[1][2](3) | | вимірювання впливу вразливості | | |
| RA-5(b)[2] | | методи сканування вразливості, які: | | | | | | | |
| RA-5(b)[2][1] | | | полегшують сумісність між інструментами та | | | | |
| RA-5(b)[2][2] | | | автоматизують частини процесу управління вразливостями, використовуючи стандарти для: | | | | |
| RA-5(b)[2][2](1) | | RA-5(b)[2][2](1)[1] | | обліку платформ |
| RA-5(b)[2][2](1)[2] | | обліку недоліків програмного забезпечення |
| RA-5(b)[2][2](1)[3] | | обліку неправильних конфігурацій |
| RA-5(b)[2][2](2) | | RA-5(b)[2][2](2)[1] | | форматування контрольних списків тестування |
| RA-5(b)[2][2](2)[2] | | форматування процедур тестування |
| RA-5(b)[2][2](3) | | вимірювання впливу вразливості | | |
| RA-5(c) | аналізувати: | | | | | | | | | |
| RA-5(c)[1] | | звіти про сканування вразливості | | | | | | | |
| RA-5(c)[2] | | результати контрольних оцінювань | | | | | | | |
| RA-5(d) | RA-5(d)[1] | | організація визначає час, за який необхідно виправити наявні вразливості | | | | | | | |
| RA-5(d)[2] | | виправити наявні вразливості у визначений організацією час відповідно до організаційної оцінки ризику | | | | | | | |
| RA-5(e) | RA-5(e)[1] | | RA-5(e)[1]{1} | | | організація визначає персонал, серед якого поширюють інформацію, отриману у процесі сканування вразливостей та контрольного оцінювання | | | | |
| RA-5(e)[1]{2} | | | організація визначає ролі, серед яких поширюють інформацію, отриману у процесі сканування вразливостей та контрольного оцінювання | | | | |
| RA-5(e)[2] | | ділитися інформацією, отриманою у процесі: | | | | | | | |
| RA-5(e)[2][1] | | | сканування вразливостей серед: | | | | |
| RA-5(e)[2][1]{1} | | визначеного організацією персоналу, щоб допомогти усунути подібні вразливі місця в інших системах | | |
| RA-5(e)[2][1]{2} | | визначених організацією ролей, щоб допомогти усунути подібні вразливі місця в інших системах | | |
| RA-5(e)[2][2] | | | контрольного оцінювання серед: | | | | |
| RA-5(e)[2][2]{1} | | визначеного організацією персоналу, щоб допомогти усунути подібні вразливі місця в інших системах | | |
| RA-5(e)[2][2]{2} | | визначених організацією ролей, щоб допомогти усунути подібні вразливі місця в інших системах | | |
| RA-5(f) | використовувати інструменти сканування вразливості, які включають можливість легко оновлювати вразливості що були проскановані | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; процедури, що стосуються сканування вразливості; оцінка ризику; план безпеки; звіт про оцінку безпеки; засоби сканування вразливості та відповідна документація щодо конфігурації; результати сканування вразливості; записи про виправлення та вразливість; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за оцінку ризиків, оцінку контролю безпеки та сканування вразливості; організаційний персонал, відповідальний за аналіз вразливості організаційний персонал, відповідальний за усунення вразливостей; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі].  Перевірка: [ВИБІР: Організаційні процеси для сканування, аналізу, виправлення та обміну інформацією щодо вразливостей; автоматизовані механізми, що підтримують та, або впроваджують сканування, аналіз, виправлення та обмін інформацією про вразливість]. | | | | | | | | | | |

|  |  |
| --- | --- |
| RA-5(1) | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - МОЖЛИВІСТЬ ОНОВЛЕННЯ ІНСТРУМЕНТІВ |
|  | [Вилучено: включено до RА-5] |

|  |  |  |  |
| --- | --- | --- | --- |
| RA-5(2) | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ОНОВЛЕННЯ ЗА ЧАСТОТОЮ, ПЕРЕД НОВИМ СКАНУВАННЯМ АБО ПРИ ІДЕНТИФІКАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| RA-5(2)[1] | організація визначає частоту, з якою необхідно проводити оновлення переліку вразливостей системи, що були проскановані. | |
| RA-5(2)[2] | оновлювати перелік вразливостей системи, що були проскановані (один або більше): | |
| RA-5(2)[2]{1} | з визначеною організацією частотою |
| RA-5(2)[2]{2} | перед новим скануванням |
| RA-5(2)[2]{3} | коли виявлені та зареєстровані нові вразливості |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Процедури, що стосуються сканування вразливості; план безпеки; звіт про оцінку безпеки; засоби сканування вразливості та відповідна документація щодо конфігурації; результати сканування вразливості; записи про виправлення та вразливість; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який несе відповідальність за сканування вразливостей; організаційний персонал, відповідальний за аналіз вразливості організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі].  Перевірка: [ВИБІР: Організаційні процеси для сканування вразливості; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливостей]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| RA-5(3) | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ШИРОТА ТА ГЛИБИНА ПОКРИТТЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| RA-5(3)[1] | запровадити процедури сканування вразливостей, які: | |
| RA-5(3)[1][1] | дозволять визначити широту покриття |
| RA-5(3)[1][2] | дозволять визначити глибину покриття |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Процедури, що стосуються сканування вразливості; план безпеки; звіт про оцінку безпеки; засоби сканування вразливості та відповідна документація щодо конфігурації; результати сканування вразливості; записи про виправлення та вразливість; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який несе відповідальність за сканування вразливостей; організаційний персонал, відповідальний за аналіз вразливості організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для сканування вразливості; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливостей]. | | |

|  |  |  |
| --- | --- | --- |
| RA-5(4) | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ВИЯВНА ІНФОРМАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| RA-5(4)[1] | організація визначає коригувальні дії, які слід застосовувати при непередбачено виявленій інформації про інформаційну систему |
| RA-5(4)[2] | визначити непередбачено-виявну інформацію про інформаційну систему |
| RA-5(4)[3] | застосувати визначені організацією коригувальні дії при непередбачено виявленій інформації про інформаційну систему |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Процедури, що стосуються сканування вразливості; звіт про оцінку безпеки; результати тесту на проникнення; результати сканування вразливості; звіт про оцінку ризику; записи про вжиті коригувальні дії; записи реагування на події; записи аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який несе відповідальність за сканування та, або тестування на проникнення; організаційний персонал, відповідальний за аналіз вразливості; організаційний персонал, відповідальний за реагування на ризик; організаційний персонал, відповідальний за управління інцидентами та реагування на них; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для сканування вразливості; організаційні процеси реагування на ризик; організаційні процеси для управління інцидентами та реагування на них; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливості; автоматизовані механізми підтримки та, або реалізації реагування на ризик; автоматизовані механізми підтримки та, або реалізації управління та реагування на інциденти]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| RA-5(5) | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ПРИВІЛЕЙОВАНИЙ ДОСТУП | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| RA-5(5)[1] | RA-5(5)[1][1] | організація визначає компоненти системи, до яких необхідно реалізувати авторизацію привілейованого доступу |
| RA-5(5)[1][2] | організація визначає діяльність з виявлення вразливостей, яка потребує реалізації авторизації привілейованого доступу до визначених організацією компонентів системи |
| RA-5(5)[2] | реалізувати авторизацію привілейованого доступу до визначених організацією компонентів системи для визначеної організацією діяльності з виявлення вразливостей | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; процедури, що стосуються сканування вразливості; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік компонентів інформаційної системи для сканування вразливості; список дозволів на доступ персоналу; авторизаційні дані; отримати доступ до записів авторизації; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який несе відповідальність за сканування вразливостей; адміністратори системи, мережі; організаційний персонал, відповідальний за контроль доступу до інформаційної системи; організаційний персонал, відповідальний за управління конфігурацією інформаційної системи; розробники системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для сканування вразливості; організаційні процеси контролю доступу; автоматизовані механізми, що підтримують та, або впроваджують контроль доступу; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливостей]. | | |

|  |  |  |
| --- | --- | --- |
| RA-5(6) | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - АВТОМАТИЗОВАНИЙ АНАЛІЗ ТЕНДЕНЦІЙ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| RA-5(6)[1] | впровадити автоматизовані механізми для порівняння результатів сканування вразливостей з часом, щоб визначити тенденції вразливості системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; процедури, що стосуються сканування вразливості; проєктна документація інформаційної системи; документація щодо засобів та методів сканування вразливостей; результати сканування вразливості; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який несе відповідальність за сканування вразливостей; організаційний персонал, відповідальний за аналіз вразливості організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для сканування вразливості; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливості; автоматизовані механізми, що підтримують та, або впроваджують аналіз тенденцій результатів сканування вразливості]. | |

|  |  |
| --- | --- |
| RA-5(7) | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ ТА СПОВІЩЕННЯ ПРО НЕАВТОРИЗОВАНІ КОМПОНЕНТИ |
|  | [Вилучено: включено до CM-8] |

|  |  |  |
| --- | --- | --- |
| RA-5(8) | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ОГЛЯД ЖУРНАЛІВ АУДИТУ ЗА МИНУЛІ ПЕРІОДИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| RA-5(8)[1] | переглядати журнали аудиту за минулі періоди, щоб визначити, чи була уразливість, яка виявлена в системі, використана до її виявлення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; процедури, що стосуються сканування вразливості; журнали аудиту; записи оглядів журналу аудиту; результати сканування вразливості; записи про виправлення та вразливість; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який несе відповідальність за сканування вразливостей; організаційний персонал, відповідальний за аналіз вразливості ; організаційний персонал, відповідальний за перевірку аудиторських записів; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для сканування вразливості; організаційний процес для перевірки та відповіді на записи аудиту; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливості; автоматизовані механізми, що підтримують та, або впроваджують перевірку записів аудиту]. | |

|  |  |
| --- | --- |
| RA-5(9) | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ТЕСТУВАННЯ ТА АНАЛІЗ ПРОНИКНЕННЯ |
|  | [Вилучено: включено до CA-8]. |

|  |  |  |
| --- | --- | --- |
| RA-5(10) | СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - СПІВСТАВЛЕННЯ ІНФОРМАЦІЇ ПРО СКАНУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| RA-5(10)[1] | зіставляти вихідні дані з інструментів сканування вразливостей для визначення наявності численних вразливостей та мультиплікаційних (multi-hop) векторах атаки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризиків; процедури, що стосуються сканування вразливості; оцінка ризику; план безпеки; документація щодо засобів та методів сканування вразливостей; результати сканування вразливості; записи управління вразливістю; записи аудиту; журнали кореляції подій, уразливостей; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який несе відповідальність за сканування вразливостей; організаційний персонал, відповідальний за аналіз вразливості організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для сканування вразливості; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливості; автоматизовані механізми, що реалізують кореляцію результатів сканування вразливості]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| RA-6 | ЗАХОДИ ПРОТИДІЇ ТЕХНІЧНІЙ РОЗВІДКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| RA-6[1] | RA-6[1][1] | організація визначає місця, у яких необхідно використовувати заходи ПДТР |
| RA-6[1][2] | організація визначає частоту, з якою необхідно застосовувати заходи ПДТР |
| RA-6[1][3] | організація визначає події, за яких необхідно використовувати заходи ПДТР |
| RA-6[1][4] | організація визначає показники, за яких необхідно використовувати заходи ПДТР |
| RA-6[2] | використовувати заходи ПДТР у визначених організацією місцях (один або кілька): | |
| RA-6[2]{1} | з визначеною організацією частотою |
| RA-6[2]{2} | за визначеними організацією подіями |
| RA-6[2]{3} | за визначеними організацією показниками |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; процедури, що стосуються обстеження контрзаходів технічного нагляду; план безпеки; записи аудиту, журнали подій; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за обстеження контрзаходів технічного нагляду; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для обстеження контрзаходів технічного нагляду; автоматизовані механізми, інструменти, що підтримують та, або впроваджують обстеження контрзаходів технічного нагляду]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RA-7 | РЕАГУВАННЯ НА РИЗИК | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| RA-7[1] | реагувати на результати: | | |
| RA-7[1][1] | оцінки | |
| RA-7[1][1][1] | безпеки |
| RA-7[1][1][2] | приватності |
| RA-7[1][2] | моніторингу | |
| RA-7[1][2][1] | безпеки |
| RA-7[1][2][2] | приватності |
| RA-7[1][3] | аудиту | |
| RA-7[1][3][1] | безпеки |
| RA-7[1][3][2] | приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; процедури, що стосуються реагування на ризик; план безпеки; записи аудиту, журнали подій; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за реагування на інциденти; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для реагування на ризик ; автоматизовані механізми, інструменти, що підтримують та, або впроваджують реагування на ризик]. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RA-8 | ОЦІНКА ВПЛИВУ НА ПРИВАТНІСТЬ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| RA-8{1} | проводити оцінку впливу на приватність інформаційних систем, які становлять ризик приватності перед тим, як: | | | |
| RA-8{1}(a) | RA-8{1}(a){1} | розробити інформаційні технології, які: | |
| RA-8{1}(a){1}{1} | збирають |
| RA-8{1}(a){1}{2} | підтримують |
| RA-8{1}(a){1}{3} | поширюють критичну інформацію |
| RA-8{1}(a){2} | закупити інформаційні технології, які: | |
| RA-8{1}(a){2}{1} | збирають |
| RA-8{1}(a){2}{2} | підтримують |
| RA-8{1}(a){2}{3} | поширюють критичну інформацію |
| RA-8{1}(b) | Ініціювати створення нових архівів інформації, яка: | | |
| RA-8{1}(b)(1) | RA-8{1}(b)(1){1} | буде зібрана, за допомогою інформаційних технологій |
| RA-8{1}(b)(1){2} | буде збережена допомогою інформаційних технологій |
| RA-8{1}(b)(1){3} | буде розповсюджена за допомогою інформаційних технологій |
| RA-8{1}(b)(2) | включає персональні дані, які дозволяють встановити: | |
| RA-8{1}(b)(2){1} | фізичне з'єднання з конкретною особою |
| RA-8{1}(b)(2){2} | онлайн-з'єднання з конкретною особою |
| RA-8{2} | проводити оцінку впливу на приватність програм, які становлять ризик приватності перед тим, як: | | | |
| RA-8{2}(a) | RA-8{2}(a){1} | розробити інформаційні технології, які: | |
| RA-8{2}(a){1}{1} | збирають |
| RA-8{2}(a){1}{2} | підтримують |
| RA-8{2}(a){1}{3} | поширюють критичну інформацію |
| RA-8{2}(a){2} | закупити інформаційні технології, які: | |
| RA-8{2}(a){2}{1} | збирають |
| RA-8{2}(a){2}{2} | підтримують |
| RA-8{2}(a){2}{3} | поширюють критичну інформацію |
| RA-8{2}(b) | ініціювати створення нових архівів інформації, яка: | | |
| RA-8{2}(b)(1) | RA-8{2}(b)(1){1} | буде зібрана за допомогою інформаційних технологій |
| RA-8{2}(b)(1){2} | буде збережена допомогою інформаційних технологій |
| RA-8{2}(b)(1){3} | буде розповсюджена за допомогою інформаційних технологій |
| RA-8{2}(b)(2) | включає персональні дані, які дозволяють встановити: | |
| RA-8{2}(b)(2){1} | фізичне з'єднання з конкретною особою |
| RA-8{2}(b)(2){2} | онлайн-з'єднання з конкретною особою |
| RA-8{3} | проводити оцінку впливу на приватність інших заходів, які становлять ризик приватності перед тим, як: | | | |
| RA-8{2}(a) | RA-8{2}(a){1} | розробити інформаційні технології, які: | |
| RA-8{2}(a){1}{1} | збирають |
| RA-8{2}(a){1}{2} | підтримують |
| RA-8{2}(a){1}{3} | поширюють критичну інформацію |
| RA-8{2}(a){2} | закупити інформаційні технології, які: | |
| RA-8{2}(a){2}{1} | збирають |
| RA-8{2}(a){2}{2} | підтримують |
| RA-8{2}(a){2}{3} | поширюють критичну інформацію |
| RA-8{2}(b) | ініціювати створення нових архівів інформації, яка: | | |
| RA-8{2}(b)(1) | RA-8{2}(b)(1){1} | буде зібрана, за допомогою інформаційних технологій |
| RA-8{2}(b)(1){2} | буде збережена допомогою інформаційних технологій |
| RA-8{2}(b)(1){3} | буде розповсюджена за допомогою інформаційних технологій |
| RA-8{2}(b)(2) | включає персональні дані, які дозволяють встановити: | |
| RA-8{2}(b)(2){1} | фізичне з'єднання з конкретною особою |
| RA-8{2}(b)(2){2} | онлайн-з'єднання з конкретною особою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; процедури, що стосуються реагування на ризик; план безпеки; записи аудиту, журнали подій; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за реагування на інциденти; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для реагування на ризик ; автоматизовані механізми, інструменти, що підтримують та, або впроваджують реагування на ризик]. | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RA-9 | АНАЛІЗ КРИТИЧНОСТІ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| RA-9[1] | RA-9[1]{1} | організація визначає системи, для яких необхідно виконувати аналіз критичності | |
| RA-9[1]{2} | організація визначає компоненти системи, для яких необхідно виконувати аналіз критичності. | |
| RA-9[1]{3} | організація визначає системні служби, для яких необхідно виконувати аналіз критичності. | |
| RA-9[2] | організація визначає точки прийняття рішень в життєвому циклі розробки системи, у яких необхідно виконувати аналіз критичності | | |
| RA-9[3] | RA-9[3][1] | визначити критичні компоненти інформаційної системи, виконавши аналіз критичності для визначених організацією: | |
| RA-9[3][1]{1} | систем у визначених організацією точках прийняття рішень в життєвому циклі розробки системи |
| RA-9[3][1]{2} | компонентів системи в визначених організацією точках прийняття рішень в життєвому циклі розробки системи |
| RA-9[3][1]{3} | системних служб у визначених організацією точках прийняття рішень в життєвому циклі розробки системи |
| RA-9[3][2] | визначити критичні функції, виконавши аналіз критичності для визначених організацією: | |
| RA-9[3][2]{1} | систем у визначених організацією точках прийняття рішень в життєвому циклі розробки системи |
| RA-9[3][2]{2} | компонентів системи в визначених організацією точках прийняття рішень в життєвому циклі розробки системи |
| RA-9[3][2]{3} | системних служб у визначених організацією точках прийняття рішень в життєвому циклі розробки системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика оцінки ризику; процедури, що стосуються аналізу критичності; план безпеки; записи аудиту, журнали подій; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за аналізу критичності; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для аналізу критичності; автоматизовані механізми, інструменти, що підтримують та, або впроваджують аналіз критичності]. | | | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ SA – ПРИДБАННЯ СИСТЕМИ ТА ПОСЛУГ**

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SA-2 | РОЗПОДІЛ РЕСУРСІВ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SA-2(a) | SA-2(a){1} | визначити вимоги щодо інформаційної безпеки та приватності для систем при: | | | |
| SA-2(a){1}[1] | плануванні завдань | | |
| SA-2(a){1}[2] | плануванні процесів | | |
| SA-2(a){2} | визначити вимоги щодо інформаційної безпеки та приватності для системних послуг при: | | | |
| SA-2(a){2}[1] | плануванні завдань | | |
| SA-2(a){2}[2] | плануванні процесів | | |
| SA-2(b) | SA-2(b)[1] | SA-2(b)[1]{1} | визначити, задокументувати ресурси, які необхідні для захисту систем в рамках: | | |
| SA-2(b)[1]{1}[1] | процесу фінансового планування в організації | |
| SA-2(b)[1]{1}[2] | процесу управління інвестиціями | |
| SA-2(b)[1]{2} | визначити, задокументувати ресурси, які необхідні для захисту системних послуг в рамках: | | |
| SA-2(b)[1]{2}[1] | | процесу фінансового планування в організації |
| SA-2(b)[1]{2}[2] | | процесу управління інвестиціями |
| SA-2(b)[2] | SA-2(b)[2]{1} | розподілити ресурси, які необхідні для захисту систем в рамках: | | |
| SA-2(b)[2]{1}[1] | | процесу фінансового планування в організації |
| SA-2(b)[2]{1}[2] | | процесу управління інвестиціями |
| SA-2(b)[2]{2} | розподілити ресурси, які необхідні для захисту системних послуг в рамках: | | |
| SA-2(b)[2]{2}[1] | | процесу фінансового планування в організації |
| SA-2(b)[2]{2}[2] | | процесу управління інвестиціями |
| SA-2(c) | створити окрему позицію бюджету для фінансування заходів із забезпечення інформаційної безпеки та приватності | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються розподілу ресурсів відповідно до вимог інформаційної безпеки; процедури, що стосуються планування капіталу та контролю інвестицій; документація щодо організаційного програмування та бюджетування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за планування капіталу, контроль інвестицій, організаційне програмування та бюджетування; організаційний персонал, відповідальний за визначення вимог інформаційної безпеки до інформаційних систем, послуг; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення вимог до інформаційної безпеки; організаційні процеси для капітального планування, програмування та бюджетування; автоматизовані механізми підтримки та, або реалізації планування, програмування та бюджетування організаційного капіталу]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-3 | ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-3(a) | SA-3(a)[1] | організація визначає життєвий цикл розробки, який включає питання захисту інформації та приватності |
| SA-3(a)[2] | керувати системою, використовуючи визначений організацією життєвий цикл розробки, який включає питання захисту інформації та приватності |
| SA-3(b) | SA-3(b)[1] | визначити та задокументувати ролі по забезпеченню безпеки та приватності інформації протягом усього життєвого циклу розробки системи |
| SA-3(b)[2] | визначити та задокументувати обов'язки по забезпеченню безпеки та приватності інформації протягом усього життєвого циклу розробки системи |
| SA-3(c) | визначити осіб, які мають: | |
| SA-3(c)[1] | повноваження в області інформаційної безпеки та приватності |
| SA-3(c)[2] | обов'язки в області інформаційної безпеки та приватності |
| SA-3(d) | інтегрувати процес управління інформаційною безпекою та приватністю в процеси життєвого циклу розробки системи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції інформаційної безпеки в процес життєвого циклу розробки системи; документація життєвого циклу розробки інформаційної системи; стратегія управління ризиками інформаційної безпеки, програмна документація; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за інформаційну безпеку та життєвий цикл системи; організаційний персонал, відповідальний за управління ризиками інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення та документування життєвого циклу розробки системи (ЖЦРС); організаційні процеси для визначення ролей та відповідальності ЖЦРС; організаційний процес для інтеграції управління ризиками інформаційної безпеки в ЖЦРС; автоматизовані механізми підтримки та, або реалізації ЖЦРС]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-3(1) | ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ - УПРАВЛІННЯ СЕРЕДОВИЩЕМ РОЗРОБКИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-3(1)[1] | забезпечити захист: | | |
| SA-3(1)[1] | середовища розробки інформаційної системи, відповідно до ризиків протягом всього життєвого циклу розробки системи для: | |
| SA-3(1)[1]{1} | системи |
| SA-3(1)[1]{2} | компонентів системи |
| SA-3(1)[1]{3} | системних служб |
| SA-3(1)[2] | тестування інформаційної системи, відповідно до ризиків протягом всього життєвого циклу розробки системи для: | |
| SA-3(1)[2]{1} | системи |
| SA-3(1)[2]{2} | компонентів системи |
| SA-3(1)[2]{3} | системних служб |
| SA-3(1)[3] | інтеграції інформаційної системи, відповідно до ризиків протягом всього життєвого циклу розробки системи для:: | |
| SA-3(1)[3]{1} | системи |
| SA-3(1)[3]{2} | компонентів системи |
| SA-3(1)[3]{3} | системних служб |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР : Політика придбання системи та послуг; процедури, що стосуються інтеграції інформаційної безпеки в процес життєвого циклу розробки системи; документація життєвого циклу розробки інформаційної системи; стратегія управління ризиками інформаційної безпеки, програмна документація; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за інформаційну безпеку та життєвий цикл системи; організаційний персонал, відповідальний за управління ризиками інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення та документування ЖЦРС; організаційні процеси для визначення ролей та відповідальності ЖЦРС; організаційний процес для інтеграції управління ризиками інформаційної безпеки в ЖЦРС; автоматизовані механізми підтримки та, або реалізації ЖЦРС]. | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SA-3(2) | ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ - ВИКОРИСТАННЯ РЕАЛЬНИХ ДАНИХ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| SA-3(2)(a) | SA-3(2)(a)[1] | підтвердити, задокументувати використання реальних даних в: | | | | |
| SA-3(2)(a)[1][1] | | середовищах розробки | | |
| SA-3(2)(a)[1][2] | | середовищі тестування | | |
| SA-3(2)(a)[1][3] | | середовищі інтеграції системи | | |
| SA-3(2)(a)[1][4] | | SA-3(2)(a)[1][4]{1} | | компонентах системи |
| SA-3(2)(a)[1][4]{2} | | компонентах системних служб |
| SA-3(2)(a)[2] | контролювати використання реальних даних в: | | | | |
| SA-3(2)(a)[2][1] | | середовищах розробки | | |
| SA-3(2)(a)[2][2] | | середовищі тестування | | |
| SA-3(2)(a)[2][3] | | середовищі інтеграції системи | | |
| SA-3(2)(a)[2][4] | | SA-3(2)(a)[2][4]{1} | | компонентах системи |
| SA-3(2)(a)[2][4]{2} | | компонентах системних служб |
| SA-3(2)(b) | Переконатися, що на тому ж рівні, що й будь-які реальні дані, які використовуються, є захищеними: | | | | | |
| SA-3(2)(b)[1] | | середовища розробки | | | |
| SA-3(2)(b)[2] | | середовища тестування | | | |
| SA-3(2)(b)[3] | | середовища інтеграції системи | | | |
| SA-3(2)(b)[4] | | SA-3(2)(b)[4]{1} | | компоненти системи | |
| SA-3(2)(b)[4]{2} | | компоненти системних служб | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції інформаційної безпеки в процес життєвого циклу розробки системи; документація життєвого циклу розробки інформаційної системи; стратегія управління ризиками інформаційної безпеки, програмна документація; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за інформаційну безпеку та життєвий цикл системи; організаційний персонал, відповідальний за управління ризиками інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення та документування ЖЦРС; організаційні процеси для визначення ролей та відповідальності ЖЦРС; організаційний процес для інтеграції управління ризиками інформаційної безпеки в ЖЦРС; автоматизовані механізми підтримки та, або реалізації ЖЦРС]. | | | | | | |

|  |  |  |
| --- | --- | --- |
| SA-3(3) | ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ - ОНОВЛЕННЯ ТЕХНОЛОГІЙ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-3(3)[1] | планувати графік оновлення технологій для підтримки системи протягом всього життєвого циклу розробки системи |
| SA-3(3)[2] | впровадити графік оновлення технологій для підтримки системи протягом всього життєвого циклу розробки системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції інформаційної безпеки в процес життєвого циклу розробки системи; документація життєвого циклу розробки інформаційної системи; стратегія управління ризиками інформаційної безпеки, програмна документація; інші відповідні документи або записи].  Співбесіда: [ВИБІР : Організаційний персонал, відповідальний за інформаційну безпеку та життєвий цикл системи; організаційний персонал, відповідальний за управління ризиками інформаційної безпеки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для визначення та документування ЖЦРС; організаційні процеси для визначення ролей та відповідальності ЖЦРС; організаційний процес для інтеграції управління ризиками інформаційної безпеки в ЖЦРС; автоматизовані механізми підтримки та, або реалізації ЖЦРС]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-4 | ПРОЦЕС ЗАКУПІВЕЛЬ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-4{1} | Включити явно такі вимоги, описи та критерії: | | |
| SA-4{1}(a) | Функціональні вимоги безпеки та приватності; | |
| SA-4{1}(b) | Вимоги до стійкості механізму; | |
| SA-4{1}(c) | Вимоги до забезпечення безпеки та приватності | |
| SA-4{1}(d) | Вимоги до документації з безпеки та приватності | |
| SA-4{1}(e) | Вимоги до захисту документації з безпеки та приватності | |
| SA-4{1}(f) | Опис середовища розробки системи та середовища, в якому система призначена для роботи | |
| SA-4{1}(g) | Розподіл відповідальності або визначення сторін, відповідальних за управління інформаційною безпекою, приватністю та управлінням ланцюгами постачання | |
| SA-4{1}(h) | Критерії прийнятності | |
| SA-4{2} | включити за допомогою посилання на: | | |
| SA-4{2}{1} | контракт щодо закупівлі системи, такі вимоги, описи та критерії: | |
| SA-4{2}{1}(a) | Функціональні вимоги безпеки та приватності |
| SA-4{2}{1}(b) | Вимоги до стійкості механізму |
| SA-4{2}{1}(c) | Вимоги до забезпечення безпеки та приватності |
| SA-4{2}{1}(d) | Вимоги до документації з безпеки та приватності |
| SA-4{2}{1}(e) | Вимоги до захисту документації з безпеки та приватності |
| SA-4{2}{1}(f) | Опис середовища розробки системи та середовища, в якому система призначена для роботи |
| SA-4{2}{1}(g) | Розподіл відповідальності або визначення сторін, відповідальних за управління інформаційною безпекою, приватністю та управлінням ланцюгами постачання |
| SA-4{2}{1}(h) | Критерії прийнятності |
| SA-4{2}{2} | контракт щодо закупівлі системного компонента такі вимоги, описи та критерії: | |
| SA-4{2}{2}(a) | Функціональні вимоги безпеки та приватності |
| SA-4{2}{2}(b) | Вимоги до стійкості механізму; |
| SA-4{2}{2}(c) | Вимоги до забезпечення безпеки та приватності |
| SA-4{2}{2}(d) | Вимоги до документації з безпеки та приватності |
| SA-4{2}{2}(e) | Вимоги до захисту документації з безпеки та приватності |
| SA-4{2}{2}(f) | Опис середовища розробки системи та середовища, в якому система призначена для роботи |
| SA-4{2}{2}(g) | Розподіл відповідальності або визначення сторін, відповідальних за управління інформаційною безпекою, приватністю та управлінням ланцюгами постачання |
| SA-4{2}{2}(h) | Критерії прийнятності |
| SA-4{2}{3} | контракт щодо закупівлі системної служби, такі вимоги, описи та критерії: | |
| SA-4{2}{3}(a) | Функціональні вимоги безпеки та приватності |
| SA-4{2}{3}(b) | Вимоги до стійкості механізму |
| SA-4{2}{3}(c) | Вимоги до забезпечення безпеки та приватності |
| SA-4{2}{3}(d) | Вимоги до документації з безпеки та приватності |
| SA-4{2}{3}(e) | Вимоги до захисту документації з безпеки та приватності |
| SA-4{2}{3}(f) | Опис середовища розробки системи та середовища, в якому система призначена для роботи |
| SA-4{2}{3}(g) | Розподіл відповідальності або визначення сторін, відповідальних за управління інформаційною безпекою, приватністю та управлінням ланцюгами постачання |
| SA-4{2}{3}(h) | Критерії прийнятності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процесі придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; проєктна документація інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог до функціональних можливостей, міцності та впевненості в безпеці інформаційної системи; адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення вимог до функціональних можливостей безпеки, міцності та впевненості в інформаційній системі; організаційні процеси для розробки контрактів на придбання; автоматизовані механізми підтримки та, або реалізації придбань та включення вимог безпеки до контрактів]. | | | |

|  |  |  |
| --- | --- | --- |
| SA-4(1) | ПРОЦЕС ЗАКУПІВЕЛЬ - ФУНКЦІОНАЛЬНІ ВЛАСТИВОСТІ ЗАХОДІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-4(1){1} | вимагати від розробника системи надати опис функціональних властивостей заходів, які повинні бути реалізовані |
| SA-4(1){2} | вимагати від розробника компонента системи надати опис функціональних властивостей заходів, які повинні бути реалізовані |
| SA-4(1){3} | вимагати від розробника системної служби надати опис функціональних властивостей заходів, які повинні бути реалізовані |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процесі придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; проєктна документація інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог до функціональних можливостей, міцності та впевненості в безпеці інформаційної системи; адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення вимог до функціональних можливостей безпеки, міцності та впевненості в інформаційній системі; організаційні процеси для розробки контрактів на придбання; автоматизовані механізми підтримки та, або реалізації придбань та включення вимог безпеки до контрактів]. | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SA-4(2) | ПРОЦЕС ЗАКУПІВЕЛЬ - РОЗРОБКА ТА ВПРОВАДЖЕННЯ ІНФОРМАЦІЇ ДЛЯ ЗАХОДІВ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| SA-4(2)[1] | SA-4(2)[1][1] | організація визначає інформацію щодо розробки вибраних заходів | | | | | |
| SA-4(2)[1][2] | організація визначає інформацію щодо впровадження вибраних заходів | | | | | |
| SA-4(2)[1][3] | визначений організацією рівень деталізації вибраних заходів | | | | | |
| SA-4(2)[2] | вимагати від розробника: | | | | | | |
| SA-4(2)[2]{1} | | надати інформацію про розробку для вибраних заходів, яка містить(один або більше): | | | | |
| SA-4(2)[2]{1}{1} | пов’язані з безпекою зовнішні системні інтерфейси на визначений організацією рівень деталізації | | | |
| SA-4(2)[2]{1}{2} | архітектуру (проєкт) високого рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[2]{1}{3} | архитектуру (проєкт) низького рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[2]{1}{4} | SA-4(2)[2]{1}{4}{1} | | | вихідний код на визначений організацією рівень деталізації |
| SA-4(2)[2]{1}{4}{2} | | | апаратні схеми на визначений організацією рівень деталізації |
| SA-4(2)[2]{1}{5} | SA-4(2)[2]{1}{5}[1] | | | визначена організацією інформація щодо розробки на визначений організацією рівень деталізації |
| SA-4(2)[2]{1}{5}[2] | | | визначена організацією інформація щодо впровадження на визначений організацією рівень деталізації |
| SA-4(2)[2]{2} | | компонента системи надати інформацію про розробку для вибраних заходів, яка містить(один або більше): | | | | |
| SA-4(2)[2]{2}{1} | пов’язані з безпекою зовнішні системні інтерфейси на визначений організацією рівень деталізації | | | |
| SA-4(2)[2]{2}{2} | архітектуру (проєкт) високого рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[2]{2}{3} | архитектуру (проєкт) низького рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[2]{2}{4} | SA-4(2)[2]{2}{4}{1} | | | вихідний код на визначений організацією рівень деталізації |
| SA-4(2)[2]{2}{4}{2} | | | апаратні схеми на визначений організацією рівень деталізації |
| SA-4(2)[2]{2}{5} | SA-4(2)[2]{2}{5}[1] | | | визначена організацією інформація щодо розробки на визначений організацією рівень деталізації |
| SA-4(2)[2]{2}{5}[2] | | | визначена організацією інформація щодо впровадження на визначений організацією рівень деталізації |
| SA-4(2)[2]{3} | | системної служби надати інформацію про розробку для вибраних заходів, яка містить(один або більше): | | | | |
| SA-4(2)[2]{3}{1} | пов’язані з безпекою зовнішні системні інтерфейси на визначений організацією рівень деталізації | | | |
| SA-4(2)[2]{3}{2} | архітектуру (проєкт) високого рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[2]{3}{3} | архитектуру (проєкт) низького рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[2]{3}{4} | SA-4(2)[2]{3}{4}{1} | | | вихідний код на визначений організацією рівень деталізації |
| SA-4(2)[2]{3}{4}{2} | | | апаратні схеми на визначений організацією рівень деталізації |
| SA-4(2)[2]{3}{5} | SA-4(2)[2]{3}{5}[1] | | | визначена організацією інформація щодо розробки на визначений організацією рівень деталізації |
| SA-4(2)[2]{3}{5}[2] | | | визначена організацією інформація щодо впровадження на визначений організацією рівень деталізації |
| SA-4(2)[3] | вимагати від розробника системи: | | | | | | |
| SA-4(2)[3]{1} | | надати інформацію про реалізацію для вибраних заходів, яка містить (один або більше): | | | | |
| SA-4(2)[3]{1}{1} | пов’язані з безпекою зовнішні системні інтерфейси на визначений організацією рівень деталізації | | | |
| SA-4(2)[3]{1}{2} | архітектуру (проєкт) високого рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[3]{1}{3} | архитектуру (проєкт) низького рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[3]{1}{4} | SA-4(2)[3]{1}{4}{1} | | | вихідний код на визначений організацією рівень деталізації |
| SA-4(2)[3]{1}{4}{2} | | | апаратні схеми на визначений організацією рівень деталізації |
| SA-4(2)[3]{1}{5} | SA-4(2)[3]{1}{5}[1] | | | визначена організацією інформація щодо розробки на визначений організацією рівень деталізації |
| SA-4(2)[3]{1}{5}[2] | | | визначена організацією інформація щодо впровадження на визначений організацією рівень деталізації |
| SA-4(2)[3]{2} | | компонента системи надати інформацію про реалізацію для вибраних заходів, яка містить(один або більше): | | | | |
| SA-4(2)[3]{2}{1} | пов’язані з безпекою зовнішні системні інтерфейси на визначений організацією рівень деталізації | | | |
| SA-4(2)[3]{2}{2} | архітектуру (проєкт) високого рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[3]{2}{3} | архитектуру (проєкт) низького рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[3]{2}{4} | SA-4(2)[3]{2}{4}{1} | | вихідний код на визначений організацією рівень деталізації | |
| SA-4(2)[3]{2}{4}{2} | | апаратні схеми на визначений організацією рівень деталізації | |
| SA-4(2)[3]{2}{5} | SA-4(2)[3]{2}{5}[1] | | визначена організацією інформація щодо розробки на визначений організацією рівень деталізації | |
| SA-4(2)[3]{2}{5}[2] | | визначена організацією інформація щодо впровадження на визначений організацією рівень деталізації | |
| SA-4(2)[3]{3} | | системній службі надати інформацію про реалізацію для вибраних заходів, яка містить(один або більше): | | | | |
| SA-4(2)[3]{3}{1} | пов’язані з безпекою зовнішні системні інтерфейси на визначений організацією рівень деталізації | | | |
| SA-4(2)[3]{3}{2} | архітектуру (проєкт) високого рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[3]{3}{3} | архитектуру (проєкт) низького рівня на визначений організацією рівень деталізації | | | |
| SA-4(2)[3]{3}{4} | SA-4(2)[3]{3}{4}{1} | вихідний код на визначений організацією рівень деталізації | | |
| SA-4(2)[3]{3}{4}{2} | апаратні схеми на визначений організацією рівень деталізації | | |
| SA-4(2)[3]{3}{5} | SA-4(2)[3]{3}{5}[1] | визначена організацією інформація щодо розробки на визначений організацією рівень деталізації | | |
| SA-4(2)[3]{3}{5}[2] | визначена організацією інформація щодо впровадження на визначений організацією рівень деталізації | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерні документи; документація про придбання; договори придбання інформаційної системи, компонентів системи або послуг інформаційної системи; інформація про розробку та впровадження засобів контролю безпеки, що використовуються в інформаційній системі, компоненти системи або служби інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог безпеки інформаційної системи; розробник інформаційної системи або постачальник послуг; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення рівня деталізації для проєктування системи та контролю безпеки; організаційні процеси для розробки контрактів на придбання; автоматизовані механізми, що підтримують та, або впроваджують розробку деталей проєктування системи]. | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-4(3) | ПРОЦЕС ЗАКУПІВЕЛЬ - МЕТОДИ, ТЕХНІКИ ТА ПРАКТИКИ РОЗРОБКИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-4(3)[1] | визначені організацією методи проєктування (інженерії) систем | | |
| SA-4(3)[2] | SA-4(3)[2]{1} | вимагати від розробника системи продемонструвати використання процесу життєвого циклу розробки системи, що включає в себе визначені організацією методи проєктування (інженерії) систем (один або більше): | |
| SA-4(3)[2]{1}{1} | методи проєктування безпеки систем |
| SA-4(3)[2]{1}{2} | методи проєктування приватності |
| SA-4(3)[2]{1}{3} | методи розробки програмного забезпечення |
| SA-4(3)[2]{1}{4} | методи випробування, аналізу |
| SA-4(3)[2]{1}{5} | оцінки, верифікації та валідації |
| SA-4(3)[2]{1}{6} | процеси контролю якості |
| SA-4(3)[2]{2} | вимагати від системного компонента продемонструвати використання процесу життєвого циклу розробки системи, що включає в себе визначені організацією методи проєктування (інженерії) систем (один або більше): | |
| SA-4(3)[2]{2}{1} | методи проєктування безпеки систем |
| SA-4(3)[2]{2}{2} | методи проєктування приватності; |
| SA-4(3)[2]{2}{3} | методи розробки програмного забезпечення |
| SA-4(3)[2]{2}{4} | методи випробування, аналізу |
| SA-4(3)[2]{2}{5} | оцінки, верифікації та валідації |
| SA-4(3)[2]{2}{6} | процеси контролю якості |
| SA-4(3)[2]{3} | вимагати від системної служби продемонструвати використання процесу життєвого циклу розробки системи, що включає в себе визначені організацією методи проєктування (інженерії) систем (один або більше): | |
| SA-4(3)[2]{3}{1} | методи проєктування безпеки систем |
| SA-4(3)[2]{3}{2} | методи проєктування приватності |
| SA-4(3)[2]{3}{3} | методи розробки програмного забезпечення |
| SA-4(3)[2]{3}{4} | методи випробування, аналізу |
| SA-4(3)[2]{3}{5} | оцінки, верифікації та валідації |
| SA-4(3)[2]{3}{6} | процеси контролю якості |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерні документи; документація про придбання; договори придбання інформаційної системи, компонент системи або послуги інформаційної системи; перелік методів інженерної системи, безпеки, які повинні бути включені в процес життєвого циклу розробки системи розробника; перелік методів розробки програмного забезпечення, які повинні бути включені в процес життєвого циклу розробки системи розробника; перелік методів тестування, оцінки, перевірки, які повинні бути включені в процес життєвого циклу розробки системи розробника; перелік процесів контролю якості, які повинні бути включені в процес життєвого циклу розробки системи розробника; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог безпеки інформаційної системи; організаційний персонал, відповідальний за інформаційну безпеку та життєвий цикл системи; розробник інформаційної системи або постачальник послуг].  Перевірка: [ВИБІР: Організаційні процеси для методів, прийомів та процесів розробки]. | | | |

|  |  |
| --- | --- |
| SA-4(4) | ПРОЦЕС ЗАКУПІВЕЛЬ - ВІДНЕСЕННЯ КОМПОНЕНТІВ ДО СИСТЕМ |
|  | [Вилучено: включено до CM-8(9)] |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SA-4(5) | ПРОЦЕС ЗАКУПІВЕЛЬ - КОНФІГУРАЦІЇ СИСТЕМИ, КОМПОНЕНТА ТА СИСТЕМНОЇ СЛУЖБИ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| SA-4(5){1} | вимагати від розробника системи: | | | | | |
| SA-4(5){1}(a) | SA-4(5){1}(a)[1] | організація визначає конфігурації безпеки | | | |
| SA-4(5){1}(a)[2] | поставити: | | | |
| SA-4(5){1}(a)[2]{1} | | систему за допомогою визначених організацією конфігурацій безпеки | |
| SA-4(5){1}(a)[2]{2} | | компонент за допомогою визначених організацією конфігурацій безпеки | |
| SA-4(5){1}(a)[2]{3} | | системну службу за допомогою визначених організацією конфігурацій безпеки | |
| SA-4(5){1}(b) | використовувати ці конфігураційні налаштування за замовчуванням для: | | | | |
| SA-4(5){1}(b){1} | | будь-якої наступної переінсталяції | | |
| SA-4(5){1}(b){2} | | оновлення | | |
| SA-4(5){1}(b){2}{1} | | системи |
| SA-4(5){1}(b){2}{2} | | компоненту системи |
| SA-4(5){1}(b){2}{3} | | послуги |
| SA-4(5){2} | Вимагати від розробника компонента системи: | | | | | |
| SA-4(5){2}(a) | SA-4(5){2}(a)[1] | організація визначає конфігурації безпеки | | | |
| SA-4(5){2}(a)[2] | поставити: | | | |
| SA-4(5){2}(a)[2]{1} | | систему за допомогою визначених організацією конфігурацій безпеки | |
| SA-4(5){2}(a)[2]{2} | | компонент за допомогою визначених організацією конфігурацій безпеки | |
| SA-4(5){2}(a)[2]{3} | | системну службу за допомогою визначених організацією конфігурацій безпеки | |
| SA-4(5){2}(b) | використовувати ці конфігураційні налаштування за замовчуванням для: | | | | |
| SA-4(5){2}(b){1} | | будь-якої наступної переінсталяції | | |
| SA-4(5){2}(b){2} | | оновлення | | |
| SA-4(5){2}(b){2}{1} | | системи |
| SA-4(5){2}(b){2}{2} | | компоненти системи |
| SA-4(5){2}(b){2}{3} | | послуги |
| SA-4(5){3} | вимагати від розробника системної служби: | | | | | |
| SA-4(5){3}(a) | SA-4(5){3}(a)[1] | організація визначає конфігурації безпеки | | | |
| SA-4(5){3}(a)[2] | Поставити: | | | |
| SA-4(5){3}(a)[2]{1} | | систему за допомогою визначених організацією конфігурацій безпеки | |
| SA-4(5){3}(a)[2]{2} | | компоненти за допомогою визначених організацією конфігурацій безпеки | |
| SA-4(5){3}(a)[2]{3} | | системну службу за допомогою визначених організацією конфігурацій безпеки | |
| SA-4(5){3}(b) | використовувати ці конфігураційні налаштування за замовчуванням для: | | | | |
| SA-4(5){3}(b){1} | | будь-якої наступної переінсталяції | | |
| SA-4(5){3}(b){2} | | оновлення | | |
| SA-4(5){3}(b){2}{1} | | системи |
| SA-4(5){3}(b){2}{2} | | компоненти системи |
| SA-4(5){3}(b){2}{3} | | послуги |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерні документи; документація про придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; конфігурації безпеки, які повинні бути реалізовані розробником інформаційної системи, системного компонента або служби інформаційної системи; угоди про рівень обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог безпеки інформаційної системи; розробник інформаційної системи або постачальник послуг; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що використовуються для перевірки того, що конфігурація інформаційної системи, компонента чи послуги, як надається, відповідає зазначеному]. | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-4(6) | ПРОЦЕС ЗАКУПІВЕЛЬ - ВИКОРИСТАННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-4(6)(a) | SA-4(6)(a){1} | використовувати засоби захисту інформації, які пройшли державну експертизу, і які створені для: | |
| SA-4(6)(a){1}[1] | технічного захисту інформації |
| SA-4(6)(a){1}[2] | криптографічного захисту інформації |
| SA-4(6)(a){2} | використовувати засоби захисту інформації, які пройшли державну сертифікацію, і які створені для: | |
| SA-4(6)(a){2}[1] | технічного захисту інформації |
| SA-4(6)(a){2}[2] | криптографічного захисту інформації |
| SA-4(6)(b) | SA-4(6)(b)[1] | SA-4(6)(b)[1] | переконатися, що ці засоби захисту мають позитивний експертний висновок |
| SA-4(6)(b)[1] | переконатися, що ці засоби захисту мають сертифікат відповідності |
| SA-4(6)(b)[2] | відповідні дозволи для використання для захисту критичної інформації | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерні документи; документація про придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; конфігурації безпеки, які повинні бути реалізовані розробником інформаційної системи, системного компонента або служби інформаційної системи; угоди про рівень обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог безпеки інформаційної системи; організаційний персонал, відповідальний за забезпечення продуктів забезпечення інформації, затверджений АНБ та оцінює та, або перевіряє продукцією відповідно до процедур, затверджених АНБ; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для вибору та використання оцінених та, або підтверджених продуктів та послуг із забезпечення інформації, що складають рішення, затверджене АНБ, для захисту секретної інформації]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-4(7) | ПРОЦЕС ЗАКУПІВЕЛЬ - ЗАТВЕРДЖЕНІ ПРОФІЛІ ЗАХИЩЕНОСТІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-4(7)(a) | обмежити використання комерційної готової до використання технічної продукції, створеної для захисту інформації та з функцією підтримки забезпечення безпеки інформації, до тих продуктів, які були успішно оцінені відповідно профілю захищеності для конкретного типу технології, затвердженої уповноваженим державним органом, якщо такий профіль існує | |
| SA-4(7)(b) | у випадку, якщо немає профілю захищеності для певного типу технологій, затвердженого уповноваженим органом, але забезпечення політики безпеки продукту, що надається на комерційній основі, залежить від криптографічних функцій, вимагати, щоб криптографічний модуль: | |
| SA-4(7)(b)[1] | пройшов державну експертизу |
| SA-4(7)(b)[2] | мав позитивний експертний висновок та |
| SA-4(7)(b)[3] | був рекомендований до використання уповноваженим органом. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерні документи; документація про придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; Профілі захисту, затверджені профілі захищеності; Інформація про перевірку FIPS для криптографічної функціональності; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог безпеки інформаційної системи; організаційний персонал, відповідальний за забезпечення продуктів забезпечення інформації, був оцінений за затвердженим NIAP профілем захисту або за те, щоб продукти, що спираються на криптографічну функціональність, були перевірені FIPS; організаційний персонал, відповідальний за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси вибору та використання продуктів, послуг, що оцінюються на основі затвердженого NIAP профілю захисту або продуктів, підтверджених FIPS]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-4(8) |  | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-4(8)[1] | організація визначає рівень деталізації плану безперервного моніторингу ефективності заходів безпеки та приватності | |
| SA-4(8)[2] | SA-4(8)[2]{1} | вимагати від розробника системи створити план безперервного моніторингу ефективності заходів безпеки та приватності з визначеним організацією рівнем деталізації |
| SA-4(8)[2]{2} | вимагати від розробника системного компонента створити план безперервного моніторингу ефективності заходів безпеки та приватності з визначеним організацією рівнем деталізації |
| SA-4(8)[2]{3} | вимагати від розробника системної служби створити план безперервного моніторингу ефективності заходів безпеки та приватності, з визначеним організацією рівнем деталізації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються планів постійного моніторингу розробників; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; плани постійного моніторингу розробника; плани оцінки безпеки; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; документація про придбання; тендерна документація; угоди про рівень обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог безпеки інформаційної системи; розробники інформаційних систем; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Процеси постачальника для постійного моніторингу; автоматизовані механізми, що підтримують та, або впроваджують постійний моніторинг розробника]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-9 | ПРОЦЕС ЗАКУПІВЕЛЬ - ФУНКЦІЇ, ПОРТИ, ПРОТОКОЛИ ТА ПОСЛУГИ, ЩО ВИКОРИСТОВУЮТЬСЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-9{1} | вимагати від розробника системи визначити: | |
| SA-9{1}[1] | функції, призначені для використання організацією |
| SA-9{1}[2] | порти, протоколи, призначені для використання організацією |
| SA-9{1}[3] | послуги, призначені для використання організацією. |
| SA-9{2} | вимагати від розробника компонента системи визначити: | |
| SA-9{2}[1] | функції, призначені для використання організацією |
| SA-9{2}[2] | порти, протоколи, призначені для використання організацією |
| SA-9{2}[3] | послуги, призначені для використання організацією. |
| SA-9{3} | вимагати від розробника системної служби визначити: | |
| SA-9{3}[1] | функції, призначені для використання організацією |
| SA-9{3}[2] | порти, протоколи, призначені для використання організацією |
| SA-9{3}[3] | послуги, призначені для використання організацією. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; проєктна документація інформаційної системи; документація інформаційної системи, включаючи функції, порти, протоколи та послуги, призначені для організаційного використання; договори придбання інформаційних систем або послуг; документація про придбання; тендерна документація; угоди про рівень обслуговування; організаційні вимоги до безпеки, описи та критерії для розробників інформаційних систем, компонентів системи та служб інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог безпеки інформаційної системи; адміністратори системи, мережі; організаційний персонал, який працює, використовує та, або підтримує інформаційну систему; розробники інформаційних систем; організаційний персонал, відповідальний за інформаційну безпеку]. | | |

|  |  |  |
| --- | --- | --- |
| SA-4(10) | ПРОЦЕС ЗАКУПІВЕЛЬ - ВИКОРИСТАННЯ ЗАТВЕРДЖЕНИХ ПРОДУКТІВ ПІДТВЕРДЖЕННЯ ОСОБИСТОСТІ (PIV) | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-4(10)[1] | Використовувати лише ту інформаційно-технічну продукцію, що знаходиться у списку продуктів, затверджених уповноваженим органом, для можливостей підтвердження особистості (PIV), реалізованих в організаційних системах |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерна документація; документація про придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; угоди про рівень обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог безпеки інформаційної системи; організаційний персонал, відповідальний за забезпечення впровадження лише продуктів, затверджених уповноваженим органом; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси вибору та використання продуктів, схвалених уповноваженим органом]. | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SA-5 | СИСТЕМНА ДОКУМЕНТАЦІЯ | | | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | | | | | | |
| SA-5(a) | SA-5(a){1} | отримати документацію адміністратора для системи, яка описує: | | | | | | | | | | | | | |
| SA-5(a){1}(1) | | SA-5(a){1}(1)[1] | | | | безпечне налаштування: | | | | | | | |
| SA-5(a){1}(1)[1]{1} | | | | | | системи | |
| SA-5(a){1}(1)[1]{2} | | | | | | компонента | |
| SA-5(a){1}(1)[1]{3} | | | | | | служби | |
| SA-5(a){1}(1)[2] | | | | безпечну установку: | | | | | | | |
| SA-5(a){1}(1)[2]{1} | | | | | | системи | |
| SA-5(a){1}(1)[2]{2} | | | | | | компонента | |
| SA-5(a){1}(1)[2]{3} | | | | | | служби | |
| SA-5(a){1}(1)[3] | | | | безпечну роботу: | | | | | | | |
| SA-5(a){1}(1)[3]{1} | | | | | | системи | |
| SA-5(a){1}(1)[3]{2} | | | | | | компонента | |
| SA-5(a){1}(1)[3]{3} | | | | | | служби | |
| SA-5(a){1}(2) | | SA-5(a){1}(2)[1] | | | | ефективне використання безпеки та приватності | | | | | | | |
| SA-5(a){1}(2)[2] | | | | ефективну підтримку функцій безпеки та приватності | | | | | | | |
| SA-5(a){1}(2)[3] | | | | ефективні механізми безпеки та приватності | | | | | | | |
| SA-5(a){1}(3) | | SA-5(a){1}(3)[1] | | | | відомі вразливості щодо конфігурації | | | | | | | |
| SA-5(a){1}(3)[1]{1} | | | | | | адміністративних функцій | |
| SA-5(a){1}(3)[1]{2} | | | | | | привілейованих функцій | |
| SA-5(a){1}(3)[2] | | | | відомі вразливості щодо використання: | | | | | | | |
| SA-5(a){1}(3)[2]{1} | | | | | | адміністративних функцій | |
| SA-5(a){1}(3)[2]{2} | | | | | | привілейованих функцій | |
| SA-5(a){2} | отримати документацію адміністратора для системного компонента, яка описує: | | | | | | | | | | | | | |
| SA-5(a){2}(1) | | SA-5(a){2}(1)[1] | | | безпечне налаштування: | | | | | | | | |
| SA-5(a){2}(1)[1]{1} | | | | | | системи | | |
| SA-5(a){2}(1)[1]{2} | | | | | | компонента | | |
| SA-5(a){2}(1)[1]{3} | | | | | | служби | | |
| SA-5(a){2}(1)[2] | | | безпечну установку: | | | | | | | | |
| SA-5(a){2}(1)[2]{1} | | | | | | системи | | |
| SA-5(a){2}(1)[2]{2} | | | | | | компонента | | |
| SA-5(a){2}(1)[2]{3} | | | | | | служби | | |
| SA-5(a){2}(1)[3] | | | безпечну роботу: | | | | | | | | |
| SA-5(a){2}(1)[3]{1} | | | | | | системи | | |
| SA-5(a){2}(1)[3]{2} | | | | | | компонента | | |
| SA-5(a){2}(1)[3]{3} | | | | | | служби | | |
| SA-5(a){2}(2) | | SA-5(a){2}(2)[1] | | | ефективне використання безпеки та приватності | | | | | | | | |
| SA-5(a){2}(2)[2] | | | ефективну підтримку функцій безпеки та приватності | | | | | | | | |
| SA-5(a){2}(2)[3] | | | ефективні механізми безпеки та приватності | | | | | | | | |
| SA-5(a){2}(3) | | SA-5(a){2}(3)[1] | | | відомі вразливості щодо конфігурації | | | | | | | | |
| SA-5(a){2}(3)[1]{1} | | | | | | адміністративних функцій | | |
| SA-5(a){2}(3)[1]{2} | | | | | | привілейованих функцій | | |
| SA-5(a){2}(3)[2] | | | відомі вразливості щодо використання: | | | | | | | | |
| SA-5(a){2}(3)[2]{1} | | | | | | адміністративних функцій | | |
| SA-5(a){2}(3)[2]{2} | | | | | | привілейованих функцій | | |
| SA-5(a){3} | отримати документацію адміністратора для системної служби, яка описує: | | | | | | | | | | | | | |
| SA-5(a){3}(1) | | SA-5(a){3}(1)[1] | | | безпечне налаштування: | | | | | | | | |
| SA-5(a){3}(1)[1]{1} | | | | | | системи | | |
| SA-5(a){3}(1)[1]{2} | | | | | | компонента | | |
| SA-5(a){3}(1)[1]{3} | | | | | | служби | | |
| SA-5(a){3}(1)[2] | | | безпечну установку: | | | | | | | | |
| SA-5(a){3}(1)[2]{1} | | | | | | системи | | |
| SA-5(a){3}(1)[2]{2} | | | | | | компонента | | |
| SA-5(a){3}(1)[2]{3} | | | | | | служби | | |
| SA-5(a){3}(1)[3] | | | безпечну роботу: | | | | | | | | |
| SA-5(a){3}(1)[3]{1} | | | | | | системи | | |
| SA-5(a){3}(1)[3]{2} | | | | | | компонента | | |
| SA-5(a){3}(1)[3]{3} | | | | | | служби | | |
| SA-5(a){3}(2) | | SA-5(a){3}(2)[1] | | | ефективне використання безпеки та приватності | | | | | | | | |
| SA-5(a){3}(2)[2] | | | ефективну підтримку функцій безпеки та приватності | | | | | | | | |
| SA-5(a){3}(2)[3] | | | ефективні механізми безпеки та приватності | | | | | | | | |
| SA-5(a){3}(3) | | SA-5(a){3}(3)[1] | | | відомі вразливості щодо конфігурації | | | | | | | | |
| SA-5(a){3}(3)[1]{1} | | | | | | адміністративних функцій | | |
| SA-5(a){3}(3)[1]{2} | | | | | | привілейованих функцій | | |
| SA-5(a){3}(3)[2] | | | відомі вразливості щодо використання: | | | | | | | | |
| SA-5(a){3}(3)[2]{1} | | | | | | адміністративних функцій | | |
| SA-5(a){3}(3)[2]{2} | | | | | | привілейованих функцій | | |
| SA-5(b) | SA-5(b){1} | отримати документацію користувача для системи, яка описує: | | | | | | | | | | | | | |
| SA-5(b){1}(1) | | SA-5(b){1}(1)[1] | | | | | функції безпеки та приватності | | | | | | |
| SA-5(b){1}(1)[2] | | | | | механізми безпеки та приватності | | | | | | |
| SA-5(b){1}(1)[3] | | | | | способи ефективного використання цих: | | | | | | |
| SA-5(b){1}(1)[3][1] | | | | | | функцій |
| SA-5(b){1}(1)[3][2] | | | | | | механізмів |
| SA-5(b){1}(2) | | методи взаємодії з користувачем, що дозволяють окремим особам використовувати: | | | | | | | | | | | |
| SA-5(b){1}(2)[1] | | | | SA-5(b){1}(2)[1]{1} | | | | | | систему більш безпечним чином | |
| SA-5(b){1}(2)[1]{2} | | | | | | компонент системи більш безпечним чином | |
| SA-5(b){1}(2)[1]{3} | | | | | | службу більш безпечним чином | |
| SA-5(b){1}(2)[2] | | | | захищати індивідуальну приватність | | | | | | | |
| SA-5(b){1}(3) | | обов'язки користувача щодо: | | | | | | | | | | | |
| SA-5(b){1}(3)[1] | | | | SA-5(b){1}(3)[1]{1} | | | | | | забезпечення безпеки системи | |
| SA-5(b){1}(3)[1]{2} | | | | | | забезпечення безпеки компонента системи | |
| SA-5(b){1}(3)[1]{3} | | | | | | забезпечення безпеки служби | |
| SA-5(b){1}(3)[2] | | | | забезпечення безпеки приватності окремих осіб | | | | | | | |
| SA-5(b){2} | отримати документацію користувача для системного компонента, яка описує: | | | | | | | | | | | | | |
| SA-5(b){2}(1) | | SA-5(b){2}(1)[1] | | | | функції безпеки та приватності | | | | | | | |
| SA-5(b){2}(1)[2] | | | | механізми безпеки та приватності | | | | | | | |
| SA-5(b){2}(1)[3] | | | | способи ефективного використання цих: | | | | | | | |
| SA-5(b){2}(1)[3][1] | | | | | | | функцій |
| SA-5(b){2}(1)[3][2] | | | | | | | механізмів |
| SA-5(b){2}(2) | | методи взаємодії з користувачем, що дозволяють окремим особам використовувати: | | | | | | | | | | | |
| SA-5(b){2}(2)[1] | | | | SA-5(b){2}(2)[1]{1} | | | | систему більш безпечним чином | | | |
| SA-5(b){2}(2)[1]{2} | | | | компонент системи більш безпечним чином | | | |
| SA-5(b){2}(2)[1]{3} | | | | службу більш безпечним чином | | | |
| SA-5(b){2}(2)[2] | | | | захищати індивідуальну приватність | | | | | | | |
| SA-5(b){2}(3) | | обов'язки користувача щодо: | | | | | | | | | | | |
| SA-5(b){2}(3)[1] | | | | SA-5(b){2}(3)[1]{1} | | | забезпечення безпеки системи | | | | |
| SA-5(b){2}(3)[1]{2} | | | забезпечення безпеки компонента системи | | | | |
| SA-5(b){2}(3)[2]{3} | | | забезпечення безпеки служби | | | | |
| SA-5(b){2}(3)[2] | | | | забезпечення безпеки приватності окремих осіб | | | | | | | |
| SA-5(b){3} | Отримати документацію користувача для системної служби, яка описує: | | | | | | | | | | | | | |
| SA-5(b){3}(1) | | SA-5(b){3}(1)[1] | | | | функції безпеки та приватності | | | | | | | |
| SA-5(b){3}(1)[2] | | | | механізми безпеки та приватності | | | | | | | |
| SA-5(b){3}(1)[3] | | | | способи ефективного використання цих: | | | | | | | |
| SA-5(b){3}(1)[3][1] | | | | | | | функцій |
| SA-5(b){3}(1)[3][2] | | | | | | | механізмів |
| SA-5(b){3}(2) | | методи взаємодії з користувачем, що дозволяють окремим особам використовувати: | | | | | | | | | | | |
| SA-5(b){3}(2)[1] | | | | SA-5(b){3}(2)[1]{1} | | | | систему більш безпечним чином | | | |
| SA-5(b){3}(2)[1]{2} | | | | компонент системи більш безпечним чином | | | |
| SA-5(b){3}(2)[1]{3} | | | | службу більш безпечним чином | | | |
| SA-5(b){3}(2)[2] | | | | захищати індивідуальну приватність | | | | | | | |
| SA-5(b){3}(3) | | обов'язки користувача щодо: | | | | | | | | | | | |
| SA-5(b){3}(3)[1] | | | | SA-5(b){3}(3)[1]{1} | | | забезпечення безпеки системи | | | | |
| SA-5(b){3}(3)[1]{2} | | | забезпечення безпеки компонента системи | | | | |
| SA-5(b){3}(3)[2]{3} | | | забезпечення безпеки служби | | | | |
| SA-5(b){3}(3)[2] | | | | забезпечення безпеки приватності окремих осіб | | | | | | | |
| SA-5(c) | SA-5(c)[1] | організація визначає заходи, які необхідно вжити у відповідь на спроби отримати доступ до документації: | | | | | | | | | | | | | |
| SA-5(c)[1]{1} | | | системи | | | | | | | | | | |
| SA-5(c)[1]{2} | | | системного компонента | | | | | | | | | | |
| SA-5(c)[1]{3} | | | системної служби | | | | | | | | | | |
| SA-5(c)[2] | документувати спроби отримати доступ до документації: | | | | | | | | | | | | | |
| SA-5(c)[1]{1} | | | системи, коли така документація: | | | | | | | | | | |
| SA-5(c)[1]{1}{1} | | | | | недоступна | | | | | |
| SA-5(c)[1]{1}{2} | | | | | відсутня | | | | | |
| SA-5(c)[1]{2} | | | системного компонента, коли така документація: | | | | | | | | | | |
| SA-5(c)[1]{2}{1} | | | | | недоступна | | | | | |
| SA-5(c)[1]{2}{2} | | | | | відсутня | | | | | |
| SA-5(c)[1]{3} | | | системної служби, коли така документація: | | | | | | | | | | |
| SA-5(c)[1]{3}{1} | | | | | недоступна | | | | | |
| SA-5(c)[1]{3}{2} | | | | | відсутня | | | | | |
| SA-5(c)[3] | вжити визначені організацією заходи у відповідь на спроби отримати доступ до документації | | | | | | | | | | | | | |
| SA-5(c)[3]{1} | | | системи | | | | | | | | | | |
| SA-5(c)[3]{2} | | | системного компонента | | | | | | | | | | |
| SA-5(c)[3]{3} | | | системної служби | | | | | | | | | | |
| SA-5(d) | забезпечити захист документації (за потреби) відповідно до організаційної стратегії управління ризиками | | | | | | | | | | | | | | |
| SA-5(e) | SA-5(e)[1] | | SA-5(e)[1]{1} | | | організація визначає персонал, серед якого необхідно поширити документацію | | | | | | | | | |
| SA-5(e)[1]{2} | | | організація визначає посадових осіб, серед яких необхідно поширити документацію | | | | | | | | | |
| SA-5(e)[2] | | поширити документацію серед визначеного організацією: | | | | | | | | | | | | |
| SA-5(e)[2]{1} | | | персоналу | | | | | | | | | |
| SA-5(e)[2]{2} | | | посадових осіб | | | | | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються документації інформаційної системи; документація інформаційної системи, включаючи керівництва адміністратора та користувача; реєструє документування спроб отримати недоступну або відсутню документацію інформаційної системи; перелік дій, які слід вжити у відповідь на задокументовані спроби отримати інформаційну систему, компонент системи або службову документацію інформаційної системи; документація щодо стратегії управління ризиками; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог безпеки інформаційної системи; системні адміністратори; організаційний персонал, який працює, використовує та, або підтримує інформаційну систему; розробники інформаційних систем; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для отримання, захисту та розповсюдження документації адміністратора та користувачів інформаційної системи]. | | | | | | | | | | | | | | | |

|  |  |
| --- | --- |
| SA-5(1) | СИСТЕМНА ДОКУМЕНТАЦІЯ - ФУНКЦІОНАЛЬНІ ВЛАСТИВОСТІ ЗАХОДІВ БЕЗПЕКИ |
|  | [Вилучено: включено до SA-4(1)]. |

|  |  |
| --- | --- |
| SA-5(2) | СИСТЕМНА ДОКУМЕНТАЦІЯ - ЗОВНІШНІ СИСТЕМНІ ІНТЕРФЕЙСИ, ЩО СТОСУЮТЬСЯ БЕЗПЕКИ |
|  | [Вилучено: включено до SA-4(2)]. |

|  |  |
| --- | --- |
| SA-5(3) | СИСТЕМНА ДОКУМЕНТАЦІЯ - АРХІТЕКТУРА (ПРОЄКТ) ВИСОКОГО РІВНЯ |
|  | [Вилучено: включено до SA-4(2)]. |

|  |  |
| --- | --- |
| SA-5(4) | СИСТЕМНА ДОКУМЕНТАЦІЯ - АРХІТЕКТУРА (ПРОЄКТ) НИЗЬКОГО РІВНЯ |
|  | [Вилучено: включено до SA-4(2)] |

|  |  |
| --- | --- |
| SA-5(5) | СИСТЕМНА ДОКУМЕНТАЦІЯ - ВИХІДНИЙ КОД |
|  | [Вилучено: включено до SA-4(2)]. |

|  |  |
| --- | --- |
| SA-6 | ОБМЕЖЕННЯ ЩОДО ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ |
|  | [Вилучено: Включено до CM-10 та SI-7]. |

|  |  |
| --- | --- |
| SA-7 | ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ |
|  | [Вилучено: Включено до CM-11 та SI-7]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-8 | БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ (ПРОЄКТУВАННЯ) | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-8[1] | організація визначає принципи інжинірингу безпеки системи | |
| SA-8[2] | застосовувати визначені організацією принципи інжинірингу безпеки системи в: | |
| SA-8[2][1] | специфікації системи |
| SA-8[2][2] | проєктуванні системи |
| SA-8[2][3] | розробці системи |
| SA-8[2][4] | впровадженні системи |
| SA-8[2][5] | зміні системи |
| SA-8[2][6] | зміні системних компонентів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються принципів інженерної безпеки, що використовуються у специфікації, проєктуванні, розробці, впровадженні та модифікації інформаційної системи; проєктна документація інформаційної системи; вимоги щодо інформаційної безпеки та технічні характеристики інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання, підряд; організаційний персонал, відповідальний за визначення вимог безпеки інформаційної системи; організаційний персонал, який відповідає за специфікацію, розробку, впровадження та модифікацію інформаційної системи; розробники інформаційних систем; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для застосування принципів інженерної безпеки в специфікації, проєктуванні, розробці, впровадженні та модифікації інформаційної системи; автоматизовані механізми, що підтримують застосування принципів інженерної безпеки при специфікації, проєктуванні, розробці, впровадженні та модифікації інформаційних систем]. | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SA-9 | ЗОВНІШНІ СИСТЕМНІ СЛУЖБИ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SA-9(a) | SA-9(a)[1] | організація встановлює заходи безпеки та приватності, які повинні застосовувати постачальники зовнішніх системних послуг | | |
| SA-9(a)[2] | вимагати, щоб постачальники зовнішніх системних послуг: | | |
| SA-9(a)[2][1] | | відповідали вимогам безпеки та приватності в організації |
| SA-9(a)[2][2] | | застосовували встановлені організацією заходи безпеки та приватності |
| SA-9(b) | визначити та задокументувати організаційні: | | | |
| SA-9(b)[1] | нагляд користувачів щодо зовнішніх системних служб | | |
| SA-9(b)[2] | повноваження користувачів щодо зовнішніх системних служб | | |
| SA-9(b)[3] | обов'язки користувачів щодо зовнішніх системних служб | | |
| SA-9(c) | SA-9(c)[1] | організація визначає для постійного контролю за дотриманням вимог безпеки та приватності з боку зовнішніх постачальників послуг: | | |
| SA-9(c)[1][1] | процеси | |
| SA-9(c)[1][2] | методи | |
| SA-9(c)[1][3] | техніки | |
| SA-9(c)[2] | використовувати для постійного контролю за дотриманням вимог безпеки та приватності з боку зовнішніх постачальників послуг визначені організацією: | | |
| SA-9(c)[2][1] | процеси | |
| SA-9(c)[2][2] | методи | |
| SA-9(c)[2][3] | техніки | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої інформаційної системи; процедури, що стосуються методів та прийомів моніторингу дотримання контролю безпеки зовнішніми провайдерами послуг інформаційних систем; договори придбання, угоди про рівень послуг; організаційні вимоги до безпеки та технічні вимоги до послуг зовнішніх постачальників; докази оцінки контролю безпеки від зовнішніх постачальників послуг інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; зовнішні провайдери послуг інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для постійного моніторингу дотримання контролю безпеки зовнішніми постачальниками послуг; автоматизовані механізми для постійного моніторингу дотримання контролю безпеки зовнішніми постачальниками послуг]. | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SA-9(1) | ЗОВНІШНІ СИСТЕМНІ СЛУЖБИ - ОЦІНКА РИЗИКІВ ТА ОРГАНІЗАЦІЙНІ ПОГОДЖЕННЯ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SA-9(1)(a) | проводити організаційну оцінку ризиків перед | | | | |
| SA-9(1)(a){1} | створенням служб інформаційної безпеки | | | |
| SA-9(1)(a){2} | аутсорсингом служб інформаційної безпеки | | | |
| SA-9(1)(b) | SA-9(1)(b)[1] | SA-9(1)(b)[1]{1} | організація визначає персонал, з яким необхідно погоджувати: | | |
| SA-9(1)(b)[1]{1}{1} | створення спеціалізованих служб інформаційної безпеки | |
| SA-9(1)(b)[1]{1}{2} | аутсорсинг спеціалізованих служб інформаційної безпеки | |
| SA-9(1)(b)[1]{2} | організація визначає посадових осіб, з якими необхідно погоджувати: | | |
| SA-9(1)(b)[1]{1}{1} | створення спеціалізованих служб інформаційної безпеки | |
| SA-9(1)(b)[1]{1}{2} | аутсорсинг спеціалізованих служб інформаційної безпеки | |
| SA-9(1)(b)[2] | переконатися, що | | | |
| SA-9(1)(b)[2]{1} | створення спеціалізованих служб інформаційної безпеки погоджено визначеним організацією: | | |
| SA-9(1)(b)[2]{1}{1} | | персоналом |
| SA-9(1)(b)[2]{1}{2} | | посадовими особами |
| SA-9(1)(b)[2]{2} | аутсорсинг спеціалізованих служб інформаційної безпеки погоджені визначеним організацією: | | |
| SA-9(1)(b)[2]{2}{1} | | персоналом |
| SA-9(1)(b)[2]{2}{2} | | посадовими особами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої інформаційної системи; документація про придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; звіти про оцінку ризиків; записи про затвердження для придбання або передачі на замовлення спеціальних служб захисту інформації; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за безпеку інформаційної системи; зовнішні провайдери послуг інформаційної системи; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для проведення оцінки ризиків до придбання або передачі в спеціальну службу захисту інформації; організаційні процеси для затвердження аутсорсингу спеціальних служб захисту інформації; автоматизовані механізми підтримки та, або впровадження оцінки ризику; автоматизовані механізми, що підтримують та, або впроваджують процеси затвердження]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-9(2) | ЗОВНІШНІ СИСТЕМНІ СЛУЖБИ - ВИЗНАЧЕННЯ ФУНКЦІЙ, ПОРТІВ, ПРОТОКОЛІВ ТА СЛУЖБ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-9(2)[1] | організація визначає зовнішні системні служби | |
| SA-9(2)[2] | вимагати від постачальників, визначених організацією зовнішніх системних служб визначити: | |
| SA-9(2)[2][1] | функції |
| SA-9(2)[2][2] | порти |
| SA-9(2)[2][3] | протоколи |
| SA-9(2)[2][4] | інші служби, необхідні для використання таких служб |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої інформаційної системи; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; документація про придбання; заявна документація, угоди про рівень обслуговування; організаційні вимоги до безпеки та специфікації безпеки для зовнішніх постачальників послуг; перелік необхідних функцій, портів, протоколів та інших послуг; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, відповідальний за інформаційну безпеку; адміністратори системи, мережі; зовнішні провайдери послуг інформаційної системи]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-9(3) | ЗОВНІШНІ СИСТЕМНІ СЛУЖБИ - СТВОРЕННЯ ТА ПІДТРИМКА ДОВІРЧИХ ВІДНОСИН З ПОСТАЧАЛЬНИКАМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-9(3)[1] | SA-9(3)[1]{1} | організація визначає вимоги щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[1]{2} | організація визначає властивості щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[1]{3} | організація визначає фактори щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[1]{4} | організація визначає умови щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[2] | створити, задокументувати довірчі відносини з зовнішніми постачальниками послуг на основі визначених організацією: | |
| SA-9(3)[2]{1} | вимог щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[2]{2} | властивостей щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[2]{3} | факторів щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[2]{4} | умов щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[3] | підтримувати довірчі відносини з зовнішніми постачальниками послуг на основі визначених організацією: | |
| SA-9(3)[3]{1} | вимог щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[3]{2} | властивостей щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[3]{3} | факторів щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| SA-9(3)[3]{4} | умов щодо безпеки та приватності, що визначають прийнятні довірчі відносини |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої інформаційної системи; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; документація про придбання; тендерна документація; угоди про рівень обслуговування; вимоги до безпеки організації, властивості, фактори або умови, що визначають прийнятні довірчі відносини; документація довірчих відносин із зовнішніми постачальниками послуг; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, відповідальний за інформаційну безпеку; зовнішні провайдери послуг інформаційної системи]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-9(4) | ЗОВНІШНІ СИСТЕМНІ СЛУЖБИ - УЗГОДЖЕННЯ ІНТЕРЕСІВ СПОЖИВАЧІВ І ПОСТАЧАЛЬНИКІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-9(4)[1] | SA-9(4)[1][1] | організація визначає зовнішніх постачальників послуг |
| SA-9(4)[1][2] | організація визначає заходи, щоб переконатися, що інтереси визначених організацією зовнішніх постачальників послуг відповідають інтересам організації та відображають їх |
| SA-9(4)[2] | вживати визначені організацією заходи, щоб переконатися, що інтереси визначених організацією зовнішніх постачальників послу: | |
| SA-9(4)[2][1] | відповідають інтересам організації |
| SA-9(4)[2][2] | відповідають інтересам організації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої інформаційної системи; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; заявна документація; документація про придбання; угоди про рівень обслуговування; організаційні вимоги, гарантії безпеки для зовнішніх постачальників послуг; політика кадрової безпеки для зовнішніх постачальників послуг; оцінки, проведені зовнішніми постачальниками послуг; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; зовнішні провайдери послуг інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для визначення та використання гарантій для забезпечення узгоджених інтересів із зовнішніми постачальниками послуг; автоматизовані механізми, що підтримують та, або впроваджують гарантії для забезпечення узгоджених інтересів із зовнішніми постачальниками послуг]. | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SA-9(5) | ЗОВНІШНІ СИСТЕМНІ СЛУЖБИ - МІСЦЕ ОБРОБКИ, ЗБЕРІГАННЯ ТА ОБСЛУГОВУВАННЯ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| SA-9(5)[1] | SA-9(5)[1][1] | SA-9(5)[1][1]{1} | | організація визначає вимоги | | |
| SA-9(5)[1][1]{2} | | організація визначає умови | | |
| SA-9(5)[1][2] | організація визначає місця | | | | |
| SA-9(5)[2] | обмежити розташування (один або більше): | | | | | |
| SA-9(5)[2][1] | | обробка інформації до визначених організацією місць на основі визначених організацією: | | | |
| SA-9(5)[2][1]{1} | | вимог | |
| SA-9(5)[2][1]{2} | | умов | |
| SA-9(5)[2][2] | | SA-9(5)[2][2]{1} | | інформація до визначених організацією місць на основі визначених організацією: | |
| SA-9(5)[2][2]{1}{1} | вимог |
| SA-9(5)[2][2]{1}{2} | умов |
| SA-9(5)[2][2]{2} | | дані до визначених організацією місць на основі визначених організацією: | |
| SA-9(5)[2][2]{1}{1} | вимог |
| SA-9(5)[2][2]{1}{2} | умов |
| SA-9(5)[2][3] | | системні служби, визначені організацією місця на основі визначених організацією: | | | |
| SA-9(5)[2][3]{1} | | вимог | |
| SA-9(5)[2][3]{2} | | умов | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої інформаційної системи; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; заявна документація; документація про придбання; угоди про рівень обслуговування; обмежені місця для обробки інформації; інформація, дані та, або послуги інформаційної системи; обробка інформації, інформація, дані та, або послуги інформаційної системи, які будуть підтримуватися в обмежених місцях; вимоги або умови організаційної безпеки для зовнішніх постачальників; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; зовнішні провайдери послуг інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для визначення вимог щодо обмеження місць обробки інформації, інформації, даних або інформаційних служб; організаційні процеси для забезпечення розташування обмежені відповідно до вимог чи умов]. | | | | | | |

|  |  |  |
| --- | --- | --- |
| SA-9(6) | ЗОВНІШНІ СИСТЕМНІ СЛУЖБИ - КРИПТОГРАФІЧНІ КЛЮЧІ, КЕРОВАНІ ОРГАНІЗАЦІЄЮ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-9(6)[1] | підтримувати обмежене управління криптографічними ключами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої інформаційної системи; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; заявна документація; документація про придбання; угоди про рівень обслуговування; обмежені місця для обробки інформації; інформація, дані та, або послуги інформаційної системи; обробка інформації, інформація, дані та, або послуги інформаційної системи, які будуть підтримуватися в обмежених місцях; вимоги або умови організаційної безпеки для зовнішніх постачальників; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; зовнішні провайдери послуг інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для визначення вимог щодо обмеження місць обробки інформації, інформації, даних або інформаційних служб; організаційні процеси для забезпечення розташування обмежені відповідно до вимог чи умов]. | |

|  |  |  |
| --- | --- | --- |
| SA-9(7) | ЗОВНІШНІ СИСТЕМНІ СЛУЖБИ - ПЕРЕВІРКА ЦІЛІСНОСТІ, ЩО КОНТРОЛЮЄТЬСЯ ОРГАНІЗАЦІЄЮ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-9(7)[1] | забезпечити можливість перевірки цілісності організаційної інформації під час її перебування у зовнішній системі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої інформаційної системи; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; заявна документація; документація про придбання; угоди про рівень обслуговування; обмежені місця для обробки інформації; інформація, дані та, або послуги інформаційної системи; обробка інформації, інформація, дані та, або послуги інформаційної системи, які будуть підтримуватися в обмежених місцях; вимоги або умови організаційної безпеки для зовнішніх постачальників; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; зовнішні провайдери послуг інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для визначення вимог щодо обмеження місць обробки інформації, інформації, даних або інформаційних служб; організаційні процеси для забезпечення розташування обмежені відповідно до вимог чи умов]. | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SA-10 | УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА | | | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | | | | |
| SA-10[1] | вимагати від розробника системи, | | | | | | | | | | | | |
| SA-10[1](a) | виконання управління конфігурацією під час (один або кілька): | | | | | | | | | | | |
| SA-10[1](a){1} | | проєктування*:* | | | | | | | | | |
| SA-10[1](a){1}{1} | | | | | | системи | | | |
| SA-10[1](a){1}{2} | | | | | | компонента системи | | | |
| SA-10[1](a){1}{3} | | | | | | служби | | | |
| SA-10[1](a){2} | | розробки: | | | | | |  | | | |
| SA-10[1](a){2}{1} | | | | | | системи | | | |
| SA-10[1](a){2}{2} | | | | | | компонента системи | | | |
| SA-10[1](a){2}{3} | | | | | | служби | | | |
| SA-10[1](a){3} | | реалізації: | | | | | | | | | |
| SA-10[1](a){3}{1} | | | | | | системи | | | |
| SA-10[1](a){3}{2} | | | | | | компонента системи | | | |
| SA-10[1](a){3}{3} | | | | | | служби | | | |
| SA-10[1](a){4} | | експлуатації: | | | | | | | | | |
| SA-10[1](a){4}{1} | | | | | | системи | | | |
| SA-10[1](a){4}{2} | | | | | | компонента системи | | | |
| SA-10[1](a){4}{3} | | | | | | служби | | | |
| SA-10[1](a){5} | | видалення: | | | | | | | | | |
| SA-10[1](a){5}{1} | | | | | | системи | | | |
| SA-10[1](a){5}{2} | | | | | | компонента системи | | | |
| SA-10[1](a){5}{3} | | | | | | служби | | | |
| SA-10[1](b) | SA-10[1](b)[1] | | організація визначає елементи конфігурації, при управлінні конфігурацією цілісність змін в яких, необхідно: | | | | | | | | | |
| SA-10[1](b)[2][1] | | | | | | документувати | | | |
| SA-10[1](b)[2][2] | | | | | | керувати | | | |
| SA-10[1](b)[2][3] | | | | | | контролювати | | | |
| SA-10[1](b)[2] | | у визначених організацією елементах конфігурації при управлінні конфігурацією цілісність змін необхідно: | | | | | | | | | |
| SA-10[1](b)[2][1] | | | | | | документувати | | | |
| SA-10[1](b)[2][2] | | | | | | керувати | | | |
| SA-10[1](b)[2][3] | | | | | | контролювати | | | |
| SA-10[1](c) | SA-10[1](c)[1] | | організація має схвалити всі зміни в: | | | | | | | | | |
| SA-10[1](c)[1]{1} | | | | | | системі | | | |
| SA-10[1](c)[1]{2} | | | | | | компоненті системи | | | |
| SA-10[1](c)[1]{3} | | | | | | службі | | | |
| SA-10[1](c)[2] | | впроваджувати тільки схвалені організацією зміни в: | | | | | | | | | |
| SA-10[1](c)[2]{1} | | | | | | системі | | | |
| SA-10[1](c)[2]{2} | | | | | | компоненті системи | | | |
| SA-10[1](c)[2]{3} | | | | | | службі | | | |
| SA-10[1](d) | Документувати зміни в: | | | | | | | | | | | |
| SA-10[1](d)[1] | | SA-10[1](d)[1]{1} | | | | | | системі | | | |
| SA-10[1](d)[1]{2} | | | | | | компоненті системи | | | |
| SA-10[1](d)[1]{3} | | | | | | службі | | | |
| SA-10[1](d)[2] | | можливі наслідки таких змін для безпеки та приватності | | | | | | | | | |
| SA-10[1](e) | SA-10[1](e)[1] | організація визначає персонал, якому необхідно повідомляти про результати: | | | | | | | | | | |
| SA-10[1](e)[1][1] | | відстежувати недоліки безпеки в: | | | | | | | | |
| SA-10[1](e)[1][1]{1} | | | | | | системі | | |
| SA-10[1](e)[1][1]{2} | | | | | | компоненті системи | | |
| SA-10[1](e)[1][1]{3} | | | | | | службі | | |
| SA-10[1](e)[1][2] | | відстежувати усунення дефектів в: | | | | | | | | |
| SA-10[1](e)[1][2]{1} | | | | | системі | | | |
| SA-10[1](e)[1][2]{2} | | | | | компоненті системи | | | |
| SA-10[1](e)[1][2]{3} | | | | | службі | | | |
| SA-10[1](e)[2] | відстежувати недоліки безпеки в: | | | | | | | | | | |
| SA-10[1](e)[2]{1} | | | | системі | | | | | | |
| SA-10[1](e)[2]{2} | | | | компоненті системи | | | | | | |
| SA-10[1](e)[2]{3} | | | | службі | | | | | | |
| SA-10[1](e)[3] | відстежувати усунення дефектів в: | | | | | | | | | | |
| SA-10[1](e)[3]{1} | | | | системі | | | | | | |
| SA-10[1](e)[3]{2} | | | | компоненті системи | | | | | | |
| SA-10[1](e)[3]{3} | | | | службі | | | | | | |
| SA-10[1](e)[4] | повідомляти визначеному організацією персоналу про результати: | | | | | | | | | | |
| SA-10[1](e)[4][1] | | | відстежування недоліків безпеки в: | | | | | | | |
| SA-10[1](e)[4][1]{1} | | | | | | системі | |
| SA-10[1](e)[4][1]{2} | | | | | | компоненті системи | |
| SA-10[1](e)[4][1]{3} | | | | | | службі | |
| SA-10[1](e)[4][2] | | | відстежування усунення дефектів в: | | | | | | | |
| SA-10[1](e)[4][2]{1} | | | | | | системі | |
| SA-10[1](e)[4][2]{2} | | | | | | компоненті системи | |
| SA-10[1](e)[4][2]{3} | | | | | | службі | |
| SA-10[2] | вимагати від розробника системного компонента | | | | | | | | | | | | |
| SA-10[2](a) | виконання управління конфігурацією під час (один або кілька): | | | | | | | | | | | |
| SA-10[2](a){1} | проєктування*:* | | | | | | | | | | |
| SA-10[2](a){1}{1} | | | | | | системи | | | | |
| SA-10[2](a){1}{2} | | | | | | компонента системи | | | | |
| SA-10[2](a){1}{3} | | | | | | служби | | | | |
| SA-10[2](a){2} | розробки: | | | | | | | | | | |
| SA-10[2](a){2}{1} | | | | | | системи | | | | |
| SA-10[2](a){2}{2} | | | | | | компонента системи | | | | |
| SA-10[2](a){2}{3} | | | | | | служби | | | | |
| SA-10[2](a){3} | реалізації: | | | | | | | | | | |
| SA-10[2](a){3}{1} | | | | | | системи | | | | |
| SA-10[2](a){3}{2} | | | | | | компонента системи | | | | |
| SA-10[2](a){3}{3} | | | | | | служби | | | | |
| SA-10[2](a){4} | експлуатації: | | | | | | | | | | |
| SA-10[2](a){4}{1} | | | | | | системи | | | | |
| SA-10[2](a){4}{2} | | | | | | компонента системи | | | | |
| SA-10[2](a){4}{3} | | | | | | служби | | | | |
| SA-10[2](a){5} | видалення: | | | | | | | | | | |
| SA-10[2](a){5}{1} | | | | | | системи | | | | |
| SA-10[2](a){5}{2} | | | | | | компонента системи | | | | |
| SA-10[2](a){5}{3} | | | | | | служби | | | | |
| SA-10[2](b) | SA-10[2](b)[1] | організація визначає елементи конфігурації при управлінні конфігурацією цілісність змін в яких необхідно: | | | | | | | | | | |
| SA-10[2](b)[2][1] | | | | | | документувати | | | | |
| SA-10[2](b)[2][2] | | | | | | керувати | | | | |
| SA-10[2](b)[2][3] | | | | | | контролювати | | | | |
| SA-10[2](b)[2] | у визначених організацією елементах конфігурації при управлінні конфігурацією цілісність змін необхідно: | | | | | | | | | | |
| SA-10[2](b)[2][1] | | | | | | документувати | | | | |
| SA-10[2](b)[2][2] | | | | | | керувати | | | | |
| SA-10[2](b)[2][3] | | | | | | контролювати | | | | |
| SA-10[2](c) | SA-10[2](c)[1] | Організація має схвалити всі зміни в: | | | | | | | | | | |
| SA-10[2](c)[1]{1} | | | | | | системі | | | | |
| SA-10[2](c)[1]{2} | | | | | | компоненті системи | | | | |
| SA-10[2](c)[1]{3} | | | | | | службі | | | | |
| SA-10[2](c)[2] | впроваджувати тільки схвалені організацією зміни в: | | | | | | | | | | |
| SA-10[2](c)[2]{1} | | | | | | системі | | | | |
| SA-10[2](c)[2]{2} | | | | | | компоненті системи | | | | |
| SA-10[2](c)[2]{3} | | | | | | службі | | | | |
| SA-10[2](d) | документувати зміни в: | | | | | | | | | | | |
| SA-10[2](d)[1] | SA-10[2](d)[1]{1} | | | | | | системі | | | | |
| SA-10[2](d)[1]{2} | | | | | | компоненті системи | | | | |
| SA-10[2](d)[1]{3} | | | | | | службі | | | | |
| SA-10[2](d)[2] | можливі наслідки таких змін для безпеки та приватності | | | | | | | | | | |
| SA-10[2](e) | SA-10[2](e)[1] | організація визначає персонал, якому необхідно повідомляти про результати: | | | | | | | | | | |
| SA-10[2](e)[1][1] | | | відстежувати недоліки безпеки в: | | | | | | | |
| SA-10[2](e)[1][1]{1} | | | | | | системі | |
| SA-10[2](e)[1][1]{2} | | | | | | компоненті системи | |
| SA-10[2](e)[1][1]{3} | | | | | | службі | |
| SA-10[2](e)[1][2] | | | відстежувати усунення дефектів в: | | | | | | | |
| SA-10[2](e)[1][2]{1} | | | | | | системі | |
| SA-10[2](e)[1][2]{2} | | | | | | компоненті системи | |
| SA-10[2](e)[1][2]{3} | | | | | | службі | |
| SA-10[2](e)[2] | відстежувати недоліки безпеки в: | | | | | | | | | | |
| SA-10[2](e)[2]{1} | | | системі | | | | | | | |
| SA-10[2](e)[2]{2} | | | компоненті системи | | | | | | | |
| SA-10[2](e)[2]{3} | | | службі | | | | | | | |
| SA-10[2](e)[3] | відстежувати усунення дефектів в: | | | | | | | | | | |
| SA-10[2](e)[3]{1} | | | системі | | | | | | | |
| SA-10[2](e)[3]{2} | | | компоненті системи | | | | | | | |
| SA-10[2](e)[3]{3} | | | службі | | | | | | | |
| SA-10[2](e)[4] | повідомляти визначеному організацією персоналу про результати: | | | | | | | | | | |
| SA-10[2](e)[4][1] | | | відстежування недоліків безпеки в: | | | | | | | |
| SA-10[2](e)[4][1]{1} | | | | | | системі | |
| SA-10[2](e)[4][1]{2} | | | | | | компоненті системи | |
| SA-10[2](e)[4][1]{3} | | | | | | службі | |
| SA-10[2](e)[4][2] | | | відстежування усунення дефектів в: | | | | | | | |
| SA-10[2](e)[4][2]{1} | | | | | | системі | |
| SA-10[2](e)[4][2]{2} | | | | | | компоненті системи | |
| SA-10[2](e)[4][2]{3} | | | | | | службі | |
| SA-10[3] | вимагати від розробника системної служби: | | | | | | | | | | | | |
| SA-10[3](a) | виконання управління конфігурацією під час (один або кілька): | | | | | | | | | | | |
| SA-10[3](a){1} | проєктування*:* | | | | | | | | | | |
| SA-10[3](a){1}{1} | | | | | системи | | | | | |
| SA-10[3](a){1}{2} | | | | | компонента системи | | | | | |
| SA-10[3](a){1}{3} | | | | | служби | | | | | |
| SA-10[3](a){2} | розробки: | | | | | | | | | | |
| SA-10[3](a){2}{1} | | | | | системи | | | | | |
| SA-10[3](a){2}{2} | | | | | компонента системи | | | | | |
| SA-10[3](a){2}{3} | | | | | служби | | | | | |
| SA-10[3](a){3} | реалізації: | | | | | | | | | | |
| SA-10[3](a){3}{1} | | | | | системи | | | | | |
| SA-10[3](a){3}{2} | | | | | компонента системи | | | | | |
| SA-10[3](a){3}{3} | | | | | служби | | | | | |
| SA-10[3](a){4} | експлуатації: | | | | | | | | | | |
| SA-10[3](a){4}{1} | | | | | системи | | | | | |
| SA-10[3](a){4}{2} | | | | | компонента системи | | | | | |
| SA-10[3](a){4}{3} | | | | | служби | | | | | |
| SA-10[3](a){5} | видалення: | | | | | | | | | | |
| SA-10[3](a){5}{1} | | | | | системи | | | | | |
| SA-10[3](a){5}{2} | | | | | компонента системи | | | | | |
| SA-10[3](a){5}{3} | | | | | служби | | | | |  |
| SA-10[3](b) | SA-10[3](b)[1] | організація визначає елементи конфігурації при управлінні конфігурацією цілісність змін в яких необхідно: | | | | | | | | | | |
| SA-10[3](b)[2][1] | | | | | документувати | | | | | |
| SA-10[3](b)[2][2] | | | | | керувати | | | | | |
| SA-10[3](b)[2][3] | | | | | контролювати | | | | | |
| SA-10[3](b)[2] | у визначених організацією елементах конфігурації при управлінні конфігурацією цілісність змін необхідно: | | | | | | | | | | |
| SA-10[3](b)[2][1] | | | | | документувати | | | | | |
| SA-10[3](b)[2][2] | | | | | керувати | | | | | |
| SA-10[3](b)[2][3] | | | | | контролювати | | | | | |
| SA-10[3](c) | SA-10[3](c)[1] | організація має схвалити всі зміни в: | | | | | | | | | | |
| SA-10[3](c)[1]{1} | | | | | системі | | | | | |
| SA-10[3](c)[1]{2} | | | | | компоненті системи | | | | | |
| SA-10[3](c)[1]{3} | | | | | службі | | | | | |
| SA-10[3](c)[2] | впроваджувати тільки схвалені організацією зміни в: | | | | | | | | | | |
| SA-10[3](c)[2]{1} | | | | | системі | | | | | |
| SA-10[3](c)[2]{2} | | | | | компоненті системи | | | | | |
| SA-10[3](c)[2]{3} | | | | | службі | | | | | |
| SA-10[3](d) | Документувати зміни в: | | | | | | | | | | | |
| SA-10[3](d)[1] | SA-10[3](d)[1]{1} | | | | | | системі, | | | | |
| SA-10[3](d)[1]{2} | | | | | | компоненті системи | | | | |
| SA-10[3](d)[1]{3} | | | | | | службі | | | | |
| SA-10[3](d)[2] | можливі наслідки таких змін для безпеки та приватності | | | | | | | | | | |
| SA-10[3](e) | SA-10[3](e)[1] | організація визначає персонал, якому необхідно повідомляти про результати: | | | | | | | | | | |
| SA-10[3](e)[1][1] | | | відстежувати недоліки безпеки в: | | | | | | | |
| SA-10[3](e)[1][1]{1} | | | | | | системі | |
| SA-10[3](e)[1][1]{2} | | | | | | компоненті системи | |
| SA-10[3](e)[1][1]{3} | | | | | | службі | |
| SA-10[3](e)[1][2] | | | відстежувати усунення дефектів в: | | | | | | | |
| SA-10[3](e)[1][2]{1} | | | | | | системі, | |
| SA-10[3](e)[1][2]{2} | | | | | | компоненті системи | |
| SA-10[3](e)[1][2]{3} | | | | | | службі | |
| SA-10[3](e)[2] | відстежувати недоліки безпеки в: | | | | | | | | | | |
| SA-10[3](e)[2]{1} | | | системі | | | | | | | |
| SA-10[3](e)[2]{2} | | | компоненті системи | | | | | | | |
| SA-10[3](e)[2]{3} | | | службі | | | | | | | |
| SA-10[3](e)[3] | відстежувати усунення дефектів в: | | | | | | | | | | |
| SA-10[3](e)[3]{1} | | | системі | | | | | | | |
| SA-10[3](e)[3]{2} | | | компоненті системи | | | | | | | |
| SA-10[3](e)[3]{3} | | | службі | | | | | | | |
| SA-10[3](e)[4] | повідомляти визначеному організацією персоналу про результати: | | | | | | | | | | |
| SA-10[3](e)[4][1] | | | відстежування недоліків безпеки в: | | | | | | | |
| SA-10[3](e)[4][1]{1} | | | | | | системі | |
| SA-10[3](e)[4][1]{2} | | | | | | компоненті системи | |
| SA-10[3](e)[4][1]{3} | | | | | | службі | |
| SA-10[3](e)[4][2] | | | відстежування усунення дефектів в: | | | | | | | |
| SA-10[3](e)[4][2]{1} | | | | | | системі | |
| SA-10[3](e)[4][2]{2} | | | | | | компоненті системи | |
| SA-10[3](e)[4][2]{3} | | | | | | службі | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи; системний компонент, або послуга інформаційної системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за управління конфігурацією; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника]. | | | | | | | | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-10(1) | УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ПЕРЕВІРКА ЦІЛІСНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА МІКРОПРОГРАМ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-10(1)[1] | вимагати забезпечення перевірки цілісності програмного забезпечення від розробника: | |
| SA-10(1)[1]{1} | системи |
| SA-10(1)[1]{2} | системного компонента |
| SA-10(1)[1]{3} | системної служби |
| SA-10(1)[2] | вимагати забезпечення перевірки цілісності компонентів програмного забезпечення від розробника: | |
| SA-10(1)[2]{1} | системи |
| SA-10(1)[2]{2} | системного компонента |
| SA-10(1)[2]{3} | системної служби |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи; системний компонент, або послуга інформаційної системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за управління конфігурацією; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника]. | | |

|  |  |  |
| --- | --- | --- |
| SA-10(2) | УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - АЛЬТЕРНАТИВНІ ПРОЦЕСИ КЕРУВАННЯ КОНФІГУРАЦІЄЮ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-10(2)[1] | забезпечувати альтернативний процес керування конфігурацією за допомогою організаційного персоналу за відсутності спеціалізованої команди керування конфігурацією розробників |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи; системний компонент, або послуга інформаційної системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за управління конфігурацією; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-10(3) | УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ПЕРЕВІРКА ЦІЛІСНОСТІ АПАРАТНИХ ЗАСОБІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-10(3)[1] | вимагати забезпечувати перевірку цілісності апаратних компонентів від розробника: | |
| SA-10(3)[1]{1} | системи |
| SA-10(3)[1]{2} | системного компонента |
| SA-10(3)[1]{3} | системної служби |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи; системний компонент, або послуга інформаційної системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за управління конфігурацією; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-10(4) | УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ДОВІРЧЕ ГЕНЕРУВАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-10(4)[1] | вимагати використовувати інструменти для порівняння новозгенерованих версій апаратних описів, вихідного коду та об'єктного коду, що стосуються безпеки, з попередніми версіями від: | |
| SA-10(4)[1]{1} | розробника системи |
| SA-10(4)[1]{2} | системного компонента |
| SA-10(4)[1]{3} | системної служби |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи; системний компонент, або послуга інформаційної системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за управління конфігурацією; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-10(5) | УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ЦІЛІСНІСТЬ ВІДОБРАЖЕННЯ ДЛЯ КЕРУВАННЯ ВЕРСІЯМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-10(5){1} | вимагати від розробника системи підтримувати цілісність відображення оригінальних даних проєктування, а саме: | | |
| SA-10(5){1}[1] | апаратних креслень програмного забезпечення, прошивки, описуючи поточну версію: | |
| SA-10(5){1}[1][1] | апаратного обладнання, що пов’язані з безпекою |
| SA-10(5){1}[1][2] | програмного забезпечення, що пов’язані з безпекою |
| SA-10(5){1}[1][3] | прошивки, що пов’язані з безпекою |
| SA-10(5){1}[2] | коду програмного забезпечення, прошивки, описуючи поточну версію: | |
| SA-10(5){1}[2][1] | апаратного обладнання, що пов’язані з безпекою |
| SA-10(5){1}[2][2] | програмного забезпечення, що пов’язані з безпекою |
| SA-10(5){1}[2][3] | прошивки, що пов’язані з безпекою |
| SA-10(5){2} | вимагати від розробника системного компонента підтримувати цілісність відображення оригінальних даних проєктування, а саме: | | |
| SA-10(5){2}[1] | апаратних креслень програмного забезпечення, прошивки, описуючи поточну версію: | |
| SA-10(5){2}[1][1] | апаратного обладнання, що пов’язані з безпекою |
| SA-10(5){2}[1][2] | програмного забезпечення, що пов’язані з безпекою |
| SA-10(5){2}[1][3] | прошивки, що пов’язані з безпекою |
| SA-10(5){2}[2] | коду програмного забезпечення, прошивки, описуючи поточну версію: | |
| SA-10(5){2}[2][1] | апаратного обладнання, що пов’язані з безпекою |
| SA-10(5){2}[2][2] | програмного забезпечення, що пов’язані з безпекою |
| SA-10(5){2}[2][3] | прошивки, що пов’язані з безпекою |
| SA-10(5){3} | вимагати від розробника системної служби підтримувати цілісність відображення оригінальних даних проєктування, а саме: | | |
| SA-10(5){2}[1] | апаратних креслень програмного забезпечення, прошивки, описуючи поточну версію: | |
| SA-10(5){2}[1][1] | апаратного обладнання, що пов’язані з безпекою |
| SA-10(5){2}[1][2] | програмного забезпечення, що пов’язані з безпекою |
| SA-10(5){2}[1][3] | прошивки, що пов’язані з безпекою |
| SA-10(5){2}[2] | коду програмного забезпечення, прошивки, описуючи поточну версію: | |
| SA-10(5){2}[2][1] | апаратного обладнання, що пов’язані з безпекою |
| SA-10(5){2}[2][2] | програмного забезпечення, що пов’язані з безпекою |
| SA-10(5){2}[2][3] | прошивки, що пов’язані з безпекою |
| SA-10(5){3} | зберігати оригінальну копію даних для поточної версії на сайті | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи; системний компонент, або послуга інформаційної системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за управління конфігурацією; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-10(6) | УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ДОВІРЕНА ПОСТАВКА | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-10(6){1} | вимагати від розробника системи виконувати процедури для забезпечення того, щоб: | | |
| SA-10(6){1}[1] | апаратні засоби, що: | |
| SA-10(6){1}[1][1] | стосуються безпеки, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){1}[1][2] | які оновлюються в організації, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){1}[2] | програмне забезпечення, що: | |
| SA-10(6){1}[2][1] | стосуються безпеки, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){1}[2][2] | які оновлюються в організації, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){1}[3] | оновлення прошивки, що: | |
| SA-10(6){1}[3][1] | стосуються безпеки, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){1}[3][2] | які оновлюються в організації, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){2} | вимагати від розробника системного компонента виконувати процедури для забезпечення того, щоб: | | |
| SA-10(6){2}[1] | апаратні засоби, що: | |
| SA-10(6){2}[1][1] | стосуються безпеки, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){2}[1][2] | які оновлюються в організації, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){2}[2] | програмне забезпечення, що: | |
| SA-10(6){2}[2][1] | стосуються безпеки, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){2}[2][2] | які оновлюються в організації, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){2}[3] | оновлення прошивки, що: | |
| SA-10(6){2}[3][1] | стосуються безпеки, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){2}[3][2] | які оновлюються в організації, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){3} | вимагати від розробника системної служби виконувати процедури для забезпечення того, щоб: | | |
| SA-10(6){3}[1] | апаратні засоби, що: | |
| SA-10(6){3}[1][1] | стосуються безпеки, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){3}[1][2] | які оновлюються в організації, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){3}[2] | програмне забезпечення, що: | |
| SA-10(6){3}[2][1] | стосуються безпеки, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){3}[2][2] | які оновлюються в організації, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){2}[3] | оновлення прошивки, що: | |
| SA-10(6){2}[3][1] | стосуються безпеки, відповідали тому, що зазначено в оригінальних копіях |
| SA-10(6){2}[3][2] | які оновлюються в організації, відповідали тому, що зазначено в оригінальних копіях |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи; системний компонент, або послуга інформаційної системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за управління конфігурацією; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника]. | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SA-11 | ТЕСТУВАННЯ ТА ОЦІНКА РОЗРОБНИКА | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | |
| SA-11{1} | вимагати від розробника системи, на всіх етапах проєктування та життєвого циклу розробки системи: | | | | | | | | | |
| SA-11{1}(a) | SA-11{1}[1][1] | створити план з оцінки безпеки та приватності | | | | | | | |
| SA-11{1}[1][2] | впровадити план з оцінки безпеки та приватності | | | | | | | |
| SA-11{1}(b) | SA-11{1}(b)[1] | організація визначає частоту, з якою необхідно проводити: | | | | | | | |
| SA-11{1}(b)[1][1] | | | тестування: | | | | |
| SA-11{1}(b)[1][1]{1} | | | | одиниці |
| SA-11{1}(b)[1][1]{2} | | | | інтеграції |
| SA-11{1}(b)[1][1]{3} | | | | системи |
| SA-11{1}(b)[1][1]{4} | | | | регресії |
| SA-11{1}(b)[1][2] | | | оцінку: | | | | |
| SA-11{1}(b)[1][2]{1} | | | | одиниці |
| SA-11{1}(b)[1][2]{2} | | | | інтеграції |
| SA-11{1}(b)[1][2]{3} | | | | системи |
| SA-11{1}(b)[1][2]{4} | | | | регресії |
| SA-11{1}(b)[2] | організація визначає глибину, з якою необхідно проводити: | | | | | | | |
| SA-11{1}(b)[2][1] | | | тестування: | | | | |
| SA-11{1}(b)[2][1]{1} | | | | одиниці |
| SA-11{1}(b)[2][1]{2} | | | | інтеграції |
| SA-11{1}(b)[2][1]{3} | | | | системи |
| SA-11{1}(b)[2][1]{4} | | | | регресії |
| SA-11{1}(b)[2][2] | | | оцінку: | | | | |
| SA-11{1}(b)[2][2]{1} | | | | одиниці |
| SA-11{1}(b)[2][2]{2} | | | | інтеграції |
| SA-11{1}(b)[2][2]{3} | | | | системи |
| SA-11{1}(b)[2][2]{4} | | | | регресії |
| SA-11{1}(b)[3] | організація визначає охоплення з яким необхідно проводити: | | | | | | | |
|  | SA-11{1}(b)[3][1] | | | тестування: | | | | |
| SA-11{1}(b)[3][1]{1} | | | | одиниці |
| SA-11{1}(b)[3][1]{2} | | | | інтеграції |
| SA-11{1}(b)[3][1]{3} | | | | системи |
| SA-11{1}(b)[3][1]{4} | | | | регресії |
| SA-11{1}(b)[3][2] | | | оцінку: | | | | |
| SA-11{1}(b)[3][2]{1} | | | | одиниці |
| SA-11{1}(b)[3][2]{2} | | | | інтеграції |
| SA-11{1}(b)[3][2]{3} | | | | системи |
| SA-11{1}(b)[3][2]{4} | | | | регресії |
| SA-11{1}(b)[4] | виконати (один або кілька): | | | | | | | |
| SA-11{1}(b)[4]{1} | | | | одиниця: | | | |
| SA-11{1}(b)[4]{1}[1] | | тестування з визначеною організацією частотою та з визначеною організацією глибиною та охоплення | |
| SA-11{1}(b)[4]{1}[2] | | оцінку з визначеною організацією частотою та з визначеною організацією глибиною охоплення | |
| SA-11{1}(b)[4]{2} | | | | інтеграція: | | | |
| SA-11{1}(b)[4]{2}[1] | | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{1}(b)[4]{2}[2] | | оцінку з визначеною організацією частотою та з визначеною організацією глибиною охоплення | |
| SA-11{1}(b)[4]{3} | | | | система | | | |
| SA-11{1}(b)[4]{3}[1] | | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{1}(b)[4]{3}[2] | | оцінку з визначеною організацією частотою та з визначена організацією глибиною охоплення | |
| SA-11{1}(b)[4]{4} | | | | регресія | | | |
| SA-11{1}(b)[4]{4}[1] | | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{1}(b)[4]{4}[2] | | оцінку з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{1}(c) | надати докази (свідчення) виконання: | | | | | | | | |
| SA-11{1}(c)[1] | | | плану оцінки | | | | | |
| SA-11{1}(c)[2] | | | результати тестування | | | | | |
| SA-11{1}(c)[3] | | | результати оцінок | | | | | |
| SA-11{1}(d) | впровадити перевірку процесу виправлення недоліків | | | | | | | | |
| виправити дефекти, які виявлені під час: | | | | | | | | |
| SA-11{1}(d)[1] | | | тестування | | | | | |
| SA-11{1}(d)[2] | | | оцінки | | | | | |
| SA-11{2} | вимагати від розробника системного компонента, на всіх етапах проєктування та життєвого циклу розробки системи: | | | | | | | | | |
| SA-11{2}(a) | SA-11{2}[1][1] | створити план з оцінки безпеки та приватності | | | | | | | |
| SA-11{2}[1][2] | впровадити план з оцінки безпеки та приватності | | | | | | | |
| SA-11{2}(b) | SA-11{2}(b)[1] | організація визначає частоту, з якою необхідно проводити: | | | | | | | |
| SA-11{2}(b)[1][1] | | | тестування: | | | | |
| SA-11{2}(b)[1][1]{1} | | | | одиниці |
| SA-11{2}(b)[1][1]{2} | | | | інтеграції |
| SA-11{2}(b)[1][1]{3} | | | | системи |
| SA-11{2}(b)[1][1]{4} | | | | регресії |
| SA-11{2}(b)[1][2] | | | оцінку: | | | | |
| SA-11{2}(b)[1][2]{1} | | | | одиниці |
| SA-11{2}(b)[1][2]{2} | | | | інтеграції |
| SA-11{2}(b)[1][2]{3} | | | | системи |
| SA-11{2}(b)[1][2]{4} | | | | регресії |
| SA-11{2}(b)[2] | організація визначає глибину, з якою необхідно проводити: | | | | | | | |
| SA-11{2}(b)[2][1] | | | тестування: | | | | |
| SA-11{2}(b)[2][1]{1} | | | | одиниці |
| SA-11{2}(b)[2][1]{2} | | | | інтеграції |
| SA-11{2}(b)[2][1]{3} | | | | системи |
| SA-11{2}(b)[2][1]{4} | | | | регресії |
| SA-11{2}(b)[2][2] | | | оцінку: | | | | |
| SA-11{2}(b)[2][2]{1} | | | | одиниці |
| SA-11{2}(b)[2][2]{2} | | | | інтеграції |
| SA-11{2}(b)[2][2]{3} | | | | системи |
| SA-11{2}(b)[2][2]{4} | | | | регресії |
| SA-11{2}(b)[3] | організація визначає охоплення, з яким необхідно проводити: | | | | | | | |
| SA-11{2}(b)[3][1] | | | Тестування: | | | | |
| SA-11{2}(b)[3][1]{1} | | | | одиниці |
| SA-11{2}(b)[3][1]{2} | | | | інтеграції |
| SA-11{2}(b)[3][1]{3} | | | | системи |
| SA-11{2}(b)[3][1]{4} | | | | регресії |
| SA-11{2}(b)[3][2] | | | оцінку: | | | | |
| SA-11{2}(b)[3][2]{1} | | | | одиниці |
| SA-11{2}(b)[3][2]{2} | | | | інтеграції |
| SA-11{2}(b)[3][2]{3} | | | | системи |
| SA-11{2}(b)[3][2]{4} | | | | регресії |
| SA-11{2}(b)[4] | виконати (один або кілька): | | | | | | | |
| SA-11{2}(b)[4]{1} | | | | одиниця: | | | |
| SA-11{2}(b)[4]{1}[1] | | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{2}(b)[4]{1}[2] | | оцінку з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{2}(b)[4]{2} | | | | інтеграція: | | | |
| SA-11{2}(b)[4]{2}[1] | | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{2}(b)[4]{2}[2] | | оцінку з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{2}(b)[4]{3} | | | | система | | | |
| SA-11{2}(b)[4]{3}[1] | | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{2}(b)[4]{3}[2] | | оцінку з визначеною організацією частотою та визначена організацією глибиною охоплення | |
| SA-11{2}(b)[4]{4} | | | | регресія | | | |
| SA-11{2}(b)[4]{4}[1] | | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{2}(b)[4]{4}[2] | | оцінку з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{2}(c) | надати докази (свідчення) виконання: | | | | | | | | |
| SA-11{2}(c)[1] | | плану оцінки | | | | | | |
| SA-11{2}(c)[2] | | результати тестування | | | | | | |
| SA-11{2}(c)[3] | | результати оцінок | | | | | | |
| SA-11{2}(d) | впровадити перевірку процесу виправлення недоліків | | | | | | | | |
| виправити дефекти, які виявлені під час: | | | | | | | | |
| SA-11{2}(d)[1] | | тестування | | | | | | |
| SA-11{2}(d)[2] | | оцінки | | | | | | |
| SA-11{3} | вимагати від розробника системної служби, на всіх етапах проєктування та життєвого циклу розробки системи: | | | | | | | | | |
| SA-11{3}(a) | SA-11{3}[1][1] | створити план з оцінки безпеки та приватності | | | | | | | |
| SA-11{3}[1][2] | впровадити план з оцінки безпеки та приватності | | | | | | | |
| SA-11{3}(b) | SA-11{3}(b)[1] | організація визначає частоту, з якою необхідно проводити: | | | | | | | |
| SA-11{3}(b)[1][1] | | | тестування: | | | | |
| SA-11{3}(b)[1][1]{1} | | | | одиниці |
| SA-11{3}(b)[1][1]{2} | | | | інтеграції |
| SA-11{3}(b)[1][1]{3} | | | | системи |
| SA-11{3}(b)[1][1]{4} | | | | регресії |
| SA-11{3}(b)[1][2] | | | оцінку: | | | | |
| SA-11{3}(b)[1][2]{1} | | | | одиниці |
| SA-11{3}(b)[1][2]{2} | | | | інтеграції |
| SA-11{3}(b)[1][2]{3} | | | | системи |
| SA-11{3}(b)[1][2]{4} | | | | регресії |
| SA-11{3}(b)[2] | організація визначає глибину, з якою необхідно проводити: | | | | | | | |
| SA-11{3}(b)[2][1] | | | Тестування: | | | | |
| SA-11{3}(b)[2][1]{1} | | | | одиниці |
| SA-11{3}(b)[2][1]{2} | | | | інтеграції |
| SA-11{3}(b)[2][1]{3} | | | | системи |
| SA-11{3}(b)[2][1]{4} | | | | регресії |
| SA-11{3}(b)[2][2] | | | оцінку: | | | | |
| SA-11{3}(b)[2][2]{1} | | | | одиниці |
| SA-11{3}(b)[2][2]{2} | | | | інтеграції |
| SA-11{3}(b)[2][2]{3} | | | | системи |
| SA-11{3}(b)[2][2]{4} | | | | регресії |
| SA-11{3}(b)[3] | організація визначає охоплення, з яким необхідно проводити: | | | | | | | |
| SA-11{3}(b)[3][1] | | | тестування: | | | | |
| SA-11{3}(b)[3][1]{1} | | | | одиниці |
| SA-11{3}(b)[3][1]{2} | | | | інтеграції |
| SA-11{3}(b)[3][1]{3} | | | | системи |
| SA-11{3}(b)[3][1]{4} | | | | регресії |
| SA-11{3}(b)[3][2] | | | оцінку: | | | | |
| SA-11{3}(b)[3][2]{1} | | | | одиниці |
| SA-11{3}(b)[3][2]{2} | | | | інтеграції |
| SA-11{3}(b)[3][2]{3} | | | | системи |
| SA-11{3}(b)[3][2]{4} | | | | регресії |
| SA-11{3}(b)[4] | виконати (один або кілька): | | | | | | | |
| SA-11{3}(b)[4]{1} | | | | одиниця: | | | |
| SA-11{3}(b)[4]{1}[1] | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | | |
| SA-11{3}(b)[4]{1}[2] | оцінку з визначеною організацією частотою та визначеною організацією глибиною охоплення | | |
| SA-11{3}(b)[4]{2} | | | | інтеграція: | | | |
| SA-11{3}(b)[4]{2}[1] | | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{3}(b)[4]{2}[2] | | оцінку з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{3}(b)[4]{3} | | | | система | | | |
| SA-11{3}(b)[4]{3}[1] | | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{3}(b)[4]{3}[2] | | оцінку з визначеною організацією частотою та визначена організацією глибиною охоплення | |
| SA-11{3}(b)[4]{4} | | | | регресія | | | |
| SA-11{3}(b)[4]{4}[1] | | тестування з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{3}(b)[4]{4}[2] | | оцінку з визначеною організацією частотою та визначеною організацією глибиною охоплення | |
| SA-11{3}(c) | Надати докази (свідчення) виконання: | | | | | | | | |
| SA-11{3}(c)[1] | | | плану оцінки | | | | | |
| SA-11{3}(c)[2] | | | результати тестування | | | | | |
| SA-11{3}(c)[3] | | | результати оцінок | | | | | |
| SA-11{3}(d) | впровадити перевірку процесу виправлення недоліків | | | | | | | | |
| виправити дефекти, які виявлені під час: | | | | | | | | |
| SA-11{3}(d)[1] | | | тестування | | | | | |
| SA-11{3}(d)[2] | | | оцінки | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; процедури, що стосуються усунення недоліків; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; плани тестування безпеки розробника системи; записи результатів тестування безпеки розробника для інформаційної системи, компонента системи або служби інформаційної системи; записи про виявлення недоліків безпеки та усунення несправностей; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за тестування безпеки розробника; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника]. | | | | | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-11(1) | ТЕСТУВАННЯ ТА ОЦІНКА РОЗРОБНИКА - АНАЛІЗ СТАТИЧНОГО КОДУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-11(1)[1] | SA-11(1)[1]{1} | вимагати від розробника системи використовувати інструменти аналізу статичних кодів для виявлення поширених недоліків |
| SA-11(1)[1]{2} | вимагати від розробника системного компонента використовувати інструменти аналізу статичних кодів для виявлення поширених недоліків |
| SA-11(1)[1]{3} | вимагати від розробника системної служби використовувати інструменти аналізу статичних кодів для виявлення поширених недоліків |
| SA-11(1)[2] | документувати результатів аналізу статичних кодів | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; процедури, що стосуються усунення недоліків; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; плани тестування безпеки розробника системи; результати тестування безпеки розробника системи; записи про виявлення недоліків безпеки та усунення несправностей; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за тестування безпеки розробника; організаційний персонал, який відповідає за управління конфігурацією; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника; засоби аналізу статичного коду]. | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SA-11(2) | ТЕСТУВАННЯ ТА ОЦІНКА РОЗРОБНИКА - МОДЕЛЮВАННЯ ЗАГРОЗ ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| SA-11(2)[1] | SA-11(2)[1][1] | організація визначає широту | | | | | |
| SA-11(2)[1][2] | організація визначає глибину | | | | | |
| SA-11(2)[1][3] | організація визначає інформацію щодо критичності | | | | | |
| SA-11(2)[1][4] | організація визначає інформацію щодо середовища функціонування | | | | | |
| SA-11(2)[1][5] | SA-11(2)[1][5]{1} | організація визначає інформацію щодо відомих загроз | | | | |
| SA-11(2)[1][5]{2} | організація визначає інформацію щодо передбачуваних загроз | | | | |
| SA-11(2)[1][6] | організація визначає інформацію щодо прийнятних рівнів ризику | | | | | |
| SA-11(2)[1][7] | організація визначає інструменти | | | | | |
| SA-11(2)[1][8] | організація визначає методи | | | | | |
| SA-11(2)[1][9] | організація визначає критеріям прийняття рішень | | | | | |
| SA-11(2)[2] | вимагати виконання: | | | | | | |
| SA-11(2)[2][1] | моделювання загроз під час | | | | | |
| SA-11(2)[2][1][1] | розробки системи, компонента або служби, що: | | | | |
| SA-11(2)[2][1][1](a) | використовує визначену організацією інформацію щодо: | | | |
| SA-11(2)[2][1][1](a)[1] | критичності | | |
| SA-11(2)[2][1][1](a)[2] | середовища функціонування | | |
| SA-11(2)[2][1][1](a)[3] | SA-11(2)[2][1][1](a)[3]{1} | відомих загроз | |
| SA-11(2)[2][1][1](a)[3]{2} | передбачуваних загроз | |
| SA-11(2)[2][1][1](a)[4] | прийнятних рівнів ризику | | |
| SA-11(2)[2][1][1](b) | впровадити визначені організацією: | | | |
| SA-11(2)[2][1][1](b)[1] | інструменти | | |
| SA-11(2)[2][1][1](b)[2] | методи | | |
| SA-11(2)[2][1][1](c) | надає докази (свідчення), які відповідають визначеним організацією критеріям прийняття | | | |
| SA-11(2)[2][1][2] | подальшого тестування системи, компонента або служби, що: | | | | |
| SA-11(2)[2][1][2](a) | використовує визначену організацією інформацію щодо: | | | |
| SA-11(2)[2][1][2](a)[1] | критичності | | |
| SA-11(2)[2][1][2](a)[2] | середовища функціонування | | |
| SA-11(2)[2][1][2](a)[3] | SA-11(2)[2][1][2](a)[3]{1} | | відомих загроз |
| SA-11(2)[2][1][2](a)[3]{2} | | передбачуваних загроз |
| SA-11(2)[2][1][2](a)[4] | прийнятних рівнів ризику | | |
| SA-11(2)[2][1][2](b) | впровадити визначені організацією: | | | |
| SA-11(2)[2][1][2](b)[1] | інструменти | | |
| SA-11(2)[2][1][2](b)[2] | методи | | |
| SA-11(2)[2][1][2](c) | надає докази (свідчення), які відповідають визначеним організацією критеріям прийняття | | | |
| SA-11(2)[2][1][3] | оцінки системи, компонента або служби, що: | | | | |
| SA-11(2)[2][1][3](a) | використовує визначену організацією інформацію щодо: | | | |
| SA-11(2)[2][1][3](a)[1] | критичності | | |
| SA-11(2)[2][1][3](a)[2] | середовища функціонування | | |
| SA-11(2)[2][1][3](a)[3] | SA-11(2)[2][1][3](a)[3]{1} | | відомих загроз |
| SA-11(2)[2][1][3](a)[3]{2} | | передбачуваних загроз |
| SA-11(2)[2][1][3](a)[4] | прийнятних рівнів ризику | | |
| SA-11(2)[2][1][3](b) | впровадити визначені організацією: | | | |
| SA-11(2)[2][1][3](b)[1] | інструменти | | |
| SA-11(2)[2][1][3](b)[2] | методи | | |
| SA-11(2)[2][1][3](c) | надає докази (свідчення), які відповідають визначеним організацією критеріям прийняття | | | |
| SA-11(2)[2][2] | аналіз вразливостей на | | | | | |
| SA-11(2)[2][2][1] | розробки системи, компонента або служби, що: | | | | |
| SA-11(2)[2][2][1](a) | використовує визначену організацією інформацію щодо: | | | |
| SA-11(2)[2][2][1](a)[1] | критичності | | |
| SA-11(2)[2][2][1](a)[2] | середовища функціонування | | |
| SA-11(2)[2][2][1](a)[3] | SA-11(2)[2][2][1](a)[3]{1} | відомих загроз | |
| SA-11(2)[2][2][1](a)[3]{2} | передбачуваних загроз | |
| SA-11(2)[2][2][1](a)[4] | прийнятних рівнів ризику | | |
| SA-11(2)[2][2][1](b) | впровадити визначені організацією: | | | |
| SA-11(2)[2][2][1](b)[1] | інструменти | | |
| SA-11(2)[2][2][1](b)[2] | методи | | |
| SA-11(2)[2][2][1](c) | надає докази (свідчення), які відповідають визначеним організацією критеріям прийняття | | | |
| SA-11(2)[2][2][2] | подальшого тестування системи, компонента або служби, що: | | | | |
| SA-11(2)[2][2][2](a) | використовує визначену організацією інформацію щодо: | | | |
| SA-11(2)[2][2][2](a)[1] | критичності | | |
| SA-11(2)[2][2][2](a)[2] | середовища функціонування | | |
| SA-11(2)[2][2][2](a)[3] | SA-11(2)[2][2][2](a)[3]{1} | відомих загроз | |
| SA-11(2)[2][2][2](a)[3]{2} | передбачуваних загроз | |
| SA-11(2)[2][2][2](a)[4] | прийнятних рівнів ризику | | |
| SA-11(2)[2][2][2](b) | впровадити визначені організацією: | | | |
| SA-11(2)[2][2][2](b)[1] | інструменти | | |
| SA-11(2)[2][2][2](b)[2] | методи | | |
| SA-11(2)[2][2][2](c) | Надає докази (свідчення), які відповідають визначеним організацією критеріям прийняття | | | |
| SA-11(2)[2][2][3] | оцінки системи, компонента або служби, що: | | | | |
| SA-11(2)[2][2][3](a) | використовує визначену організацією інформацію щодо: | | | |
| SA-11(2)[2][2][3](a)[1] | критичності | | |
| SA-11(2)[2][2][3](a)[2] | середовища функціонування | | |
| SA-11(2)[2][2][3](a)[3] | SA-11(2)[2][2][3](a)[3]{1} | | відомих загроз |
| SA-11(2)[2][2][3](a)[3]{2} | | передбачуваних загроз |
| SA-11(2)[2][2][3](a)[4] | прийнятних рівнів ризику | | |
| SA-11(2)[2][2][3](b) | впровадити визначені організацією: | | | |
| SA-11(2)[2][2][3](b)[1] | інструменти | | |
| SA-11(2)[2][2][3](b)[2] | методи | | |
| SA-11(2)[2][2][3](c) | надає докази (свідчення), які відповідають визначеним організацією критеріям прийняття рішень | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; плани тестування безпеки розробника системи; записи результатів тестування безпеки розробника для інформаційної системи, компонента системи або служби інформаційної системи; результати сканування вразливості; звіти про оцінку ризиків інформаційної системи; звіти про аналіз загроз та вразливості; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за тестування безпеки розробника; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника]. | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SA-11(3) | ТЕСТУВАННЯ ТА ОЦІНКА РОЗРОБНИКА - НЕЗАЛЕЖНА ПЕРЕВІРКА ПЛАНІВ ОЦІНКИ ТА ДОКАЗІВ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SA-11(3)(a) | SA-11(3)(a)[1] | організація визначає критерії незалежності, яким має відповідати незалежний агент | | |
| SA-11(3)(a)[2] | вимагати від незалежного агента, що задовольняє визначеним організацією критеріям незалежності, перевірити: | | |
| SA-11(3)(a)[2][1] | правильність виконання планів оцінки безпеки та приватності розробника та | |
| SA-11(3)(a)[2][2] | правильність доказів (свідчень), отриманих під час: | |
| SA-11(3)(a)[2][2][1] | тестування |
| SA-11(3)(a)[2][2][2] | оцінки |
| SA-11(3)(b) | переконатися, що незалежному агенту: | | | |
| SA-11(3)(b){1} | надано достатньо інформації для завершення процесу верифікації або | | |
| SA-11(3)(b){2} | надані повноваження для отримання такої інформації. | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; звіти про незалежну перевірку та валідацію; плани тестування та оцінки безпеки; результати перевірки та оцінки безпеки інформаційної системи, компонента системи або служби інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за тестування безпеки розробника; розробники системи; незалежний агент верифікації].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника]. | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-11(4) | ТЕСТУВАННЯ ТА ОЦІНКА РОЗРОБНИКА - РУЧНИЙ АНАЛІЗ КОДІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-11(4)[1] | SA-11(4)[1][1] | організація визначає певний код, який підлягає ручному аналізу. | |
| SA-11(4)[1][2] | SA-11(4)[1][3]{1} | організація визначає процеси, які слід використовувати при ручному аналізі коду, та, або |
| SA-11(4)[1][3]{2} | організація визначає процедури, які слід використовувати при ручному аналізі коду, та, або |
| SA-11(4)[1][3]{3} | організація визначає методики, які слід використовувати при ручному аналізі коду. |
| SA-11(4)[2] | SA-11(4)[2]{1} | вимагати від розробника системи виконувати ручний аналіз визначеного організацією певного коду, використовуючи (один або кілька): | |
| SA-11(4)[2]{1}{1} | визначені організацією процеси |
| SA-11(4)[2]{1}{2} | визначені організацією процедури |
| SA-11(4)[2]{1}{3} | визначені організацією методики |
| SA-11(4)[2]{2} | вимагати від розробника системного компонента виконувати ручний аналіз визначеного організацією певного коду, використовуючи (один або кілька): | |
| SA-11(4)[2]{2}{1} | визначені організацією процеси |
| SA-11(4)[2]{2}{2} | визначені організацією процедури |
| SA-11(4)[2]{2}{3} | визначені організацією методики |
| SA-11(4)[2]{3} | вимагати від розробника системної служби виконувати ручний аналіз визначеного організацією певного коду, використовуючи(один або кілька): | |
| SA-11(4)[2]{3}{1} | визначені організацією процеси |
| SA-11(4)[2]{3}{2} | визначені організацією процедури |
| SA-11(4)[2]{3}{3} | визначені організацією методики |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; процеси, процедури та, або техніки виконання ручного аналізу коду; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; плани тестування та оцінки безпеки розробника системи; результати тестування та оцінки безпеки розробника системи; список коду, що вимагає перевірки вручну; записи ручного перегляду коду; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за тестування безпеки розробника; розробники системи; незалежний агент верифікації].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-11(5) | ТЕСТУВАННЯ ТА ОЦІНКА РОЗРОБНИКА - ТЕСТУВАННЯ НА ПРОНИКНЕННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-11(5)[1] | SA-11(5)[1][1] | організація визначає широту тестування на проникнення | |
| SA-11(5)[1][2] | організація визначає глибину тестування на проникнення | |
| SA-11(5)[1][3] | організація визначає обмеженнями тестування на проникнення | |
| SA-11(5)[2] | SA-11(5)[2]{1} | вимагати від розробника системи виконувати тестування на проникнення з: | |
| SA-11(5)[2]{1}[1] | визначеною організацією широтою |
| SA-11(5)[2]{1}[2] | визначеною організацією глибиною |
| SA-11(5)[2]{1}[3] | визначеними організацією обмеженнями |
| SA-11(5)[2]{2} | вимагати від розробника системного компонента виконувати тестування на проникнення з: | |
| SA-11(5)[2]{2}[1] | визначеною організацією широтою |
| SA-11(5)[2]{2}[2] | визначеною організацією глибиною |
| SA-11(5)[2]{2}[3] | визначеними організацією обмеженнями |
| SA-11(5)[2]{3} | вимагати від розробника системної служби виконувати тестування на проникнення з: | |
| SA-11(5)[2]{3}[1] | визначеною організацією широтою |
| SA-11(5)[2]{3}[2] | визначеною організацією глибиною |
| SA-11(5)[2]{3}[3] | визначеними організацією обмеженнями |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; плани тестування та оцінки проникнення розробника системи; результати тестування та оцінки проникнення розробника системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за тестування безпеки розробника; розробники системи; незалежний агент верифікації].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника]. | | | |

|  |  |  |
| --- | --- | --- |
| SA-11(6) | ТЕСТУВАННЯ ТА ОЦІНКА РОЗРОБНИКА - АНАЛІЗ ПОВЕРХНІ АТАКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-11(6){1} | Вимагати від розробника системи виконувати аналіз поверхні атаки (вразливостей) |
| SA-11(6){2} | Вимагати від розробника компонента системи виконувати аналіз поверхні атаки (вразливостей) |
| SA-11(6){3} | Вимагати від розробника системної служби виконувати аналіз поверхні атаки (вразливостей) |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; плани тестування та оцінки безпеки розробника системи; результати тестування та оцінки безпеки розробника системи; записи поверхневих оглядів атаки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за тестування безпеки розробника; організаційний персонал, який відповідає за управління конфігурацією; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SA-11(7) | ТЕСТУВАННЯ ТА ОЦІНКА РОЗРОБНИКА - ПЕРЕВІРКА ОБСЯГУ ТЕСТУВАННЯ ТА ОЦІНКИ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SA-11(7)[1] | SA-11(7)[1][1] | визначену організацією глибину тестування | | |
| SA-11(7)[1][2] | визначену організацією глибину оцінки | | |
| SA-11(7)[2] | SA-11(7)[2]{1} | вимагати від розробника системи перевіряти, що: | | |
| SA-11(7)[2]{1}[1] | обсяг тестування забезпечує повне охоплення необхідних засобів безпеки та приватності на визначену організацією: | |
| SA-11(7)[2]{1}[1][1] | глибину тестування |
| SA-11(7)[2]{1}[1][2] | глибину оцінки |
| SA-11(7)[2]{1}[2] | обсяг оцінки забезпечує повне охоплення необхідних засобів безпеки та приватності на визначену організацією глибину тестування та оцінки | |
| SA-11(7)[2]{1}[2][1] | глибину тестування |
| SA-11(7)[2]{1}[2][2] | глибину оцінки |
| SA-11(7)[2]{2} | вимагати від розробника системного компонента перевіряти, що: | | |
| SA-11(7)[2]{1}[1] | обсяг тестування забезпечує повне охоплення необхідних засобів безпеки та приватності на визначену організацією: | |
| SA-11(7)[2]{1}[1][1] | глибину тестування |
| SA-11(7)[2]{1}[1][2] | глибину оцінки |
| SA-11(7)[2]{1}[2] | обсяг оцінки забезпечує повне охоплення необхідних засобів безпеки та приватності на визначену організацією глибину тестування та оцінки | |
| SA-11(7)[2]{1}[2][1] | глибину тестування |
| SA-11(7)[2]{1}[2][2] | глибину оцінки |
| SA-11(7)[2]{3} | Вимагати від розробника системної служби перевіряти, що: | | |
| SA-11(7)[2]{1}[1] | обсяг тестування забезпечує повне охоплення необхідних засобів безпеки та приватності на визначену організацією: | |
| SA-11(7)[2]{1}[1][1] | глибину тестування |
| SA-11(7)[2]{1}[1][2] | глибину оцінки |
| SA-11(7)[2]{1}[2] | обсяг оцінки забезпечує повне охоплення необхідних засобів безпеки та приватності на визначену організацією глибину тестування та оцінки | |
| SA-11(7)[2]{1}[2][1] | глибину тестування |
| SA-11(7)[2]{1}[2][2] | глибину оцінки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; плани тестування та оцінки безпеки розробника системи; результати тестування та оцінки безпеки розробника системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за тестування безпеки розробника; розробники системи; незалежний агент верифікації].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-11(8) | ТЕСТУВАННЯ ТА ОЦІНКА РОЗРОБНИКА - АНАЛІЗ ДИНАМІЧНОГО КОДУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-11(8){1} | вимагати від розробника системи використовувати динамічні інструменти аналізу коду для: | |
| SA-11(8){1}[1] | виявлення загальних недоліків |
| SA-11(8){1}[2] | документування результатів аналізу |
| SA-11(8){2} | вимагати від розробника системного компонента використовувати динамічні інструменти аналізу коду для: | |
| SA-11(8){2}[1] | виявлення загальних недоліків |
| SA-11(8){2}[2] | документування результатів аналізу |
| SA-11(8){3} | вимагати від розробника системної служби використовувати динамічні інструменти аналізу коду для: | |
| SA-11(8){3}[1] | виявлення загальних недоліків |
| SA-11(8){3}[2] | документування результатів аналізу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; процедури, що стосуються усунення недоліків; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; плани тестування та оцінки безпеки розробника системи; результати тестування та оцінки безпеки; звіти про виявлення недоліків та виправлення несправностей; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за тестування безпеки розробника; організаційний персонал, який відповідає за управління конфігурацією; розробники системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника]. | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SA-12 | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SA-12(a) | SA-12(a)[1] | організація визначає заходи безпеки ланцюга постачання | | | |
| SA-12(a)[2] | впровадити визначені організацією заходи безпеки ланцюга постачання для захисту від ризиків ланцюга постачання для: | | | |
| SA-12(a)[2]{1} | системи: | | |
| SA-12(a)[2]{1}{1} | | для обмеження шкоди від подій, пов'язаних з ланцюгом постачання |
| SA-12(a)[2]{1}{2} | | для обмеження наслідків від подій, пов'язаних з ланцюгом постачання |
| SA-12(a)[2]{2} | системного компонента: | | |
| SA-12(a)[2]{2}{1} | | для обмеження шкоди від подій, пов'язаних з ланцюгом постачання |
| SA-12(a)[2]{2}{2} | | для обмеження наслідків від подій, пов'язаних з ланцюгом постачання |
| SA-12(a)[2]{3} | системної служби | | |
| SA-12(a)[2]{3}{1} | | для обмеження шкоди від подій, пов'язаних з ланцюгом постачання |
| SA-12(a)[2]{3}{2} | | для обмеження наслідків від подій, пов'язаних з ланцюгом постачання |
| SA-12(b) | SA-12(b)[1] | SA-12(b)[1][1] | організація визначає документ, в якому документують обрані заходи безпеки ланцюга постачання | | |
| SA-12(b)[1][2] | організація визначає документ, в якому документують впроваджені заходи безпеки ланцюга постачання | | |
| SA-12(b)[2] | задокументувати обрані заходи безпеки ланцюга постачання в: | | | |
| SA-12(b)[2][1] | | плани безпеки та приватності | |
| SA-12(b)[2][2] | | план управління ризиками ланцюга постачання | |
| SA-12(b)[2][3] | | визначений організацією документ | |
| SA-12(b)[3] | задокументувати впроваджені заходи безпеки ланцюга постачання в: | | | |
| SA-12(b)[3][1] | | плани безпеки та приватності | |
| SA-12(b)[3][2] | | план управління ризиками ланцюга постачання | |
| SA-12(b)[3][3] | | визначений організацією документ | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; процедури, що стосуються інтеграції вимог інформаційної безпеки до процесу придбання; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; перелік загроз ланцюгу постачання; перелік гарантій безпеки, які слід вжити проти загроз ланцюгу постачання; документація життєвого циклу розробки системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для визначення запобіжних заходів та захисту від загроз ланцюгу постачання; автоматизовані механізми, що підтримують та, або впроваджують запобіжні заходи для загроз ланцюгу постачання]. | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-12(1) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - СТРАТЕГІЇ, ІНСТРУМЕНТИ ТА МЕТОДИ ЗАКУПІВЕЛЬ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-12(1)[1] | SA-12(1)[1][1] | організація визначає стратегії закупівель | |
| SA-12(1)[1][2] | організація визначає інструменти контракту | |
| SA-12(1)[1][3] | організація визначає методи закупівель | |
| SA-12(1)[2] | SA-12(1)[2][1] | застосовувати для захисту від загроз ланцюга постачання: | |
| SA-12(1)[2][1][1] | визначені організацією стратегії закупівель |
| SA-12(1)[2][1][2] | визначені організацією інструменти контракту та |
| SA-12(1)[2][1][3] | визначені організацією методи закупівель |
| SA-12(1)[2][2] | застосовувати для виявлення ризиків ланцюга постачання: | |
| SA-12(1)[2][2][1] | визначені організацією стратегії закупівель |
| SA-12(1)[2][2][2] | визначені організацією інструменти контракту та |
| SA-12(1)[2][2][3] | визначені організацією методи закупівель |
| SA-12(1)[2][3] | застосовувати для пом'якшення ризиків ланцюга постачання: | |
| SA-12(1)[2][3][1] | визначені організацією стратегії закупівель |
| SA-12(1)[2][3][2] | визначені організацією інструменти контракту та |
| SA-12(1)[2][3][3] | визначені організацією методи закупівель |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; процедури, що стосуються інтеграції вимог інформаційної безпеки до процесу придбання; процедури, що стосуються інтеграції стратегій придбання, інструментів контракту та методів закупівлі в процес придбання; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційних систем або послуг; замовлення, заявки на придбання для інформаційної системи; компонент системи; або обслуговування інформаційної системи від постачальників; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для визначення та використання спеціальних стратегій придбання, контрактних інструментів та методів закупівель; автоматизовані механізми, що підтримують та, або впроваджують визначення та використання спеціальних стратегій придбання, інструментів контракту та методів закупівель]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-12(2) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - АНАЛІЗ ПОСТАЧАЛЬНИКІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-12(2)[1] | організація визначає частоту, з якою необхідно проводити аналіз ризиків, пов'язаних з ланцюгом постачання | |
| SA-12(2)[2] | Проводити аналіз ризиків, з визначеною організацією частотою, пов'язаних з ланцюгом постачання, а саме з: | |
| SA-12(2)[2]{1} | постачальниками та системою |
| SA-12(2)[2]{2} | постачальниками та системним компонентом |
| SA-12(2)[2]{3} | постачальниками та системною службою |
| SA-12(2)[2]{4} | підрядниками та системою |
| SA-12(2)[2]{5} | підрядниками та системним компонентом |
| SA-12(2)[2]{6} | підрядниками та системною службою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; процедури, що стосуються інтеграції вимог інформаційної безпеки до процесу придбання; записи перевірок належної перевірки постачальників; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для проведення перевірок постачальників; автоматизовані механізми, що підтримують та, або впроваджують відгуки постачальників]. | | |

|  |  |
| --- | --- |
| SA-12(3) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - НАДІЙНЕ ПЕРЕВЕЗЕННЯ ТА ЗБЕРІГАННЯ |
|  | [Вилучено: включено до SA-12(1)]. |

|  |  |
| --- | --- |
| SA-12(4) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ДИВЕРСИФІКАЦІЯ ПОСТАЧАЛЬНИКІВ |
|  | [Вилучено: включено до SA-12(13)]. |

|  |  |  |
| --- | --- | --- |
| SA-12(5) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОБМЕЖЕННЯ ШКОДИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-12(5)[1] | організація визначає заходи безпеки для обмеження шкоди від потенційних зловмисників, дії яких спрямовані на порушення безпеки ланцюга постачання |
| SA-12(5)[2] | використовувати визначені організацією заходи безпеки для обмеження шкоди від потенційних зловмисників, дії яких спрямовані на порушення безпеки ланцюга постачання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика управління конфігурацією; процедури, що стосуються захисту ланцюга постачання; процедури, що стосуються інтеграції вимог інформаційної безпеки до процесу придбання; процедури, що стосуються базової конфігурації інформаційної системи; план управління конфігурацією; проєктна документація інформаційної системи; архітектура інформаційної системи та відповідна документація конфігурації; тендерна документація; документація про придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; перелік гарантій безпеки, які слід вжити для захисту організаційного ланцюжка постачання від потенційних загроз ланцюгу постачання; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для визначення та застосування запобіжних заходів для обмеження шкоди від зловмисників організаційного ланцюжка постачання; автоматизовані механізми, що підтримують та, або впроваджують визначення та використання гарантій для захисту організаційного ланцюжка постачання]. | |

|  |  |
| --- | --- |
| SA-12(6) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - МІНІМІЗАЦІЯ ЧАСУ ЗАКУПІВЕЛЬ |
|  | [Вилучено: включено до SA-12(1)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-12(7) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОЦІНКИ ПЕРЕД ВИБОРОМ, ПРИЙНЯТТЯМ ТА ОНОВЛЕННЯМ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-12(7)[1] | оцінювати систему до моменту: | |
| SA-12(7)[1]{1} | вибору |
| SA-12(7)[1]{2} | прийняття |
| SA-12(7)[1]{3} | модифікації |
| SA-12(7)[1]{4} | оновлення |
| SA-12(7)[2] | оцінювати системний компонент до моменту: | |
| SA-12(7)[2]{1} | вибору |
| SA-12(7)[2]{2} | прийняття |
| SA-12(7)[2]{3} | модифікації |
| SA-12(7)[2]{4} | оновлення |
| SA-12(7)[3] | оцінювати системну службу до моменту: | |
| SA-12(7)[3]{1} | вибору |
| SA-12(7)[3]{2} | прийняття |
| SA-12(7)[3]{3} | модифікації |
| SA-12(7)[3]{4} | оновлення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; процедури, що стосуються інтеграції вимог інформаційної безпеки до процесу придбання; результати тестування та оцінки безпеки; результати оцінки вразливості; результати тестування на проникнення; результати оцінки організаційних ризиків; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для проведення оцінок перед відбором, прийняттям чи оновленням; автоматизовані механізми, що підтримують та, або впроваджують проведення оцінок перед відбором, прийняттям чи оновленням]. | | |

|  |  |  |
| --- | --- | --- |
| SA-12(8) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ВИКОРИСТАННЯ ВСЕБІЧНОЇ РОЗВІДУВАЛЬНОЇ ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-12(8)[1] | використовувати всебічну розвідувальну інформацію для аналізу ризику ланцюга постачання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; тендерна документація; документація про придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; записи аналізів розвідувальних даних із усіх джерел; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для використання аналізу всіх джерел постачальників та потенційних постачальників; автоматизовані механізми, що підтримують та, або впроваджують використання аналізу всіх джерел постачальників та потенційних постачальників]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-12(9) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОПЕРАЦІЙНА БЕЗПЕКА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-12(9)[1] | організація визначає заходи операційної безпеки (OPSEC) | |
| SA-12(9)[2] | застосовувати визначені організацією заходи операційної безпеки (OPSEC) для захисту інформації, пов'язаної з ланцюгом постачання для: | |
| SA-12(9)[2]{1} | системи |
| SA-12(9)[2]{2} | компонентів системи |
| SA-12(9)[2]{3} | системної служби |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; тендерна документація; документація про придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; записи аналізів розвідувальних даних з усіх джерел; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для визначення та використання гарантій OPSEC; автоматизовані механізми, що підтримують та, або впроваджують визначення та застосування гарантій OPSEC]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-12(10) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ПЕРЕВІРКА НА СПРАВЖНІСТЬ І НЕ ЗМІНЕНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-12(10)[1] | організація визначає заходи безпеки підтвердити, що отримана: | |
| SA-12(10)[1]{1} | система є справжньою і не були змінені |
| SA-12(10)[1]{2} | компонент системи є справжнім і не був змінений |
| SA-12(10)[2] | використовувати визначені організацією заходи безпеки, щоб підтвердити, що отримана: | |
| SA-12(10)[2]{1} | система є справжньою і не були змінені |
| SA-12(10)[2]{2} | компонент системи є справжнім і не був змінений |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; процедури стосуються інтеграції вимог інформаційної безпеки в процес придбання; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; доказова документація (включаючи застосовні конфігурації) із зазначенням інформаційної системи, компонента системи чи служби інформаційної системи є справжньою і не змінювалась; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для визначення та використання гарантій перевірки; автоматизовані механізми, що підтримують та, або впроваджують визначення та застосовують гарантії валідації]. | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SA-12(11) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ТЕСТУВАННЯ ТА АНАЛІЗ НА ПРОНИКНЕННЯ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| SA-12(11)[1] | SA-12(11)[1]{1} | | організація визначає елементи ланцюга постачання | | | | |
| SA-12(11)[1]{2] | | організація визначає процеси ланцюга постачання | | | | |
| SA-12(11)[1]{3} | | організація визначає суб'єкти ланцюга постачання | | | | |
| SA-12(11)[2] | використовувати (один або більше): | | | | | | |
| SA-12(11)[2]{1} | організаційний аналіз, щодо визначених організацією: | | | | | |
| SA-12(11)[2]{1}[1] | | елементів ланцюга постачання, пов'язаних з: | | | |
| SA-12(11)[2]{1}[1]{1} | системою | | |
| SA-12(11)[2]{1}[1]{2} | системним компонентом | | |
| SA-12(11)[2]{1}[1]{3} | системною службою | | |
| SA-12(11)[2]{1}[2] | | процесів ланцюга постачання, пов'язаних з: | | | |
| SA-12(11)[2]{1}[2]{1} | | системою | |
| SA-12(11)[2]{1}[2]{2} | | системним компонентом | |
| SA-12(11)[2]{1}[2]{3} | | системною службою | |
| SA-12(11)[2]{1}[3] | | суб'єктів ланцюга постачання, які пов'язані з системою, системним компонентом або системною службою | | | |
| SA-12(11)[2]{1}[3]{1} | | | системою |
| SA-12(11)[2]{1}[3]{2} | | | системним компонентом |
| SA-12(11)[2]{1}[3]{3} | | | системною службою |
| SA-12(11)[2]{2} | незалежний аналіз третіх сторін, щодо визначених організацією: | | | | | |
| SA-12(11)[2]{2}[1] | | елементів ланцюга постачання, пов'язаних з: | | | |
| SA-12(11)[2]{2}[1]{1} | системою | | |
| SA-12(11)[2]{2}[1]{2} | системним компонентом | | |
| SA-12(11)[2]{2}[1]{3} | системною службою | | |
| SA-12(11)[2]{2}[2] | | процесів ланцюга постачання, пов'язаних з: | | | |
| SA-12(11)[2]{2}[2]{1} | | системою | |
| SA-12(11)[2]{2}[2]{2} | | системним компонентом | |
| SA-12(11)[2]{2}[2]{3} | | системною службою | |
| SA-12(11)[2]{2}[3] | | суб'єктів ланцюга постачання, які пов'язані з системою, системним компонентом або системною службою | | | |
| SA-12(11)[2]{2}[3]{1} | | | системою |
| SA-12(11)[2]{2}[3]{2} | | | системним компонентом |
| SA-12(11)[2]{2}[3]{3} | | | системною службою |
| SA-12(11)[2]{3} | організаційне тестування на проникнення щодо визначених організацією: | | | | | |
| SA-12(11)[2]{3}[1] | | елементів ланцюга постачання, пов'язаних з: | | | |
| SA-12(11)[2]{3}[1]{1} | системою | | |
| SA-12(11)[2]{3}[1]{2} | системним компонентом | | |
| SA-12(11)[2]{3}[1]{3} | системною службою | | |
| SA-12(11)[2]{3}[2] | | процесів ланцюга постачання, пов'язаних з: | | | |
| SA-12(11)[2]{3}[2]{1} | | системою | |
| SA-12(11)[2]{3}[2]{2} | | системним компонентом | |
| SA-12(11)[2]{3}[2]{3} | | системною службою | |
| SA-12(11)[2]{3}[3] | | суб'єктів ланцюга постачання, які пов'язані з системою, системним компонентом або системною службою | | | |
| SA-12(11)[2]{3}[3]{1} | | | системою |
| SA-12(11)[2]{3}[3]{2} | | | системним компонентом |
| SA-12(11)[2]{3}[3]{3} | | | системною службою |
| SA-12(11)[2]{4} | незалежне тестування на проникнення третіх сторін щодо визначених організацією: | | | | | |
| SA-12(11)[2]{4}[1] | | елементів ланцюга постачання, пов'язаних з: | | | |
| SA-12(11)[2]{4}[1]{1} | системою | | |
| SA-12(11)[2]{4}[1]{2} | системним компонентом | | |
| SA-12(11)[2]{4}[1]{3} | системною службою | | |
| SA-12(11)[2]{4}[2] | | процесів ланцюга постачання, пов'язаних з: | | | |
| SA-12(11)[2]{4}[2]{1} | | системою | |
| SA-12(11)[2]{4}[2]{2} | | системним компонентом | |
| SA-12(11)[2]{4}[2]{3} | | системною службою | |
| SA-12(11)[2]{4}[3] | | суб'єктів ланцюга постачання, які пов'язані з системою, системним компонентом або системною службою | | | |
| SA-12(11)[2]{4}[3]{1} | | | системою |
| SA-12(11)[2]{4}[3]{2} | | | системним компонентом |
| SA-12(11)[2]{4}[3]{3} | | | системною службою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються захисту ланцюга постачання; докази організаційного аналізу, незалежного аналізу, тестування на організаційне проникнення та, або незалежного тестування на проникнення; перелік елементів, процесів та суб’єктів ланцюга постачання (пов’язаних з інформаційною системою, компонентом системи чи послугою інформаційної системи), що підлягають аналізу та, або тестуванню; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за захист ланцюга постачання; організаційний персонал, відповідальний за аналіз та, або тестування елементів, процесів та суб’єктів ланцюга постачання].  Перевірка: [ВИБІР: Організаційні процеси для визначення та використання методів аналізу, тестування елементів, процесів та суб’єктів ланцюга постачання; автоматизовані механізми, що підтримують та, або здійснюють аналіз, тестування елементів, процесів та суб'єктів ланцюга постачання]. | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SA-12 | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - УГОДИ ПРО ПОВІДОМЛЕННЯ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| SA-12(a) | SA-12(a)[1] | організація визначає заходи безпеки ланцюга постачання для захисту від ризиків ланцюга постачання | | | | |
| SA-12(a)[2] | впровадити визначені організацією заходи безпеки ланцюга постачання для захисту від ризиків ланцюга постачання для: | | | | |
| SA-12(a)[2]{1} | | системи: | | |
| SA-12(a)[2]{1}{1} | | для обмеження шкоди від подій, пов'язаних з ланцюгом постачання |
| SA-12(a)[2]{1}{2} | | для обмеження наслідків від подій, пов'язаних з ланцюгом постачання |
| SA-12(a)[2]{2} | | системного компонента: | | |
| SA-12(a)[2]{2}{1} | | для обмеження шкоди від подій, пов'язаних з ланцюгом постачання |
| SA-12(a)[2]{2}{2} | | для обмеження наслідків від подій, пов'язаних з ланцюгом постачання |
| SA-12(a)[2]{3} | | системної служби: | | |
| SA-12(a)[2]{3}{1} | | для обмеження шкоди від подій, пов'язаних з ланцюгом постачання |
| SA-12(a)[2]{3}{2} | | для обмеження наслідків від подій, пов'язаних з ланцюгом постачання |
| SA-12(b) | SA-12(b)[1] | | організація визначає документ, у якому необхідно задокументовувати: | | | |
| SA-12(b)[1][1] | | обрані заходи безпеки ланцюга постачання | |
| SA-12(b)[1][2] | | впроваджені заходи безпеки ланцюга постачання | |
| SA-12(b)[2] | | задокументувати обрані заходи безпеки ланцюга постачання в: | | | |
| SA-12(b)[2]{1} | | плани безпеки та приватності; | |
| SA-12(b)[2]{2} | | план управління ризиками ланцюга постачання; | |
| SA-12(b)[2]{3} | | визначений організацією документ | |
| SA-12(b)[3] | | задокументувати впроваджені заходи безпеки ланцюга постачання в: | | | |
| SA-12(b)[3]{1} | | плани безпеки та приватності | |
| SA-12(b)[3]{2} | | план управління ризиками ланцюга постачання | |
| SA-12(b)[3]{3} | | визначений організацією документ | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-12(1) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - СТРАТЕГІЇ, ІНСТРУМЕНТИ ТА МЕТОДИ ЗАКУПІВЕЛЬ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-12(1)[1] | SA-12(1)[1][1] | організація визначає стратегії закупівель | |
| SA-12(1)[1][2] | організація визначає інструменти контракту | |
| SA-12(1)[1][3] | організація визначає методи закупівель | |
| SA-12(1)[2] | SA-12(1)[2][1] | застосовувати визначені організацією стратегії закупівель для: | |
| SA-12(1)[2][1][1] | захисту від загроз |
| SA-12(1)[2][1][2] | виявлення ризиків ланцюга постачання |
| SA-12(1)[2][1][3] | пом'якшення ризиків ланцюга постачання |
| SA-12(1)[2][2] | застосовувати визначені організацією інструменти контракту для: | |
| SA-12(1)[2][2][1] | захисту від загроз |
| SA-12(1)[2][2][2] | виявлення ризиків ланцюга постачання |
| SA-12(1)[2][2][3] | пом'якшення ризиків ланцюга постачання |
| SA-12(1)[2][3] | застосовувати методи закупівель для: | |
| SA-12(1)[2][3][1] | захисту від загроз |
| SA-12(1)[2][3][2] | виявлення ризиків ланцюга постачання |
| SA-12(1)[2][3][3] | пом'якшення ризиків ланцюга постачання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-12(2) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - АНАЛІЗ ПОСТАЧАЛЬНИКІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-12(2)[1] | організація визначає частоту, з якою необхідно проводити аналіз ризиків, пов'язаних з ланцюгом постачання | | |
| SA-12(2)[2] | проводити аналіз ризиків, пов'язаних з ланцюгом постачання, а сааме: | | |
| SA-12(2)[2]{1} | SA-12(2)[2]{1}{1} | з постачальниками та системою, які вони надають з визначеною організацією частотою |
| SA-12(2)[2]{1}{2} | з постачальниками та системним компонентом, з визначеною організацією частотою |
| SA-12(2)[2]{1}{3} | з постачальниками та системною службою, з визначеною організацією частотою |
| SA-12(2)[2]{2} | SA-12(2)[2]{2}{1} | з підрядниками та системою, з визначеною організацією частотою |
| SA-12(2)[2]{2}{2} | з підрядниками та системним компонентом, з визначеною організацією частотою |
| SA-12(2)[2]{2}{3} | з підрядниками та системною службою, з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | | |

|  |  |
| --- | --- |
| SA-12(3) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - НАДІЙНЕ ПЕРЕВЕЗЕННЯ ТА ЗБЕРІГАННЯ |
|  | [Вилучено: включено до SA-12(1)]. |

|  |  |
| --- | --- |
| SA-12(4) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ДИВЕРСИФІКАЦІЯ ПОСТАЧАЛЬНИКІВ |
|  | [Вилучено: включено до SA-12(13)]. |

|  |  |  |
| --- | --- | --- |
| SA-12(5) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОБМЕЖЕННЯ ШКОДИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-12(5)[1] | організація визначає заходи безпеки для обмеження шкоди від потенційних зловмисників |
| SA-12(5)[2] | використовувати визначені організацією заходи безпеки для обмеження шкоди від потенційних зловмисників, дія яких спрямована на порушення безпеки ланцюга постачання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | |

|  |  |
| --- | --- |
| SA-12(6) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - МІНІМІЗАЦІЯ ЧАСУ ЗАКУПІВЕЛЬ |
|  | [Вилучено: включено до SA-12(1)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-12(7) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОЦІНКИ ПЕРЕД ВИБОРОМ, ПРИЙНЯТТЯМ ТА ОНОВЛЕННЯМ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-12(7){1} | оцінювати систему до моменту: | |
| SA-12(7){1}{1} | вибору |
| SA-12(7){1}{2} | прийняття |
| SA-12(7){1}{3} | модифікації |
| SA-12(7){1}{4} | оновлення |
| SA-12(7){2} | оцінювати системний компонент до моменту: | |
| SA-12(7){1}{1} | вибору |
| SA-12(7){1}{2} | прийняття |
| SA-12(7){1}{3} | модифікації |
| SA-12(7){1}{4} | оновлення |
| SA-12(7){3} | оцінювати системну службу до моменту: | |
| SA-12(7){1}{1} | вибору |
| SA-12(7){1}{2} | прийняття |
| SA-12(7){1}{3} | модифікації |
| SA-12(7){1}{4} | оновлення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | |

|  |  |  |
| --- | --- | --- |
| SA-12(8) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ВИКОРИСТАННЯ ВСЕБІЧНОЇ РОЗВІДУВАЛЬНОЇ ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-12(8)[1] | використовувати всебічну розвідувальну інформацію для аналізу ризику ланцюга постачання. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-12(9) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОПЕРАЦІЙНА БЕЗПЕКА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-12(9)[1] | організація визначає заходи операційної безпеки (OPSEC) для захисту інформації, пов'язаної з ланцюгом постачання | |
| SA-12(9)[2] | застосовувати визначені організацією заходи операційної безпеки (OPSEC) для захисту інформації, пов'язаної з ланцюгом постачання для: | |
| SA-12(9)[2]{1} | системи |
| SA-12(9)[2]{2} | компонента системи |
| SA-12(9)[2]{3} | системної служби |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-12(10) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ПЕРЕВІРКА НА СПРАВЖНІСТЬ І НЕ ЗМІНЕНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-12(10)[1] | організація визначає заходи безпеки для підтвердження справжності: | |
| SA-12(10)[1]{1} | системи |
| SA-12(10)[1]{2} | компонента системи |
| SA-12(10)[2] | використовувати визначені організацією заходи безпеки, щоб підтвердити, що отримана: | |
| SA-12(10)[2]{1} | система є справжньою і не була змінена |
| SA-12(10)[2]{2} | компонент системи є справжнім і не був змінений |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SA-12(11) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ТЕСТУВАННЯ ТА АНАЛІЗ НА ПРОНИКНЕННЯ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SA-12(11)[1] | SA-12(11)[1][1] | | організація визначає елементи ланцюга постачання | | |
| SA-12(11)[1][2] | | організація визначає процеси ланцюга постачання | | |
| SA-12(11)[1][3] | | організація визначає суб'єкти ланцюга постачання | | |
| SA-12(11)[2] | використовувати (один або більше): | | | | |
| SA-12(11)[2]{1} | організаційний аналіз: | | | |
|  | SA-12(11)[2]{1}[1] | | елементів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{1}[1]{1} | системою |
| SA-12(11)[2]{1}[1]{2} | системним компонентом |
| SA-12(11)[2]{1}[1]{3} | системною службою |
| SA-12(11)[2]{1}[2] | | процесів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{1}[2]{1} | системою |
| SA-12(11)[2]{1}[2]{2} | системним компонентом |
| SA-12(11)[2]{1}[2]{3} | системною службою |
| SA-12(11)[2]{1}[3] | | суб'єктів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{1}[3]{1} | системою |
| SA-12(11)[2]{1}[3]{2} | системним компонентом |
| SA-12(11)[2]{1}[3]{3} | системною службою |
| SA-12(11)[2]{2} | незалежний аналіз третіх сторін, | | | |
| SA-12(11)[2]{2}[1] | | елементів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{2}[1]{1} | системою |
| SA-12(11)[2]{2}[1]{2} | системним компонентом |
| SA-12(11)[2]{2}[1]{3} | системною службою |
| SA-12(11)[2]{2}[2] | | процесів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{2}[2]{1} | системою |
| SA-12(11)[2]{2}[2]{2} | системним компонентом |
| SA-12(11)[2]{2}[2]{3} | системною службою |
| SA-12(11)[2]{2}[3] | | суб'єктів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{2}[3]{1} | системою |
| SA-12(11)[2]{2}[3]{2} | системним компонентом |
| SA-12(11)[2]{2}[3]{3} | системною службою |
| SA-12(11)[2]{3} | організаційне тестування на проникнення, | | | |
| SA-12(11)[2]{3}[1] | | елементів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{3}[1]{1} | системою |
| SA-12(11)[2]{3}[1]{2} | системним компонентом |
| SA-12(11)[2]{3}[1]{3} | системною службою |
| SA-12(11)[2]{3}[2] | | процесів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{3}[2]{1} | системою |
| SA-12(11)[2]{3}[2]{2} | системним компонентом |
| SA-12(11)[2]{3}[2]{3} | системною службою |
| SA-12(11)[2]{3}[3] | | суб'єктів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{3}[3]{1} | системою |
| SA-12(11)[2]{3}[3]{2} | системним компонентом |
| SA-12(11)[2]{3}[3]{3} | системною службою |
| SA-12(11)[2]{4} | незалежне тестування на проникнення третіх сторін, щодо визначених організацією: | | | |
| SA-12(11)[2]{4}[1] | | елементів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{4}[1]{1} | системою |
| SA-12(11)[2]{4}[1]{2} | системним компонентом |
| SA-12(11)[2]{4}[1]{3} | системною службою |
| SA-12(11)[2]{4}[2] | | процесів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{4}[2]{1} | системою |
| SA-12(11)[2]{4}[2]{2} | системним компонентом |
| SA-12(11)[2]{4}[2]{3} | системною службою |
| SA-12(11)[2]{4}[3] | | суб'єктів ланцюга постачання, що пов'язані з: | |
| SA-12(11)[2]{4}[3]{1} | системою |
| SA-12(11)[2]{4}[3]{2} | системним компонентом |
| SA-12(11)[2]{4}[3]{3} | системною службою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SA-12(12) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - УГОДИ ПРО ПОВІДОМЛЕННЯ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SA-12(12)[1] | організація визначає інформацію, яка необхідна для встановлення: | | | | |
| SA-12(12)[1][1] | угод з суб'єктами | | | |
| SA-12(12)[1][2] | процедури з суб'єктами | | | |
| SA-12(12)[2] | SA-12(12)[2][1] | встановлювати угоди з суб'єктами, які беруть участь у ланцюжку постачання або для (один або більше): | | | |
| SA-12(12)[2][1]{1} | системи | | |
| SA-12(12)[2][1]{1}[1] | повідомлення про компрометацію ланцюжка постачання | |
| SA-12(12)[2][1]{1}[2] | SA-12(12)[2][1]{1}[2]{1} | результати оцінок або |
| SA-12(12)[2][1]{1}[2]{2} | результати аудитів |
| SA-12(12)[2][1]{1}[3] | визначена організацією інформація | |
| SA-12(12)[2][1]{2} | компоненту системи | | |
| SA-12(12)[2][1]{2}[1] | повідомлення про компрометацію ланцюжка постачання | |
| SA-12(12)[2][1]{2}[2] | SA-12(12)[2][1]{2}[2]{1} | результати оцінок або |
| SA-12(12)[2][1]{2}[2]{2} | результати аудитів |
| SA-12(12)[2][1]{2}[3] | визначена організацією інформація | |
| SA-12(12)[2][1]{3} | системної служби | | |
| SA-12(12)[2][1]{3}[1] | повідомлення про компрометацію ланцюжка постачання | |
| SA-12(12)[2][1]{3}[2] | SA-12(12)[2][1]{3}[2]{1} | результати оцінок або |
| SA-12(12)[2][1]{3}[2]{2} | результати аудитів |
| SA-12(12)[2][1]{3}[3] | визначена організацією інформація | |
| SA-12(12)[2][2] | встановлювати процедури з суб'єктами, які беруть участь у ланцюжку постачання або для (один або більше): | | | |
| SA-12(12)[2][2]{1} | системи | | |
| SA-12(12)[2][2]{1}[1] | повідомлення про компрометацію ланцюжка постачання | |
| SA-12(12)[2][2]{1}[2] | SA-12(12)[2][2]{1}[2]{1} | результати оцінок або |
| SA-12(12)[2][2]{1}[2]{2} | результати аудитів |
| SA-12(12)[2][2]{1}[3] | визначена організацією інформація | |
| SA-12(12)[2][2]{2} | компоненту системи | | |
| SA-12(12)[2][2]{2}[1] | повідомлення про компрометацію ланцюжка постачання | |
| SA-12(12)[2][2]{2}[2] | SA-12(12)[2][2]{2}[2]{1} | результати оцінок або |
| SA-12(12)[2][2]{2}[2]{2} | результати аудитів |
| SA-12(12)[2][2]{2}[3] | визначена організацією інформація | |
| SA-12(12)[2][2]{3} | системної служби | | |
| SA-12(12)[2][2]{3}[1] | повідомлення про компрометацію ланцюжка постачання | |
| SA-12(12)[2][2]{3}[2] | SA-12(12)[2][2]{3}[2]{1} | результати оцінок або |
| SA-12(12)[2][2]{3}[2]{2} | результати аудитів |
| SA-12(12)[2][2]{3}[3] | визначена організацією інформація | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | | | | |

|  |  |
| --- | --- |
| SA-12(13) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - КОМПОНЕНТИ КРИТИЧНИХ СИСТЕМ |
|  | [Вилучено: включено до МA-6 та RA-9]. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SA-12(14) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ІДЕНТИЧНІСТЬ ТА ПРОСТЕЖУВАНІСТЬ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| SA-12(14)[1] | SA-12(14)[1][1] | організація визначає елементи ланцюга постачання | | | | |
| SA-12(14)[1][2] | організація визначає процеси ланцюга постачання | | | | |
| SA-12(14)[1][3] | організація визначає персонал ланцюга постачання | | | | |
| SA-12(14)[1][4] | організація визначає систем? | | | | |
| SA-12(14)[1][5] | організація визначає критичні компоненти системи | | | | |
| SA-12(14)[2] | SA-12(14)[2][1] | Встановити унікальну ідентифікацію визначених організацією: | | | | |
| SA-12(14)[2][1][1] | елементів ланцюга постачання, які пов'язані з визначеною організацією: | | | |
| SA-12(14)[2][1][1][1] | | системою | |
| SA-12(14)[2][1][1][2] | | критичними компонентами системи | |
| SA-12(14)[2][1][2] | процесів ланцюга постачання, які пов'язані з визначеною організацією: | | | |
| SA-12(14)[2][1][2][1] | | системою | |
| SA-12(14)[2][1][2][2] | | критичними компонентами системи | |
| SA-12(14)[2][1][3] | персоналу ланцюга постачання, які пов'язані з визначеною організацією: | | | |
| SA-12(14)[2][1][3][1] | | системою | |
| SA-12(14)[2][1][3][2] | | критичними компонентами системи | |
| SA-12(14)[2][2] | підтримувати унікальну ідентифікацію визначених організацією: | | | | |
| SA-12(14)[2][2][1] | | елементів ланцюга постачання, які пов'язані з визначеною організацією: | | |
| SA-12(14)[2][2][1][1] | | системою |
| SA-12(14)[2][2][1][2] | | критичними компонентами системи |
| SA-12(14)[2][2][2] | | процесів ланцюга постачання, які пов'язані з визначеною організацією: | | |
| SA-12(14)[2][2][2][1] | | системою |
| SA-12(14)[2][2][2][2] | | критичними компонентами системи |
| SA-12(14)[2][2][3] | | персоналу ланцюга постачання, які пов'язані з визначеною організацією: | | |
| SA-12(14)[2][2][3][1] | | системою |
| SA-12(14)[2][2][3][2] | | критичними компонентами системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-12(15) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ПРОЦЕСИ ДЛЯ УСУНЕННЯ НЕДОЛІКІВ АБО ДЕФЕКТІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-12(15)[1] | визначеним організацією персоналом ланцюга постачання | |
| SA-12(15)[2] | Впровадити процес або процеси для усунення: | |
| SA-12(15)[2]{1} | недоліків елементів ланцюга постачання у координації з визначеним організацією персоналом ланцюга постачання |
| SA-12(15)[2]{2} | дефектів елементів ланцюга постачання у координації з визначеним організацією персоналом ланцюга постачання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-12(16) | КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ПОХОДЖЕННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-12(16)[1] | SA-12(16)[1][1] | визначених організацією систем, | |
| SA-12(16)[1][2] | визначених організацією компонентів систем | |
| SA-12(16)[1][3] | визначених організацією, пов'язаних з ними даних | |
| SA-12(16)[2] | SA-12(16)[2][1] | документувати дійсне походження визначених організацією: | |
| SA-12(16)[2][1] | систем |
| SA-12(16)[2][2] | компонентів систем |
| SA-12(16)[2][3] | пов'язані з ними дані |
| SA-12(16)[2][1] | проводити моніторинг дійсного походження визначених організацією: | |
| SA-12(16)[2][1] | систем |
| SA-12(16)[2][2] | компонентів систем |
| SA-12(16)[2][3] | пов'язані з ними дані |
| SA-12(16)[2][1] | підтримувати дійсне походження визначених організацією: | |
| SA-12(16)[2][1] | систем |
| SA-12(16)[2][2] | компонентів систем |
| SA-12(16)[2][3] | пов'язані з ними дані |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; міжорганізаційні угоди та процедури; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за захист ланцюжка постачання].  Перевірка: [ВИБІР: Організаційні процеси для встановлення міжорганізаційних домовленостей та процедур із суб’єктами ланцюга постачання]. | | | |

|  |  |
| --- | --- |
| SA-13 | ДОВІРЧІСТЬ |
|  | [Вилучено: Включено до SA-8]. |

|  |  |
| --- | --- |
| SA-14 | АНАЛІЗ КРИТИЧНОСТІ |
|  | [Вилучено: Включено до RA-9] |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SA-15 | ПРОЦЕСИ, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ | | | | | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | | | | | |
| SA-15(a)  SA-15(b) | SA-15(a){1} | вимагати від розробника системи, слідувати документованому процесу розробки, який: | | | | | | | | | |
| SA-15(a){1}(1) | | явно задовільняє вимогам безпеки | | | | | | | |
| SA-15(a){1}(2) | | SA-15(a){1}(2)[1] | | визначає стандарти, які використовуються в процесі розробки | | | | | |
| SA-15(a){1}(2)[2] | | визначає інструменти, які використовуються в процесі розробки | | | | | |
| SA-15(a){1}(3) | | SA-15(a){1}(3)[1] | | документує конкретні параметри інструментарію, що використовуються в процесі розробки | | | | | |
| SA-15(a){1}(3)[2] | | документує конкретні конфігурації інструментарію, що використовуються в процесі розробки; | | | | | |
| SA-15(a){1}(4) | | SA-15(a){1}(3)[1] | | документує конкретні параметри інструментарію, що використовуються в процесі розробки | | | | | |
| SA-15(a){1}(3)[2] | | документує конкретні конфігурації інструментарію, що використовуються в процесі розробки | | | | | |
| SA-15(a){1}(4)[1] | | SA-15(a){1}(4)[1][1] | | документує цілісність змін в (та, або): | | | |
| SA-15(a){1}(4)[1][1]{1} | | | процесах, які використовуються в розробці |
| SA-15(a){1}(4)[1][1]{2} | | | інструментах, які використовуються в розробці |
| SA-15(a){1}(4)[1][2] | | управляє цілісністю змін в (та, або): | | | |
| SA-15(a){1}(4)[1][2]{1} | | | процесах, які використовуються в розробці |
| SA-15(a){1}(4)[1][2]{2} | | | інструментах, які використовуються в розробці |
| SA-15(a){1}(4)[1][3] | | забезпечує цілісність змін в (та, або): | | | |
| SA-15(a){1}(4)[1]{1} | | | процесах, які використовуються в розробці |
| SA-15(a){1}(4)[1]{2} | | | інструментах, які використовуються в розробці |
| SA-15(a){2} | вимагати від розробника системного компонента слідувати документованому процесу розробки, який: | | | | | | | | | |
| SA-15(a){2}(1) | | явно задовільняє вимогам безпеки | | | | | | | |
| SA-15(a){2}(2) | | SA-15(a){2}(2)[1] | | визначає стандарти, які використовуються в процесі розробки; | | | | | |
| SA-15(a){2}(2)[2] | | визначає інструменти, які використовуються в процесі розробки; | | | | | |
| SA-15(a){2}(3) | | SA-15(a){2}(3)[1] | | документує конкретні параметри інструментарію, що використовуються в процесі розробки; | | | | | |
| SA-15(a){2}(3)[2] | | документує конкретні конфігурації інструментарію, що використовуються в процесі розробки; | | | | | |
| SA-15(a){2}(4) | | SA-15(a){2}(3)[1] | | документує конкретні параметри інструментарію, що використовуються в процесі розробки | | | | | |
| SA-15(a){2}(3)[2] | | документує конкретні конфігурації інструментарію, що використовуються в процесі розробки | | | | | |
| SA-15(a){2}(4)[1] | | SA-15(a){2}(4)[1][1] | | документує цілісність змін в (та, або): | | | |
| SA-15(a){2}(4)[1][1]{1} | | | процесах, які використовуються в розробці |
| SA-15(a){2}(4)[1][1]{2} | | | інструментах, які використовуються в розробці |
| SA-15(a){2}(4)[1][2] | | управляє цілісністю змін в (та, або): | | | |
| SA-15(a){2}(4)[1][2]{1} | | | процесах, які використовуються в розробці |
| SA-15(a){2}(4)[1][2]{2} | | | інструментах, які використовуються в розробці |
| SA-15(a){2}(4)[1][3] | | забезпечує цілісність змін в (та, або): | | | |
| SA-15(a){2}(4)[1]{1} | | | процесах, які використовуються в розробці |
| SA-15(a){2}(4)[1]{2} | | | інструментах, які використовуються в розробці |
| SA-15(a){3} | Вимагати від розробника системної служби слідувати документованому процесу розробки, який: | | | | | | | | | |
| SA-15(a){3}(1) | | явно задовільняє вимогам безпеки | | | | | | | |
| SA-15(a){3}(2) | | SA-15(a){3}(2)[1] | | визначає стандарти, які використовуються в процесі розробки; | | | | | |
| SA-15(a){3}(2)[2] | | визначає інструменти, які використовуються в процесі розробки; | | | | | |
| SA-15(a){3}(3) | | SA-15(a){3}(3)[1] | | документує конкретні параметри інструментарію, що використовуються в процесі розробки; | | | | | |
| SA-15(a){3}(3)[2] | | документує конкретні конфігурації інструментарію, що використовуються в процесі розробки; | | | | | |
| SA-15(a){3}(4) | | SA-15(a){3}(3)[1] | | документує конкретні параметри інструментарію, що використовуються в процесі розробки | | | | | |
| SA-15(a){3}(3)[2] | | документує конкретні конфігурації інструментарію, що використовуються в процесі розробки | | | | | |
| SA-15(a){3}(4)[1] | | SA-15(a){3}(4)[1][1] | | документує цілісність змін в (та, або): | | | |
| SA-15(a){3}(4)[1][1]{1} | | | процесах, які використовуються в розробці |
| SA-15(a){3}(4)[1][1]{2} | | | інструментах, які використовуються в розробці |
| SA-15(a){3}(4)[1][2] | | управляє цілісністю змін в (та, або): | | | |
| SA-15(a){3}(4)[1][2]{1} | | | процесах, які використовуються в розробці |
| SA-15(a){3}(4)[1][2]{2} | | | інструментах, які використовуються в розробці |
| SA-15(a){3}(4)[1][3] | | забезпечує цілісність змін в (та, або): | | | |
| SA-15(a){3}(4)[1]{1} | | | процесах, які використовуються в розробці |
| SA-15(a){3}(4)[1]{2} | | | інструментах, які використовуються в розробці |
| SA-15(b)[1] | | SA-15(b)[1][1] | | організація визначає вимоги до безпеки та приватності | | | | | | |
| SA-15(b)[1][2] | | організація визначає частоту, з якою необхідно ознайомлюватися з: | | | | | | |
| SA-15(b)[1][2][1] | | | | процесом розробки | | |
| SA-15(b)[1][2][2] | | | | стандартами | | |
| SA-15(b)[1][2][3] | | | | інструментами | | |
| SA-15(b)[1][2][4] | | | | параметрами інструментарію | | |
| SA-15(b)[1][2][5] | | | | конфігураціями інструментів | | |
| SA-15(b)[2] | | SA-15(b)[2][1] | | ознайомитися з процесом розробки з визначеною організацією частотою, щоб визначити, чи можуть: | | | | | | |
| SA-15(b)[2][1][1] | | обрані: | | | | |
| SA-15(b)[2][1][1][1] | | | процеси, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][1][1][2] | | | стандарти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][1][1][3] | | | інструменти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][1][1][4] | | | параметри, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][1][1][5] | | | конфігурації інструментів, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][1][2] | | використовувані | | | | |
| SA-15(b)[2][1][2][1] | | | процеси, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][1][2][2] | | | стандарти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][1][2][3] | | | інструменти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][1][2][4] | | | параметри, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][1][2][5] | | | конфігурації інструментів, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][2] | | ознайомитися зі стандартами з визначеною організацією частотою, щоб визначити, чи можуть: | | | | | | |
| SA-15(b)[2][2][1] | | обрані: | | | | |
| SA-15(b)[2][2][1][1] | | | процеси, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][2][1][2] | | | стандарти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][2][1][3] | | | інструменти, задовольнити визначені організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][2][1][4] | | | параметри, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][2][1][5] | | | конфігурації інструментів, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][2][2] | | використовувані | | | | |
| SA-15(b)[2][2][2][1] | | | процеси, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][2][2][2] | | | стандарти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][2][2][3] | | | інструменти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][2][2][4] | | | параметри, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][2][2][5] | | | конфігурації інструментів, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][3] | | ознайомитися з інструментами з визначеною організацією частотою, щоб визначити, чи можуть: | | | | | | |
| SA-15(b)[2][3][1] | | обрані: | | | | |
| SA-15(b)[2][3][1][1] | | | процеси задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][3][1][2] | | | стандарти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][3][1][3] | | | інструменти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][3][1][4] | | | параметри, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][3][1][5] | | | конфігурації інструментів, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][3][2] | | використовувані | | | | |
| SA-15(b)[2][3][2][1] | | | процеси, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][3][2][2] | | | стандарти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][3][2][3] | | | інструменти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][3][2][4] | | | параметри, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][3][2][5] | | | конфігурації інструментів, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][4] | | ознайомитися з параметрами інструментарію з визначеною організацією частотою, щоб визначити, чи можуть: | | | | | | |
| SA-15(b)[2][4][1] | | обрані: | | | | |
| SA-15(b)[2][4][1][1] | | | процеси, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][4][1][2] | | | стандарти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][4][1][3] | | | інструменти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][4][1][4] | | | параметри, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][4][1][5] | | | конфігурації інструментів, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][4][2] | | використовувані | | | | |
| SA-15(b)[2][4][2][1] | | | процеси, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][4][2][2] | | | стандарти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][4][2][3] | | | інструменти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][4][2][4] | | | параметри, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][4][2][5] | | | конфігурації інструментів, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][5] | | Ознайомитися з конфігураціями інструментів з визначеною організацією частотою, щоб визначити, чи можуть: | | | | | | |
| SA-15(b)[2][5][1] | | Обрані: | | | | |
| SA-15(b)[2][5][1][1] | | | процеси,  задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][5][1][2] | | | стандарти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][5][1][3] | | | інструменти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][5][1][4] | | | параметри, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][5][1][5] | | | конфігурації інструментів, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][5][2] | | використовувані | | | | |
| SA-15(b)[2][5][2][1] | | | процеси, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][5][2][2] | | | стандарти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][5][2][3] | | | інструменти, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][5][2][4] | | | параметри, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| SA-15(b)[2][5][2][5] | | | конфігурації інструментів, задовольнити визначеним організацією вимогам до безпеки та приватності | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІРІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; процедури, що стосуються інтеграції вимог безпеки в процесі розробки; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; документація розробника системи з переліком параметрів інструменту, посібників з налаштування, записів управління конфігурацією; змінити записи контролю; записи контролю конфігурації; задокументовані огляди процесу розробки, стандартів, інструментів та варіантів, конфігурацій інструментів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи]. | | | | | | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SA-15(1) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПОКАЗНИКИ ЯКОСТІ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SA-15(1)[1] | вимагати від розробника системи, компонента системи або системної служби: | | | |
| SA-15(1)[1](a) | визначити показники якості на початку процесу розробки | | |
| SA-15(1)[1](b) | SA-15(1)[1](b)[1] | SA-15(1)[1](b)[1][1] | організація визначає частоту, з якою необхідно надавати докази відповідності показникам якості |
| SA-15(1)[1](b)[1][2] | організація визначає етапи розгляду програми, на яких необхідно надавати докази відповідності показникам якості |
| SA-15(1)[1](b)[2] | надати докази відповідності показникам якості (один або більше): | |
| SA-15(1)[1](b)[2]{1} | визначена організацією частота |
| SA-15(1)[1](b)[2]{2} | визначені організацією етапи розгляду програми |
| SA-15(1)[1](b)[2]{3} | після постачання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; процедури, що стосуються інтеграції вимог безпеки до процесу придбання; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; перелік показників якості; документальне підтвердження відповідності показників якості; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-15(2) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ЗАСОБИ ВІДСТЕЖЕННЯ БЕЗПЕКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-15(2){1} | вимагати від розробника системи: | |
| SA-15(2){1}[1] | обирати засоби відстеження безпеки під час розробки |
| SA-15(2){1}[2] | використовувати засоби відстеження безпеки під час розробки |
| SA-15(2){2} | вимагати від розробника системного компонента: | |
| SA-15(2){2}[1] | обирати засоби відстеження безпеки під час розробки |
| SA-15(2){2}[2] | використовувати засоби відстеження безпеки під час розробки |
| SA-15(2){3} | вимагати від розробника системної служби: | |
| SA-15(2){3}[1] | обирати засоби відстеження безпеки під час розробки |
| SA-15(2){3}[2] | використовувати засоби відстеження безпеки під час розробки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; процедури, що стосуються інтеграції вимог безпеки до процесу придбання; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; перелік показників якості; документальне підтвердження відповідності показників якості; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи]. | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SA-15(3) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - АНАЛІЗ КРИТИЧНОСТІ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SA-15(3)[1] | SA-15(3)[1][1] | визначена організацією ширина аналізу критичності | | |
| SA-15(3)[1][2] | визначена організацією глибина аналізу критичності | | |
| SA-15(3)[1][3] | визначені організацією точки прийняття рішень в життєвому циклі розробки системи | | |
| SA-15(3)[2] | SA-15(3)[2]{1} | вимагати від розробника системи виконати аналіз критичності на визначену організацією: | | |
| SA-15(3)[2]{1}[1] | SA-15(3)[2]{1}[1]{1} | ширина |
| SA-15(3)[2]{1}[1]{2} | глибина |
| SA-15(3)[2]{1}[2] | точки прийняття рішень в життєвому циклі розробки системи | |
| SA-15(3)[2]{2} | вимагати від розробника системного компонента виконати аналіз критичності на визначену організацією: | | |
| SA-15(3)[2]{2}[1] | SA-15(3)[2]{2}[1]{1} | ширина |
| SA-15(3)[2]{2}[1]{2} | глибина |
| SA-15(3)[2]{2}[2] | точки прийняття рішень в життєвому циклі розробки системи | |
| SA-15(3)[2]{3} | вимагати від розробника системної служби виконати аналіз критичності на визначену організацією: | | |
| SA-15(3)[2]{3}[1] | SA-15(3)[2]{3}[1]{1} | ширина |
| SA-15(3)[2]{3}[1]{2} | глибина |
| SA-15(3)[2]{3}[2] | точки прийняття рішень в життєвому циклі розробки системи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; процедури, що стосуються вимог до аналізу критичності інформаційної системи, компонента системи або послуги інформаційної системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; документація з аналізу критичності; документація з аналізу впливу на бізнес; документація життєвого циклу розробки програмного забезпечення; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; відповідальність організаційного персоналу за проведення аналізу критичності; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для проведення аналізу критичності; автоматизовані механізми, що підтримують та, або впроваджують аналіз критичності]. | | | | |

|  |  |
| --- | --- |
| SA-15(4) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - МОДЕЛЮВАННЯ ЗАГРОЗ ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ |
|  | [Вилучено: Включено до SA-11(2)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-15(5) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ЗМЕНШЕННЯ ПОВЕРХНІ АТАКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-15(5)[1] | визначені організацією межі для зменшення поверхні атаки | |
| SA-15(5)[2] | SA-15(5)[2]{1} | вимагати від розробника системи, зменшити поверхню атаки до визначеної організацією межі |
| SA-15(5)[2]{2} | вимагати від розробника системного компонента зменшити поверхню атаки до визначеної організацією межі |
| SA-15(5)[2]{3} | вимагати від розробника системної служби зменшити поверхню атаки до визначеної організацією межі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; процедури, що стосуються зменшення поверхні атаки; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи або послуги інформаційної системи; проєктна документація інформаційної системи; схема мережі; налаштування конфігурації інформаційної системи та супутньої документації, що встановлюють, забезпечують визначені організацією порогові значення для зменшення поверхонь атаки; перелік обмежених портів, протоколів, функцій та послуг; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; відповідальність організаційного персоналу за порогові значення зменшення поверхні атаки; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для визначення порогів зменшення поверхні атаки]. | | |

|  |  |  |
| --- | --- | --- |
| SA-15(6) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПОСТІЙНЕ ВДОСКОНАЛЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-15(6){1} | Вимагає від розробника системи реалізувати явний процес для постійного вдосконалення процесу розробки. |
| SA-15(6){2} | Вимагає від розробника системного компонента реалізувати явний процес для постійного вдосконалення процесу розробки. |
| SA-15(6){3} | Вимагає від розробника системної служби реалізувати явний процес для постійного вдосконалення процесу розробки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; цілі та показники якості для вдосконалення процесу розробки системи; оцінки безпеки та, або огляди контролю якості процесу розробки системи; плани дій та етапи вдосконалення процесу розробки системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SA-15(7) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - АВТОМАТИЗОВАНИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SA-15(7){1} | вимагати від розробника системи: | | | |
| SA-15(7){1}(a) | SA-15(7){1}(a)[1] | організація визначає інструменти для виконання автоматизованого аналізу вразливостей | |
| SA-15(7){1}(a)[2] | виконувати автоматизований аналіз вразливостей за допомогою визначених організацією інструментів | |
| SA-15(7){1}(b) | визначити потенціал експлуатації для виявлених вразливостей | | |
| SA-15(7){1}(c) | визначити потенційні можливості зменшення ризику для вразливих місць | | |
| SA-15(7){1}(d) | SA-15(7){1}(d)[1] | SA-15(7){1}(d)[1]{1} | організація визначає персонал |
| SA-15(7){1}(d)[1]{2} | організація визначає посадових осіб |
| SA-15(7){1}(d)[2] | надавати результати аналізу визначеному організацією: | |
| SA-15(7){1}(d)[2]{1} | персоналу |
| SA-15(7){1}(d)[2]{2} | посадовим особам |
| SA-15(7){2} | вимагати від розробника компонента системи: | | | |
| SA-15(7){2}(a) | SA-15(7){2}(a)[1] | організація визначає інструменти для виконання автоматизованого аналізу вразливостей | |
| SA-15(7){2}(a)[2] | виконувати автоматизований аналіз вразливостей за допомогою визначених організацією інструментів | |
| SA-15(7){2}(b) | визначити потенціал експлуатації для виявлених вразливостей | | |
| SA-15(7){2}(c) | визначити потенційні можливості зменшення ризику для вразливих місць | | |
| SA-15(7){2}(d) | SA-15(7){2}(d)[1] | SA-15(7){2}(d)[1]{1} | організація визначає персонал |
| SA-15(7){2}(d)[1]{2} | організація визначає посадових осіб |
| SA-15(7){2}(d)[2] | надавати результати аналізу визначеному організацією: | |
| SA-15(7){2}(d)[2]{1} | персоналу |
| SA-15(7){2}(d)[2]{2} | посадовим особам |
| SA-15(7){3} | вимагати від розробника системної служби: | | | |
| SA-15(7){3}(a) | SA-15(7){3}(a)[1] | організація визначає інструменти для виконання автоматизованого аналізу вразливостей | |
| SA-15(7){3}(a)[2] | виконувати автоматизований аналіз вразливостей за допомогою визначених організацією інструментів | |
| SA-15(7){3}(b) | визначити потенціал експлуатації для виявлених вразливостей | | |
| SA-15(7){3}(c) | визначити потенційні можливості зменшення ризику для вразливих місць | | |
| SA-15(7){3}(d) | SA-15(7){3}(d)[1] | SA-15(7){3}(d)[1]{1} | організація визначає персонал |
| SA-15(7){3}(d)[1]{2} | організація визначає посадових осіб |
| SA-15(7){3}(d)[2] | надавати результати аналізу визначеному організацією: | |
| SA-15(7){3}(d)[2]{1} | персоналу |
| SA-15(7){3}(d)[2]{2} | посадовим особам |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; засоби аналізу вразливості та супутньої документації; звіти про оцінку ризиків; результати аналізу вразливості; звіти про пом'якшення вразливості; документація щодо стратегії зменшення ризику; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що здійснює автоматизований аналіз вразливості в інформаційній системі].  Перевірка: [ВИБІР: Організаційні процеси для аналізу вразливості інформаційних систем, системних компонентів або служб інформаційної системи, що розробляється; автоматизовані механізми, що підтримують та, або впроваджують аналіз вразливості інформаційних систем, компонентів системи або служб інформаційної системи, що розробляються]. | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-15(8) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПОВТОРНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЇ ПРО ЗАГРОЗИ ТА ВРАЗЛИВОСТІ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-15(8){1} | вимагати від розробника системи використовувати: | | |
| SA-15(8){1}[1] | моделювання загроз з аналогічних: | |
| SA-15(8){1}[1]{1} | Систем для інформування про поточний процес розробки |
| SA-15(8){1}[1]{2} | компонентів для інформування про поточний процес розробки |
| SA-15(8){1}[1]{3} | Служб систем для інформування про поточний процес розробки |
| SA-15(8){1}[2] | аналіз вразливостей з аналогічних: | |
| SA-15(8){1}[2]{1} | Систем для інформування про поточний процес розробки |
| SA-15(8){1}[2]{2} | компонентів для інформування про поточний процес розробки |
| SA-15(8){1}[2]{3} | Служб систем для інформування про поточний процес розробки |
| SA-15(8){2} | вимагати від розробника компонента системи використовувати: | | |
| SA-15(8){2}[1] | моделювання загроз з аналогічних: | |
| SA-15(8){2}[1]{1} | Систем для інформування про поточний процес розробки |
| SA-15(8){2}[1]{2} | компонентів для інформування про поточний процес розробки |
| SA-15(8){2}[1]{3} | Служб систем для інформування про поточний процес розробки |
| SA-15(8){2}[2] | аналіз вразливостей з аналогічних: | |
| SA-15(8){2}[2]{1} | Систем для інформування про поточний процес розробки |
| SA-15(8){2}[2]{2} | компонентів для інформування про поточний процес розробки |
| SA-15(8){2}[2]{3} | Служб систем для інформування про поточний процес розробки |
| SA-15(8){3} | вимагати від розробника системної служби використовувати: | | |
| SA-15(8){3}[1] | моделювання загроз з аналогічних: | |
| SA-15(8){3}[1]{1} | Систем для інформування про поточний процес розробки |
| SA-15(8){3}[1]{2} | компонентів для інформування про поточний процес розробки |
| SA-15(8){3}[1]{3} | Служб систем для інформування про поточний процес розробки |
| SA-15(8){3}[2] | аналіз вразливостей з аналогічних: | |
| SA-15(8){3}[2]{1} | Систем для інформування про поточний процес розробки |
| SA-15(8){3}[2]{2} | компонентів для інформування про поточний процес розробки |
| SA-15(8){3}[2]{3} | Служб систем для інформування про поточний процес розробки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; моделювання загроз та аналіз вразливості з подібних інформаційних систем, системних компонентів або служби інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи]. | | | |

|  |  |
| --- | --- |
| SA-15(9) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ВИКОРИСТАННЯ РЕАЛЬНИХ ДАНИХ |
|  | [Вилучено: Включено до SA-3(2)] |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-15(10) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-15(10){1} | вимагати від розробника системи: | |
| SA-15(10){1}[1] | надавати план реагування на інциденти |
| SA-15(10){1}[2] | реалізовувати план реагування на інциденти |
| SA-15(10){1}[3] | перевіряти план реагування на інциденти |
| SA-15(10){2} | вимагати від розробника системи, компонента системи або системної служби надавати, реалізовувати та перевіряти план реагування на інциденти. | |
| SA-15(10){2}[1] | надавати план реагування на інциденти |
| SA-15(10){2}[2] | реалізовувати план реагування на інциденти |
| SA-15(10){2}[3] | перевіряти план реагування на інциденти |
| SA-15(10){3} | вимагати від розробника системи, компонента системи або системної служби надавати, реалізовувати та перевіряти план реагування на інциденти. | |
| SA-15(10){3}[1] | надавати план реагування на інциденти |
| SA-15(10){3}[2] | реалізовувати план реагування на інциденти |
| SA-15(10){3}[3] | перевіряти план реагування на інциденти |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи або послуг; документація про придбання; заявна документація; угоди про рівень обслуговування; план реагування на аварії розробника; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-15(11) | ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - РЕЗЕРВУВАННЯ СИСТЕМИ АБО КОМПОНЕНТУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-15(11){1} | вимагати від розробника системи резервування: | | |
| SA-15(11){1}{1} | системи, яка буде: | |
| SA-15(11){1}{1}{1} | випущений разом з відповідними доказами, що підтверджують остаточну перевірку безпеки та приватності. |
| SA-15(11){1}{1}{2} | доставлений разом з відповідними доказами, що підтверджують остаточну перевірку безпеки та приватності. |
| SA-15(11){1}{2} | компоненти системи, яка буде: | |
| SA-15(11){1}{2}{1} | випущений разом з відповідними доказами, що підтверджують остаточну перевірку безпеки та приватності. |
| SA-15(11){1}{2}{2} | доставлений разом з відповідними доказами, що підтверджують остаточну перевірку безпеки та приватності. |
| SA-15(11){2} | вимагати від розробника системного компонента резервуваня: | | |
| SA-15(11){2}{1} | систему, яка буде: | |
| SA-15(11){2}{1}{1} | випущений разом з відповідними доказами, що підтверджують остаточну перевірку безпеки та приватності. |
| SA-15(11){2}{1}{2} | доставлений разом з відповідними доказами, що підтверджують остаточну перевірку безпеки та приватності. |
| SA-15(11){2}{2} | компоненти системи, яка буде: | |
| SA-15(11){2}{2}{1} | випущений разом з відповідними доказами, що підтверджують остаточну перевірку безпеки та приватності. |
| SA-15(11){2}{2}{2} | доставлений разом з відповідними доказами, що підтверджують остаточну перевірку безпеки та приватності. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи або послуг; документація про придбання; заявна документація; угоди про рівень обслуговування; план реагування на аварії розробника; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи]. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SA-16 | НАВЧАННЯ, ЩО НАДАЄТЬСЯ РОЗРОБНИКАМИ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SA-16[1] | організація визначає навчання правильному: | | | | |
| SA-16[1][1] | використанню: | | | |
| SA-16[1][1][1] | | реалізованих безпеки та приватності | |
| SA-16[1][1][2] | | функцій безпеки та приватності | |
| SA-16[1][1][3] | | заходів безпеки та приватності | |
| SA-16[1][1][4] | | механізмів безпеки та приватності | |
| SA-16[1][2] | функціонуванню | | | |
| SA-16[1][2][1] | | реалізованих безпеки та приватності | |
| SA-16[1][2][2] | | функцій безпеки та приватності | |
| SA-16[1][2][3] | | заходів безпеки та приватності | |
| SA-16[1][2][4] | | механізмів безпеки та приватності | |
| SA-16[2] | SA-16[2]{1} | вимагати від розробника системи надання визначеного організацією навчання правильному: | | | |
| SA-16[2]{1}[1] | використанню: | | |
| SA-16[2]{1}[1][1] | | реалізованих безпеки та приватності |
| SA-16[2]{1}[1][2] | | функцій безпеки та приватності |
| SA-16[2]{1}[1][3] | | заходів безпеки та приватності |
| SA-16[2]{1}[1][4] | | механізмів безпеки та приватності |
| SA-16[2]{1}[2] | функціонуванню | | |
| SA-16[1][2][1] | | реалізованих безпеки та приватності |
| SA-16[1][2][2] | | функцій безпеки та приватності |
| SA-16[1][2][3] | | заходів безпеки та приватності |
| SA-16[1][2][4] | | механізмів безпеки та приватності |
| SA-16[2]{2} | вимагати від розробника системного компонента надання визначеного організацією навчання правильному: | | | |
| SA-16[2]{1}[1] | використанню: | | |
| SA-16[2]{1}[1][1] | | реалізованих безпеки та приватності |
| SA-16[2]{1}[1][2] | | функцій безпеки та приватності |
| SA-16[2]{1}[1][3] | | заходів безпеки та приватності |
| SA-16[2]{1}[1][4] | | механізмів безпеки та приватності |
| SA-16[2]{1}[2] | функціонуванню | | |
| SA-16[1][2][1] | | реалізованих безпеки та приватності |
| SA-16[1][2][2] | | функцій безпеки та приватності |
| SA-16[1][2][3] | | заходів безпеки та приватності |
| SA-16[1][2][4] | | механізмів безпеки та приватності |
| SA-16[2]{3} | вимагати від розробника системної служби надання визначеного організацією навчання, правильному: | | | |
| SA-16[2]{1}[1] | використанню: | | |
| SA-16[2]{1}[1][1] | | реалізованих безпеки та приватності |
| SA-16[2]{1}[1][2] | | функцій безпеки та приватності |
| SA-16[2]{1}[1][3] | | заходів безпеки та приватності |
| SA-16[2]{1}[1][4] | | механізмів безпеки та приватності |
| SA-16[2]{1}[2] | функціонуванню | | |
| SA-16[1][2][1] | | реалізованих безпеки та приватності |
| SA-16[1][2][2] | | функцій безпеки та приватності |
| SA-16[1][2][3] | | заходів безпеки та приватності |
| SA-16[1][2][4] | | механізмів безпеки та приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються навчання, яке проводить розробник; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; навчальні матеріали, надані розробником; записи про навчання; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за безпеку інформаційної системи; розробник системи; організаційні або сторонні розробники, які відповідають за підготовку інформаційної системи, компонента системи чи служби інформаційної системи]. | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SA-17 | ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ РОЗРОБНИКА | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| SA-17{1} | вимагати від розробника системи створення специфікації: | | | | | | |
| SA-17{1}[1] | проєкту безпеки, яка: | | | | | |
| SA-17{1}[1](a) | SA-17{1}[1](a)[1] | узгоджується з архітектурою безпеки організації | | | |
| SA-17{1}[1](a)[2] | підтримує саме ту архітекту, яка: | | | |
| SA-17{1}[1](a)[2][1] | встановлена | | |
| SA-17{1}[1](a)[2][2] | є інтегрованою частиною корпоративної архітектури організації | | |
| SA-17{1}[1](b) | точно та повністю описує: | | | | |
| SA-17{1}[1](b)[1] | необхідні функціональні можливості безпеки | | | |
| SA-17{1}[1](b)[2] | розподіл заходів безпеки між фізичними та логічними компонентами | | | |
| SA-17{1}[1](c) | пояснює, як для забезпечення: | | | | |
| SA-17{1}[1](c)[1] | необхідних можливостей безпеки, разом працюють окремі: | | | |
| SA-17{1}[1](c)[1][1] | | функцій безпеки | |
| SA-17{1}[1](c)[1][2] | | механізми безпеки | |
| SA-17{1}[1](c)[1][3] | | служби безпеки | |
| SA-17{1}[1](c)[2] | єдиного підходу до захисту | | | |
| SA-17{1}[1](c)[2][1] | | функції безпеки | |
| SA-17{1}[1](c)[2][2] | | механізми безпеки | |
| SA-17{1}[1](c)[2][3] | | служби безпеки | |
| SA-17{1}[2] | архітектури безпеки, яка: | | | | | |
| SA-17{1}[2](a) | SA-17{1}[2](a)[1] | узгоджується з архітектурою безпеки організації | | | |
| SA-17{1}[2](a)[2] | підтримує ту архітекту, яка: | | | |
| SA-17{1}[2](a)[2][1] | встановлена | | |
| SA-17{1}[2](a)[2][2] | є інтегрованою частиною корпоративної архітектури організації | | |
| SA-17{1}[2](b) | точно та повністю описує: | | | | |
| SA-17{1}[2](b)[1] | необхідні функціональні можливості безпеки | | | |
| SA-17{1}[2](b)[2] | розподіл заходів безпеки між фізичними та логічними компонентами | | | |
| SA-17{1}[2](c) | пояснює, як для забезпечення: | | | | |
| SA-17{1}[2](c)[1] | необхідних можливостей безпеки, разом працюють окремі: | | | |
| SA-17{1}[2](c)[1][1] | | функції безпеки | |
| SA-17{1}[2](c)[1][2] | | механізми безпеки | |
| SA-17{1}[2](c)[1][3] | | служби безпеки | |
| SA-17{1}[2](c)[2] | єдиного підходу до захисту. | | | |
| SA-17{1}[2](c)[2][1] | | функції безпеки | |
| SA-17{1}[2](c)[2][2] | | механізми безпеки | |
| SA-17{1}[2](c)[2][3] | | служби безпеки | |
| SA-17{2} | Вимагати від розробника системного компонента створення специфікації: | | | | | | |
| SA-17{2}[1] | проєкту безпеки, яка: | | | | | |
| SA-17{2}[1](a) | SA-17{2}[1](a)[1] | узгоджується з архітектурою безпеки організації | | | |
| SA-17{2}[1](a)[2] | підтримує ту архітекту, яка: | | | |
| SA-17{1}[1](a)[2][1] | встановлена | | |
| SA-17{1}[1](a)[2][2] | є інтегрованою частиною корпоративної архітектури організації | | |
| SA-17{2}[1](b) | точно та повністю описує: | | | | |
| SA-17{2}[1](b)[1] | необхідні функціональні можливості безпеки | | | |
| SA-17{2}[1](b)[2] | розподіл заходів безпеки між фізичними та логічними компонентами | | | |
| SA-17{2}[1](c) | пояснює, як для забезпечення: | | | | |
| SA-17{2}[1](c)[1] | необхідних можливостей безпеки, разом працюють окремі: | | | |
| SA-17{2}[1](c)[1][1] | | функції безпеки | |
| SA-17{2}[1](c)[1][2] | | механізми безпеки | |
| SA-17{2}[1](c)[1][3] | | служби безпеки | |
| SA-17{2}[1](c)[2] | єдиного підходу до захисту. | | | |
| SA-17{2}[1](c)[2][1] | | | функції безпеки |
| SA-17{2}[1](c)[2][2] | | | механізми безпеки |
| SA-17{2}[1](c)[2][3] | | | служби безпеки |
| SA-17{2}[2] | архітектури безпеки, яка: | | | | | |
| SA-17{2}[2](a) | SA-17{2}[2](a)[1] | узгоджується з архітектурою безпеки організації | | | |
| SA-17{2}[2](a)[2] | підтримує ту архітекту, яка: | | | |
| SA-17{2}[2](a)[2][1] | встановлена | | |
| SA-17{2}[2](a)[2][2] | є інтегрованою частиною корпоративної архітектури організації | | |
| SA-17{2}[2](b) | точно та повністю описує: | | | | |
| SA-17{2}[2](b)[1] | необхідні функціональні можливості безпеки | | | |
| SA-17{2}[2](b)[2] | розподіл заходів безпеки між фізичними та логічними компонентами | | | |
| SA-17{2}[2](c) | пояснює, як для забезпечення: | | | | |
| SA-17{2}[2](c)[1] | необхідних можливостей безпеки, разом працюють окремі: | | | |
| SA-17{2}[2](c)[1][1] | | функції безпеки | |
| SA-17{2}[2](c)[1][2] | | механізми безпеки | |
| SA-17{2}[2](c)[1][3] | | служби безпеки | |
| SA-17{2}[2](c)[2] | єдиного підходу до захисту. | | | |
| SA-17{2}[2](c)[2][1] | | функції безпеки | |
| SA-17{2}[2](c)[2][2] | | механізми безпеки | |
| SA-17{2}[2](c)[2][3] | | служби безпеки | |
| SA-17{3} | Вимагати від розробника системної служби створення специфікації: | | | | | | |
| SA-17{2}[1] | проєкту безпеки, яка: | | | | | |
| SA-17{2}[1](a) | SA-17{2}[1](a)[1] | узгоджується з архітектурою безпеки організації | | | |
| SA-17{2}[1](a)[2] | підтримує ту архітекту, яка: | | | |
| SA-17{1}[1](a)[2][1] | встановлена усередині | | |
| SA-17{1}[1](a)[2][2] | є інтегрованою частиною корпоративної архітектури організації | | |
| SA-17{2}[1](b) | точно та повністю описує: | | | | |
| SA-17{2}[1](b)[1] | необхідні функціональні можливості безпеки | | | |
| SA-17{2}[1](b)[2] | розподіл заходів безпеки між фізичними та логічними компонентами | | | |
| SA-17{2}[1](c) | пояснює, як для забезпечення: | | | | |
| SA-17{2}[1](c)[1] | необхідних можливостей безпеки, разом працюють окремі: | | | |
| SA-17{2}[1](c)[1][1] | | | функції безпеки |
| SA-17{2}[1](c)[1][2] | | | механізми безпеки |
| SA-17{2}[1](c)[1][3] | | | служби безпеки |
| SA-17{2}[1](c)[2] | єдиного підходу до захисту. | | | |
| SA-17{2}[1](c)[2][1] | | | функції безпеки |
| SA-17{2}[1](c)[2][2] | | | механізми безпеки |
| SA-17{2}[1](c)[2][3] | | | служби безпеки |
| SA-17{2}[2] | архітектури безпеки, яка: | | | | | |
| SA-17{2}[2](a) | SA-17{2}[2](a)[1] | узгоджується з архітектурою безпеки організації | | | |
| SA-17{2}[2](a)[2] | підтримує ту архітекту, яка: | | | |
| SA-17{2}[2](a)[2][1] | встановлена усередині | | |
| SA-17{2}[2](a)[2][2] | є інтегрованою частиною корпоративної архітектури організації | | |
| SA-17{2}[2](b) | точно та повністю описує: | | | | |
| SA-17{2}[2](b)[1] | необхідні функціональні можливості безпеки | | | |
| SA-17{2}[2](b)[2] | розподіл заходів безпеки між фізичними та логічними компонентами | | | |
| SA-17{2}[2](c) | пояснює, як для забезпечення: | | | | |
| SA-17{2}[2](c)[1] | необхідних можливостей безпеки, разом працюють окремі: | | | |
| SA-17{2}[2](c)[1][1] | | | функції безпеки |
| SA-17{2}[2](c)[1][2] | | | механізми безпеки |
| SA-17{2}[2](c)[1][3] | | | служби безпеки |
| SA-17{2}[2](c)[2] | єдиного підходу до захисту. | | | |
| SA-17{2}[2](c)[2][1] | | | функції безпеки |
| SA-17{2}[2](c)[2][2] | | | механізми безпеки |
| SA-17{2}[2](c)[2][3] | | | служби безпеки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для інформаційної системи; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; специфікація проєкту та документація архітектури безпеки для системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал з архітектурою безпеки та дизайнерськими обов'язками]. | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-17(1) | ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ РОЗРОБНИКА - ФОРМАЛЬНА МОДЕЛЬ ПОЛІТИКИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-17(1){1} | вимагати від розробника системи: | | |
| SA-17(1){1}(a) | SA-17(1){1}(a)[1] | організація визначає елементи організаційної політики безпеки |
| SA-17(1){1}(a)[2] | створювати, як невід'ємну частину процесу розробки, формальну модель політики, що описує визначені організацією елементи організаційної політики безпеки, що підлягають виконанню |
| SA-17(1){1}(b) | довести, що формальна модель політики є: | |
| SA-17(1){1}(b)[1] | внутрішньо послідовною і |
| SA-17(1){1}(b)[2] | достатньою для виконання визначених елементів політики безпеки організації, коли вона реалізована |
| SA-17(1){2} | вимагати від розробника компонента системи: | | |
| SA-17(1){2}(a) | SA-17(1){2}(a)[1] | організація визначає елементи організаційної політики безпеки |
| SA-17(1){2}(a)[2] | створювати, як невід'ємну частину процесу розробки, формальну модель політики, що описує визначені організацією елементи організаційної політики безпеки, що підлягають виконанню |
| SA-17(1){2}(b) | довести, що формальна модель політики є: | |
| SA-17(1){2}(b)[1] | внутрішньо послідовною і |
| SA-17(1){2}(b)[2] | достатньою для виконання визначених елементів політики безпеки організації, коли вона реалізована |
| SA-17(1){3} | вимагати від розробника системної служби: | | |
| SA-17(1){2}(a) | SA-17(1){2}(a)[1] | організація визначає елементи організаційної політики безпеки |
| SA-17(1){2}(a)[2] | створювати, як невід'ємну частину процесу розробки, формальну модель політики, що описує визначені організацією елементи організаційної політики безпеки, що підлягають виконанню |
| SA-17(1){2}(b) | довести, що формальна модель політики є: | |
| SA-17(1){2}(b)[1] | внутрішньо послідовною і |
| SA-17(1){2}(b)[2] | достатньою для виконання визначених елементів політики безпеки організації, коли вона реалізована |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для інформаційної системи; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; специфікація проєкту та документація архітектури безпеки для системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал з архітектурою безпеки та дизайнерськими обов'язками]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-17(2) | ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ РОЗРОБНИКА - КОМПОНЕНТИ, ЩО НЕОБХІДНІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-17(2){1} | вимагати від розробника системи: | | |
| SA-17(2){1}(a) | визначити: | |
| SA-17(2){1}(a)[1] | апаратне забезпечення, що необхідне для забезпечення безпеки |
| SA-17(2){1}(a)[2] | програмне забезпечення, що необхідне для забезпечення безпеки |
| SA-17(2){1}(a)[3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки |
| SA-17(2){1}(b) | надати обґрунтування того, що визначення: | |
| SA-17(2){1}(b)[1] | апаратного забезпечення, що необхідно для забезпечення безпеки, є повним |
| SA-17(2){1}(b)[2] | програмного забезпечення, що необхідно для забезпечення безпеки, є повним |
| SA-17(2){1}(b)[3] | мікропрограмного забезпечення, що необхідно для забезпечення безпеки, є повним |
| SA-17(2){2} | Вимагати від розробника компонента системи: | | |
| SA-17(2){2}(a) | визначити: | |
| SA-17(2){2}(a)[1] | апаратне забезпечення, що необхідне для забезпечення безпеки |
| SA-17(2){2}(a)[2] | програмне забезпечення, що необхідне для забезпечення безпеки |
| SA-17(2){2}(a)[3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки |
| SA-17(2){2}(b) | надати обґрунтування того, що застосування: | |
| SA-17(2){2}(b)[1] | апаратного забезпечення, що необхідно для забезпечення безпеки, є повним |
| SA-17(2){2}(b)[2] | програмного забезпечення, що необхідно для забезпечення безпеки, є повним |
| SA-17(2){2}(b)[3] | мікропрограмного забезпечення, що необхідно для забезпечення безпеки, є повним |
| SA-17(2){3} | Вимагати від розробника системної служби: | | |
| SA-17(2){3}(a) | визначити: | |
| SA-17(2){3}(a)[1] | Апаратне забезпечення, що необхідне для забезпечення безпеки |
| SA-17(2){3}(a)[2] | програмне забезпечення, що необхідне для забезпечення безпеки |
| SA-17(2){3}(a)[3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки |
| SA-17(2){3}(b) | Надати обґрунтування того, що застосування: | |
| SA-17(2){3}(b)[1] | апаратного забезпечення, що необхідно для забезпечення безпеки, є повним |
| SA-17(2){3}(b)[2] | програмного забезпечення, що необхідно для забезпечення безпеки, є повним |
| SA-17(2){3}(b)[3] | мікропрограмного забезпечення, що необхідно для забезпечення безпеки, є повним |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для інформаційної системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; перелік компонентів обладнання, програмного забезпечення та мікропрограми, що стосуються безпеки; задокументоване обґрунтування повноти щодо визначень, що надаються для обладнання, програмного забезпечення та мікропрограми, що стосується безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, відповідальний за інформаційну безпеку; розробники системи; організаційний персонал з архітектурою безпеки та дизайнерськими обов'язками]. | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SA-17(3) | ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ РОЗРОБНИКА - ФОРМАЛЬНА ВІДПОВІДНІСТЬ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| SA-17(3){1} | вимагати від розробника системи: | | | | | |
| SA-17(3){1}(a) | створювати, як невід'ємну частину процесу розробки, офіційну специфікацію верхнього рівня, яка визначає інтерфейси: | | | | |
| SA-17(3){1}(a)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки, з точки зору:; | | | |
| SA-17(3){1}(a)[1][1] | | виключень | |
| SA-17(3){1}(a)[1][2] | | повідомлень про помилки | |
| SA-17(3){1}(a)[1][2] | | ефектів | |
| SA-17(3){1}(a)[2] | програмного забезпечення, що необхідне для забезпечення безпеки, з точки зору | | | |
| SA-17(3){1}(a)[2][1] | | | виключень |
| SA-17(3){1}(a)[2][2] | | | повідомлень про помилки |
| SA-17(3){1}(a)[2][3] | | | ефектів |
| SA-17(3){1}(a)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки, з точки зору виключень, повідомлень про помилки та ефектів; | | | |
| SA-17(3){1}(a)[3][1] | | | виключень, |
| SA-17(3){1}(a)[3][2] | | | повідомлень про помилки |
| SA-17(3){1}(a)[3][3] | | | ефектів |
| SA-17(3){1}(b) | надавати докази, якщо це можливо, то з додатковою неофіційною демонстрацією, що формальна специфікація верхнього рівня відповідає формальній моделі політики | | | | |
| SA-17(3){1}(c) | показувати через неофіційну демонстрацію, що формальна специфікація верхнього рівня повністю охоплює інтерфейси: | | | | |
| SA-17(3){1}(c)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){1}(c)[2] | програмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){1}(c)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){1}(d) | демонструвати, що формальна специфікація верхнього рівня є точним описом реалізованого: | | | | |
| SA-17(3){1}(d)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){1}(d)[2] | програмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){1}(d)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){1}(e) | описувати: | | | | |
| SA-17(3){1}(e)[1] | апаратне забезпечення, що необхідне для забезпечення безпеки, яке не розглядається в офіційній специфікації верхнього рівня, але є строго внутрішніми для: | | | |
| SA-17(3){1}(e)[1][1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){1}(e)[1][2] | програмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){1}(e)[1][3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){1}(e)[2] | програмне забезпечення, що необхідне для забезпечення безпеки, яке не розглядається в офіційній специфікації верхнього рівня, але є строго внутрішніми для апаратного, програмного та мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){1}(e)[1][1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){1}(e)[1][2] | програмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){1}(e)[1][3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){1}(e)[3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки, яке не розглядається в офіційній специфікації верхнього рівня, але є строго внутрішніми для апаратного, програмного та мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){1}(e)[1][1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){1}(e)[1][2] | програмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){1}(e)[1][3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){2} | вимагати від розробника компонента системи: | | | | | |
| SA-17(3){2}(a) | створювати, як невід'ємну частину процесу розробки, офіційну специфікацію верхнього рівня, яка визначає інтерфейси: | | | | |
| SA-17(3){2}(a)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки, з точки зору:; | | | |
| SA-17(3){2}(a)[1][1] | | виключень | |
| SA-17(3){2}(a)[1][2] | | повідомлень про помилки | |
| SA-17(3){2}(a)[1][2] | | ефектів | |
| SA-17(3){2}(a)[2] | програмного забезпечення, що необхідне для забезпечення безпеки, з точки зору | | | |
| SA-17(3){2}(a)[2][1] | | | виключень |
| SA-17(3){2}(a)[2][2] | | | повідомлень про помилки |
| SA-17(3){2}(a)[2][3] | | | ефектів |
| SA-17(3){2}(a)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки, з точки зору виключень, повідомлень про помилки та ефектів; | | | |
| SA-17(3){2}(a)[3][1] | | | виключень |
| SA-17(3){2}(a)[3][2] | | | повідомлень про помилки |
| SA-17(3){2}(a)[3][3] | | | ефектів |
| SA-17(3){2}(b) | Надавати докази, якщо це можливо, то з додатковою неофіційною демонстрацією, що формальна специфікація верхнього рівня відповідає формальній моделі політики | | | | |
| SA-17(3){2}(c) | Показувати через неофіційну демонстрацію, що формальна специфікація верхнього рівня повністю охоплює інтерфейси: | | | | |
| SA-17(3){2}(c)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){2}(c)[2] | програмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){2}(c)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){2}(d) | демонструвати, що формальна специфікація верхнього рівня є точним описом реалізованого: | | | | |
| SA-17(3){2}(d)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){2}(d)[2] | програмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){2}(d)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){2}(e) | описувати: | | | | |
| SA-17(3){2}(e)[1] | апаратне забезпечення, що необхідне для забезпечення безпеки, яке не розглядається в офіційній специфікації верхнього рівня, але є строго внутрішніми для: | | | |
| SA-17(3){2}(e)[1][1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){2}(e)[1][2] | програмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){2}(e)[1][3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){2}(e)[2] | програмне забезпечення, що необхідне для забезпечення безпеки, яке не розглядається в офіційній специфікації верхнього рівня, але є строго внутрішніми для апаратного, програмного та мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){2}(e)[1][1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){2}(e)[1][2] | програмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){2}(e)[1][3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){2}(e)[3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки, яке не розглядається в офіційній специфікації верхнього рівня, але є строго внутрішніми для апаратного, програмного та мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){2}(e)[1][1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){2}(e)[1][2] | програмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){2}(e)[1][3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){3} | вимагати від розробника системної служби: | | | | | |
| SA-17(3){3}(a) | створювати, як невід'ємну частину процесу розробки, офіційну специфікацію верхнього рівня, яка визначає інтерфейси: | | | | |
| SA-17(3){3}(a)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки, з точки зору:; | | | |
| SA-17(3){3}(a)[1][1] | | виключень | |
| SA-17(3){3}(a)[1][2] | | повідомлень про помилки | |
| SA-17(3){3}(a)[1][2] | | ефектів | |
| SA-17(3){3}(a)[2] | програмного забезпечення, що необхідне для забезпечення безпеки, з точки зору | | | |
| SA-17(3){3}(a)[2][1] | | | виключень |
| SA-17(3){3}(a)[2][2] | | | повідомлень про помилки |
| SA-17(3){3}(a)[2][3] | | | ефектів |
| SA-17(3){3}(a)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки, з точки зору виключень, повідомлень про помилки та ефектів | | | |
| SA-17(3){3}(a)[3][1] | | | виключень |
| SA-17(3){3}(a)[3][2] | | | повідомлень про помилки |
| SA-17(3){3}(a)[3][3] | | | ефектів |
| SA-17(3){3}(b) | Надавати докази, якщо це можливо, то з додатковою неофіційною демонстрацією, що формальна специфікація верхнього рівня відповідає формальній моделі політики | | | | |
| SA-17(3){3}(c) | Показувати через неофіційну демонстрацію, що формальна специфікація верхнього рівня повністю охоплює інтерфейси: | | | | |
| SA-17(3){3}(c)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){3}(c)[2] | програмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){3}(c)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){3}(d) | демонструвати, що формальна специфікація верхнього рівня є точним описом реалізованого: | | | | |
| SA-17(3){3}(d)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){3}(d)[2] | програмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){3}(d)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){3}(e) | описувати: | | | | |
| SA-17(3){3}(e)[1] | апаратне забезпечення, що необхідне для забезпечення безпеки, яке не розглядається в офіційній специфікації верхнього рівня, але є строго внутрішніми для: | | | |
| SA-17(3){3}(e)[1][1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){3}(e)[1][2] | програмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){3}(e)[1][3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){3}(e)[2] | програмне забезпечення, що необхідне для забезпечення безпеки, яке не розглядається в офіційній специфікації верхнього рівня, але є строго внутрішніми для апаратного, програмного та мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){3}(e)[1][1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){3}(e)[1][2] | програмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){3}(e)[1][3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){3}(e)[3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки, яке не розглядається в офіційній специфікації верхнього рівня, але є строго внутрішніми для апаратного, програмного та мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | | |
| SA-17(3){3}(e)[1][1] | апаратного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){3}(e)[1][2] | програмного забезпечення, що необхідне для забезпечення безпеки | | |
| SA-17(3){3}(e)[1][3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР З: Політика придбання систем та послуг; політика архітектури підприємства; формальна політична модель; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для інформаційної системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; офіційна технічна документація вищого рівня; архітектура безпеки інформаційної системи та проєктна документація; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація, що описує механізми апаратного забезпечення, програмного забезпечення та програмного забезпечення, що стосуються безпеки, не зафіксовані в офіційній документації технічного завдання верхнього рівня; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал з архітектурою безпеки та дизайнерськими обов'язками]. | | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SA-17(4) | ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ РОЗРОБНИКА - НЕФОРМАЛЬНА ВІДПОВІДНІСТЬ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SA-17(4){1} | вимагати від розробника системи: | | | |
| SA-17(4){1}(a) | створювати, як невід'ємну частину процесу розробки, неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси: | | |
| SA-17(4){1}(a)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки, з точки зору: | |
| SA-17(4){1}(a)[1][1] | виключень |
| SA-17(4){1}(a)[1][2] | повідомлень про помилки |
| SA-17(4){1}(a)[1][3] | ефекти |
| SA-17(4){1}(a)[2] | програмного забезпечення, що необхідне для забезпечення безпеки, з точки зору: виключень, повідомлень про помилки та ефекти | |
| SA-17(4){1}(a)[2][1] | виключень, |
| SA-17(4){1}(a)[2][2] | повідомлень про помилки |
| SA-17(4){1}(a)[2][3] | ефекти |
| SA-17(4){1}(a)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки, з точки зору: виключень, повідомлень про помилки та ефекти | |
| SA-17(4){1}(a)[3][1] | виключень, |
| SA-17(4){1}(a)[3][2] | повідомлень про помилки |
| SA-17(4){1}(a)[3][3] | ефекти |
| SA-17(4){1}(b) | демонструвати через: | | |
| SA-17(4){1}(b)[1] | неофіційна демонстрація, що описова специфікація верхнього рівня узгоджується з формальною моделлю політики | |
| SA-17(4){1}(b)[2] | переконливий аргумент з формальними методами та т.д., що описова специфікація верхнього рівня узгоджується з формальною моделлю політики | |
| SA-17(4){2} | вимагати від розробника компонента системи: | | | |
| SA-17(4){2}(a) | створювати, як невід'ємну частину процесу розробки, неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси: | | |
| SA-17(4){2}(a)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки, з точки зору: | |
| SA-17(4){2}(a)[1][1] | виключень |
| SA-17(4){2}(a)[1][2] | повідомлень про помилки |
| SA-17(4){2}(a)[1][3] | ефекти |
| SA-17(4){2}(a)[2] | програмного забезпечення, що необхідне для забезпечення безпеки, з точки зору: виключень, повідомлень про помилки та ефекти | |
| SA-17(4){2}(a)[2][1] | виключень, |
| SA-17(4){2}(a)[2][2] | повідомлень про помилки |
| SA-17(4){2}(a)[2][3] | ефекти |
| SA-17(4){2}(a)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки, з точки зору: виключень, повідомлень про помилки та ефекти | |
| SA-17(4){2}(a)[3][1] | виключень, |
| SA-17(4){2}(a)[3][2] | повідомлень про помилки |
| SA-17(4){2}(a)[3][3] | ефекти |
| SA-17(4){2}(b) | демонструвати через: | | |
| SA-17(4){2}(b)[1] | неофіційна демонстрація, що описова специфікація верхнього рівня узгоджується з формальною моделлю політики | |
| SA-17(4){2}(b)[2] | переконливий аргумент з формальними методами та т.д., що описова специфікація верхнього рівня узгоджується з формальною моделлю політики | |
| SA-17(4){3} | вимагати від розробника системної служби: | | | |
| SA-17(4){3}(a) | створювати, як невід'ємну частину процесу розробки, неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси: | | |
| SA-17(4){3}(a)[1] | апаратного забезпечення, що необхідне для забезпечення безпеки, з точки зору: | |
| SA-17(4){3}(a)[1][1] | виключень, |
| SA-17(4){3}(a)[1][2] | повідомлень про помилки |
| SA-17(4){3}(a)[1][3] | ефекти |
| SA-17(4){3}(a)[2] | програмного забезпечення, що необхідне для забезпечення безпеки, з точки зору: виключень, повідомлень про помилки та ефекти | |
| SA-17(4){3}(a)[2][1] | виключень, |
| SA-17(4){3}(a)[2][2] | повідомлень про помилки |
| SA-17(4){3}(a)[2][3] | ефекти |
| SA-17(4){3}(a)[3] | мікропрограмного забезпечення, що необхідне для забезпечення безпеки, з точки зору: виключень, повідомлень про помилки та ефекти | |
| SA-17(4){3}(a)[3][1] | виключень |
| SA-17(4){3}(a)[3][2] | повідомлень про помилки |
| SA-17(4){3}(a)[3][3] | ефекти |
| SA-17(4){3}(b) | демонструвати через: | | |
| SA-17(4){3}(b)[1] | неофіційна демонстрація, що описова специфікація верхнього рівня узгоджується з формальною моделлю політики | |
| SA-17(4){3}(b)[2] | переконливий аргумент з формальними методами і т.д., що описова специфікація верхнього рівня узгоджується з формальною моделлю політики | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; формальна політична модель; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для інформаційної системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; неофіційна описова технічна документація вищого рівня; архітектура безпеки інформаційної системи та проєктна документація; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація, що описує механізми апаратного забезпечення, програмного забезпечення та програмного забезпечення, що стосуються безпеки, не розглядаються в неофіційній описовій документації специфікації верхнього рівня; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал з архітектурою безпеки та дизайнерськими обов'язками]. | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-17(5) | ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ РОЗРОБНИКА - КОНЦЕПТУАЛЬНИЙ ПРОЄКТ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-17(5){1} | вимагати від розробника системи: | | |
| SA-17(5){1}(a)[1] | розробити: | |
| SA-17(5){1}(a)[1][1] | апаратне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){1}(a)[1][2] | програмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){1}(a)[1][3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){1}(a)[2] | структурувати: апаратне, програмне та мікропрограмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою | |
| SA-17(5){1}(a)[2][1] | апаратне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){1}(a)[2][2] | програмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){1}(a)[2][3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){2} | вимагати від розробника компонента системи: | | |
| SA-17(5){2}(a)[1] | розробити: | |
| SA-17(5){2}(a)[1][1] | апаратне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){2}(a)[1][2] | програмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){2}(a)[1][3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){2}(a)[2] | структурувати: апаратне, програмне та мікропрограмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою | |
| SA-17(5){2}(a)[2][1] | апаратне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){2}(a)[2][2] | програмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){2}(a)[2][3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){3} | вимагати від розробника системної служби: | | |
| SA-17(5){3}(a)[1] | розробити: | |
| SA-17(5){3}(a)[1][1] | апаратне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){3}(a)[1][2] | програмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){3}(a)[1][3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){3}(a)[2] | структурувати: апаратне, програмне та мікропрограмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою | |
| SA-17(5){3}(a)[2][1] | апаратне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){3}(a)[2][2] | програмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| SA-17(5){3}(a)[2][3] | мікропрограмне забезпечення, що необхідне для забезпечення безпеки, що використовують повний, концептуально простий механізм захисту з точно визначеною семантикою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для інформаційної системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; проєктна документація інформаційної системи; документація архітектури безпеки інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація для розробників, що описує дизайн та структуру відповідного обладнання, програмного забезпечення та компонентів мікропрограмного забезпечення; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, відповідальний за інформаційну безпеку; розробка системи] | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-17(6) | ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ РОЗРОБНИКА - СТРУКТУРА ДЛЯ ТЕСТУВАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-17(6){1} | вимагати від розробника системи, системного компонента або системної служби структурувати відповідне: | |
| SA-17(6){1}[1] | апаратне забезпечення для тестування |
| SA-17(6){1}[2] | програмне забезпечення для тестування |
| SA-17(6){1}[3] | мікропрограмне забезпечення для тестування |
| SA-17(6){2} | вимагати від розробника системи, системного компонента або системної служби структурувати відповідне: | |
| SA-17(6){2}[1] | апаратне забезпечення для тестування |
| SA-17(6){2}[2] | програмне забезпечення для тестування |
| SA-17(6){2}[3] | мікропрограмне забезпечення для тестування |
| SA-17(6){3} | вимагати від розробника системи, системного компонента або системної служби структурувати відповідне: | |
| SA-17(6){3}[1] | апаратне забезпечення для тестування |
| SA-17(6){3}[2] | програмне забезпечення для тестування |
| SA-17(6){3}[3] | мікропрограмне забезпечення для тестування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для інформаційної системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; проєктна документація інформаційної системи; документація архітектури безпеки інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація для розробників, що описує дизайн та структуру відповідного обладнання, програмного забезпечення та компонентів мікропрограмного забезпечення для полегшення тестування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з архітектурою безпеки та дизайнерськими обов'язками]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-17(7) | ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ РОЗРОБНИКА - СТРУКТУРА ДЛЯ НАЙМЕНШОЇ ПРИВІЛЕЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-17(7){1} | вимагати від розробника системи структурувати: | |
| SA-17(7){1}[1] | апаратне забезпечення, що необхідно для забезпечення безпеки, таким чином, щоб забезпечить управління доступом з найменшими привілеями |
| SA-17(7){1}[2] | програмне забезпечення, що необхідно для забезпечення безпеки, таким чином, щоб забезпечить управління доступом з найменшими привілеями |
| SA-17(7){1}[3] | мкропрограмне забезпечення, що необхідно для забезпечення безпеки, таким чином, щоб забезпечить управління доступом з найменшими привілеями |
| SA-17(7){2} | вимагати від розробника системного компонента структурувати: | |
| SA-17(7){2}[1] | апаратне забезпечення, що необхідно для забезпечення безпеки, таким чином, щоб забезпечить управління доступом з найменшими привілеями |
| SA-17(7){2}[2] | програмне забезпечення, що необхідно для забезпечення безпеки, таким чином, щоб забезпечить управління доступом з найменшими привілеями |
| SA-17(7){2}[3] | мкропрограмне забезпечення, що необхідно для забезпечення безпеки, таким чином, щоб забезпечить управління доступом з найменшими привілеями |
| SA-17(7){3} | вимагати від розробника системної служби структурувати апаратне забезпечення, програмне забезпечення та мкропрограмне забезпечення, що необхідно для забезпечення безпеки, таким чином, щоб забезпечить управління доступом з найменшими привілеями. | |
| SA-17(7){3}[1] | апаратне забезпечення, що необхідно для забезпечення безпеки, таким чином, щоб забезпечить управління доступом з найменшими привілеями |
| SA-17(7){3}[2] | програмне забезпечення, що необхідно для забезпечення безпеки, таким чином, щоб забезпечить управління доступом з найменшими привілеями |
| SA-17(7){3}[3] | мкропрограмне забезпечення, що необхідно для забезпечення безпеки, таким чином, щоб забезпечить управління доступом з найменшими привілеями |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для інформаційної системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; проєктна документація інформаційної системи; документація архітектури безпеки інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація для розробників, що описує дизайн та структуру відповідного обладнання, програмного забезпечення та компонентів мікропрограми для забезпечення безпеки, щоб полегшити контроль доступу з найменшими привілеями; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал з архітектурою безпеки та дизайнерськими обов'язками]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-18 | ЗАХИСТ ТА ВИЯВЛЕННЯ ПІДРОБКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-18[1] | впроваджувати програму захисту від несанкціонованого доступу для: | |
| SA-18[1]{1} | системи |
| SA-18[1]{2} | системного компонента |
| SA-18[1]{3} | системної служби |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються опору та виявлення фальсифікації; документація програми захисту від втручання; документація про засоби та методи захисту від втручання; Документація щодо засобів та методів виявлення та захисту від втручання; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання системи та послуг; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, відповідальний за програму захисту від втручання].  Перевірка: [ВИБІР: Організаційні процеси для реалізації програми захисту від несанкціонованого доступу; автоматизовані механізми, що підтримують та, або реалізують програму захисту від втручання]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-18(1) | ЗАХИСТ ТА ВИЯВЛЕННЯ ПІДРОБКИ - ЕТАПИ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ СИСТЕМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-18(1)[1] | використовувати | | |
| SA-18(1)[1][1] | технології протизлочинного впливу під час різних етапів життєвого циклу розробки системи, включаючи: | |
| SA-18(1)[1][1][1] | проєктування |
| SA-18(1)[1][1][2] | розробку |
| SA-18(1)[1][1][3] | інтеграцію |
| SA-18(1)[1][1][4] | експлуатацію |
| SA-18(1)[1][1][5] | технічне обслуговування |
| SA-18(1)[1][2] | засоби протизлочинного впливу під час різних етапів життєвого циклу розробки системи, включаючи: | |
| SA-18(1)[1][1][1] | проєктування |
| SA-18(1)[1][1][2] | розробку |
| SA-18(1)[1][1][3] | інтеграцію |
| SA-18(1)[1][1][4] | експлуатацію |
| SA-18(1)[1][1][5] | технічне обслуговування |
| SA-18(1)[1][3] | методи протизлочинного впливу під час різних етапів життєвого циклу розробки системи, включаючи: | |
| SA-18(1)[1][1][1] | проєктування |
| SA-18(1)[1][1][2] | розробку |
| SA-18(1)[1][1][3] | інтеграцію |
| SA-18(1)[1][1][4] | експлуатацію |
| SA-18(1)[1][1][5] | технічне обслуговування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються опору та виявлення фальсифікації; документація програми захисту від втручання; документація на засоби та методи захисту від несанкціонованого доступу; Документи інструментів (технологій) та методів виявлення та захисту від втручань; документація життєвого циклу розробки системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за програму захисту від втручання; організаційний персонал, який відповідає за SDLC].  Перевірка: [ВИБІР: Організаційні процеси із застосуванням технологій протидії фальсифікації; автоматизовані механізми, що підтримують та, або впроваджують технології проти злому]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-18(2) | ЗАХИСТ ТА ВИЯВЛЕННЯ ПІДРОБКИ - ПЕРЕВІРКА СИСТЕМ АБО КОМПОНЕНТІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-18(2)[1] | SA-18(2)[1][1] | SA-18(2)[1][1]{1} | організація визначає системи, які необхідно перевіряти для виявлення порушення |
| SA-18(2)[1][1]{2} | організація визначає компоненти системи, які необхідно перевіряти для виявлення порушення |
| SA-18(2)[1][2] | організація визначає частоту, з якою необхідно проводити перевірки | |
| SA-18(2)[1][3] | організація визначає ознаки необхідності проведення перевірки для виявлення порушення | |
| SA-18(2)[2] | перевіряти для виявлення порушення: | | |
| SA-18(2)[2]{1} | визначені організацією системи (один або більше): | |
| SA-18(2)[2]{1}{1} | випадковим чином |
| SA-18(2)[2]{1}{2} | з визначеною організацією частотою |
| SA-18(2)[2]{1}{3} | визначені організацією ознаки необхідності перевірки |
| SA-18(2)[2]{2} | визначені організацією компоненти системи (один або більше): | |
| SA-18(2)[2]{2}{1} | випадковим чином |
| SA-18(2)[2]{2}{2} | визначена організацією частота |
| SA-18(2)[2]{2}{3} | визначені організацією ознаки необхідності перевірки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються захисту та виявлення фальсифікації; записи випадкових перевірок; звіти, результати перевірок; звіти, результати оцінки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за програму захисту від втручання].  Перевірка: [ВИБІР: Організаційні процеси для перевірки інформаційних систем, системних компонентів або пристроїв для виявлення підробки; автоматизовані механізми, що підтримують та, або реалізують виявлення підробки]. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SA-19 | СПРАВЖНІСТЬ КОМПОНЕНТА | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SA-19(a) | SA-19(a)[1] | розробити антипідроблюючу: | | | |
| SA-19(a)[1][1] | політику, які включають: | | |
| SA-19(a)[1][1][1] | | засоби виявлення проникнення підроблених компонентів в систему |
| SA-19(a)[1][1][2] | | засоби запобігання проникненню підроблених компонентів в систему |
| SA-19(a)[1][2] | процедури, які включають: | | |
| SA-19(a)[1][2][1] | засоби виявлення проникнення підроблених компонентів в систему | |
| SA-19(a)[1][2][2] | засоби запобігання проникнення підроблених компонентів в систему | |
| SA-19(a)[2] | впровадити антипідроблюючу: | | | |
| SA-19(a)[2][1] | політику, яка включає: | | |
| SA-19(a)[2][1][1] | засоби виявлення проникнення підроблених компонентів в систему | |
| SA-19(a)[2][1][2] | засоби запобігання проникненню підроблених компонентів в систему | |
| SA-19(a)[2][2] | процедури, які включають: | | |
| SA-19(a)[2][2][1] | засоби виявлення проникнення підроблених компонентів в систему | |
| SA-19(a)[2][2][2] | засоби запобігання проникненню підроблених компонентів в систему | |
| SA-19(b) | SA-19(b)[1] | SA-19(b)[1][1] | організація визначає зовнішні звітні організації, до яких необхідно повідомляти про компоненти підробленої системи | | |
| SA-19(b)[1][2] | SA-19(b)[1][2]{1} | організація визначає персонал, який необхідно повідомляти про компоненти підробленої системи | |
| SA-19(b)[1][2]{2} | організація визначає посадові особи, яких необхідно повідомляти про компоненти підробленої системи | |
| SA-19(b)[2] | повідомляти про компоненти підробленої системи в (один або кілька): | | | |
| SA-19(b)[2][1] | джерело підробленого компонента | | |
| SA-19(b)[2][2] | визначені організацією зовнішні звітні організації | | |
| SA-19(b)[2][3] | SA-19(b)[2][3]{1} | визначений організацією персонал | |
| SA-19(b)[2][3]{2} | визначений організацією посадові особи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика та процедури боротьби з підробкою; політика розпорядження носіїв інформації; політика захисту носіїв інформації; політика реагування на інциденти; навчальні матеріали, присвячені підробці компонентів інформаційної системи; навчальні записи щодо виявлення та запобігання потраплянню підроблених компонентів в інформаційну систему; звіти, що повідомляють розробників, виробників, постачальників, підрядників та, або зовнішні організації, що звітують, про компоненти підробленої інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за політику, процедури та звітність щодо боротьби з підробками].  Перевірка: [ВИБІР: Організаційні процеси для виявлення, запобігання та звітності проти підробок; автоматизовані механізми, що підтримують та, або впроваджують виявлення, запобігання та звітування про підробку]. | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-19(1) | СПРАВЖНІСТЬ КОМПОНЕНТА - НАВЧАННЯ БОРОТЬБІ З ПІДРОБКОЮ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-19(1)[1] | SA-19(1)[1]{1} | визначені організацією персонал | |
| SA-19(1)[1]{2} | визначені організацією посадові особи | |
| SA-19(1)[2] | SA-19(1)[2]{1} | навчативизначений організацією персонал виявленню підроблених компонентів системи, включаючи: | |
| SA-19(1)[2]{1}[1] | апаратне забезпечення |
| SA-19(1)[2]{1}[2] | програмне забезпечення |
| SA-19(1)[2]{1}[3] | мікропрограмне забезпечення |
| SA-19(1)[2]{2} | навчати визначені посадові особи виявленню підроблених компонентів системи, включаючи: | |
| SA-19(1)[2]{2}[1] | апаратне забезпечення |
| SA-19(1)[2]{2}[2] | програмне забезпечення |
| SA-19(1)[2]{2}[3] | мікропрограмне забезпечення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика та процедури щодо підробки; політика розпорядження ЗМІ; політика захисту засобів масової інформації; політика реагування на інциденти; навчальні матеріали, присвячені підробці компонентів інформаційної системи; навчальні записи щодо виявлення підроблених компонентів інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за політику, процедури та навчання у сфері боротьби з підробкою].  Перевірка: [ВИБІР: Організаційні процеси для навчання протидії підробкам]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SA-19(2) | СПРАВЖНІСТЬ КОМПОНЕНТА - УПРАВЛІННЯ КОНФІГУРАЦІЄЮ ДЛЯ ОБСЛУГОВУВАННЯ ТА РЕМОНТУ КОМПОНЕНТІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SA-19(2)[1] | організація визначає компонент системи | | |
| SA-19(2)[2] | підтримувати контроль конфігурації: | | |
| SA-19(2)[2][1] | визначених організацією компонент системи, що: | |
| SA-19(2)[2][1]{1} | очікують обслуговування |
| SA-19(2)[2][1]{2} | очікують ремонту |
| SA-19(2)[2][2] | готові до використання компоненти, які очікують повернення до ремонту. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика та процедури боротьби з підробкою; політика захисту носіїв інформації; план управління конфігурацією; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи контролю конфігурації для компонентів, що очікують на обслуговування, ремонт; записи контролю конфігурації для обслуговуваних, відремонтованих компонентів, що очікують повернення в експлуатацію; записи технічного обслуговування інформаційної системи; записи аудиту інформаційної системи; записи управління запасами; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за політику та процедури боротьби з підробкою; організаційний персонал, відповідальний за управління конфігурацією].  Перевірка: [ВИБІР: Організаційні процеси для управління конфігурацією; автоматизовані механізми підтримки та, або реалізації управління конфігурацією]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-19(3) | СПРАВЖНІСТЬ КОМПОНЕНТА - УТИЛІЗАЦІЯ КОМПОНЕНТІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-19(3)[1] | SA-19(3)[1][1] | організація визначає техніки, за допомогою яких утилізують компоненти системи |
| SA-19(3)[1][2] | організація визначає методи, за допомогою яких утилізують компоненти системи |
| SA-19(3)[2] | утилізувати компоненти системи за допомогою визначеної організацією: | |
| SA-19(3)[2][1] | техніки |
| SA-19(3)[2][2] | методів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика та процедури щодо підробки; політика розпорядження носіїв інформації; політика захисту носіїв інформації; записи про утилізацію компонентів інформаційної системи; документація щодо технік та методів утилізації, що застосовуються для компонентів інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за політику та процедури боротьби з підробкою; організаційний персонал, відповідальний за утилізацію компонентів інформаційної системи].  Перевірка: [ВИБІР: Організаційні техніки та методи утилізації компонентів інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують утилізацію компонентів системи]. | | |

|  |  |  |
| --- | --- | --- |
| SA-19(4) | СПРАВЖНІСТЬ КОМПОНЕНТА - СКАНУВАННЯ НА ПІДРОБКУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SA-19(4)[1] | організація визначає частоту, з якою необхідно сканувати на підроблені компоненти системи |
| SA-19(4)[2] | Сканувати на підроблені компоненти системи з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика та процедури щодо підробки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; засоби сканування та супутня документація; результати сканування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за політику та процедури боротьби з підробкою; організаційний персонал, відповідальний за сканування підробок].  Перевірка: [ВИБІР: Організаційні процеси для сканування проти підробок; автоматизовані механізми, що підтримують та, або впроваджують сканування підробок]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-20 | ІНДИВІДУАЛЬНА РОЗРОБКА КРИТИЧНИХ КОМПОНЕНТІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-20[1] | організація визначає критичні компоненти системи | |
| SA-20[2] | SA-20[2]{1} | повторно реалізувати визначені організацією критичні компоненти системи |
| SA-20[2]{2} | налаштувати визначені організацією критичні компоненти системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються індивідуального розвитку важливих компонентів інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація життєвого циклу розробки системи, що стосується нестандартної розробки важливих компонентів інформаційної системи; записи управління конфігурацією; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за повторне впровадження або налаштування важливих компонентів інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для повторного впровадження або налаштування важливих компонентів інформаційної системи; автоматизовані механізми, що підтримують та, або реалізують повторне впровадження або налаштування важливих компонентів інформаційної системи]. | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SA-21 | СКРИНІНГ РОЗРОБНИКА | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| SA-21[1] | SA-21[1]{1} | організація визначає системи для скринінгу | | | | | |
| SA-21[1]{2} | організація визначає системні компоненти для скринінгу | | | | | |
| SA-21[1]{3} | організація визначає системні служби для скринінгу | | | | | |
| SA-21[2] | SA-21[2]{1} | вимагати, щоб розробник визначених організацією системи | | | | | |
| SA-21[2]{1}(a) | SA-21[2]{1}(a)[1] | | організація визначає уповноважений орган, який призначає дозволи доступу | | |
| SA-21[2]{1}(a)[2] | | мав відповідні дозволи доступу, як визначено призначеним організацією уповноваженим органом | | |
| SA-21[2]{1}(b) | SA-21[2]{1}(b)[1] | | організація визначає додаткові критерії перевірки персоналу | | |
| SA-21[2]{1}(b)[2] | | задовольняв визначеним організацією додатковим критеріям перевірки персоналу | | |
| SA-21[2]{1}(c) | надавав інформацію про те, що повноваження доступу і критерії відбору, зазначені в: | | | | |
| SA-21[2]{1}(c)[1] | | | пункті а., є виконаними | |
| SA-21[2]{1}(c)[2] | | | пункті b., є виконаними | |
| SA-21[2]{2} | вимагати, щоб розробник визначених організацією системних компонент: | | | | | |
| SA-21[2]{2}(a) | SA-21[2]{2}(a)[1] | | | організація визначає уповноважений орган, який призначає дозволи доступу | |
| SA-21[2]{2}(a)[2] | | | мав відповідні дозволи доступу, як визначено призначеним організацією уповноваженим органом | |
| SA-21[2]{2}(b) | SA-21[2]{2}(b)[1] | | | організація визначає додаткові критерії перевірки персоналу | |
| SA-21[2]{2}(b)[2] | | | задовольняв визначеним організацією додатковим критеріям перевірки персоналу | |
| SA-21[2]{2}(c) | надавав інформацію про те, що повноваження доступу і критерії відбору, зазначені в: | | | | |
| SA-21[2]{2}(c)[1] | пункті а., є виконаними | | | |
| SA-21[2]{2}(c)[2] | пункті b., є виконаними | | | |
| SA-21[2]{3} | вимагати, щоб розробник визначених організацією системних служб: | | | | | |
| SA-21[2]{3}(a) | SA-21[2]{3}(a)[1] | | | організація визначає уповноважений орган, який призначає дозволи доступу | |
| SA-21[2]{3}(a)[2] | | | мав відповідні дозволи доступу, як визначено призначеним організацією уповноваженим органом | |
| SA-21[2]{3}(b) | SA-21[2]{3}(b)[1] | | | організація визначає додаткові критерії перевірки персоналу | |
| SA-21[2]{3}(b)[2] | | | задовольняв визначеним організацією додатковим критеріям перевірки персоналу | |
| SA-21[2]{3}(c) | надавав інформацію про те, що повноваження доступу і критерії відбору, зазначені в: | | | | |
| SA-21[2]{3}(c)[1] | | | | пункті а., є виконаними |
| SA-21[2]{3}(c)[2] | | | | пункті b., є виконаними |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; політика та процедури забезпечення персоналу; процедури, що стосуються скринінгу персоналу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік відповідних дозволів на доступ, необхідних розробникам інформаційної системи; критерії перевірки персоналу та відповідна документація; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за перевірку розробників].  Перевірка: [ВИБІР: Організаційні процеси для перевірки розробниками; автоматизовані механізми, що підтримують скринінг розробників]. | | | | | | | |

|  |  |
| --- | --- |
| SA-21(1) | СКРИНІНГ РОЗРОБНИКА - ПЕРЕВІРКА СКРИНІНГУ |
|  | [Вилучено: включено до SA-21] |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-22 | КОМПОНЕНТИ СИСТЕМИ, ЩО НЕ ПІДТРИМУЮТЬСЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-22[1] | замінюють компоненти системи, якщо підтримка компонентів більше не доступна: | |
| SA-22[1]{1} | розробнику |
| SA-22[1]{2} | постачальнику |
| SA-22[1]{3} | виробнику |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються заміни або постійного використання непідтримуваних компонентів інформаційної системи; документальне підтвердження заміни непідтримуваних компонентів інформаційної системи; документально підтверджені погодження (включаючи обґрунтування) для подальшого використання непідтримуваних компонентів інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; життєвий цикл розвитку системи відповідальності організаційного персоналу; організаційний персонал, відповідальний за управління конфігурацією].  Перевірка: [ВИБІР: Організаційні процеси для заміни непідтримуваних системних компонентів; автоматизовані механізми, що підтримують та, або здійснюють заміну непідтримуваних компонентів системи]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-22(1) | КОМПОНЕНТИ СИСТЕМИ, ЩО НЕ ПІДТРИМУЮТЬСЯ - АЛЬТЕРНАТИВНІ ДЖЕРЕЛА ДЛЯ ПОСТІЙНОЇ ПІДТРИМКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SA-22(1)[1] | організація визначає підтримку від зовнішніх постачальників для компонентів системи, що не підтримуються | |
| SA-22(1)[2] | забезпечити (один або більше): | |
| SA-22(1)[2]{1} | внутрішня підтримка для компонентів системи, що не підтримуються |
| SA-22(1)[2]{2} | визначена організацією підтримка від зовнішніх постачальників для компонентів системи, що не підтримуються |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються підтримки непідтримуваних компонентів інформаційної системи; заявна документація; документація про придбання; договори придбання; угоди про рівень обслуговування; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за придбання систем та послуг; організаційний персонал, який відповідає за інформаційну безпеку; життєвий цикл розвитку системи відповідальності організаційного персоналу; організаційний персонал або сторонні постачальники, що підтримують компоненти інформаційної системи, які більше не підтримуються оригінальними розробниками, постачальниками чи виробниками].  Перевірка: [ВИБІР: Організаційні процеси для підтримки системних компонентів, які більше не підтримуються оригінальними розробниками, постачальниками чи виробниками; автоматизовані механізми, що забезпечують підтримку системних компонентів, які більше не підтримуються оригінальними розробниками, постачальниками чи виробниками]. | | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ SC – ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА КОМУНІКАЦІЙ**

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

|  |  |  |
| --- | --- | --- |
| SC-2 | РОЗДІЛЕННЯ ФУНКЦІЙ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-2[1] | розділяти функціональність користувача, включаючи служби, що призначені для користувача інтерфейсу, від функціональності системного управління |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту систем та комунікацій; процедури, що стосуються розділення додатків; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Відокремлення функціональності користувача від функцій управління інформаційною системою]. | |

|  |  |  |
| --- | --- | --- |
| SC-2(1) | РОЗДІЛЕННЯ ФУНКЦІЙ - ІНТЕРФЕЙСИ ДЛЯ НЕПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-2(1)[1] | запобігати представленню функціональності системного управління в інтерфейсі для непривілейованих користувачів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту систем та комунікацій; процедури, що стосуються розділення додатків; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; непривілейовані користувачі інформаційної системи; розробник системи].  Перевірка: [ВИБІР: Відокремлення функціональності користувача від функцій управління інформаційною системою]. | |

|  |  |  |
| --- | --- | --- |
| SC-3 | ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-3[1] | ізолювати функції безпеки від інших функцій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються ізоляції функції безпеки; перелік функцій безпеки, які слід ізолювати від незахищених функцій; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Поділ функцій безпеки від функцій, що не стосуються безпеки, в межах інформаційної системи]. | |

|  |  |  |
| --- | --- | --- |
| SC-3(1) | ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - РОЗДІЛЕННЯ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-3(1)[1] | використовувати механізми розділення апаратних засобів для реалізації ізоляції функцій безпеки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту систем та комунікацій; процедури, що стосуються ізоляції функції безпеки; проєктна документація інформаційної системи; механізми апаратного розділення; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Розділення функцій безпеки від функцій, що не стосуються безпеки, в межах інформаційної системи]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-3(2) | ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - ФУНКЦІЇ УПРАВЛІННЯ ДОСТУПОМ ТА ПОТОКОМ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-3(2)[1] | ізолювати функції безпеки, що забезпечують: | |
| SC-3(2)[1][1] | управління доступом щодо функцій, не пов’язаних з безпекою, та інших функцій безпеки |
| SC-3(2)[1][2] | управління інформаційним потоком щодо функцій, не пов’язаних з безпекою, та інших функцій безпеки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються ізоляції функції безпеки; перелік важливих функцій безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Ізоляція функцій безпеки, що забезпечують контроль доступу та управління потоком інформації]. | | |

|  |  |  |
| --- | --- | --- |
| SC-3(3) | ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - МІНІМІЗАЦІЯ ФУНКЦІОНАЛЬНОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-3(3)[1] | мінімізувати кількість функцій, не пов’язаних з безпекою, що входять до сфери ізоляції, яка містить функції безпеки. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються ізоляції функції безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують границю ізоляції]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-3(4) | ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - З’ЄДНАННЯ МОДУЛІВ ТА ЗВ’ЯЗНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-3(4)[1] | впроваджувати функції безпеки в основному як незалежні модулі, які: | |
| SC-3(4)[1][1] | максимізують внутрішню зв’язність у модулях і |
| SC-3(4)[1][2] | мінімізують зв'язок між модулями |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються ізоляції функції безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для максимізації внутрішньої зв’язності в модулях та мінімізації зв’язку між модулями; автоматизовані механізми, що підтримують та, або реалізують функції безпеки як незалежні модулі]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-3(5) | ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - БАГАТОРІВНЕВА СТРУКТУРА | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-3(5)[1] | реалізувати функції безпеки як багаторівневу структуру, що: | | |
| SC-3(5)[1][1] | мінімізує взаємодію між рівнями конструкції та | |
| SC-3(5)[1][2] | уникає будь-якої залежності нижчих рівнів від: | |
| SC-3(5)[1][2]{1} | функціональності вищих рівнів |
| SC-3(5)[1][2]{2} | правильності вищих рівнів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються ізоляції функції безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для реалізації функцій захисту як багаторівнева структура, яка мінімізує взаємодію між рівнями та уникає залежності нижчих рівнів від функціональності, правильності вищих рівнів; автоматизовані механізми, що підтримують та, або реалізують функції безпеки як багаторівневу структуру]. | | | |

|  |  |  |
| --- | --- | --- |
| SC-4 | ІНФОРМАЦІЯ В ЗАГАЛЬНИХ СИСТЕМНИХ РЕСУРСАХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-4[1] | запобігати несанкціонованій передачі інформації через спільні системні ресурси |
| SC-4[2] | запобігати ненавмисній передачі інформації через спільні системні ресурси |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації у спільних системних ресурсах; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що запобігають несанкціонованому та ненавмисному передаванню інформації через спільні системні ресурси]. | |

|  |  |
| --- | --- |
| SC-4(1) | ІНФОРМАЦІЯ В ЗАГАЛЬНИХ СИСТЕМНИХ РЕСУРСАХ - РІВНІ БЕЗПЕКИ |
|  | [Вилучено: включено до SC-4]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-4(2) | ІНФОРМАЦІЯ В ЗАГАЛЬНИХ СИСТЕМНИХ РЕСУРСАХ - БАГАТОРІВНЕВА АБО ПЕРІОДИЧНА ОБРОБКА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-4(2)[1] | визначені організацією процедури щодо запобігання несанкціонованої передачі інформації | |
| SC-4(2)[2] | запобігати несанкціонованій передачі інформації через спільні ресурси відповідно до визначених організацією процедур, коли системна обробка явно перемикається між: | |
| SC-4(2)[2]{1} | різними категоріями таємності інформації або |
| SC-4(2)[2]{2} | різними категоріями безпеки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації у спільних системних ресурсах; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що запобігають несанкціонованій передачі інформації через спільні системні ресурси]. | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SC-5 | ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SC-5[1] | SC-5[1][1] | SC-5[1][1]{1} | | визначені організацією типи подій відмови в обслуговуванні |
| SC-5[1][1]{2} | | визначені організацією типи подій відмови в посиланні на джерела для такої інформації |
| SC-5[1][2] | організація визначає заходи безпеки для | | |
| SC-5[1][2]{1} | | забезпечення захисту подій відмови в обслуговуванні |
| SC-5[1][2]{2} | | обмеження наслідків подій відмови в обслуговуванні |
| SC-5 | SC-5{1} | забезпечити захист наступних типів подій відмови в обслуговуванні (DoS): | | |
| SC-5{1}{1} | визначені організацією типи подій відмови в послугах використовуючи визначені організацією заходи безпеки | |
| SC-5{1}{2} | визначені організацією типи подій відмови посилання на джерела для такої інформації, використовуючи визначені організацією заходи безпеки | |
| SC-5{2} | обмежити наслідки наступних типів подій відмови в обслуговуванні (DoS): | | |
| SC-5{2}{1} | визначені організацією типи подій відмови в послугах, використовуючи визначені організацією заходи безпеки | |
| SC-5{2}{2} | визначені організацією типи подій відмови посилання на джерела для такої інформації, використовуючи визначені організацією заходи безпеки | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація інформаційної системи; план безпеки; перелік атак на відмову в послугах, що вимагають застосування гарантій безпеки для захисту від або обмеження наслідків таких атак; перелік засобів безпеки, що захищають від або обмежують наслідки атак відмови в обслуговуванні; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за реагування на інциденти; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що захищають або обмежують наслідки атак відмови в обслуговуванні]. | | | | |

|  |  |  |
| --- | --- | --- |
| SC-5(1) | ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» - ОБМЕЖЕННЯ ВНУТРІШНІХ КОРИСТУВАЧІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-5(1)[1] | організація визначає атаки на відмову в обслуговуванні |
| SC-5(1)[2] | обмежити здатність осіб запускати визначені організацією атаки на відмову в обслуговуванні проти інших систем |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація інформаційної системи; план безпеки; перелік атак відмови в обслуговуванні, розпочатих приватними особами проти інформаційних систем; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за реагування на інциденти; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що обмежують можливість запуску атак відмови в обслуговуванні проти інших інформаційних систем]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-5(2) | ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» - ПРОДУКТИВНІСТЬ, ПРОПУСКНА ЗДАТНІСТЬ ТА НАДМІРНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-5(2)[1] | для обмеження наслідків атак «відмова в обслуговуванні» управляти: | |
| SC-5(2)[1]{1} | продуктивністю |
| SC-5(2)[1]{2} | пропускною здатністю |
| SC-5(2)[1]{3} | іншою надмірністю. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за реагування на інциденти; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують управління пропускною спроможністю та надмірністю інформаційної системи, щоб обмежити наслідки затоплення інформацією атак відмови в обслуговуванні]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-5(3) | ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» - ВИЯВЛЕННЯ ТА МОНІТОРИНГ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-5(3)(a) | SC-5(3)(a)[1] | організація визначає засоби моніторингу для виявлення показників атаки «відмова в обслуговуванні» системи |
| SC-5(3)(a)[2] | використовувати визначені організацією засоби моніторингу для виявлення показників атаки «відмова в обслуговуванні» системи |
| SC-5(3)(b) | SC-5(3)(b)[1] | організація визначає системні ресурси щодо яких необхідно проводити моніторинг |
| SC-5(3)(b)[2] | проводити моніторинг визначених організацією системних ресурсів, щоб визначити, чи існують достатні ресурси для запобігання ефективним атакам «відмова в обслуговуванні». |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за виявлення та моніторинг].  Перевірка: [ВИБІР: Автоматизовані механізми, інструменти, що реалізують моніторинг інформаційної системи для атак відмови в обслуговуванні]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-6 | ДОСТУПНІСТЬ РЕСУРСІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-6[1] | SC-6[1][1] | організація визначає ресурси, які необхідно виділити для забезпечення захисту доступності ресурсів |
| SC-6[1][2] | організація визначає заходи з безпеки для забезпечення захисту доступності ресурсів |
| SC-6[2] | забезпечити захист доступності ресурсів, виділивши визначені організацією ресурси, по (один або кілька): | |
| SC-6[2] | пріоритет |
| SC-6[2] | квоти |
| SC-6[2] | визначені організацією заходи з безпеки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються пріоритетності ресурсів інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливості розподілу ресурсів; гарантії, що застосовуються для захисту доступності ресурсів]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-7 | ЗАХИСТ ПЕРИМЕТРА | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-7(a) | SC-7(a)[1] | контролювати зв'язком?: | |
| SC-7(a)[1][1] | на зовнішньому периметрі системи |
| SC-7(a)[1][2] | на ключових внутрішніх периметрах всередині системи |
| SC-7(a)[2] | управляти зв'язком: на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи | |
| SC-7(a)[2][1] | на зовнішньому периметрі системи |
| SC-7(a)[2][2] | на ключових внутрішніх периметрах всередині системи |
| SC-7(b) | Реалізувати підмережі для загальнодоступних системних компонентів, які є: | | |
| SC-7(b){1} | фізично відділені від внутрішніх мереж організації | |
| SC-7(b){2} | логічно відділені від внутрішніх мереж організації | |
| SC-7(c) | підключатись тільки через керовані інтерфейси, що складаються з пристроїв захисту периметру, розташованих відповідно до архітектури безпеки та приватності організації до: | | |
| SC-7(c){1} | зовнішніх мереж або | |
| SC-7(c){2} | зовнішніх систем | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; перелік ключових внутрішніх меж інформаційної системи; проєктна документація інформаційної системи; апаратне та програмне забезпечення захисту периметра; налаштування конфігурації інформаційної системи та відповідна документація; документація архітектури безпеки підприємства; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливість захисту периметра]. | | | |

|  |  |
| --- | --- |
| SC-7(1) | ЗАХИСТ ПЕРИМЕТРА - ФІЗИЧНО ВІДДІЛЕНІ ПІДМЕРЕЖІ |
|  | [Вилучено: Включено до SC-7]. |

|  |  |
| --- | --- |
| SC-7(2) | ЗАХИСТ ПЕРИМЕТРА - ПУБЛІЧНИЙ ДОСТУП |
|  | [Вилучено: Включено до SC-7]. |

|  |  |  |
| --- | --- | --- |
| SC-7(3) | ЗАХИСТ ПЕРИМЕТРА - ТОЧКИ ДОСТУПУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-7(3)[1] | обмежити кількість зовнішніх мережевих підключень до системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються охорони кордону; проєктна документація інформаційної системи; апаратне та програмне забезпечення захисту периметра; архітектура інформаційної системи та документація конфігурації; налаштування конфігурації інформаційної системи та відповідна документація; журнали моніторингу зв'язку та мережевого трафіку; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал з обов'язками щодо охорони кордонів].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливості захисту периметра; автоматизовані механізми, що обмежують кількість зовнішніх мережевих підключень до інформаційної системи]. | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SC-7(4) | ЗАХИСТ ПЕРИМЕТРА - ЗОВНІШНІ ТЕЛЕКОМУНІКАЦІЙНІ СЛУЖБИ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SC-7(4)(a) | запровадити керований інтерфейс для кожної зовнішньої телекомунікаційної служби | | | |
| SC-7(4)(b) | створити політику управління трафіком для кожного керованого інтерфейсу | | | |
| SC-7(4)(c) | SC-7(4)(c)[1] | забезпечити конфіденційність інформації, що передається через кожний інтерфейс | | |
| SC-7(4)(c)[2] | забезпечити цілісність інформації, що передається через кожний інтерфейс | | |
| SC-7(4)(d) | документувати кожне виключення з політики управління трафіком за допомогою: | | | |
| SC-7(4)(d)[1] | SC-7(4)(d)[1]{1} | підтримки завдань | |
| SC-7(4)(d)[1]{2} | підтримки потреби | |
| SC-7(4)(d)[2] | тривалості цієї потреби | | |
| SC-7(4)(e) | SC-7(4)(e)[1] | організація визначає частоту перегляду виключення з політики управління трафіком | | |
| SC-7(4)(e)[2] | SC-7(4)(e)[2][1] | переглянути виключення з політики управління трафіком з визначеною організацією частотою та | |
| SC-7(4)(e)[2][2] | видалити виключання, які більше не явно підтримуються: | |
| SC-7(4)(e)[2][2]{1} | цілями |
| SC-7(4)(e)[2][2]{2} | бизнес-потребою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика руху транспортних потоків; політика управління інформаційним потоком; процедури, що стосуються охорони кордону; архітектура безпеки інформаційної системи; проєктна документація інформаційної системи; апаратне та програмне забезпечення захисту периметра; архітектура інформаційної системи та документація конфігурації; налаштування конфігурації інформаційної системи та відповідна документація; записи про винятки з політики руху транспорту; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Організаційні процеси для документування та перегляду винятків із політики руху потоків; організаційні процеси для усунення винятків із політики руху транспорту; автоматизовані механізми, що реалізують можливість захисту периметра; керовані інтерфейси, що реалізують політику руху потоків]. | | | | |

|  |  |  |
| --- | --- | --- |
| SC-7(5) | ЗАХИСТ ПЕРИМЕТРА - ВІДМОВА ЗА ЗАМОВЧУВАННЯМ - ДОЗВІЛ ЗА ВИНЯТКОМ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-7(5)[1] | заборонити трафік мережевих комунікацій, за замовчуванням |
| SC-7(5)[2] | дозволити трафік мережевих комунікацій, за винятком керованих інтерфейсів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо безпеки захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують управління трафіком на керованих інтерфейсах]. | |

|  |  |
| --- | --- |
| SC-7(6) | ЗАХИСТ ПЕРИМЕТРА - ВІДПОВІДЬ НА РОЗПІЗНАНІ ПОМИЛКИ |
|  | [Вилучено: Включено до SC-7(18)]. |

|  |  |  |
| --- | --- | --- |
| SC-7(7) | ЗАХИСТ ПЕРИМЕТРА - ЗАПОБІГАННЯ ПОДІЛУ ТУНЕЛЮВАННЯ ДЛЯ ВІДДАЛЕНИХ ПРИСТРОЇВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-7(7)[1] | заборонити віддаленому приладу одночасне встановлення не віддалених підключень до системи та зв'язок через інші сполуки з ресурсами в зовнішніх мережах. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливості захисту периметра; автоматизовані механізми, що підтримують, обмежують віддалені з'єднання]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-7(8) | ЗАХИСТ ПЕРИМЕТРА -- МАРШРУТИЗАЦІЯ ТРАФІКУ З АВТЕНТИФІКОВАНИХ ПРОКСІ-СЕРВЕРІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-7(8)[1] | SC-7(8)[1][1] | визначений організацією внутрішній трафік комунікацій |
| SC-7(8)[1][2] | визначені організацією зовнішні мережі |
| SC-7(8)[2] | здійснювати маршрутизацію визначеного організацією внутрішнього трафіку комунікацій до визначених організацією зовнішніх мереж через автентифіковані проксі-сервери на керованих інтерфейсах | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметру].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують управління трафіком через автентифіковані проксі-сервери на керованих інтерфейсах]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-7(9) | ЗАХИСТ ПЕРИМЕТРА - ОБМЕЖЕННЯ ТРАФІКУ ВИХІДНИХ ПОВІДОМЛЕНЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-7(9)(a) | SC-7(9)(a)[1] | виявляти вихідний трафік зв'язку, що створює загрозу для зовнішніх систем |
| SC-7(9)(a)[2] | забороняти вихідний трафік зв'язку, що створює загрозу для зовнішніх систем |
| SC-7(9)(b) | проводити аудит ідентичності внутрішніх користувачів, пов'язаних з відмовою у зв'язку | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливість захисту периметра; автоматизовані механізми, що реалізують виявлення та заперечення загрози вихідному комунікаційному трафіку; автоматизовані механізми, що реалізують аудит вихідного комунікаційного трафіку]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-7(10) | ЗАХИСТ ПЕРИМЕТРА - ЗАПОБІГАННЯ ЕКСФІЛЬТРАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-7(10)(a) | запобігати ексфільтрації інформації | |
| SC-7(10)(b) | SC-7(10)(b)[1] | організація визначає частоту, з якою необхідно проводити тести на ексфільтрацію |
| SC-7(10)(b)[2] | проводити тести на ексфільтрацію з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливості захисту периметра; запобігання несанкціонованому розповсюдженню інформації через керовані інтерфейси]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-7(11) | ЗАХИСТ ПЕРИМЕТРА - ОБМЕЖЕННЯ ТРАФІКУ ВХІДНИХ ПОВІДОМЛЕНЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-7(11)[1] | SC-7(11)[1][1] | організація визначає авторизовані джерела від яких дозволено вхідні повідомлення |
| SC-7(11)[1][2] | організація визначає місця призначення куди направляє вхідні повідомлення від визначених організацією авторизованих джерел |
| SC-7(11)[2] | SC-7(11)[2][1] | дозволяти вхідні повідомлення від визначених організацією авторизованих джерел |
| SC-7(11)[2][2] | направляє вхідні повідомлення від визначених організацією авторизованих джерел до визначених організацією місць призначення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливості захисту меж щодо пар адрес джерела, призначення]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-7(12) | ЗАХИСТ ПЕРИМЕТРА - ЗАХИСТ НА ОСНОВІ ХОСТУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-7(12)[1] | SC-7(12)[1][1] | організація визначає механізми захисту периметру на основі хосту |
| SC-7(12)[1][2] | організація визначає компоненти системи, в яких реалізують визначені організацією механізми захисту периметру на основі хосту |
| SC-7(12)[2] | реалізувати визначені організацією механізми захисту периметру на основі хосту в визначені організацією компоненти системи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення захисту периметра; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, який відповідає за захисту периметра; користувачі інформаційної системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливості захисту на основі хосту]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-7(13) | ЗАХИСТ ПЕРИМЕТРА - ІЗОЛЯЦІЯ ЗАСОБІВ БЕЗПЕКИ, МЕХАНІЗМІВ І КОМПОНЕНТІВ ПІДТРИМКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-7(13)[1] | організація визначає: | |
| SC-7(13)[1][1] | засоби підтримки, пов’язані з інформаційною безпекою |
| SC-7(13)[1][2] | механізми підтримки, пов’язані з інформаційною безпекою |
| SC-7(13)[1][3] | компоненти підтримки, пов’язані з інформаційною безпекою |
| SC-7(13)[2] | ізолювати визначені організацією: засоби, механізми та компоненти підтримки, пов’язані з інформаційною безпекою від інших внутрішніх компонентів системи шляхом реалізації фізично окремих підмереж з керованими інтерфейсами з іншими компонентами системи | |
| SC-7(13)[2][1] | засоби підтримки, пов’язані з інформаційною безпекою від інших внутрішніх компонентів системи шляхом реалізації фізично окремих підмереж з керованими інтерфейсами з іншими компонентами системи |
| SC-7(13)[2][2] | механізми підтримки, пов’язані з інформаційною безпекою від інших внутрішніх компонентів системи шляхом реалізації фізично окремих підмереж з керованими інтерфейсами з іншими компонентами системи |
| SC-7(13)[2][3] | компоненти підтримки, пов’язані з інформаційною безпекою від інших внутрішніх компонентів системи шляхом реалізації фізично окремих підмереж з керованими інтерфейсами з іншими компонентами системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки та компонентів підтримки, які слід ізолювати від інших компонентів внутрішньої інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал з обов'язками щодо охорони кордонів].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують ізоляцію інструментів, механізмів та компонентів інформаційної безпеки]. | | |

|  |  |  |
| --- | --- | --- |
| SC-7(14) | ЗАХИСТ ПЕРИМЕТРА - ЗАХИСТ ВІД НЕСАНКЦІОНОВАНИХ ФІЗИЧНИХ З'ЄДНАНЬ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-7(14)[1] | організація визначає керовані інтерфейси, через які забезпечують захист від несанкціонованих фізичних з'єднань |
| SC-7(14)[2] | забезпечити захист від несанкціонованих фізичних з'єднань через визначені організацією керовані інтерфейси |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; комунікації та схема підключення об’єкта; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують захист від несанкціонованих фізичних з’єднань]. | |

|  |  |  |
| --- | --- | --- |
| SC-7(15) | ЗАХИСТ ПЕРИМЕТРА - МАРШРУТИЗАЦІЯ ДОСТУПУ ДО ПРИВІЛЕЙОВАНОЇ МЕРЕЖІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-7(15)[1] | здійснювати маршрутизацію всього мережевого привілейованого доступу через спеціальний, керований інтерфейс в цілях управління доступом та аудиту |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; журнали аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують маршрутизацію мережевого, привілейованого доступу через виділені керовані інтерфейси]. | |

|  |  |  |
| --- | --- | --- |
| SC-7(16) | ЗАХИСТ ПЕРИМЕТРА - ЗАПОБІГАННЯ ВИЯВЛЕННЮ КОМПОНЕНТІВ І ПРИСТРОЇВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-7(16)[1] | запобігати виявленню конкретних компонентів системи, які представляють керований інтерфейс |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують запобігання виявленню системних компонентів на керованих інтерфейсах]. | |

|  |  |  |
| --- | --- | --- |
| SC-7(17) | ЗАХИСТ ПЕРИМЕТРА - АВТОМАТИЧНЕ ПРИМУСОВЕ ВИКОНАННЯ ФОРМАТІВ ПРОТОКОЛІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-7(17)[1] | дотримуватися форматів протоколів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують примусове дотримання форматів протоколів]. | |

|  |  |  |
| --- | --- | --- |
| SC-7(18) | ЗАХИСТ ПЕРИМЕТРА - ЗБІЙ У БЕЗПЕЦІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-7(18)[1] | запобігати входу систем у незахищені стани у разі аварійного завершення роботи пристрою захисту периметра |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують захищений збій]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-7(19) | ЗАХИСТ ПЕРИМЕТРА - БЛОКУВАННЯ КОМУНІКАЦІЇ ВІД ХОСТІВ, ЩО НАЛАШТОВАНІ ПОЗА ОРГАНІЗАЦІЄЮ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-7(19)[1] | організація визначає клієнтів комунікацій, які незалежно налаштовуються кінцевими користувачами та зовнішніми постачальниками послуг | | |
| SC-7(19)[2] | блокувати трафік: | | |
| SC-7(19)[2][1] | вхідних повідомлень між визначеними організацією клієнтами комунікацій, які незалежно налаштовуються: | |
| SC-7(19)[2][1][1] | кінцевими користувачами |
| SC-7(19)[2][1][2] | зовнішніми постачальниками послуг |
| SC-7(19)[2][2] | вихідних повідомлень між визначені організацією клієнти комунікацій, які незалежно налаштовуються: | |
| SC-7(19)[2][2][1] | кінцевими користувачами |
| SC-7(19)[2][2][2] | зовнішніми постачальниками послуг |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР:Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік клієнтів зв'язку, які самостійно налаштовуються кінцевими користувачами та зовнішніми постачальниками послуг; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують блокування вхідного та вихідного комунікаційного трафіку між клієнтами зв'язку, незалежно налаштованими кінцевими користувачами та зовнішніми постачальниками послуг]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-7(20) | ЗАХИСТ ПЕРИМЕТРА - ДИНАМІЧНА ІЗОЛЯЦІЯ ТА ВІДОКРЕМЛЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-7(20)[1] | організація визначає системні компоненти, які необхідно: | |
| SC-7(20)[1][1] | динамічно ізолювати |
| SC-7(20)[1][2] | відокремлювати |
| SC-7(20)[2] | надавати можливість динамічно: | |
| SC-7(20)[2]{1} | ізолювати визначені організацією системні компоненти від інших компонентів системи |
| SC-7(20)[2]{2} | відокремлювати визначені організацією системні компоненти від інших компонентів системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік компонентів інформаційної системи, які слід динамічно ізолювати, відокремити від інших компонентів системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість динамічної ізоляції, відокремлення компонентів інформаційної системи]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-7(21) | ЗАХИСТ ПЕРИМЕТРА - ІЗОЛЯЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-7(21)[1] | SC-7(21)[1][1] | організація визначає компонент системи | |
| SC-7(21)[1][2] | організація визначає (один або кілька): | |
| SC-7(21)[1][2]{1} | цілі |
| SC-7(21)[1][2]{2} | бізнес-функції |
| SC-7(21)[2] | впровадити механізми захисту периметру, щоб відокремити визначений організацією компонент системи, який підтримує визначені організацією (один або кілька): | | |
| SC-7(21)[2]{1} | цілі | |
| SC-7(21)[2]{2} | бізнес-функції | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; документація з архітектури підприємства; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість розділення компонентів інформаційної системи, що підтримують організаційні місії та, або ділові функції]. | | | |

|  |  |  |
| --- | --- | --- |
| SC-7(22) | ЗАХИСТ ПЕРИМЕТРА - ОКРЕМІ ПІДМЕРЕЖІ ДЛЯ ПІДКЛЮЧЕННЯ ДО РІЗНИХ ДОМЕНІВ БЕЗПЕКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-7(22)[1] | реалізувати окремі мережні адреси для підключення до систем у різних доменах безпеки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують окремі мережеві адреси, різні підмережі]. | |

|  |  |  |
| --- | --- | --- |
| SC-7(23) | ЗАХИСТ ПЕРИМЕТРА - ВІДКЛЮЧЕННЯ ФУНКЦІЇ ЗВОРОТНОГО ЗВ'ЯЗКУ ВІДПРАВНИКА ПРО ПОМИЛКУ ПЕРЕВІРКИ ПРОТОКОЛУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-7(23)[1] | відключити зворотний зв'язок з відправниками при збої перевірки формату протоколу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують відключення зворотного зв’язку відправникам про помилку перевірки формату протоколу]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-7(24) | ЗАХИСТ ПЕРИМЕТРА - ПЕРСОНАЛЬНІ ДАНІ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-7(24){1} | для систем, які обробляють персональні дані: | | |
| SC-7(24){1}(a) | SC-7(24){1}(a)[1] | організація визначає правила обробки елементів персональних даних |
| SC-7(24){1}(a)[2] | застосовувати визначені організацією правила обробки до елементів персональних даних |
| SC-7(24){1}(b) | проводити контроль за дозволеною обробкою даних: | |
| SC-7(24){1}(b)[1] | на зовнішньому периметрі системи |
| SC-7(24){1}(b)[2] | на ключових внутрішніх периметрах у системі |
| SC-7(24){1}(c) | документувати кожне виключення при обробці | |
| SC-7(24){1}(d) | SC-7(24){1}(d)[1] | переглядати винятки, які більше не підтримуються |
| SC-7(24){1}(d)[2] | видаляти винятки, які більше не підтримуються |
| SC-7(24){2} | для систем, які зберігають персональні дані: | | |
| SC-7(24){2}(a) | SC-7(24){2}(a)[1] | організація визначає правила обробки елементів персональних даних |
| SC-7(24){2}(a)[2] | застосовувати визначені організацією правила обробки до елементів персональних даних |
| SC-7(24){2}(b) | проводити контроль за дозволеною обробкою даних: | |
| SC-7(24){2}(b)[1] | на зовнішньому периметрі системи |
| SC-7(24){2}(b)[2] | на ключових внутрішніх периметрах у системі |
| SC-7(24){2}(c) | документувати кожне виключення при обробці | |
| SC-7(24){2}(d) | SC-7(24){2}(d)[1] | переглядати винятки, які більше не підтримуються |
| SC-7(24){2}(d)[2] | видаляти винятки, які більше не підтримуються |
| SC-7(24){3} | для систем, які передають персональні дані: | | |
| SC-7(24){3}(a) | SC-7(24){3}(a)[1] | організація визначає правила обробки елементів персональних даних |
| SC-7(24){3}(a)[2] | застосовувати визначені організацією правила обробки до елементів персональних даних |
| SC-7(24){3}(b) | проводити контроль за дозволеною обробкою даних: | |
| SC-7(24){3}(b)[1] | на зовнішньому периметрі системи |
| SC-7(24){3}(b)[2] | на ключових внутрішніх периметрах у системі |
| SC-7(24){3}(c) | документувати кожне виключення при обробці | |
| SC-7(24){3}(d) | SC-7(24){3}(d)[1] | переглядати винятки, які більше не підтримуються |
| SC-7(24){3}(d)[2] | видаляти винятки, які більше не підтримуються |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація інформаційної системи; апаратне та програмне забезпечення інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал з обов'язками щодо захисту периметра].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують відключення зворотного зв’язку відправникам про помилку перевірки формату протоколу]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-8 | КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-8[1] | забезпечити для інформації, що передається (один або кілька): | |
| SC-8[1]{1} | конфіденційність |
| SC-8[1]{2} | цілісність |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують конфіденційність та, або цілісність передачі]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-8(1) | КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - КРИПТОГРАФІЧНИЙ ЗАХИСТ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-8(1)[1] | реалізувати механізми криптографічного захисту під час передачі для (один або більше): | |
| SC-8(1)[1]{1} | запобігання несанкціонованого розкриття інформації |
| SC-8(1)[1]{2} | вияву зміни в інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Криптографічні механізми, що підтримують та, або реалізують конфіденційність та, або цілісність передачі; автоматизовані механізми, що підтримують та, або впроваджують альтернативні фізичні запобіжні заходи; організаційні процеси для визначення та впровадження альтернативних фізичних гарантій]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-8(2) | КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ПОПЕРЕДНЯ І ПОСТ ОБРОБКА | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-8(2)[1] | підтримувати: | | |
| SC-8(2)[1][1] | під час підготовки до передачі (один або більше): | |
| SC-8(2)[1][1]{1} | конфіденційність |
| SC-8(2)[1][1]{2} | цілісність |
| SC-8(2)[1][2] | під час приймання інформації (один або більше): | |
| SC-8(2)[1][2]{1} | конфіденційність |
| SC-8(2)[1][2]{2} | цілісність |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують конфіденційність та, або цілісність передачі]. | | | |

|  |  |  |
| --- | --- | --- |
| SC-8(3) | КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - КРИПТОГРАФІЧНИЙ ЗАХИСТ ПОВІДОМЛЕНЬ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-8(3)[1] | організація визначає альтернативні фізичні заходи захисту |
| SC-8(3)[2] | реалізувати криптографічні механізми захисту зовнішніх повідомлень, якщо вони не захищені визначеними організацією альтернативними фізичним заходами захисту |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Криптографічні механізми, що підтримують та, або реалізують конфіденційність та, або цілісність для зовнішніх повідомлень; автоматизовані механізми, що підтримують та, або впроваджують альтернативні фізичні запобіжні заходи; організаційні процеси для визначення та впровадження альтернативних фізичних гарантій]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-8(4) | КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ПРИХОВУВАННЯ АБО РАНДОМІЗАЦІЯ КОМУНІКАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-8(4)[1] | організація визначає альтернативні фізичні заходи безпеки | |
| SC-8(4)[2] | впровадити криптографічні механізми для: | |
| SC-8(4)[2]{1} | приховування шаблонів комунікації, якщо вони не захищені визначеними організацією альтернативними фізичними заходами безпеки |
| SC-8(4)[2]{2} | рандомізації шаблонів комунікації, якщо вони не захищені визначеними організацією альтернативними фізичними заходами безпеки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Криптографічні механізми, що підтримують та, або реалізують приховування або рандомізацію шаблонів зв'язку; автоматизовані механізми, що підтримують та, або впроваджують альтернативні фізичні запобіжні заходи; організаційні процеси для визначення та впровадження альтернативних фізичних гарантій]. | | |

|  |  |
| --- | --- |
| SC-9 | КОНФІДЕНЦІЙНІСТЬ ПЕРЕДАЧІ |
|  | [Вилучено: Включено до SC-8]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-10 | ВІДКЛЮЧЕННЯ МЕРЕЖІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-10[1] | організація визначає період часу бездіяльності, після якого необхідно завершити з'єднання з мережею | |
| SC-10[2] | Завершити з'єднання з мережею, яке пов'язане з сеансом зв'язку в: | |
| SC-10[2]{1} | кінці сеансу |
| SC-10[2]{2} | після визначеного організацією періоду часу бездіяльності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: політика захисту системи та комунікацій; процедури розв’язання проблеми відключення мережі; проєктна документація інформаційної системи; план безпеки; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість відключення мережі]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-11 | ДОВІРЕНИЙ КАНАЛ ЗВ’ЯЗКУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-11(a) | ізольований надійний канал зв'язку для зв'язку між користувачем і довіреними компонентами системи надати: | | |
| SC-11(a){1} | фізично | |
| SC-11(a){2} | логічно | |
| SC-11(b) | SC-11(b)[1] | організація визначає функції безпеки для обміну даними, з яким користувач може запросити довірений канал зв'язку | |
| SC-11(b)[2] | дозволити користувачам запросити довірений канал зв'язку для обміну даними між користувачем і наступними функціями безпеки системи, включаючи як мінімум: | |
| SC-11(b)[2][1] | автентифікацію |
| SC-11(b)[2][2] | повторну автентифікацію |
| SC-11(b)[2][3] | визначені організацією функції безпеки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються надійних шляхів зв'язку; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; результати оцінки незалежними випробувальними організаціями; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують довірені шляхи зв'язку]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-11(1) | ДОВІРЕНИЙ КАНАЛ ЗВ’ЯЗКУ - ЛОГІЧНА ІЗОЛЯЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-11(1)(a) | забезпечити надійний канал зв’язку, який незаперечно відрізняється від інших каналів зв'язку | |
| SC-11(1)(b) | SC-11(1)(b)[1] | організація визначає функції безпеки |
| SC-11(1)(b)[2] | Ініціювати надійний канал зв'язку для зв'язку між визначеними організацією функціями безпеки системи та користувачем. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються надійних шляхів зв'язку; план безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; результати оцінки незалежними випробувальними організаціями; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують довірені шляхи зв'язку]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-12 | ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-12[1] | організація визначає вимоги до: | | |
| SC-12[1][1] | генерації | |
| SC-12[1][2] | поширення | |
| SC-12[1][3] | зберігання | |
| SC-12[1][4] | доступу | |
| SC-12[1][5] | знищення ключів | |
| SC-12[2] | SC-12[2][1] | встановити криптографічні ключі для криптографічних засобів, які використовуються в системі відповідно до визначених організацією вимог до: | |
| SC-12[2][1][1] | генерації |
| SC-12[2][1][2] | поширення |
| SC-12[2][1][3] | зберігання |
| SC-12[2][1][4] | доступу |
| SC-12[2][1][5] | знищення ключів |
| SC-12[2][2] | управляти криптографічними ключами для криптографічних засобів, які використовуються в системі відповідно до визначених організацією вимог до: | |
| SC-12[2][2][1] | генерації |
| SC-12[2][2][2] | поширення |
| SC-12[2][2][3] | зберігання |
| SC-12[2][2][4] | доступу |
| SC-12[2][2][5] | знищення ключів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються встановлення та управління криптографічним ключем; проєктна документація інформаційної системи; криптографічні механізми; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, відповідальний за встановлення та, або управління криптографічним ключем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують встановлення та управління криптографічним ключем]. | | | |

|  |  |  |
| --- | --- | --- |
| SC-12(1) | ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - ДОСТУПНІСТЬ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-12(1)[1] | підтримувати доступність інформації у разі втрати користувачами криптографічних ключів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються встановлення, управління та відновлення криптографічного ключа; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, відповідальний за створення та управління криптографічним ключем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують встановлення та управління криптографічним ключем]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-12(2) | ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СИМЕТРИЧНІ КЛЮЧІ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-12(2)[1] | встановити симетричні криптографічні ключі, використовуючи | | |
| SC-12(2)[1]{1} | стандартизовані уповноваженим органом: | |
| SC-12(2)[1]{1}[1] | технології управління ключами |
| SC-12(2)[1]{1}[2] | процеси управління ключами |
| SC-12(2)[1]{2} | узгоджені уповноваженим органом | |
| SC-12(2)[1]{2}[1] | технології управління ключами |
| SC-12(2)[1]{2}[2] | процеси управління ключами |
| SC-12(2)[2] | контролювати симетричні криптографічні ключі, використовуючи | | |
| SC-12(2)[2]{1} | стандартизовані уповноваженим органом: | |
| SC-12(2)[2]{1}[1] | технології управління ключами |
| SC-12(2)[2]{1}[2] | процеси управління ключами |
| SC-12(2)[2]{2} | узгоджені уповноваженим органом | |
| SC-12(2)[2]{2}[1] | технології управління ключами |
| SC-12(2)[2]{2}[2] | процеси управління ключами |
| SC-12(2)[3] | розповсюджувати симетричні криптографічні ключі, використовуючи: | | |
| SC-12(2)[3]{1} | стандартизовані уповноваженим органом: | |
| SC-12(2)[3]{1}[1] | технології управління ключами |
| SC-12(2)[3]{1}[2] | процеси управління ключами |
| SC-12(2)[3]{2} | узгоджені уповноваженим органом: | |
| SC-12(2)[3]{2}[1] | технології управління ключами |
| SC-12(2)[3]{2}[2] | процеси управління ключами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються встановлення та управління криптографічним ключем; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік криптографічних продуктів, підтверджених уповноваженим органом; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал, відповідальний за створення та управління криптографічним ключем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують симетричне встановлення та управління криптографічним ключем]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-12(3) | ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - АСИМЕТРИЧНІ КЛЮЧІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-12(3)[1] | організація визначає «ключовий» матеріал для: | |
| SC-12(3)[1][1] | вироблення асиметричних криптографічних ключів |
| SC-12(3)[1][2] | керування асиметричними криптографічними ключами |
| SC-12(3)[1][3] | поширення асиметричних криптографічних ключів |
| SC-12(3)[2] | Виробляти асиметричні криптографічні ключі, використовуючи: | |
| SC-12(3)[2]{1} | затверджені уповноваженим органом технології |
| SC-12(3)[2]{2} | затверджені уповноваженим органом процеси управління ключами |
| SC-12(3)[2]{3} | посилені сертифікати відкритого ключа |
| SC-12(3)[2]{4} | попередньо визначений «ключовий» матеріал |
| SC-12(3)[2]{5} | кваліфіковані сертифікати відкритого ключа |
| SC-12(3)[2]{6} | надійні апаратні засоби цифрового підпису (токени), які захищають особистий ключ користувача |
| SC-12(3)[2]{7} | сертифікати, видані відповідно до визначених організацією вимог |
| SC-12(3)[3] | керувати асиметричними криптографічними ключами, використовуючи: | |
| SC-12(3)[3]{1} | затверджені уповноваженим органом технології |
| SC-12(3)[3]{2} | затверджені уповноваженим органом процеси управління ключами |
| SC-12(3)[3]{3} | посилені сертифікати відкритого ключа |
| SC-12(3)[3]{4} | попередньо визначений «ключовий» матеріал |
| SC-12(3)[3]{5} | кваліфіковані сертифікати відкритого ключа |
| SC-12(3)[3]{6} | надійні апаратні засоби цифрового підпису (токени), які захищають особистий ключ користувача |
| SC-12(3)[3]{7} | сертифікати, видані відповідно до визначених організацією вимог |
| SC-12(3)[4] | поширювати асиметричні криптографічні ключі, використовуючи: | |
| SC-12(3)[4]{1} | затверджені уповноваженим органом технології |
| SC-12(3)[4]{2} | затверджені уповноваженим органом процеси управління ключами |
| SC-12(3)[4]{3} | посилені сертифікати відкритого ключа |
| SC-12(3)[4]{4} | попередньо визначений «ключовий» матеріал |
| SC-12(3)[4]{5} | кваліфіковані сертифікати відкритого ключа |
| SC-12(3)[4]{6} | надійні апаратні засоби цифрового підпису (токени), які захищають особистий ключ користувача |
| SC-12(3)[4]{7} | сертифікати, видані відповідно до визначених організацією вимог |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються встановлення та управління криптографічним ключем; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік криптографічних продуктів, затверджених уповноваженим органом; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; розробник системи; організаційний персонал, відповідальний за створення та управління криптографічним ключем; організаційний персонал, відповідальний за сертифікати відкритих ключів].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують асиметричне встановлення та управління криптографічним ключем]. | | |

|  |  |
| --- | --- |
| SC-12(4) | ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СЕРТИФІКАТИ PKI |
|  | [Вилучено: Включено до SC-12]. |

|  |  |
| --- | --- |
| SC-12(5) | ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СЕРТИФІКАТИ PKI, АПАРАТНІ ТОКЕНИ |
|  | [Вилучено: Включено до SC-12] |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-13 | КРИПТОГРАФІЧНИЙ ЗАХИСТ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-13[1] | SC-13[1][1] | організація визначає криптографічні застосування, які необхідні для кожного застосування |
| SC-13[1][2] | організація визначає тип криптографічного захисту, який необхідний для кожного застосування |
| SC-13[2] | впроваджувати наступні криптографічні засоби та тип криптографічного захисту для кожного застосування: | |
| SC-13[2][1] | визначені організацією криптографічні застосування, які необхідні для кожного застосування |
| SC-13[2][2] | визначені організацією тип криптографічного захисту, який необхідний для кожного застосування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються криптографічного захисту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; сертифікати перевірки криптографічного модуля; перелік перевірених криптографічних модулів; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, відповідальний за криптографічний захист].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують криптографічний захист]. | | |

|  |  |
| --- | --- |
| SC-13(1) | КРИПТОГРАФІЧНИЙ ЗАХИСТ - СТАНДАРТНА КРИПТОГРАФІЯ |
|  | [Вилучено: Включено до SC-13]. |

|  |  |
| --- | --- |
| SC-13(2) | КРИПТОГРАФІЧНИЙ ЗАХИСТ - ЗАТВЕРДЖЕНА УПОВНОВАЖЕНИМ ОРГАНОМ КРИПТОГРАФІЯ |
|  | [Вилучено: Включено до SC-13]. |

|  |  |
| --- | --- |
| SC-13(3) | КРИПТОГРАФІЧНИЙ ЗАХИСТ - ОСОБИ БЕЗ ОФІЦІЙНИХ ПОВНОВАЖЕНЬ |
|  | [Вилучено: Включено до SC-13]. |

|  |  |
| --- | --- |
| SC-13(4) | КРИПТОГРАФІЧНИЙ ЗАХИСТ - ЦИФРОВІ ПІДПИСИ |
|  | [Вилучено: Включено до SC-13]. |

|  |  |
| --- | --- |
| SC-14 | ЗАХИСТ ГРОМАДСЬКОГО ДОСТУПУ |
|  | [Вилучено: Включено до AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10]. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-15 | СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ ТА ДОДАТКИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-15(a) | SC-15(a)[1] | організація визначає виключення, в яких дозволена віддалена активація | |
| SC-15(a)[2] | заборонити віддалену активацію: | |
| SC-15(a)[2][1] | спільних обчислювальних пристроїв (хмар), визначених організацією виключення в яких, дозволена віддалена активація |
| SC-15(a)[2][2] | додатків з наступними виключеннями, визначених організацією виключення в яких дозволена віддалена активація |
| SC-15(b) | надати явну вказівку щодо використання користувачами фізично присутніми пристроями | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються спільних обчислень; політика та процедури контролю доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, відповідальний за управління спільними обчислювальними пристроями].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують управління віддаленою активацією спільних обчислювальних пристроїв; автоматизовані механізми, що забезпечують індикацію використання спільних обчислювальних пристроїв]. | | | |

|  |  |  |
| --- | --- | --- |
| SC-15(1) | СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - ФІЗИЧНЕ ВІДКЛЮЧЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-15(1)[1] | забезпечити фізичне відключення спільних обчислювальних пристроїв у спосіб, який підтримує зручність використання. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються спільних обчислень; політика та процедури контролю доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, відповідальний за управління спільними обчислювальними пристроями].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують фізичне відключення спільних обчислювальних пристроїв]. | |

|  |  |
| --- | --- |
| SC-15(2) | СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - БЛОКУВАННЯ ТРАФІКУ ВХІДНИХ І ВИХІДНИХ ПОВІДОМЛЕНЬ |
|  | [Вилучено: Включено до SC-7]. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SC-15(3) | СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - ВІДКЛЮЧЕННЯ ТА ВИДАЛЕННЯ В БЕЗПЕЧНИХ РОБОЧИХ ЗОНАХ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SC-15(3)[1] | SC-15(3)[1][1] | SC-15(3)[1][1]{1} | | визначені організацією системи | |
| SC-15(3)[1][1]{2} | | визначені організацією компоненти системи | |
| SC-15(3)[1][2] | визначені організацією безпечні робочі зони | | | |
| SC-15(3)[2] | SC-15(3)[2]{1} | відключати: | | | |
| SC-15(3)[2]{1}[1] | спільні обчислювальні пристрої з визначених організацією: | | |
| SC-15(3)[2]{1}[1]{1} | | систем у визначених організацією безпечних робочих зонах |
| SC-15(3)[2]{1}[1]{2} | | компонентів систем у визначених організацією безпечних робочих зонах |
| SC-15(3)[2]{1}[2] | додатки з визначених організацією: | | |
| SC-15(3)[2]{1}[1]{1} | | систем у визначених організацією безпечних робочих зонах |
| SC-15(3)[2]{1}[1]{2} | | компонентів систем у визначених організацією безпечних робочих зонах |
| SC-15(3)[2]{2} | Видаляти: | | | |
| SC-15(3)[2]{2}[1] | спільні обчислювальні пристрої з визначених організацією: | | |
| SC-15(3)[2]{2}[1]{1} | | систем у визначених організацією безпечних робочих зонах |
| SC-15(3)[2]{2}[1]{2} | | компонентів систем у визначених організацією безпечних робочих зонах |
| SC-15(3)[2]{2}[2] | додатки з визначених організацією: | | |
| SC-15(3)[2]{2}[1]{1} | | систем у визначених організацією безпечних робочих зонах |
| SC-15(3)[2]{2}[1]{2} | | компонентів систем у визначених організацією безпечних робочих зонах |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються спільних обчислень; політика та процедури контролю доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік безпечних робочих місць; інформаційні системи або компоненти інформаційної системи в захищених робочих зонах, де спільні обчислювальні пристрої слід вимкнути або видалити; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за управління спільними обчислювальними пристроями].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість вимкнення спільних обчислювальних пристроїв]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-15(4) | СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - ЧІТКА ІДЕНТИФІКАЦІЯ ПОТОЧНИХ УЧАСНИКІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-15(4)[1] | організація визначає: | |
| SC-15(4)[1][1] | онлайн-зустрічі |
| SC-15(4)[1][2] | телеконференції |
| SC-15(4)[1] | забезпечити явну ідентифікацію поточних учасників визначених організацією: | |
| SC-15(4)[1][1] | онлайн-зустрічей |
| SC-15(4)[1][2] | телеконференцій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються спільних обчислень; політика та процедури контролю доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; перелік видів зустрічей та телеконференцій, що вимагають чіткого зазначення поточних учасників; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за управління спільними обчислювальними пристроями].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість вказувати учасників на спільних обчислювальних пристроях]. | | |

|  |  |  |
| --- | --- | --- |
| SC-16 | ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-16[1] | організація визначає атрибути безпеки та приватності |
| SC-16[2] | пов’язувати визначені організацією атрибути безпеки та приватності з інформацією, яка передається між системами та компонентами системи. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються передачі атрибутів безпеки; політика та процедури контролю доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують передачу атрибутів безпеки між інформаційними системами]. | |

|  |  |  |
| --- | --- | --- |
| SC-16(1) | ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПЕРЕВІРКА ЦІЛІСНОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-16(1)[1] | перевіряти цілісність переданих атрибутів безпеки та приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються передачі атрибутів безпеки; політика та процедури контролю доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують перевірку цілісності переданих атрибутів безпеки]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-17 | СЕРТИФІКАТИ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-17[1] | організація визначає політика сертифікації | |
| SC-17[2] | випускати сертифікати відкритого ключа відповідно до: | |
| SC-17[2]{1} | визначена організацією політика сертифікації |
| SC-17[2]{2} | або отримувати сертифікати відкритого ключа від затвердженого постачальника послуг |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються сертифікатів інфраструктури відкритих ключів; політика або політики щодо сертифікатів відкритих ключів; процес видачі відкритого ключа; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за видачу сертифікатів відкритих ключів; постачальники послуг].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують управління сертифікатами інфраструктури відкритих ключів]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-18 | МОБІЛЬНИЙ КОД | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-18(a) | SC-18(a)[1] | визначати прийнятні: | |
| SC-18(a)[1][1] | мобільні коди |
| SC-18(a)[1][2] | технології мобільних кодів |
| SC-18(a)[2] | визначати неприйнятні: | |
| SC-18(a)[2][1] | мобільні коди |
| SC-18(a)[2][2] | технології мобільних кодів |
| SC-18(b) | Встановити | | |
| SC-18(b)[1] | обмеження на використання щодо впровадження прийнятних мобільних кодів та технологій мобільного коду | |
| SC-18(b)[1][1] | мобільні коди |
| SC-18(b)[1][2] | технології мобільних кодів |
| SC-18(b)[2] | рекомендації щодо впровадження прийнятних мобільних кодів та технологій мобільного коду | |
| SC-18(b)[2][1] | мобільні коди |
| SC-18(b)[2][2] | технології мобільних кодів |
| SC-18(c) | для мобільного коду всередині системи: | | |
| SC-18(c)[1] | проводити авторизацію використання | |
| SC-18(c)[2] | відстежувати використання | |
| SC-18(c)[3] | контролювати використання | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; обмеження використання мобільного коду, політика та процедури впровадження мобільного коду; перелік прийнятних мобільних кодів та технологій мобільних кодів; перелік неприйнятних мобільних кодів та мобільних технологій; авторизаційні записи; записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за управління мобільним кодом].  Перевірка: [ВИБІР: Організаційний процес контролю, авторизації, моніторингу та обмеження мобільного коду; автоматизовані механізми підтримки та, або реалізації управління мобільним кодом; автоматизовані механізми підтримки та, або реалізації моніторингу мобільного коду]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-18(1) | МОБІЛЬНИЙ КОД - ІДЕНТИФІКАЦІЯ НЕПРИЙНЯТНОГО КОДУ ТА ВЖИВАННЯ ВИПРАВНИХ ДІЙ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-18(1)[1] | SC-18(1)[1][1] | організація визначає неприйнятний мобільний код |
| SC-18(1)[1][2] | організація визначає виправні дії, які вживають у разі неприйнятного мобільного коду |
| SC-18(1)[2] | визначити неприйнятний мобільний код та вжити визначені організацією виправні дії | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; обмеження використання мобільного коду, політика та процедури впровадження мобільного коду; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; список неприйнятного мобільного коду; перелік коригувальних дій, які слід вжити при виявленні неприйнятного мобільного коду; записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, відповідальний за управління мобільним кодом].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість виявлення, перевірки та коригування мобільного коду]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-18(2) | МОБІЛЬНИЙ КОД - ПРИДБАННЯ, РОЗРОБКА ТА ВИКОРИСТАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-18(2)[1] | організація визначає вимоги до мобільного коду | |
| SC-18(2)[2] | переконатися, що: | |
| SC-18(2)[2][1] | придбання мобільного коду, який буде розгорнуто в системі, відповідає визначеним організацією вимогам до мобільного коду |
| SC-18(2)[2][2] | розробка мобільного коду, який буде розгорнуто в системі, відповідає визначеним організацією вимогам до мобільного коду |
| SC-18(2)[2][3] | використання мобільного коду, який буде розгорнуто в системі, відповідає визначеним організацією вимогам до мобільного коду |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; вимоги до мобільного коду; обмеження використання мобільного коду, політика та процедури впровадження мобільного коду; документація про придбання; договори придбання інформаційної системи, компонента системи або послуги інформаційної системи; документація життєвого циклу розробки системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за управління мобільним кодом; організаційний персонал, який відповідає за придбання та укладання контрактів]  Перевірка: [ВИБІР: Організаційні процеси для придбання, розробки та використання мобільного коду]. | | |

|  |  |  |
| --- | --- | --- |
| SC-18(3) | МОБІЛЬНИЙ КОД - ЗАПОБІГАННЯ ЗАВАНТАЖЕННЯ ТА ВИКОНАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-18(3)[1] | організація визначає неприйнятний мобільний код |
| SC-18(3)[2] | запобігати завантаженню та виконанню визначеного організацією неприйнятного мобільного коду |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; обмеження використання мобільного коду, політика та процедури впровадження мобільного коду; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, відповідальний за управління мобільним кодом].  Перевірка: [ВИБІР: Автоматизовані механізми, що перешкоджають завантаженню та виконанню неприйнятного мобільного коду]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-18(4) | МОБІЛЬНИЙ КОД - ЗАПОБІГАННЯ АВТОМАТИЧНОГО ВИКОНАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-18(4)[1] | SC-18(4)[1][1] | визначене організацією програмне забезпечення |
| SC-18(4)[1][2] | визначені організацією дії |
| SC-18(4)[2] | SC-18(4)[2][1] | запобігати автоматичному виконанню мобільного коду у визначеному організацією програмному забезпеченню |
| SC-18(4)[2][2] | забезпечити виконання визначених організацією дій перед виконанням коду |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; обмеження використання мобільного коду; політика та процедури впровадження мобільного коду; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік програмних програм, для яких повинно бути заборонено автоматичне виконання мобільного коду; перелік дій, необхідних перед виконанням мобільного коду; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, відповідальний за управління мобільним кодом].  Перевірка: [ВИБІР: Автоматизовані механізми, що запобігають автоматичному виконанню неприйнятного мобільного коду; автоматизовані механізми, що забезпечують дії, які слід вжити до виконання мобільного коду]. | | |

|  |  |  |
| --- | --- | --- |
| SC-18(5) | МОБІЛЬНИЙ КОД - ДОЗВІЛ ВИКОНАННЯ ТІЛЬКИ В ОБМЕЖЕНИХ СЕРЕДОВИЩАХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-18(5)[1] | допускати виконання дозволеного мобільного коду лише на обмежених віртуальних машинних середовищах |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; дозволи на використання мобільного коду; обмеження використання мобільного коду; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік обмежених середовищ віртуальних машин, для яких дозволено виконання організаційно прийнятного мобільного коду; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, відповідальний за управління мобільним кодом].  Перевірка: [ВИБІР: Автоматизовані механізми, що дозволяють виконувати дозволений мобільний код в обмежених середовищах віртуальної машини]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-19 | ІНТЕРНЕТ-ПРОТОКОЛ ГОЛОСОВОГО ЗВ’ЯЗКУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-19(a) | Встановити обмеження на: | |
| SC-19(a)[1] | використання щодо впровадження VoIP-технологій |
| SC-19(a)[2] | рекомендації щодо впровадження VoIP-технологій |
| SC-19(b) | SC-19(b)[1] | проводити авторизацію при використанні VoIP-технологій в системі |
| SC-19(b)[2] | відстежувати використання VoIP-технологій в системі |
| SC-19(b)[3] | контролювати використання VoIP-технологій в системі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються VoIP; Обмеження використання VoIP; Вказівки щодо впровадження VoIP; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за управління VoIP].  Перевірка: [ВИБІР: Організаційний процес авторизації, моніторингу та контролю VoIP; автоматизовані механізми, що підтримують та, або впроваджують авторизацію, моніторинг та контроль VoIP]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-20 | БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-20(a) | разом з офіційними даними розпізнавання імен, які система повертає у відповідь на запити дозволу імен, адрес, надати додаткові дані: | |
| SC-20(a)[1] | автентифікації джерела даних |
| SC-20(a)[2] | перевірки цілісності джерела даних |
| SC-20(b) | SC-20(b)[1] | надати засоби для вказівки статусу безпеки дочірніх зон і |
| SC-20(b)[2] | якщо дочірня зона підтримує служби безпечного дозволу, забезпечити перевірку ланцюга довіри між батьківськими та дочірніми доменами при роботі у складі розподіленого ієрархічного простору імен |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються служби захисту імен, адрес (авторитетне джерело); проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; інші відповідні документи або записи].  Співбесіда: [ВИБІР: адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за управління DNS].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують безпечну службу дозволу імен, адрес]. | | |

|  |  |
| --- | --- |
| SC-20(1) | БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) - ДОЧІРНІЙ ПІДПРОСТІР |
|  | [Вилучено: включено до SC-20]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-20(2) | БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) - ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-20(2)[1] | забезпечити: | |
| SC-20(2)[1][1] | справжність джерела походження |
| SC-20(2)[1][2] | цілісність запитів внутрішніх імен, адрес |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються служби захисту імен, адрес (авторитетне джерело); проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за управління DNS].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують захист походження та цілісності даних для внутрішніх запитів служби дозволу імен, адрес]. | | |

|  |  |  |
| --- | --- | --- |
| SC-21 | БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (РЕКУРСИВНИЙ АБО КЕШУЮЧИЙ ПЕРЕТВОРЮВАЧ) | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-21[1] | зробити запит щодо автентичності джерела даних у відповідях на дозвіл імен, адрес, які система отримує від уповноважених джерел |
| SC-21[2] | виконати перевірку автентичності джерела даних у відповідях на дозвіл імен, адрес, які система отримує від уповноважених джерел |
| SC-21[3] | виконати перевірку цілісності даних у відповідях на дозвіл імен, адрес, які система отримує від уповноважених джерел. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захищеної служби імен, адрес (перетворювач рекурсивного або кешування); проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за управління DNS].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують аутентифікацію походження даних та перевірку цілісності даних для служб розрізнення імен, адрес]. | |

|  |  |
| --- | --- |
| SC-21(1) | БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (РЕКУРСИВНИЙ АБО КЕШУЮЧИЙ ПЕРЕТВОРЮВАЧ) - ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ |
|  | [Вилучено: Включено до SC-21] |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-22 | АРХІТЕКТУРА І ЗАБЕЗПЕЧЕННЯ СЛУЖБИ ІМЕН, АДРЕС | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-22[1] | переконатися, що системи, які спільно надають послуги розпізнавання імен, адрес для організації: | | |
| SC-22[1][1] | є відмовостійкими | |
| SC-22[1][2] | забезпечують поділ: | |
| SC-22[1][2][1] | внутрішніх ролей |
| SC-22[1][[2]2] | зовнішніх ролей |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються архітектури та надання послуг з розпізнавання імен, адрес; політика та процедури контролю доступу; проєктна документація інформаційної системи; результати оцінки незалежними випробувальними організаціями; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за управління DNS].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують службу розпізнавання імен, адрес для відмовостійкості та поділу ролей]. | | | |

|  |  |  |
| --- | --- | --- |
| SC-23 | АВТЕНТИФІКАЦІЯ СЕСІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-23[1] | забезпечити автентифікацію сеансів зв'язку. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються справжності сесії; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують автентичність сеансу]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-23(1) | АВТЕНТИФІКАЦІЯ СЕСІЇ - АНУЛЮВАННЯ ІДЕНТИФІКАТОРА СЕАНСУ ЗВ’ЯЗКУ ПРИ ВИХОДІ З СИСТЕМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-23(1)[1] | анулювати ідентифікатор сеансу зв’язку після: | |
| SC-23(1)[1]{1} | виходу користувача |
| SC-23(1)[1]{2} | іншого припинення сеансу зв’язку |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: політика захисту системи та комунікацій; процедури, що стосуються справжності сесії; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують недійсність ідентифікатора сеансу після завершення сеансу]. | | |

|  |  |
| --- | --- |
| SC-23(2) | АВТЕНТИФІКАЦІЯ СЕСІЇ - ІНІЦІЙОВАНІ КОРИСТУВАЧЕМ ВИХОДИ ТА ПОВІДОМЛЕННЯ |
|  | [Вилучено: Включено до SC-21(1)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-23(3) | АВТЕНТИФІКАЦІЯ СЕСІЇ - УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-23(3)[1] | організація визначає вимоги до випадковостей, за допомогою яких створюють унікальний ідентифікатор сеансу зв’язку для кожного сеансу зв’язку | |
| SC-23(3)[2] | SC-23(3)[2][1] | створювати унікальний ідентифікатор сеансу зв’язку для кожного сеансу зв’язку за допомогою визначених організацією вимог до випадковостей |
| SC-23(3)[2][2] | розпізнавати лише ідентифікатори сеансів зв’язку, які генеруються системою. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються справжності сесії; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують створення та моніторинг унікальних ідентифікаторів сеансу; автоматизовані механізми, що підтримують та, або реалізують вимоги щодо випадковості]. | | |

|  |  |
| --- | --- |
| SC-23(4) | АВТЕНТИФІКАЦІЯ СЕСІЇ - УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ |
|  | [Вилучено: Включено до SC-23(3)]. |

|  |  |  |
| --- | --- | --- |
| SC-23(5) | АВТЕНТИФІКАЦІЯ СЕСІЇ - ДОЗВОЛЕНІ УПОВНОВАЖЕННІ З СЕРТИФІКАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-23(5)[1] | організація визначає уповноважених зі сертифікації для перевірки встановлення захищених сеансів |
| SC-23(5)[2] | дозволяти використання лише визначених організацією уповноважених зі сертифікації для перевірки встановлення захищених сеансів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються справжності сесії; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік органів сертифікації, дозволених для перевірки встановлення захищених сесій; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують управління органами сертифікації]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-24 | УВЕДЕННЯ У ВІДОМИЙ СТАН | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-24[1] | SC-24[1][1] | організація визначає відомий системний стан |
| SC-24[1][2] | організація визначає типи збоїв системи |
| SC-24[1][3] | організація визначає інформація про стан системи |
| SC-24[2] | увести систему у визначений організацією відомий системний стан у разі виникнення визначених організацією типів збоїв системи зі збереженням визначеної організацією інформації про стан системи при збої. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються відмови інформаційної системи до відомого стану; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік відмов, що вимагають відмови інформаційної системи у відомому стані; інформація про стан, яка повинна зберігатися при відмові системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість відомого стану відмов; автоматизовані механізми, що зберігають інформацію про стан системи у разі відмови системи]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-25 | ТОНКІ ВУЗЛИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-25[1] | організація визначає системні компоненти з: | |
| SC-25[1][1] | мінімальною функціональністю |
| SC-25[1][2] | зберіганням інформації |
| SC-25[2] | використовувати визначені організацією системні компоненти з: | |
| SC-25[2][1] | мінімальною функціональністю |
| SC-25[2][2] | зберіганням інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються використання тонких вузлів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують тонкі вузли]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-26 | ПРИМАНКА ДЛЯ ЗЛОВМИСНИКІВ (HONEYPOTS) | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-26[1] | включати в систему компоненти, які спеціально призначені як об’єкти атак, з метою: | |
| SC-26[1][1] | виявлення таких атак |
| SC-26[1][2] | відбиття таких атак |
| SC-26[1][3] | аналізу таких атак |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються використання приманок; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та, або впроваджують приманки]. | | |

|  |  |
| --- | --- |
| SC-26(1) | ПРИМАНКА ДЛЯ ЗЛОВМИСНИКІВ (HONEYPOTS) - ВИЯВЛЕННЯ ШКІДЛИВОГО КОДУ |
|  | [Вилучено: Включено до SC-35] |

|  |  |  |
| --- | --- | --- |
| SC-27 | НЕЗАЛЕЖНІ ВІД ПЛАТФОРМИ ДОДАТКИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-27[1] | організація визначає незалежні від платформи додатки |
| SC-27[2] | включити до системи визначені організацією незалежні від платформи додатки |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються незалежних від платформи додатків; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік незалежних від платформи програм; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують незалежні від платформи програми]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-28 | ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-28[1] | організація визначає інформацію, яку властивість у стані спокою необхідно забезпечити (один або кілька): | |
| SC-28[1]{1} | конфіденційність |
| SC-28[1]{2} | цілісність |
| SC-28[2] | визначена організацією інформація в стані спокою щодо забезпечення (один або кілька): | |
| SC-28[2]{1} | конфіденційність |
| SC-28[2]{2} | цілісність |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації в стані спокою; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; криптографічні механізми та пов'язана з ними конфігураційна документація; перелік інформації в стані спокою, що вимагає конфіденційності та захисту цілісності; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують захист конфіденційності та цілісності для інформації, що перебуває в стані спокою]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-28(1) | ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ - КРИПТОГРАФІЧНИЙ ЗАХИСТ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-28(1)[1] | SC-28(1)[1][1] | організація визначає інформацію, яка потребує впровадженню криптографічних механізмів для запобігання: | |
| SC-28(1)[1][1][1] | несанкціонованого розкриття |
| SC-28(1)[1][1][2] | несанкціонованої модифікації |
| SC-28(1)[1][2] | організація визначає компоненти системи, на яких знаходиться визначена організацією інформація в стані спокою | |
| SC-28(1)[2] | впровадити криптографічні механізми для запобігання: | | |
| SC-28(1)[2][1] | несанкціонованого розкриття визначеної організацією інформації у стані спокою відносно визначених організацією компонентів системи | |
| SC-28(1)[2][2] | несанкціонованої модифікації визначеної організацією інформації у стані спокою відносно визначених організацією компонентів системи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації в стані спокою; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; криптографічні механізми та пов'язана з ними конфігураційна документація; перелік інформації в стані спокою, що вимагає конфіденційності та захисту цілісності; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують захист конфіденційності та цілісності для інформації, що перебуває в стані спокою]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-28(2) | ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ - АВТОНОМНЕ СХОВИЩЕ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-28(2)[1] | організація визначає інформацію, яку необхідно: | |
| SC-28(2)[1][1] | видаляти з онлайнового сховища |
| SC-28(2)[1][2] | зберігати її в автономному(off-line) режимі у безпечному місці |
| SC-28(2)[2] | SC-28(2)[2][1] | видаляти визначену організацією інформацію з онлайнового сховища |
| SC-28(2)[2][2] | зберігати її в автономному(off-line) режимі у безпечному місці |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації в стані спокою; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; криптографічні механізми та пов'язана з ними конфігураційна документація; автономні місця зберігання інформації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують видалення інформації з Інтернет-сховища; автоматизовані механізми підтримки та, або реалізації зберігання інформації в режимі офлайн]. | | |

|  |  |  |
| --- | --- | --- |
| SC-29 | ГЕТЕРОГЕННІСТЬ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-29[1] | організація визначає системні компоненти, для яких слід використовувати різноманітний набір інформаційних технологій при впровадженні системи |
| SC-29[2] | використовувати різноманітний набір інформаційних технологій для визначених організацією системних компонентів при впровадженні системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік технологій, що застосовуються в інформаційній системі; документація про придбання; договори придбання компонентів або послуг інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який відповідає за придбання, розробку та впровадження інформаційної системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують використання різноманітного набору інформаційних технологій]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-29(1) | ГЕТЕРОГЕННІСТЬ - МЕТОДИ ВІРТУАЛІЗАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-29(1)[1] | організація визначає частоту, з якою необхідно використовувати методи віртуалізації для підтримки розгортання різноманітних операційних систем і програм | |
| SC-29(1)[2] | використовувати методи віртуалізації для підтримки розгортання різноманітних операційних: | |
| SC-29(1)[2][1] | систем, що змінюються з визначеною організацією частотою |
| SC-29(1)[2][2] | програм, що змінюються з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту систем та комунікацій; політика та процедури управління конфігурацією; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; перелік операційних систем та додатків, розгорнутих з використанням методів віртуалізації; записи контролю; записи управління конфігурацією; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за впровадження затверджених методів віртуалізації в інформаційну систему].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують використання різноманітного набору інформаційних технологій; автоматизовані механізми, що підтримують та, або впроваджують методи віртуалізації]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-30 | МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-30[1] | SC-30[1][1] | Організація визначає методи маскування | |
| SC-30[1][2] | Організація визначає методи хибного напряму | |
| SC-30[1][3] | Організація визначає системи | |
| SC-30[1][4] | Організація визначає період часу | |
| SC-30[2] | використовувати визначені організацією методи: | | |
| SC-30[2][1] | маскування для визначеної організацією системи у визначений організацією період часу, щоб: | |
| SC-30[2][1][1] | заплутати зловмисників |
| SC-30[2][1][2] | ввести в оману зловмисників |
| SC-30[2][2] | хибного напряму для визначеної організацією системи у визначений організацією період часу, щоб: | |
| SC-30[2][2][1] | заплутати зловмисників |
| SC-30[2][2][2] | ввести в оману зловмисників |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються методів маскування та хибного напряму для інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; перелік методів маскування та хибного напряму, які застосовуватимуться в організаційних інформаційних системах; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за впровадження методів маскування та хибного напряму для інформаційних систем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують методи маскування та хибного напряму]. | | | |

|  |  |
| --- | --- |
| SC-30(1) | МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - МЕТОДИ ВІРТУАЛІЗАЦІЇ |
|  | [Вилучено: Включено до SC-29(1)]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-30(2) | МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - ВИПАДКОВІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-30(2)[1] | організація визначає методи для введення фактору випадковості в операції та активи організації | |
| SC-30(2)[2] | використовувати визначені організацією методи, щоб ввести фактор випадковості в: | |
| SC-30(2)[2][1] | операції організації |
| SC-30(2)[2][2] | активи організації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються методів маскування та хибного напряму для інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; перелік методів, що застосовуються для введення випадковості в організаційні операції та активи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за впровадження методів маскування та хибного напряму для інформаційних систем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують випадковість як техніку маскування та хибного напряму]. | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SC-30(3) | МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - ЗМІНА МІСЦЯ ОБРОБКИ ТА ЗБЕРІГАННЯ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SC-30(3)[1] | SC-30(3)[1][1] | SC-30(3)[1][1]{1} | організація визначає місце обробки та, або | |
| SC-30(3)[1][1]{2} | організація визначає місце зберігання | |
| SC-30(3)[1][2] | організація визначає моменти часу, у які змінюється місце обробки або зберігання | | |
| SC-30(3)[2] | змінювати визначене організацією місце (один або кілька): | | | |
| SC-30(3)[2]{1} | обробки у: | | |
| SC-30(3)[2]{1}{1} | | визначені організацією моменти часу; |
| SC-30(3)[2]{1}{2} | | випадкових часових інтервалах |
| SC-30(3)[2]{2} | зберігання у: | | |
| SC-30(3)[2]{2}{1} | | визначені організацією моменти часу; |
| SC-30(3)[2]{2}{2} | | випадкових часових інтервалах |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури управління конфігурацією; процедури, що стосуються методів маскування та хибного напряму для інформаційної системи; перелік місць обробки, зберігання, які слід змінювати через організаційні інтервали часу; змінити записи контролю; записи управління конфігурацією; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за зміну місць обробки та, або зберігання].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують змінні місця обробки та, або зберігання]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-30(4) | МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - НЕПРАВДИВА ІНФОРМАЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-30(4)[1] | Організація визначає компоненти системи | |
| SC-30(4)[2] | використовувати реалістичну, але неправдиву інформацію в: визначених організацією компонентах системи про її: | |
| SC-30(4)[2]{1} | стан безпеки |
| SC-30(4)[2]{2} | положення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури управління конфігурацією; процедури, що стосуються методів маскування та хибного напряму для інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за визначення та використання реалістичної, але оманливої інформації про стан безпеки компонентів інформаційної системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують використання реалістичної, але оманливої інформації про стан безпеки компонентів інформаційної системи]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-30(5) | МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - МАСКУВАННЯ СИСТЕМНИХ КОМПОНЕНТІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-30(5)[1] | SC-30(5)[1][1] | Організація визначає методи, щоб: | |
| SC-30(5)[1][1]{1} | приховати визначені організацією компоненти системи |
| SC-30(5)[1][1]{2} | замаскувати визначені організацією компоненти системи |
| SC-30(5)[1][2] | Організація визначає компоненти системи, які необхідно: | |
| SC-30(5)[1][2]{1} | приховати |
| SC-30(5)[1][2]{2} | замаскувати |
| SC-30(5)[2] | використовувати визначені організацією методи, щоб: | | |
| SC-30(5)[2]{1} | приховати визначені організацією компоненти системи | |
| SC-30(5)[2]{2} | замаскувати визначені організацією компоненти системи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури управління конфігурацією; процедури, що стосуються методів маскування та хибного напряму для інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік методів, що застосовуються для приховування або замаскування компонентів інформаційної системи; перелік компонентів інформаційної системи, які слід приховати або замаскувати; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за приховування компонентів системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують методи для приховування системних компонентів]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-31 | АНАЛІЗ ПРИХОВАНОГО КАНАЛУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-31(a) | проводити аналіз прихованого каналу, щоб визначити ті аспекти комунікацій в системі, які володіють потенційними можливостями для реалізації прихованих каналів (один або кілька): | |
| SC-31(a){1} | зберігання |
| SC-31(a){2} | синхронізації |
| SC-31(b) | оцінює максимальну пропускну здатність цих каналів | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються аналізу прихованих каналів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація про аналіз прихованих каналів; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який несе відповідальність за таємний аналіз каналів; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Організаційний процес для проведення аналізу прихованих каналів; автоматизовані механізми, що підтримують та, або впроваджують аналіз прихованих каналів; автоматизовані механізми, що підтримують та, або реалізують можливість оцінки пропускної можливості прихованих каналів]. | | |

|  |  |  |
| --- | --- | --- |
| SC-31(1) | АНАЛІЗ ПРИХОВАНОГО КАНАЛУ - ТЕСТУВАННЯ ПРИХОВАНИХ КАНАЛІВ ДЛЯ ЕКСПЛУАТАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-31(1)[1] | тестувати підмножини визначених прихованих каналів, щоб визначити, які канали можна використовувати |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються аналізу прихованих каналів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; список прихованих каналів; документація про аналіз прихованих каналів; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який несе відповідальність за прихований аналіз каналів]  Перевірка: [ВИБІР: Організаційний процес для тестування прихованих каналів; автоматизовані механізми, що підтримують та, або впроваджують тестування аналізу прихованих каналів]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-31(2) | АНАЛІЗ ПРИХОВАНОГО КАНАЛУ - МАКСИМАЛЬНА ПРОПУСКНА ЗДАТНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-31(2)[1] | Організація визначає значення максимальної пропускної здатності для визначених прихованих каналів: | |
| SC-31(2)[1]{1} | зберігання |
| SC-31(2)[1]{2} | синхронізації |
| SC-31(2)[2] | зменшувати максимальну пропускну здатність для визначених прихованих каналів (один або більше): | |
| SC-31(2)[2]{1} | зберігання до визначеного організацією значення |
| SC-31(2)[2]{2} | синхронізації до визначеного організацією значення |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються аналізу прихованих каналів; контракти на придбання інформаційних систем або послуг; документація про придбання; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація про аналіз прихованих каналів; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який несе відповідальність за таємний аналіз каналів; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Організаційний процес для проведення аналізу прихованих каналів; автоматизовані механізми, що підтримують та, або впроваджують аналіз прихованих каналів; автоматизовані механізми, що підтримують та, або реалізують можливість зменшення пропускної можливості прихованих каналів]. | | |

|  |  |  |
| --- | --- | --- |
| SC-31(3) | АНАЛІЗ ПРИХОВАНОГО КАНАЛУ - ВИМІРЮВАННЯ ПРОПУСКНУ ЗДАТНІСТЬ В РОБОЧИХ СЕРЕДОВИЩАХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-31(3)[1] | Організація визначає підмножину визначених прихованих каналів |
| SC-31(3)[2] | вимірювати пропускну здатність визначеної організацією підмножини визначених прихованих каналів в операційному середовищі системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються аналізу прихованих каналів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація про аналіз прихованих каналів; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який несе відповідальність за таємний аналіз каналів; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Організаційний процес для проведення аналізу прихованих каналів; автоматизовані механізми, що підтримують та, або впроваджують аналіз прихованих каналів; автоматизовані механізми, що підтримують та, або реалізують можливість вимірювання пропускної можливості прихованих каналів]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-32 | ПОДІЛ СИСТЕМИ НА ЧАСТИНИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-32[1] | SC-32[1][1] | Організація визначає системні компоненти, що знаходяться в окремих фізичних доменах або середовищах |
| SC-32[1][2] | Організація визначає умови для фізичного поділу компонентів |
| SC-32[2] | розділити систему на визначені організацією системні компоненти, що знаходяться в: | |
| SC-32[2]{1} | окремих фізичних доменах на основі визначених організацією умов для фізичного поділу компонентів |
| SC-32[2]{2} | окремих середовищах на основі визначених організацією умов для фізичного поділу компонентів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються розділення інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; перелік фізичних доменів (або середовищ) інформаційної системи; схеми об'єктів інформаційної системи; схеми мережі інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують фізичне розділення компонентів інформаційної системи]. | | |

|  |  |
| --- | --- |
| SC-33 | ПІДГОТОВКА ЦІЛІСНОСТІ ПЕРЕДАЧІ |
|  | [Вилучено: Включено до SC-8]. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-34 | НЕЗМІНЮВАНІ ВИКОНАВЧІ ПРОГРАМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-34[1] | SC-34[1][1] | Організація визначає незмінювані системні компоненти | |
| SC-34[1][2] | Організація визначає додатки, які можуть бути виконані у режимі лише для зчитування | |
| SC-34[2] | у визначені організацією системні компоненти: | | |
| SC-34[2](a) | SC-34[2](a)[1] | завантажити операційне середовище з апаратного носія, що працює у режимі лише для зчитування |
| SC-34[2](a)[2] | виконати операційне середовище з апаратного носія, що працює у режимі лише для зчитування |
| SC-34[2](b) | SC-34[2](b)[1] | завантажити визначені організацією додатки з апаратного носія, що працює у режимі лише для зчитування |
| SC-34[2](b)[2] | виконати визначені організацією додатки з апаратного носія, що працює у режимі лише для зчитування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються не модифікованих виконуваних програм; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; перелік компонентів операційної системи, що завантажуються з апаратно-захищених носіїв, доступних лише для читання; перелік програм, що завантажуються з апаратно-захищеного носія, доступного лише для читання; носії, що використовуються для завантаження та виконання операційного середовища інформаційної системи; носії, що використовуються для завантаження та виконання програм інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують завантаження та виконання операційного середовища з апаратного, лише для читання носія; автоматизовані механізми, що підтримують та, або реалізують завантаження та виконання додатків з апаратного, лише для читання носія]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-34(1) | НЕЗМІНЮВАНІ ВИКОНАВЧІ ПРОГРАМИ - ВІДСУТНІСТЬ СХОВИЩА ДОСТУПНОГО ДЛЯ ЗАПИСУ ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-34(1)[1] | Організація визначає системні компоненти | | |
| SC-34(1)[2] | використовує визначені організацією системні компоненти без можливості запису в сховище, яке є постійним при: | | |
| SC-34(1)[2]{1} | перезапуску компонента | |
| SC-34(1)[2]{2} | SC-34(1)[2]{2}{1} | включення, |
|  | SC-34(1)[2]{2}{2} | вимикання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються не модифікованих виконуваних програм; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; перелік компонентів інформаційної системи, які будуть використовуватися без можливості записування; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують використання компонентів без записуваного сховища; автоматизовані механізми, що підтримують та, або впроваджують постійне не записане сховище при перезапуску компонента та увімкненні, вимкненні живлення]. | | | |

|  |  |  |
| --- | --- | --- |
| SC-34(2) | НЕЗМІНЮВАНІ ЗДІЙСНЮВАНІ ПРОГРАМИ - ЗАХИСТ ЦІЛІСНОСТІ НА НОСІЇ, ПРИДАТНОМУ ТІЛЬКИ ДЛЯ ЧИТАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-34(2)[1] | захищає цілісність інформації перед її зберіганням на носії, придатному тільки для читання |
| SC-34(2)[2] | контролювати носій після того, як така інформація була записана |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються не модифікованих виконуваних програм; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість захисту цілісності інформації на носіях, доступних лише для читання, до зберігання та після запису інформації на носій]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-34(3) | НЕЗМІНЮВАНІ ПРОГРАМИ, ЩО ВИКОНУЮТЬСЯ - АПАРАТНИЙ ЗАХИСТ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-34(3)(a) | SC-34(3)(a)[1] | Організація визначає системні компоненти вбудованого програмного забезпечення |
| SC-34(3)(a)[2] | використовувати апаратний захист від запису для визначених організацією системних компонентів вбудованого програмного забезпечення |
| SC-34(3)(b) | SC-34(3)(b)[1] | Організація визначає уповноважених осіб, щоб вручну вимкнути апаратний захист від запису для модифікацій вбудованого програмного забезпечення і знову ввімкнути захист від запису перед поверненням до робочого режиму |
| SC-34(3)(b)[2] | впровадити спеціальні процедури для визначених організацією уповноважених осіб, щоб вручну вимкнути апаратний захист від запису для модифікацій вбудованого програмного забезпечення і знову ввімкнути захист від запису перед поверненням до робочого режиму |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються модифікацій мікропрограми; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Організаційні процеси для модифікації мікропрограми; автоматизовані механізми, що підтримують та, або впроваджують апаратне забезпечення, захист від запису для прошивки]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-35 | РОЗПІЗНАВАННЯ ПРИМАНОК ДЛЯ ЗЛОВМИСНИКІВ (HONEYCLIENT) | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-35[1] | включити системні компоненти, які активно намагаються ідентифікувати: | |
| SC-35[1][1] | мережевий шкідливий код |
| SC-35[1][2] | шкідливі вебсайти |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються розпізнавання приманок для зловмисників (honeyclient); проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; компоненти інформаційної системи, розгорнуті для ідентифікації шкідливих вебсайтів та, або веб-шкідливого коду; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують розпізнавання приманок для зловмисників (honeyclient)]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-36 | РОЗПОДІЛЕНА ОБРОБКА ТА ЗБЕРІГАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-36[1] | SC-36[1][1] | Організація визначає компоненти обробки |
| SC-36[1][2] | Організація визначає компоненти зберігання |
| SC-36[2] | розподіляти визначені організацією компоненти: | |
| SC-36[2][1] | обробки серед декількох фізичних місць |
| SC-36[2][2] | зберігання серед декількох фізичних місць |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури планування на випадок надзвичайних ситуацій; резервний план; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; перелік фізичних розташувань інформаційної системи (або середовищ) з розподіленою обробкою та зберіганням; схеми об'єктів інформаційної системи; обробка угод на сайті; угоди про місця зберігання; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, який відповідає за планування та реалізацію плану; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Організаційні процеси для розподілу обробки та зберігання у різних фізичних місцях; автоматизовані механізми, що підтримують та, або реалізовують можливості розподілу обробки та зберігання у різних фізичних місцях]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-36(1) | РОЗПОДІЛЕНА ОБРОБКА ТА ЗБЕРІГАННЯ - МЕТОДИ ОПИТУВАННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-36(1)(a) | SC-36(1)(a)[1] | організація визначає розподілені компоненти обробки | |
| SC-36(1)(a)[2] | організація визначає розподілені компоненти зберігання | |
| SC-36(1)(b) | використовувати методи опитування для виявлення потенційних: | | |
| SC-36(1)(b){1} | збоїв до визначених організацією розподілених компонентів | |
| SC-36(1)(b){1}[1] | обробки |
| SC-36(1)(b){1}[2] | зберігання |
| SC-36(1)(b){2} | помилок до визначених організацією розподілених компонентів обробки та зберігання | |
| SC-36(1)(b){2}[1] | обробки |
| SC-36(1)(b){2}[2] | зберігання |
| SC-36(1)(b){3} | компрометацій до визначених організацією розподілених компонентів обробки та зберігання | |
| SC-36(1)(b){3}[1] | обробки |
| SC-36(1)(b){3}[2] | зберігання |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; перелік розподілених компонентів обробки та зберігання, що підлягають опитуванню; методи опитування інформаційної системи та відповідна документація чи записи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують методи опитування]. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SC-37 | ПОЗАСМУГОВІ КАНАЛИ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SC-37[1] | SC-37[1][1] | Організація визначає позасмугові канали | | |
| SC-37[1][2] | SC-37[1][2]{1} | Організація визначає інформацію | |
| SC-37[1][2]{2} | Організація визначає системні компоненти | |
| SC-37[1][2]{3} | Організація визначає пристрої | |
| SC-37[1][3] | SC-37[1][3]{1} | Організація визначає особи | |
| SC-37[1][3]{2} | Організація визначає системи | |
| SC-37[2] | використовувати визначені організацією позасмугові канали для: | | | |
| SC-37[2]{1} | фізичного постачання визначеної організацією: | | |
| SC-37[2]{1}{1} | інформації до визначених організацією: | |
| SC-37[2]{1}{1}{1} | осіб |
| SC-37[2]{1}{1}{2} | систем |
| SC-37[2]{1}{2} | системних компонентів | |
| SC-37[2]{1}{2}{1} | осіб |
| SC-37[2]{1}{2}{2} | систем |
| SC-37[2]{1}{3} | пристроїв | |
| SC-37[2]{1}{3}{1} | осіб |
| SC-37[2]{1}{3}{2} | систем |
| SC-37[2]{2} | електронної передачі визначеної організацією: | | |
| SC-37[2]{2}{1} | інформації до визначених організацією: | |
| SC-37[2]{2}{1}{1} | осіб |
| SC-37[2]{2}{1}{2} | систем |
| SC-37[2]{2}{2} | системних компонентів | |
| SC-37[2]{2}{2}{1} | осіб |
| SC-37[2]{2}{2}{2} | систем |
| SC-37[2]{2}{3} | пристроїв | |
| SC-37[2]{2}{3}{1} | осіб |
| SC-37[2]{2}{3}{2} | систем |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються використання позасмугових каналів; політика та процедури контролю доступу; політика і процедури ідентифікації та автентифікації; проєктна документація інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; список позасмугових каналів; типи інформації, компоненти інформаційної системи або пристрої, що вимагають використання позасмугових каналів для фізичного постачання або електронної передачі уповноваженим особам або інформаційним системам; записи фізичного постачання; записи електронної передачі; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, що дозволяє, встановлює, налаштовує, експлуатує та, або використовує позасмугові канали; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Організаційні процеси для використання позасмугових каналів; автоматизовані механізми, що підтримують та, або реалізують використання позасмугових каналів]. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SC-37(1) | ПОЗАСМУГОВІ КАНАЛИ - ЗАБЕЗПЕЧЕННЯ ДОСТАВКИ ТА ПЕРЕДАЧІ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SC-37(1)[1] | SC-37(1)[1][1] | організація визначає заходи безпеки, щоб забезпечити, що тільки визначені організацією особи або системи отримують визначену організацією інформацію, компоненти системи або пристрої | | |
| SC-37(1)[1][2] | SC-37(1)[1][2]{1} | організація визначає осіб, які можуть отримати визначену організацією інформацію, компоненти системи або пристрої | |
| SC-37(1)[1][2]{2} | організація визначає системи, які можуть отримати визначену організацією інформацію, компоненти системи або пристрої | |
| SC-37(1)[1][3] | SC-37(1)[1][3]{1} | організація визначає інформацію | |
| SC-37(1)[1][3]{2} | організація визначає компоненти системи | |
| SC-37(1)[1][3]{3} | організація визначає пристрої | |
| SC-37(1)[2] | впровадити визначені організацією заходи безпеки, щоб забезпечити, що тільки визначені організацією: | | | |
| SC-37(1)[2]{1} | особи отримують визначену організацією | | |
| SC-37(1)[2]{1}{1} | | інформацію |
| SC-37(1)[2]{1}{2} | | компоненти системи |
| SC-37(1)[2]{1}{3} | | пристрої |
| SC-37(1)[2]{2} | системи отримують визначені організацією інформація, компоненти системи або пристрої | | |
| SC-37(1)[2]{2}{1} | | інформацію |
| SC-37(1)[2]{2}{2} | | компоненти системи |
| SC-37(1)[2]{2}{3} | | пристрої |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються використання позасмугових каналів; політика та процедури контролю доступу; політика і процедури ідентифікації та автентифікації; проєктна документація інформаційної системи; архітектура інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік гарантій безпеки, які застосовуватимуться для забезпечення отримання визначеними особами або інформаційними системами інформації, визначеної організацією, компонентів інформаційної системи або пристроїв; перелік гарантій безпеки для доставки призначеної інформації, компонентів інформаційної системи або пристроїв до зазначених осіб або інформаційних систем; перелік інформації, компонентів інформаційної системи або пристроїв, що передаються призначеним особам або інформаційним системам; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, що дозволяє, встановлює, налаштовує, експлуатує та, або використовує позасмугові канали; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Організаційні процеси для використання позасмугових каналів; автоматизовані механізми, що підтримують та, або реалізують використання позасмугових каналів; автоматизовані механізми, що підтримують, впроваджують запобіжні заходи для забезпечення доставки призначеної інформації, компонентів системи або пристроїв]. | | | | |

|  |  |  |
| --- | --- | --- |
| SC-38 | БЕЗПЕКА ОПЕРАЦІЙ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-38[1] | Організація визначає заходи з безпеки операцій для захисту ключової організаційної інформації протягом усього життєвого циклу розробки системи |
| SC-38[2] | впровадити визначені організацією заходи з безпеки операцій для захисту ключової організаційної інформації протягом усього життєвого циклу розробки системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються безпеки операцій; план безпеки; перелік гарантій безпеки операцій; оцінки контролю безпеки; оцінки ризиків; оцінки загроз та вразливості; плани дій та етапи; документація життєвого циклу розробки системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Організаційні процеси для захисту організаційної інформації в SDLC; автоматизовані механізми, що підтримують та, або впроваджують запобіжні заходи для захисту організаційної інформації в рамках SDLC]. | |

|  |  |  |
| --- | --- | --- |
| SC-39 | ІЗОЛЯЦІЯ ПРОЦЕСУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-39[1] | підтримувати окремий домен виконання для кожного процесу, що виконується в системі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Проєктна документація інформаційної системи; архітектура інформаційної системи; документація про незалежну перевірку; документація про тестування та оцінку, інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Розробники, інтегратори інформаційних систем; архітектор безпеки інформаційної системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують окремі домени виконання для кожного процесу виконання]. | |

|  |  |  |
| --- | --- | --- |
| SC-39(1) | ІЗОЛЯЦІЯ ПРОЦЕСУ - АПАРАТНЕ РОЗДІЛЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-39(1)[1] | впровадити механізми апаратного розділення для розділення процесів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; документація інформаційної системи для апаратних механізмів розділення; документація інформаційної системи від постачальників, виробників або розробників; документація про незалежну перевірку та перевірку; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Можливість інформаційної системи, що реалізує механізми розділення апаратного забезпечення для розділення процесів]. | |

|  |  |  |
| --- | --- | --- |
| SC-39(2) | ІЗОЛЯЦІЯ ПРОЦЕСУ - ІЗОЛЯЦІЯ ПОТОКІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-39(2)[1] | Організація визначає багатопотокову обробку |
| SC-39(2)[2] | підтримувати окремий домен виконання для кожного потоку в визначеній організацією багатопотоковій обробці |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; список доменів виконання інформаційної системи для кожного потоку в багатопотоковій обробці; документація інформаційної системи для багатопотокової обробки; документація інформаційної системи від постачальників, виробників або розробників; документація про незалежну перевірку та перевірку; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем].  Перевірка: [ВИБІР: Можливість інформаційної системи, що реалізує окремий домен виконання для кожного потоку в багатопотоковій обробці]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-40 | ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-40[1] | SC-40[1][1] | Організація визначає бездротові з’єднання | |
| SC-40[1][2] | SC-40[1][2]{1} | Організація визначає типи атак з параметрами сигналів |
| SC-40[1][2]{2} | Організація визначає посилання на джерела для таких атак. |
| SC-40[2] | SC-40[2][1] | забезпечити захист зовнішніх визначених організацією бездротових з’єднань від визначених організацією типів атак з: | |
| SC-40[2][1]{1} | параметрами сигналів |
| SC-40[2][1]{2} | посиланнями на джерела для таких атак |
| SC-40[2][2] | забезпечити захист внутрішніх визначених організацією бездротових з’єднань від визначених організацією типів атак з: | |
| SC-40[2][2]{1} | параметрами сигналів |
| SC-40[2][2]{2} | посиланнями на джерела для таких атак |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються захисту бездротового зв'язку; проєктна документація інформаційної системи; схеми бездротової мережі; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; типи або внутрішні та зовнішні бездротові посилання; типи атак параметрів сигналу або посилання на джерела атак; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, що дозволяє, встановлює, налаштовує та, або підтримує внутрішні та зовнішні бездротові зв’язки].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують захист бездротових ліній зв'язку]. | | | |

|  |  |  |
| --- | --- | --- |
| SC-40(1) | ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ЕЛЕКТРОМАГНІТНІ ПЕРЕШКОДИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-40(1)[1] | Організація визначає рівень захисту від впливу навмисних електромагнітних перешкод |
| SC-40(1)[2] | впровадити криптографічні механізми, що забезпечують визначений організацією рівень захисту від впливу навмисних електромагнітних перешкод |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються захисту бездротового зв'язку; проєктна документація інформаційної системи; схеми бездротової мережі; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; апаратне та програмне забезпечення комунікацій інформаційної системи; результати категоризації безпеки; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, що дозволяє, встановлює, налаштовує та, або підтримує внутрішні та зовнішні бездротові зв’язки].  Перевірка: [ВИБІР: Криптографічні механізми, що забезпечують захист від наслідків навмисних електромагнітних перешкод]. | |

|  |  |  |
| --- | --- | --- |
| SC-40(2) | ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ЗМЕНШЕННЯ ПОТЕНЦІАЛУ ВИЯВЛЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-40(2)[1] | Організація визначає рівень зниження? |
| SC-40(2)[2] | впровадити криптографічні механізми для зменшення потенціалу виявлення бездротових з'єднань до визначеного організацією рівня зниження |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються захисту бездротового зв'язку; проєктна документація інформаційної системи; схеми бездротової мережі; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; апаратне та програмне забезпечення комунікацій інформаційної системи; результати категоризації безпеки; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, що дозволяє, встановлює, налаштовує та, або підтримує внутрішні та зовнішні бездротові зв’язки].  Перевірка: [ВИБІР: Криптографічні механізми, що забезпечують захист для зменшення виявлення бездротових посилань]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-40(3) | ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ІМІТАЦІЙНИЙ АБО МАНІПУЛЯТИВНИЙ ОБМІН ПОВІДОМЛЕННЯМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-40(3)[1] | впровадити криптографічні механізми для визначення та відхилення бездротових передач, які є навмисними спробами досягти: | |
| SC-40(3)[2] | SC-40(3)[2]{1} | імітаційного обміну повідомленнями на основі параметрів сигналу |
| SC-40(3)[2]{2} | маніпулятивного обміну повідомленнями на основі параметрів сигналу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються проєктної документації інформаційної системи; схеми бездротової мережі; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; апаратне та програмне забезпечення комунікацій інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, що дозволяє, встановлює, налаштовує та, або підтримує внутрішні та зовнішні бездротові зв’язки].  Перевірка: [ВИБІР: Криптографічні механізми, що забезпечують захист бездротового зв'язку від обману імітаційних або маніпулятивних комунікацій]. | | |

|  |  |  |
| --- | --- | --- |
| SC-40(4) | ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ВИЗНАЧЕННЯ ПАРАМЕТРІВ СИГНАЛУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-40(4)[1] | Організація визначає бездротові передавачі, для яких необхідно впровадити криптографічні механізми для запобігання їх визначення |
| SC-40(4)[2] | Впровадити криптографічні механізми для запобігання визначення визначених організацією бездротових передавачів за допомогою параметрів сигналу передавача |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються проєктної документації інформаційної системи; схеми бездротової мережі; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; апаратне та програмне забезпечення комунікацій інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, що дозволяє, встановлює, налаштовує та, або підтримує внутрішні та зовнішні бездротові зв’язки].  Перевірка: [ВИБІР: Криптографічні механізми, що перешкоджають ідентифікації бездротових передавачів]. | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SC-41 | ДОСТУП ДО ПОРТІВ ТА ПРИСТРОЇВ ВВЕДЕННЯ, ВИВЕДЕННЯ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| SC-41[1] | SC-41[1][1] | SC-41[1][1]{1} | Організація визначає порти підключення | | | | |
| SC-41[1][1]{2} | Організація визначає пристрої | | | | |
| SC-41[1][1]{2}{1} | | введення | | |
| SC-41[1][1]{2}{2} | | виводу | | |
| SC-41[1][2] | SC-41[1][2]{1} | Організація визначає системи | | | | |
| SC-41[1][2]{2} | Організація визначає системні компоненти | | | | |
| SC-41[2] | SC-41[2]{1} | фізично відключити або видалити визначені організацією: | | | | | |
| SC-41[2]{1}{1} | порти підключення у визначені організацією: | | | | |
| SC-41[2]{1}{1}{1} | | системи | | |
| SC-41[2]{1}{1}{2} | | системні компоненти | | |
| SC-41[2]{1}{2} | пристрої: | | | | |
| SC-41[2]{1}{2}{1} | введення у визначені організацією | | | |
| SC-41[2]{1}{1}{1} | | | системи |
| SC-41[2]{1}{1}{2} | | | системні компоненти |
| SC-41[2]{1}{2}{2} | виводу у визначені організацією | | | |
| SC-41[2]{1}{1}{1} | | системи | |
| SC-41[2]{1}{1}{2} | | системні компоненти | |
| SC-41[2]{2} | логічно відключити або видалити визначені організацією: | | | | | |
| SC-41[2]{2}{1} | порти підключення у визначені організацією: | | | | |
| SC-41[2]{2}{1}{1} | | системи | | |
| SC-41[2]{2}{1}{2} | | системні компоненти | | |
| SC-41[2]{2}{2} | пристрої: | | | | |
| SC-41[2]{2}{2}{1} | введення у визначені організацією | | | |
| SC-41[2]{2}{1}{1} | | | системи |
| SC-41[2]{2}{1}{2} | | | системні компоненти |
| SC-41[2]{2}{2}{2} | виводу у визначені організацією | | | |
| SC-41[2]{2}{1}{1} | | системи | |
| SC-41[2]{2}{1}{2} | | системні компоненти | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються доступу до порту та пристрою введення, виводу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; інформаційні системи або компоненти інформаційної системи перелік портів підключення або пристроїв введення, виводу, що мають бути фізично відключені або видалені в інформаційних системах або компонентах інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують відключення портів підключення або пристроїв введення, виводу]. | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-42 | МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-42(a) | SC-42(a)[1] | Організація визначає виключення, в яких допускається дистанційна активація датчиків | |
| SC-42(a)[2] | заборонити дистанційну активацію можливостей зондування навколишнього середовища в: | |
| SC-42(a)[2]{1} | організаційних системах за наступними виключеннями: визначені організацією виключення, в яких допускається дистанційна активація датчиків |
| SC-42(a)[2]{2} | системних компонентах за наступними виключеннями: визначені організацією виключення, в яких допускається дистанційна активація датчиків |
| SC-42(b) | SC-42(b)[1] | Організація визначає клас користувачів | |
| SC-42(b)[2] | забезпечити явну вказівку використання датчика для визначених організацією класів користувачів | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються можливостей датчиків та збору даних; політика та процедури контролю доступу; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за роботу датчика].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують засоби контролю доступу для віддаленої активації можливостей датчика інформаційної системи; автоматизовані механізми, що реалізують можливість індикації використання датчика]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-42(1) | МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ЗВІТУВАННЯ ПЕРЕД УПОВНОВАЖЕНИМИ АБО ПОСАДОВИМИ ОСОБАМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-42(1)[1] | організація визначає датчики | | |
| SC-42(1)[2] | переконайтеся, що система налаштована таким чином, щоб: | | |
| SC-42(1)[2]{1} | дані зібрані визначеними організацією датчиками, повідомлялася лише | |
| SC-42(1)[2]{1}{1} | уповноваженим особам |
| SC-42(1)[2]{1}{2} | посадовим особам |
| SC-42(1)[2]{2} | інформація, зібрана визначеними організацією датчиками, повідомлялася лише: | |
| SC-42(1)[2]{2}{1} | уповноваженим особам |
| SC-42(1)[2]{2}{2} | посадовим особам |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються можливостей датчиків та збору даних; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за роботу датчика].  Перевірка: [ВИБІР: Автоматизовані механізми, що обмежують передачу інформації про датчик лише авторизованим; можливість збору даних і звітності датчиків для інформаційної системи]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SC-42(2) | МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ДОЗВОЛЕНЕ ВИКОРИСТАННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SC-42(2)[1] | SC-42(2)[1][1] | | Організація визначає заходи |
| SC-42(2)[1][2] | | Організація визначає датчики |
| SC-42(2)[2] | впровадити визначені організацією заходи таким чином, щоб: | | |
| SC-42(2)[2]{1} | дані зібрані за допомогою визначених організацією датчиків, використовувалися лише для дозволених цілей | |
| SC-42(2)[2]{2} | інформація, зібрані за допомогою визначених організацією датчиків, використовувалися лише для дозволених цілей | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; можливість датчика та збір даних; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; перелік заходів, що застосовуються для забезпечення того, щоб дані або інформація, зібрані датчиками, використовувались лише у дозволених цілях; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за роботу датчика].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують заходи для забезпечення того, щоб інформація датчика використовувалася лише в дозволених цілях; можливість збору інформації датчиків для інформаційної системи]. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SC-42(3) | МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ЗАБОРОНА ВИКОРИСТАННЯ ПРИСТРОЇВ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SC-42(3)[1] | SC-42(3)[1][1] | Організація визначає можливості сприйняття навколишнього середовища | | |
| SC-42(3)[1][2] | SC-42(3)[1][2]{1} | | визначені організацією об'єкти |
| SC-42(3)[1][2]{2} | | визначені організацією зони |
| SC-42(3)[1][2]{3} | | визначені організацією системи |
| SC-42(3)[2] | заборонити використання пристроїв, що володіють визначеними організацією можливостями сприйняття навколишнього середовища у визначених організацією: | | | |
| SC-42(3)[2]{1} | | об'єктах | |
| SC-42(3)[2]{2} | | зонах | |
| SC-42(3)[2]{3} | | системах | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються можливостей датчиків та збору даних; проєктна документація інформаційної системи; схеми бездротової мережі; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; об’єкти, зони або системи, де заборонено використання пристроїв, що володіють можливостями зондування довкілля; перелік приладів, що володіють можливостями зондування довкілля; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за роботу датчика]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-42(4) | МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ПОВІДОМЛЕННЯ ПРО ЗБІР | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-42(4)[1] | SC-42(4)[1][1] | організація визначає датчиками персональні дані |
| SC-42(4)[1][2] | організація визначає заходи щодо збору персональних даних |
| SC-42(4)[2] | впровадити визначені організацією заходи для повідомлення осіб про збір персональних даних визначеними організацією датчиками: | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються можливостей датчиків та збору даних; проєктна документація інформаційної системи; схеми бездротової мережі; налаштування конфігурації інформаційної системи та відповідна документація; архітектура інформаційної системи; об’єкти, зони або системи, де заборонено використання пристроїв, що володіють можливостями зондування довкілля; перелік приладів, що володіють можливостями зондування довкілля; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за роботу датчика]. | | |

|  |  |  |
| --- | --- | --- |
| SC-42(5) | МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - МІНІМІЗАЦІЯ ЗБОРУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SC-42(5)[1] | організація визначає датчики |
| SC-42(5)[2] | впровадити визначені організацією датчики, які налаштовані на мінімізацію збору непотрібних персональних даних |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються обмежень щодо використання; обмеження використання; політика та процедури впровадження; авторизаційні записи; записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему].  Перевірка: [ВИБІР: Організаційні процеси для дозволу, моніторингу та контролю використання компонентів з обмеженнями щодо використання; Автоматизовані механізми, що підтримують та, або впроваджують дозвіл, моніторинг та контроль використання компонентів з обмеженнями використання]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-43 | ОБМЕЖЕННЯ ВИКОРИСТАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-43(a) | SC-43(a)[1] | організація визначає компоненти системи |
| SC-43(a)[2] | встановити обмеження на використання та рекомендації щодо впровадження для визначених організацією компонент системи |
| SC-43(b) | проводити: | |
| SC-43(b)[1] | авторизацію використання таких компонентів у системі |
| SC-43(b)[2] | спостереження використання таких компонентів у системі |
| SC-43(b)[3] | контроль використання таких компонентів у системі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються обмежень щодо використання; обмеження використання; політика та процедури впровадження; авторизаційні записи; записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему].  Перевірка: [ВИБІР: Організаційні процеси для дозволу, моніторингу та контролю використання компонентів з обмеженнями щодо використання; Автоматизовані механізми, що підтримують та, або впроваджують дозвіл, моніторинг та контроль використання компонентів з обмеженнями використання]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SC-44 | ЕКРАНОВАНІ КАМЕРИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SC-44[1] | SC-44[1]{1} | Організація визначає систему |
| SC-44[1]{2} | Організація визначає системний компонент |
| SC-44[1]{3} | Організація визначає місце розташування |
| SC-44[2] | впровадити екрановані камери в визначеній організацією: | |
| SC-44[2]{1} | системі |
| SC-44[2]{2} | системному компоненті |
| SC-44[2]{3} | місці розташування |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються екранованих камер; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість детонаційної камери]. | | |

1. **КЛАС ЗАХОДІВ ЗАХИСТУ SI – ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ**

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-2 | ВИПРАВЛЕННЯ ДЕФЕКТІВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-2(a) | SI-2(a)[1] | виявляти недоліки системи | |
| SI-2(a)[2] | виправляти недоліки системи | |
| SI-2(a)[3] | повідомляти про недоліки системи | |
| SI-2(b) | перед установкою перевірити: | | |
| SI-2(b)[1] | програмне забезпечення, що пов'язане з усуненням дефектів, на: | |
| SI-2(b)[1][1] | ефективність |
| SI-2(b)[1][2] | можливі побічні ефекти |
| SI-2(b)[2] | оновлення вбудованого програмного забезпечення | |
| SI-2(b)[2][1] | ефективність |
| SI-2(b)[2][2] | можливі побічні ефекти |
| SI-2(c) | SI-2(c)[1] | Організація визначає певний період часу | |
| SI-2(c)[2] | інсталювати: | |
| SI-2(c)[2][1] | оновлення програмного забезпечення в межах визначеного організацією певного періоду часу випуску оновлень |
| SI-2(c)[2][2] | оновлення вбудованого програмного забезпечення в межах визначеного організацією певного періоду часу випуску оновлень |
| SI-2(d) | включити виправлення помилок в організаційний процес управління конфігурацією | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються усунення недоліків; процедури, що стосуються управління конфігурацією; перелік недоліків та уразливостей, які потенційно можуть вплинути на інформаційну систему; перелік останніх заходів щодо усунення недоліків безпеки, здійснених в інформаційній системі (наприклад, перелік встановлених виправлень, пакетів оновлень, виправлення та інші оновлення програмного забезпечення для виправлення недоліків інформаційної системи); результати тестування від встановлення програмного забезпечення та оновлення мікропрограми для виправлення недоліків інформаційної системи; записи про встановлення, контроль змін для оновлення програмного забезпечення та мікропрограми, що стосується безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за усунення недоліків; організаційний персонал, відповідальний за управління конфігурацією].  Перевірка: [ВИБІР: Організаційні процеси для виявлення, звітування та виправлення недоліків інформаційної системи; організаційний процес встановлення оновлень програмного забезпечення та мікропрограми; автоматизовані механізми підтримки та, або впровадження звітності та виправлення недоліків інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують тестові оновлення програмного забезпечення та мікропрограми]. | | | |

|  |  |  |
| --- | --- | --- |
| SI-2(1) | ВИПРАВЛЕННЯ ДЕФЕКТІВ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-2(1)[1] | впровадити централізоване управління процесом усунення дефектів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються усунення недоліків; автоматизовані механізми підтримки централізованого управління усуненням недоліків; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за усунення недоліків].  Перевірка: [ВИБІР: Організаційні процеси для централізованого управління процесом усунення недоліків; автоматизовані механізми, що підтримують та, або впроваджують централізоване управління процесом усунення недоліків]. | |

|  |  |  |
| --- | --- | --- |
| SI-2(2) | ВИПРАВЛЕННЯ ДЕФЕКТІВ - АВТОМАТИЗОВАНЕ ВИПРАВЛЕННЯ ДЕФЕКТІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-2(2)[1] | організація визначає частоту, з якою впроваджують автоматизовані механізми |
| SI-2(2)[2] | впровадити автоматизовані механізми з визначеною організацією частотою для визначення стану компонентів системи стосовно усунення дефектів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються усунення недоліків; автоматизовані механізми підтримки централізованого управління усуненням недоліків; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за усунення недоліків].  Перевірка: [ВИБІР: Автоматизовані механізми, що використовуються для визначення стану компонентів інформаційної системи щодо усунення недоліків]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-2(3) | ВИПРАВЛЕННЯ ДЕФЕКТІВ - ЧАС ДЛЯ УСУНЕННЯ ДЕФЕКТІВ ТА ОРІЄНТИРИ ДЛЯ КОРИГУВАЛЬНИХ ДІЙ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-2(3)(a) | вимірювати час між виявленням та виправленням дефектів | |
| SI-2(3)(b) | SI-2(3)(b)[1] | організація визначає орієнтири для вжиття коригувальних дій |
| SI-2(3)(b)[2] | встановити визначені організацією орієнтири для вжиття коригувальних дій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються усунення недоліків; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік еталонів для вжиття коригувальних заходів щодо виявлених недоліків; записи, що містять відмітки про час виявлення недоліків та подальші заходи щодо їх усунення; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за усунення недоліків].  Перевірка: [ВИБІР: Організаційні процеси для виявлення, звітування та виправлення недоліків інформаційної системи; автоматизовані механізми, що використовуються для вимірювання часу між виявленням та усуненням недоліків]. | | |

|  |  |
| --- | --- |
| SI-2(4) | ВИПРАВЛЕННЯ ДЕФЕКТІВ - АВТОМАТИЧНІ ЗАСОБИ УПРАВЛІННЯ ВИПРАВЛЕННЯМИ |
|  | [Вилучено: Включено до SІ-2]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-2(5) | ВИПРАВЛЕННЯ ДЕФЕКТІВ - АВТОМАТИЧНЕ ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-2(5)[1] | SI-2(5)[1][1] | організація визначає відповідне оновлення програмного забезпечення |
| SI-2(5)[1][2] | організація визначає відповідне оновлення вбудованого програмного забезпечення |
| SI-2(5)[1][3] | організація визначає компоненти системи |
| SI-2(5)[1] | встановлювати визначене організацією відповідне оновлення: | |
| SI-2(5)[1][1] | програмного забезпечення автоматично на визначені організацією компоненти системи |
| SI-2(5)[1][2] | вбудованого програмного забезпечення автоматично на визначені організацією компоненти системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються виправлення дефектів; автоматизовані механізми, що підтримують усунення несправностей та автоматичне оновлення програмного забезпечення, мікропрограми; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи останніх оновлень програмного забезпечення та мікропрограми, що стосуються безпеки, автоматично встановлюються на компоненти інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за виправлення дефектів].  Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують автоматичне оновлення програмного забезпечення, мікропрограми]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-2(6) | ВИПРАВЛЕННЯ ДЕФЕКТІВ - ВИДАЛЕННЯ ПОПЕРЕДНІХ ВЕРСІЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-2(6)[1] | SI-2(6)[1][1] | організація визначає компоненти програмного забезпечення та |
| SI-2(6)[1][2] | організація визначає компоненти вбудованого програмного забезпечення |
| SI-2(6)[2] | видаляти попередні версії визначених організацією компонент: | |
| SI-2(6)[2][1] | програмного забезпечення після інсталяції оновлених версій |
| SI-2(6)[2][2] | вбудованого програмного забезпечення після інсталяції оновлених версій |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються виправлення дефектів; автоматизовані механізми, що підтримують виправлення дефектів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи про видалення програмного забезпечення та компонентів мікропрограми після встановлення оновлених версій; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за виправлення дефектів].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або здійснюють видалення попередніх версій програмного забезпечення, прошивки]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-2(7) | ВИПРАВЛЕННЯ ДЕФЕКТІВ - ПЕРСОНАЛЬНІ ДАНІ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-2(7)(a) | SI-2(7)(a)[1] | визначити дефекти, пов'язані зі: | |
| SI-2(7)(a)[1]{1} | збором персональних даних |
| SI-2(7)(a)[1]{2} | використанням персональних даних |
| SI-2(7)(a)[1]{3} | обробкою персональних даних |
| SI-2(7)(a)[1]{4} | розповсюдженням персональних даних |
| SI-2(7)(a)[2] | виправити дефекти, пов'язані зі: | |
|  | SI-2(7)(a)[2]{1} | збором персональних даних |
| SI-2(7)(a)[2]{2} | використанням персональних даних |
| SI-2(7)(a)[2]{3} | обробкою персональних даних |
| SI-2(7)(a)[2]{4} | розповсюдженням персональних даних |
| SI-2(7)(b) | повідомляти про дефекти, пов'язані з персональними даними, до уповноваженого державного органу з питань приватності | | |
| SI-2(7)(c) | отримувати підтвердження для виправлення дефектів, пов'язаних з приватністю, від уповноваженого державного органу з питань приватності | | |
| SI-2(7)(d) | перед встановленням оцінити оновлення: | | |
| SI-2(7)(d)[1] | програмного забезпечення, які пов'язані з усуненням дефектів, на предмет: | |
| SI-2(7)(d)[1][1] | ефективності |
| SI-2(7)(d)[1][2] | узгодженості з умовами, визначеними в оцінці впливу на приватність |
| SI-2(7)(d)[2] | мікропрограмного забезпечення, які пов'язані з усуненням дефектів, на предмет: | |
| SI-2(7)(d)[2][1] | ефективності |
| SI-2(7)(d)[2][2] | узгодженості з умовами, визначеними в оцінці впливу на приватність |
| SI-2(7)(e) | SI-2(7)(e)[1] | Організація визначає період часу випуску оновлень | |
| SI-2(7)(e)[2] | встановити оновлення: | |
| SI-2(7)(e)[2][1] | програмного забезпечення, що стосуються приватності, у межах визначеного організацією періоду часу випуску оновлень |
| SI-2(7)(e)[2][2] | мікропрограмного забезпечення, що стосуються приватності, у межах визначеного організацією періоду часу випуску оновлень |
| SI-2(7)(f) | включити виправлення дефектів персональних даних в організаційний процес управління конфігурацією | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються виправлення дефектів; автоматизовані механізми, що підтримують виправлення дефектів; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи про видалення програмного забезпечення та компонентів мікропрограми після встановлення оновлених версій; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за виправлення дефектів].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або здійснюють видалення попередніх версій програмного забезпечення, прошивки]. | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SI-3 | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| SI-3(a) | впровадити механізми захисту від шкідливого коду (один або кілька): | | | | | | |
| SI-3(a){1} | на основі підпису на: | | | | | |
| SI-3(a){1}[1] | | вході системи для: | | | |
| SI-3(a){1}[1][1] | | виявлення шкідливого коду | |
| SI-3(a){1}[1][2] | | знищення шкідливого коду | |
| SI-3(a){1}[2] | | виході системи для виявлення та знищення шкідливого коду | | | |
| SI-3(a){1}[2][1] | | виявлення шкідливого коду | |
| SI-3(a){1}[2][2] | | знищення шкідливого коду | |
| SI-3(a){2} | на основі підпису на вході та виході системи для виявлення та знищення шкідливого коду | | | | | |
| SI-3(a){2}[1] | | вході системи для: | | | |
| SI-3(a){2}[1][1] | | виявлення шкідливого коду | |
| SI-3(a){2}[1][2] | | знищення шкідливого коду | |
| SI-3(a){2}[2] | | виході системи для виявлення та знищення шкідливого коду | | | |
| SI-3(a){2}[2][1] | | виявлення шкідливого коду | |
| SI-3(a){2}[2][2] | | знищення шкідливого коду | |
| SI-3(b) | автоматично оновлювати механізми захисту від шкідливого коду, коли доступні нові випуски відповідно до: | | | | | | |
| SI-3(b)[1] | політики управління конфігурацією | | | | | |
| SI-3(b)[2] | процедур управління конфігурацією | | | | | |
| SI-3(c) | налаштовувати механізми захисту від шкідливого коду для: | | | | | | |
| SI-3(c)(1) | SI-3(c)(1)[1] | Організація визначає частоту виконання періодичного сканування системи | | | | |
| SI-3(c)(1)[2] | виконання періодичного сканування системи з визначеною організацією частотою і сканування файлів в реальному часі з зовнішніх джерел в (один або кілька); | | | | |
| SI-3(c)(1)[2]{1} | | кінцевій точці, коли файли відповідно до політики організації: | | |
| SI-3(c)(1)[2]{1}{1} | | завантажуються |
| SI-3(c)(1)[2]{1}{2} | | відкриваються або |
| SI-3(c)(1)[2]{1}{3} | | виконуються |
| SI-3(c)(1)[2]{2} | | точці входу в мережу, коли файли відповідно до політики організації: | | |
| SI-3(c)(1)[2]{2}{1} | | завантажуються |
| SI-3(c)(1)[2]{2}{2} | | відкриваються або |
| SI-3(c)(1)[2]{2}{3} | | виконуються |
| SI-3(c)(1)[2]{3} | | точці виходу в мережу, коли файли: | | |
| SI-3(c)(1)[2]{3}{1} | | завантажуються |
| SI-3(c)(1)[2]{3}{2} | | відкриваються або |
| SI-3(c)(1)[2]{3}{3} | | виконуються |
| SI-3(c)(2) | SI-3(c)(2)[1] | Організація визначає дію у відповідь на виявлення шкідливого коду | | | | |
| SI-3(c)(2)[2] | SI-3(c)(2)[2]{1} | | блокування шкідливого коду у відповідь на виявлення шкідливого коду | | |
| SI-3(c)(2)[2]{2} | | відправлення шкідливого коду в карантин у відповідь на виявлення шкідливого коду | | |
| SI-3(c)(2)[2]{3} | | Надсилання попередження адміністратору у відповідь на виявлення шкідливого коду | | |
| SI-3(c)(2)[2]{4} | | визначена організацією дія у відповідь на виявлення шкідливого коду | | |
| SI-3(d) | фіксувати отримання помилкових спрацьовувань під час: | | | | | | |
| SI-3(d)[1] | виявлення шкідливого коду і, як наслідок, потенційного впливу на доступність системи | | | | | |
| SI-3(d)[2] | усунення шкідливого коду і, як наслідок, потенційного впливу на доступність системи | | | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; політика та процедури управління конфігурацією; процедури, що стосуються захисту від шкідливого коду; механізми захисту від зловмисного коду; записи оновлень захисту від шкідливого коду; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; сканувати результати від шкідливих механізмів захисту коду; запис дій, ініційованих механізмами захисту від зловмисного коду у відповідь на виявлення шкідливого коду; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за захист від шкідливого коду; організаційний персонал, відповідальний за управління конфігурацією].  Перевірка: [ВИБІР: Організаційні процеси для використання, оновлення та налаштування механізмів захисту від зловмисного коду; організаційний процес вирішення помилкових спрацьовувань та наслідків потенційного впливу; автоматизовані механізми, що підтримують та, або впроваджують використання, оновлення та налаштування механізмів захисту від шкідливого коду; автоматизовані механізми, що підтримують та, або реалізують сканування шкідливого коду та подальші дії]. | | | | | | | |

|  |  |  |
| --- | --- | --- |
| SI-3(1) | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-3(1)[1] | впровадити централізоване управління механізмами захисту від шкідливого коду |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від шкідливого коду; автоматизовані механізми, що підтримують централізоване управління механізмами захисту від зловмисного коду; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за захист від зловмисного коду].  Перевірка: [ВИБІР: Організаційні процеси для централізованого управління механізмами захисту від шкідливого коду; автоматизовані механізми, що підтримують та, або впроваджують централізоване управління механізмами захисту від зловмисного коду]. | |

|  |  |
| --- | --- |
| SI-3(2) | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - АВТОМАТИЧНІ ОНОВЛЕННЯ |
|  | [Вилучено: Включено до SІ-3]. |

|  |  |
| --- | --- |
| SI-3(3) | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - НЕПРИВІЛЕЙОВАНІ КОРИСТУВАЧІ |
|  | [Вилучено: Включено до AC-6(10)]. |

|  |  |  |
| --- | --- | --- |
| SI-3(4) | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ОНОВЛЕННЯ ТІЛЬКИ ПРИВІЛЕЙОВАНИМИ КОРИСТУВАЧАМИ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-3(4)[1] | здійснювати оновлення механізмів захисту від шкідливого коду лише привілейованими користувачами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від шкідливого коду; проєктна документація інформаційної системи; механізми захисту від зловмисного коду; записи оновлень захисту шкідливого коду; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробники системи; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за захист від зловмисного коду].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливості захисту від зловмисного коду]. | |

|  |  |
| --- | --- |
| SI-3(5) | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ПОРТАТИВНІ ПРИСТРОЇ ЗБЕРІГАННЯ ДАНИХ |
|  | [Вилучено: Включено до МР-7] |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-3(6) | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ТЕСТУВАННЯ ТА ВЕРИФІКАЦІЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-3(6)(a) | SI-3(6)(a)[1] | Організація визначає частоту, з якою необхідно перевіряти механізми захисту від шкідливого коду |
| SI-3(6)(a)[2] | Перевіряти механізми захисту від шкідливого коду з визначеною організацією частотою шляхом введення в систему відомого доброякісного, не розповсюджуваного тестового прикладу |
| SI-3(6)(b) | переконатися, що відбувається виявлення: | |
| SI-3(6)(b)[1] | тестового прикладу |
| SI-3(6)(b)[2] | відповідного повідомлення про інциденти |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від шкідливого коду; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; тестові справи; записи, що містять докази тестових справ, виконаних на механізмах захисту від шкідливого коду; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за захист від зловмисного коду].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують тестування та перевірку можливостей захисту від шкідливого коду]. | | |

|  |  |
| --- | --- |
| SI-3(7) | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ВИЯВЛЕННЯ БЕЗ ПІДПИСУ |
|  | [Вилучено: Включено до SІ-3]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-3(8) | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ КОМАНД | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-3(8)[1] | SI-3(8)[1][1] | Організація визначає неавторизовані команди операційної системи |
| SI-3(8)[1][2] | Організація визначає системні апаратні компоненти |
| SI-3(8)[2] | виявляти визначені організацією неавторизовані команди операційної системи за допомогою інтерфейсу програмування прикладних програм ядра ОС на визначені організацією системні апаратні компоненти та (один або більше): | |
| SI-3(8)[2][1] | видати попередження |
| SI-3(8)[2][2] | перевірити виконання команди |
| SI-3(8)[2][3] | запобігти виконанню команди. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від шкідливого коду; проєктна документація інформаційної системи; механізми захисту від зловмисного коду; попереджувальні повідомлення, що надсилаються при виявленні несанкціонованого виконання команди операційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробники системи; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за захист від зловмисного коду].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливості захисту від шкідливого коду; автоматизовані механізми, що підтримують та, або реалізують виявлення несанкціонованих команд операційної системи через інтерфейс програмування ядра]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-3(9) | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - АВТЕНТИФІКАЦІЯ ВІДДАЛЕНИХ КОМАНД | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-3(9)[1] | SI-3(9)[1][1] | Організація визначає заходи безпеки |
| SI-3(9)[1][2] | Організація визначає віддалені команди |
| SI-3(9)[2] | реалізувати визначені організацією заходи безпеки для автентифікації визначених організацією віддалених команд | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від шкідливого коду; проєктна документація інформаційної системи; механізми захисту від шкідливого коду; попереджувальні повідомлення, що надсилаються при виявленні несанкціонованого виконання команди операційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробники системи; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за захист від зловмисного коду].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливості захисту від шкідливого коду; автоматизовані механізми, що реалізують автентифікацію віддалених команд; автоматизовані механізми, що підтримують та, або впроваджують засоби безпеки для автентифікації віддалених команд]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-3(10) | ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - АНАЛІЗ ШКІДЛИВОГО КОДУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-3(10)(a) | SI-3(10)(a)[1] | SI-3(10)(a)[1][1] | Організація визначає інструменти для аналізу характеристик та поведінки шкідливого коду |
| SI-3(10)(a)[1][2] | Організація визначає методи для аналізу характеристик та поведінки шкідливого коду |
| SI-3(10)(a)[2] | використовувати визначені організацією: | |
| SI-3(10)(a)[2][1] | інструменти для аналізу характеристик та поведінки шкідливого коду |
| SI-3(10)(a)[2][2] | методи для аналізу характеристик та поведінки шкідливого коду |
| SI-3(10)(b) | включати результати аналізу шкідливого коду в організаційний процес реагування на інциденти та виправлення дефектів | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від шкідливого коду; процедури, що стосуються реагування на події; процедури, що стосуються усунення недоліків; проєктна документація інформаційної системи; механізми, засоби та методи захисту від зловмисного коду; налаштування конфігурації інформаційної системи та відповідна документація; результати аналізу шкідливого коду; записи подій щодо усунення недоліків, отриманих в результаті аналізу шкідливого коду; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за захист від шкідливого коду; організаційний персонал, відповідальний за усунення недоліків; організаційний персонал, відповідальний за реагування на події, управління ними].  Перевірка: [ВИБІР: Організаційний процес реагування на інциденти; організаційний процес усунення недоліків; автоматизовані механізми, що підтримують та, або реалізують можливості захисту від зловмисного коду; інструменти та методи аналізу характеристик та поведінки шкідливого коду]. | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SI-4 | МОНІТОРИНГ СИСТЕМИ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| SI-4(a) | SI-4(a)[1] | встановити організацією цілі моніторингу системи | | | | | |
| SI-4(a)[2] | здійснювати моніторинг системи для виявлення: | | | | | |
| SI-4(a)[2](1) | | SI-4(a)(1)[1] | | атак відповідно до встановлених організацією цілей моніторингу | |
| SI-4(a)(1)[2] | | індикаторів потенційних атак відповідно до встановлених організацією цілей моніторингу | |
| SI-4(a)[2](2) | | неавторизованих: | | | |
| SI-4(a)[2](2)[1] | | локальних підключень | |
| SI-4(a)[2](2)[2] | | мережевих підключень | |
| SI-4(a)[2](2)[3] | | віддалених підключень | |
| SI-4(b) | SI-4(b)[1] | SI-4(b)[1][1] | | Організація визначає методи, через які визначають несанкціоноване використання системи | | | |
| SI-4(b)[1][2] | | Організація визначає техніки, через які визначають несанкціоноване використання системи | | | |
| SI-4(b)[2] | визначати несанкціоноване використання системи через визначені організацією: | | | | | |
| SI-4(b)[2][1] | | | методи | | |
| SI-4(b)[2][2] | | | техніки | | |
| SI-4(c) | SI-4(c){1} | застосовувати можливості внутрішнього моніторингу: | | | | | |
| SI-4(c){1}(1) | | | стратегічно в рамках системи для збору необхідної для організації суттєвої інформації | | |
| SI-4(c){1}(2) | | | у спеціальних місцях в системі для відстеження конкретних видів транзакцій, що представляють інтерес для організації | | |
| SI-4(c){2} | розгортати пристрої моніторингу: | | | | | |
| SI-4(c){2}(1) | | | стратегічно в рамках системи для збору необхідної для організації суттєвої інформації | | |
| SI-4(c){2}(2) | | | у спеціальних місцях в системі для відстеження конкретних видів транзакцій, що представляють інтерес для організації | | |
| SI-4(d) | захищати інформацію, отриману від засобів моніторингу вторгнень, від: | | | | | | |
| SI-4(d)[1] | несанкціонованого доступу | | | | | |
| SI-4(d)[2] | модифікації | | | | | |
| SI-4(d)[3] | видалення | | | | | |
| SI-4(e) | регулювати рівень активності системного моніторингу при зміні ризику для: | | | | | | |
| SI-4(e){1} | | організаційних операцій і | | | | |
| SI-4(e){2} | | організаційних активів | | | | |
| SI-4(e){3} | | фізичних осіб | | | | |
| SI-4(e){4} | | інших організацій або | | | | |
| SI-4(e){5} | | держави | | | | |
| SI-4(f) | отримувати за результатами моніторингу системи юридичний висновок щодо діяльності; | | | | | | |
| SI-4(g) | SI-4(g)[1] | | SI-4(g)[1][1] | | визначена організацією інформація про моніторинг системи | | |
| SI-4(g)[1][2] | | SI-4(g)[1][2]{1} | визначений організацією персонал | |
| SI-4(g)[1][2]{2} | визначений організацією посадові особи | |
| SI-4(g)[1][3] | | визначена організацією частота | | |
| SI-4(g)[2] | | надавати визначену організацією інформацію про моніторинг системи до: | | | | |
| SI-4(g)[2]{1} | | визначеного організацією персоналу (один або кілька): | | |
| SI-4(g)[2]{1}{1} | | при необхідності |
| SI-4(g)[2]{1}{2} | | з визначеною організацією частотою |
| SI-4(g)[2]{2} | | посадових осіб (один або кілька): | | |
| SI-4(g)[2]{2}{1} | | при необхідності |
| SI-4(g)[2]{2}{2} | | з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Стратегія постійного моніторингу; політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; схема об'єкта; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; місця в інформаційній системі, де розміщені пристрої моніторингу; налаштування конфігурації інформаційної системи та відповідна документація; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу інформаційної системи]. | | | | | | | |

|  |  |  |
| --- | --- | --- |
| SI-4(1) | МОНІТОРИНГ СИСТЕМИ - ЗАГАЛЬНОСИСТЕМНА СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ (IDS) | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-4(1)[1] | підключати окремі засоби виявлення вторгнень у загальну систему виявлення вторгнень |
| SI-4(1)[2] | налаштовувати окремі засоби виявлення вторгнень у загальну систему виявлення вторгнень |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або реалізують можливість виявлення вторгнень]. | |

|  |  |  |
| --- | --- | --- |
| SI-4(2) | МОНІТОРИНГ СИСТЕМИ - АВТОМАТИЗОВАНІ ЗАСОБИ ТА МЕХАНІЗМИ АНАЛІЗУ В РЕАЛЬНОМУ ЧАСІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-4(2)[1] | впровадити автоматизовані засоби для підтримки аналізу подій у режимі близькому до реального часу |
| SI-4(2)[2] | впровадити автоматизовані механізми для підтримки аналізу подій у режимі близькому до реального часу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за реагування, управління інцидентами].  Перевірка: [ВИБІР: Організаційні процеси для аналізу подій майже у реальному часі; організаційні процеси моніторингу інформаційної системи; автоматизовані механізми підтримки та, або впровадження моніторингу інформаційної системи; автоматизовані механізми, інструменти, що підтримують та, або здійснюють аналіз подій]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-4(3) | МОНІТОРИНГ СИСТЕМИ - АВТОМАТИЗОВАНІ ЗАСОБИ ТА МЕХАНІЗМИ ІНТЕГРАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-4(3)[1] | впровадити автоматизовані засоби для інтеграції: | | |
| SI-4(3)[1][1] | інструментів виявлення вторгнень у: | |
| SI-4(3)[1][1][1] | механізми контролю доступу |
| SI-4(3)[1][1][2] | механізми контролю потоків |
| SI-4(3)[1][2] | механізмів виявлення вторгнень у: | |
| SI-4(3)[1][2][1] | механізми контролю доступу |
| SI-4(3)[1][2][2] | механізми контролю потоків |
| SI-4(3)[2] | впровадити автоматизовані механізми для інтеграції: | | |
| SI-4(3)[2][1] | інструментів виявлення вторгнень у: | |
| SI-4(3)[2][1][1] | механізми контролю доступу |
| SI-4(3)[2][1][2] | механізми контролю потоків |
| SI-4(3)[2][2] | механізмів виявлення вторгнень у: | |
| SI-4(3)[2][2][1] | механізми контролю доступу |
| SI-4(3)[2][2][2] | механізми контролю потоків |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; політика та процедури контролю доступу; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу інформаційної системи; автоматизовані механізми, інструменти, що підтримують та, або реалізують можливості контролю доступу, потоку; автоматизовані механізми, інструменти, що підтримують та, або реалізують інтеграцію засобів виявлення вторгнень у механізми контролю доступу, потоку]. | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SI-4(4) | МОНІТОРИНГ СИСТЕМИ - ТРАФІК ВХІДНИХ І ВИХІДНИХ КОМУНІКАЦІЙ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SI-4(4)[1] | організація визначає частоту, з якою необхідно проводити моніторинг: | | | |
| SI-4(4)[1][1] | вхідного комунікаційного трафіку | | |
| SI-4(4)[1][2] | вихідного комунікаційного трафіку | | |
| SI-4(4)[2] | проводити моніторинг: | | | |
| SI-4(4)[2][1] | вхідного комунікаційного трафіку з визначеною організацією частотою для виявлення: | | |
| SI-4(4)[2][1]{1} | незвичайних: | |
| SI-4(4)[2][1]{1}{1} | дій |
| SI-4(4)[2][1]{1}{2} | умов |
| SI-4(4)[2][1]{2} | несанкціонованих: | |
| SI-4(4)[2][1]{2}{1} | дій |
| SI-4(4)[2][1]{2}{2} | умов |
| SI-4(4)[2][2] | вихідного комунікаційного трафіку з визначеною організацією частотою для виявлення: | | |
| SI-4(4)[2][2]{1} | незвичайних: | |
| SI-4(4)[2][2]{1}{1} | дій |
| SI-4(4)[2][2]{1}{2} | умов |
| SI-4(4)[2][2]{2} | несанкціонованих: | |
| SI-4(4)[2][2]{2}{1} | дій |
| SI-4(4)[2][2]{2}{2} | умов |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; протоколи інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують моніторинг вхідного, вихідного комунікаційного трафіку]. | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-4(5) | МОНІТОРИНГ СИСТЕМИ - СИСТЕМНІ СПОВІЩЕННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-4(5)[1] | SI-4(5)[1][1] | SI-4(5)[1][1]{1} | організація визначає персонал |
| SI-4(5)[1][1]{2} | організація визначає посадові особи |
| SI-4(5)[1][2] | організація визначає показники компрометації | |
| SI-4(5)[2] | попереджати визначений організацією: | | |
| SI-4(5)[2]{1} | персонал, коли виникають, як системні ознаки, визначені організацією показники: | |
| SI-4(5)[2]{1}{1} | компрометації |
| SI-4(5)[2]{1}{2} | потенційної компрометації |
| SI-4(5)[2]{2} | посадові особи, коли виникають, як системні ознаки, визначені організацією показники: | |
| SI-4(5)[2]{2}{1} | компрометації |
| SI-4(5)[2]{2}{2} | потенційної компрометації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; попередження, сповіщення, що генеруються на основі показників компрометації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробники системи ; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують попередження щодо показників компрометації]. | | | |

|  |  |
| --- | --- |
| SI-4(6) | МОНІТОРИНГ СИСТЕМИ - ЗАБОРОНА ДЛЯ НЕПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ |
|  | [Вилучено: Включено до AC-6(10)]. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-4(7) | МОНІТОРИНГ СИСТЕМИ - АВТОМАТИЧНЕ РЕАГУВАННЯ НА ПІДОЗРІЛІ ПОДІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-4(7)[1] | SI-4(7)[1][1] | організація визначає персонал реагування на інциденти ідентифікований по (один або кілька): | |
| SI-4(7)[1][1]{1} | імені |
| SI-4(7)[1][1]{2} | посаді |
| SI-4(7)[1][2] | організація визначає мінімально руйнівні дії для припинення підозрілих подій | |
| SI-4(7)[2] | SI-4(7)[2][1] | повідомляти про виявлені підозрілі події визначений організацією персонал реагування на інциденти ідентифікований по: | |
| SI-4(7)[2][1]{1} | імені |
| SI-4(7)[2][1]{2} | посаді |
| SI-4(7)[2][2] | вжити визначені організацією мінімально руйнівні дії для припинення підозрілих подій | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; попередження, повідомлення, що генеруються на основі виявлених підозрілих подій; записи дій, здійснених для припинення підозрілих подій; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробники системи; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу інформаційної системи; автоматизовані механізми підтримки та, або впровадження повідомлень персоналу реагування на інциденти; автоматизовані механізми, що підтримують та, або здійснюють дії щодо припинення підозрілих подій]. | | | |

|  |  |
| --- | --- |
| SI-4(8) | МОНІТОРИНГ СИСТЕМИ - ЗАХИСТ ІНФОРМАЦІЇ МОНІТОРИНГУ |
|  | [Вилучено: Включено до SI-4]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-4(9) | МОНІТОРИНГ СИСТЕМИ - ТЕСТУВАННЯ ЗАСОБІВ І МЕХАНІЗМІВ МОНІТОРИНГУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-4(9)[1] | організація визначає частоту | |
| SI-4(9)[2] | Тестувати з визначеною організацією частотою: | |
| SI-4(9)[2][1] | інструменти моніторингу вторгнень |
| SI-4(9)[2][2] | механізми моніторингу вторгнень |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються тестування інструментів та механізмів моніторингу інформаційної системи; документація, що підтверджує тестування засобів контролю за вторгненням; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або реалізують можливість виявлення вторгнень, моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують тестування засобів контролю за вторгненням]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-4(10) | МОНІТОРИНГ СИСТЕМИ - ВИДИМІСТЬ ЗАШИФРОВАНИХ КОМУНІКАЦІЙ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-4(10)[1] | SI-4(10)[1][1] | організація визначає зашифрований трафік зв'язку |
| SI-4(10)[1][2] | організація визначає засоби моніторингу системи |
| SI-4(10)[1][3] | організація визначає механізми моніторингу системи |
| SI-4(10)[2] | уживати заходи, щоб визначений організацією зашифрований трафік зв'язку було видно на визначених організацією: | |
| SI-4(10)[2][1] | засобах моніторингу системи |
| SI-4(10)[2][2] | механізмах моніторингу системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; протоколи інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або реалізують видимість зашифрованого комунікаційного трафіку для інструментів моніторингу]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-4(11) | МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ АНОМАЛІЙ ТРАФІКУ КОМУНІКАЦІЙ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-4(11)[1] | організація визначає внутрішні точки всередині системи, в яких необхідно проводити аналіз трафіку вихідних комунікацій для виявлення аномалій | |
| SI-4(11)[2] | проводити аналіз трафіку вихідних комунікацій для виявлення аномалій на: | |
| SI-4(11)[2][1] | зовнішній межі системи |
| SI-4(11)[2][2] | в окремих визначених організацією внутрішніх точках всередині системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; схема мережі; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; журнали або записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу інформаційної системи; автоматизовані механізми підтримки та, або реалізації аналізу комунікаційного трафіку]. | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SI-4(12) | МОНІТОРИНГ СИСТЕМИ - СТВОРЕНІ ОРГАНІЗАЦІЄЮ АВТОМАТИЗОВАНІ СПОВІЩЕННЯ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SI-4(12)[1] | SI-4(12)[1][1] | SI-4(12)[1][1]{1} | організація визначає персонал | |
| SI-4(12)[1][1]{2} | організація визначає посадові особи | |
| SI-4(12)[1][2] | організація визначає заходи, які викликають сповіщення | | |
| SI-4(12)[2] | впровадити автоматизовані механізми для оповіщення визначених організацією | | | |
| SI-4(12)[2]{1} | персоналу, коли виникають визначені організацією заходи, які викликають сповіщення з наслідками для: | | |
| SI-4(12)[2]{1}{1} | | безпеки |
| SI-4(12)[2]{1}{2} | | приватності |
| SI-4(12)[2]{2} | посадових осіб, коли виникають визначені організацією заходи, які викликають сповіщення з наслідками для: | | |
| SI-4(12)[2]{1}{1} | | безпеки |
| SI-4(12)[2]{1}{2} | | приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік невідповідних або незвичних дій (із наслідками для безпеки), які викликають оповіщення; попередження, повідомлення, що надаються працівникам служби безпеки; журнали або записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробники системи; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують автоматизовані оповіщення персоналу служби безпеки]. | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SI-4(13) | МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ ТРАФІКУ ТА ШАБЛОНІВ ПОДІЙ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SI-4(13)(a) | SI-4(13)(a)[1] | аналізувати трафік подій для системи | | |
| SI-4(13)(a)[2] | аналізувати шаблони подій для системи | | |
| SI-4(13)(b) | розробити профілі, що представляють загальну модель: | | | |
| SI-4(13)(b)[1] | | трафіку | |
| SI-4(13)(b)[2] | | шаблони подій | |
| SI-4(13)(c) | використовувати профілі | | | |
| SI-4(13)(c)[1] | | трафіку в налаштуванні пристроїв моніторингу системи, щоб зменшити кількість помилкових: | |
| SI-4(13)(c)[1][1] | позитивних спрацювань |
| SI-4(13)(c)[1][2] | негативних спрацювань |
| SI-4(13)(c)[2] | | подій в налаштуванні пристроїв моніторингу системи, щоб зменшити кількість помилкових: | |
| SI-4(13)(c)[2][1] | позитивних спрацювань |
| SI-4(13)(c)[2][2] | негативних спрацювань |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; список профілів, що представляють загальні схеми трафіку та, або події; документація протоколів інформаційної системи; перелік допустимих порогових значень для помилкових спрацьовувань та помилкових негативних результатів; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або здійснюють аналіз комунікаційного трафіку, моделей подій]. | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-4(14) | МОНІТОРИНГ СИСТЕМИ - ВИЯВЛЕННЯ БЕЗДРОТОВОГО ВТОРГНЕННЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-4(14)[1] | впровадити бездротову систему виявлення вторгнень, щоб: | | |
| SI-4(14)[1][1] | визначати зловмисні бездротові пристрої та | |
| SI-4(14)[1][2] | виявляти спроби атаки та | |
| SI-4(14)[1][3] | SI-4(14)[1][3]{1} | виявляти потенційні компрометації |
| SI-4(14)[1][3]{2} | виявляти порушення системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; протоколи інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень; автоматизовані механізми, що підтримують та, або реалізують можливість бездротового виявлення вторгнень]. | | | |

|  |  |  |
| --- | --- | --- |
| SI-4(15) | МОНІТОРИНГ СИСТЕМИ - ПЕРЕХІД ВІД БЕЗДРОТОВОГО ЗВ’ЯЗКУ ДО ПРОВІДНИХ МЕРЕЖ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-4(15)[1] | впровадити систему виявлення вторгнень для моніторингу трафіку бездротового зв'язку, коли трафік переходить від бездротових до дротових мереж. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація протоколів інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР З: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або реалізують можливість бездротового виявлення вторгнень]. | |

|  |  |  |
| --- | --- | --- |
| SI-4(16) | МОНІТОРИНГ СИСТЕМИ - ЗІСТАВЛЕННЯ ІНФОРМАЦІЇ МОНІТОРИНГУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-4(16)[1] | зіставляти інформацію з інструментів та механізмів моніторингу, що використовуються в системі |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; журнали або записи кореляції подій; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують співвідношення інформації з інструментів моніторингу]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-4(17) | МОНІТОРИНГ СИСТЕМИ - ІНТЕГРОВАНА СИТУАЦІЙНА ОБІЗНАНІСТЬ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-4(17)[1] | зіставляти інформацію, отриману через моніторинг: | |
| SI-4(17)[1][1] | фізичної, з метою досягнення інтегрованої, всеосяжної ситуаційної обізнаності |
| SI-4(17)[1][2] | кібердіяльності, з метою досягнення інтегрованої, всеосяжної ситуаційної обізнаності |
| SI-4(17)[1][3] | діяльності ланцюга постачання, з метою досягнення інтегрованої, всеосяжної ситуаційної обізнаності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; журнали кореляції подій або записи, що є результатом фізичної, кібердіяльності та діяльності ланцюжка постачання; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або реалізують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують співвідношення інформації з інструментів моніторингу]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-4(18) | МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ ТРАФІКУ ТА ПРИХОВАНОЇ ЕКСФІЛЬТРАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-4(18)[1] | організація визначає внутрішні точки всередині системи | | |
| SI-4(18)[2] | для виявлення прихованої ексфільтрації інформації аналізувати трафік вихідних комунікацій на: | | |
| SI-4(18)[2][1] | зовнішній межі | |
| SI-4(18)[2][2] | SI-4(18)[2][2]{1} | периметрі системи |
| SI-4(18)[2][2]{2} | визначених організацією внутрішніх точках всередині системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; схема мережі; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; журнали або записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи; організаційний персонал, відповідальний за систему виявлення вторгнень].  Перевірка: [ВИБІР: Організаційні процеси для виявлення вторгнень, моніторинг інформаційної системи; автоматизовані механізми, що підтримують та, або реалізують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми підтримки та, або реалізації аналізу вихідного комунікаційного трафіку]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-4(19) | МОНІТОРИНГ СИСТЕМИ - ОСОБИ, ЯКІ ПРЕДСТАВЛЯЮТЬ БІЛЬШИЙ РИЗИК | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-4(19)[1] | SI-4(19)[1][1] | організація визначає додатковий моніторинг |
| SI-4(19)[1][2] | організація визначає джерелами |
| SI-4(19)[2] | здійснювати визначений організацією додатковий моніторинг осіб, які були визначені організаційними джерелами, як такі, що представляють підвищений рівень ризику | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються моніторингу інформаційної системи; проєктна документація інформаційної системи; перелік осіб, які були визнані такими, що становлять підвищений рівень ризику; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи]. | | |

|  |  |  |
| --- | --- | --- |
| SI-4(20) | МОНІТОРИНГ СИСТЕМИ - ПРИВІЛЕЙОВАНІ КОРИСТУВАЧІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-4(20)[1] | організація визначає додатковий моніторинг привілейованих користувачів |
| SI-4(20)[2] | реалізувати визначений організацією додатковий моніторинг привілейованих користувачів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; список пільгових користувачів; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; журнали або записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-4(21) | МОНІТОРИНГ СИСТЕМИ - ВИПРОБУВАЛЬНІ ТЕРМІНИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-4(21)[1] | SI-4(21)[1][1] | організація визначає додатковий моніторинг |
| SI-4(21)[1][2] | організація визначає випробувальний період |
| SI-4(21)[2] | реалізувати визначений організацією додатковий моніторинг осіб під час визначений організацією випробувальний період | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; журнали або записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи]. | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SI-4(22) | МОНІТОРИНГ СИСТЕМИ - НЕСАНКЦІОНОВАНІ ПОСЛУГИ МЕРЕЖІ | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | |
| SI-4(22)[1] | SI-4(22)[1][1] | SI-4(22)[1][1]{1} | | організація визначає процеси авторизації | | |
| SI-4(22)[1][1]{2} | | організація визначає процеси затвердження | | |
| SI-4(22)[1][2] | SI-4(22)[1][2]{1} | | організація визначає персонал | | |
| SI-4(22)[1][2]{2} | | організація визначає посадових осіб | | |
| SI-4(22)[2] | SI-4(22)[2][1] | виявляти послуги мережі, які: | | | | |
| SI-4(22)[2][1]{1} | не були дозволені: | | | |
| SI-4(22)[2][1]{1}{1} | | | визначені організацією процеси авторизації |
| SI-4(22)[2][1]{1}{2} | | | визначені організацією процеси затвердження та |
| SI-4(22)[2][1]{2} | не були схвалені: | | | |
| SI-4(22)[2][1]{2}{1} | | | визначені організацією процеси авторизації |
| SI-4(22)[2][1]{2}{2} | | | визначені організацією процеси затвердження та |
| SI-4(22)[2][2] | здійснити*:* | | | | |
| SI-4(22)[2][2][1] | перевірку; | | | |
| SI-4(22)[2][2][2] | попередження : | | | |
| SI-4(22)[2][2][2]{1} | | визначеного організацією персоналу | |
| SI-4(22)[2][2][2]{2} | | визначених організацією посадових осіб | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; задокументована авторизація, затвердження мережевих послуг; повідомлення або попередження про несанкціоновані послуги мережі; журнали або записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи; автоматизовані механізми аудиту мережевих послуг; автоматизовані механізми надання сповіщень]. | | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-4(23) | МОНІТОРИНГ СИСТЕМИ - ПРИСТРОЇ НА ОСНОВІ ХОСТА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-4(23)[1] | SI-4(23)[1][1] | організація визначає механізми моніторингу на основі хоста |
| SI-4(23)[1][2] | організація визначає компоненти системи на яких реалізують механізми моніторингу на основі хоста |
| SI-4(23)[2] | реалізувати визначені організацією механізми моніторингу на основі хоста на визначених організацією компонентах системи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу інформаційної системи; проєктна документація інформаційної системи; механізми моніторингу на основі хоста; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік компонентів інформаційної системи, що вимагають моніторингу на основі хоста; журнали або записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, відповідальний за інформаційну безпеку; організаційний персонал, який встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг хостів інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу інформаційної системи; автоматизовані механізми, що підтримують та, або впроваджують можливість моніторингу на основі хоста]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-4(24) | МОНІТОРИНГ СИСТЕМИ - ОЗНАКИ КОМПРОМЕТАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-4(24)[1] | SI-4(24)[1]{1} | організація визначає персонал | |
| SI-4(24)[1]{2} | організація визначає посадових осіб | |
| SI-4(24)[2] | SI-4(24)[2][1] | досліджувати ознаки компрометації серед визначених організацією: | |
| SI-4(24)[2][1]{1} | персонал |
| SI-4(24)[2][1]{2} | посадових осіб |
| SI-4(24)[2][2] | збирати ознаки компрометації серед визначених організацією: | |
| SI-4(24)[2][2]{1} | персонал |
| SI-4(24)[2][2]{2} | посадових осіб |
| SI-4(24)[2][3] | поширювати ознаки компрометації серед визначених організацією: | |
| SI-4(24)[2][3]{1} | персонал |
| SI-4(24)[2][3]{2} | посадових осіб |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; журнали або записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг хостів інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу інформаційної системи; організаційні процеси для виявлення, збору, розподілу та використання ознак компрометації; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують виявлення, збір, розподіл та використання ознак компрометації]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-4(25) | МОНІТОРИНГ СИСТЕМИ - МОНІТОРИНГ ПЕРСОНАЛЬНИХ ДАНИХ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-4(25)[1] | використовувати автоматизовані механізми для моніторингу: | | |
| SI-4(25)[1](a) | SI-4(25)[1](a){1} | несанкціонованого доступу |
| SI-4(25)[1](a){2} | використання персональних даних |
| SI-4(25)[1](b) | SI-4(25)[1](b)[1] | збору персональних даних |
| SI-4(25)[1](b)[2] | створення персональних даних |
| SI-4(25)[1](b)[3] | точності персональних даних |
| SI-4(25)[1](b)[4] | актуальності персональних даних |
| SI-4(25)[1](b)[5] | своєчасності персональних даних |
| SI-4(25)[1](b)[6] | критичності персональних даних |
| SI-4(25)[1](b)[7] | повноти персональних даних |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються моніторингу інформаційної системи; проєктна документація інформаційної системи; документація засобів і методів моніторингу інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; журнали або записи моніторингу інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи; організаційний персонал, що встановлює, налаштовує та, або підтримує інформаційну систему; організаційний персонал, відповідальний за моніторинг хостів інформаційної системи].  Перевірка: [ВИБІР: Організаційні процеси для моніторингу інформаційної системи; організаційні процеси для виявлення, збору, розподілу та використання ознак компрометації; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують виявлення, збір, розподіл та використання ознак компрометації]. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SI-5 | ПОПЕРЕДЖЕННЯ, РЕКОМЕНДАЦІЇ ТА ДИРЕКТИВИ З БЕЗПЕКИ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SI-5(a) | SI-5(a)[1] | організація визначає зовнішні організації | | | |
| SI-5(a)[2] | отримувати системні: | | | |
| SI-5(a)[2][1] | попередження безпеки від визначених організацією зовнішніх організацій на постійній основі | | |
| SI-5(a)[2][2] | рекомендації від визначених організацією зовнішніх організацій на постійній основі | | |
| SI-5(a)[2][3] | директиви від визначених організацією зовнішніх організацій на постійній основі | | |
| SI-5(b) | генерувати за необхідністю внутрішні: | | | | |
| SI-5(b)[1] | попередження безпеки | | | |
| SI-5(b)[2] | рекомендації | | | |
| SI-5(b)[3] | директиви | | | |
| SI-5(c) | SI-5(c)[1] | SI-5(c)[1][1] | SI-5(c)[1][1]{1} | організація визначає персонал | |
| SI-5(c)[1][1]{2} | організація визначає посадові особи | |
| SI-5(c)[1][2] | організація визначає елементи всередині організації | | |
| SI-5(c)[1][3] | організація визначає зовнішні організації | | |
| SI-5(c)[2] | SI-5(c)[2][1] | поширювати попередження безпеки для (один або кілька): | | |
| SI-5(c)[2][1]{1} | | визначений організацією персонал |
| SI-5(c)[2][1]{2} | | визначений організацією посадові особи |
| SI-5(c)[2][1]{3} | | визначені організацією елементи всередині організації |
| SI-5(c)[2][1]{4} | | визначені організацією зовнішні організації |
| SI-5(c)[2][2] | Поширювати рекомендації безпеки для: (один або кілька): | | |
| SI-5(c)[2][2]{1} | | визначений організацією персонал |
| SI-5(c)[2][2]{2} | | визначений організацією посадові особи |
| SI-5(c)[2][2]{3} | | визначені організацією елементи всередині організації |
| SI-5(c)[2][2]{4} | | визначені організацією зовнішні організації |
| SI-5(c)[2][3] | поширювати директиви безпеки для: (один або кілька): | | |
| SI-5(c)[2][3]{1} | | визначений організацією персонал |
| SI-5(c)[2][3]{2} | | визначений організацією посадові особи |
| SI-5(c)[2][3]{3} | | визначені організацією елементи всередині організації |
| SI-5(c)[2][1]{4} | | визначені організацією зовнішні організації |
| SI-5(d) | SI-5(d)[1] | впровадити директиви безпеки відповідно до встановлених термінів та | | | |
| SI-5(d)[2] | повідомити організацію-емітента про ступінь невідповідності | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються попереджень, рекомендацій та вказівок щодо безпеки; записи попереджень щодо безпеки; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який несе відповідальність за попередження та консультування; організаційний персонал, що впроваджує, експлуатує, підтримує та використовує інформаційну систему; організаційний персонал, організаційні елементи та, або зовнішні організації, яким слід поширювати попередження, рекомендації та директиви; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення, приймання, генерування, розповсюдження та дотримання сповіщень про безпеку, рекомендацій та директив; автоматизовані механізми, що підтримують та, або впроваджують визначення, отримання, генерування та розповсюдження попереджень, рекомендацій та директив безпеки; автоматизовані механізми, що підтримують та, або впроваджують директиви безпеки]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-5(1) | ПОПЕРЕДЖЕННЯ, РЕКОМЕНДАЦІЇ ТА ДИРЕКТИВИ З БЕЗПЕКИ - АВТОМАТИЧНІ ПОПЕРЕДЖЕННЯ ТА РЕКОМЕНДАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-5(1)[1] | впровадити автоматизовані механізми, щоб зробити: | |
| SI-5(1)[1][1] | попередження з безпеки доступними для всієї організації |
| SI-5(1)[1][2] | рекомендації з безпеки доступними для всієї організації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються попереджень, рекомендацій та вказівок щодо безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; автоматизовані механізми підтримки розповсюдження попереджувальної та рекомендаційної інформації щодо безпеки; записи попереджень та рекомендацій щодо безпеки; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який несе відповідальність за попередження та консультування; організаційний персонал, що впроваджує, експлуатує, підтримує та використовує інформаційну систему; організаційний персонал, організаційні елементи та, або зовнішні організації, яким слід поширювати попередження та рекомендації; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення, приймання, генерування та розповсюдження попереджень та рекомендацій щодо безпеки; автоматизовані механізми, що підтримують та, або впроваджують розповсюдження попереджень та рекомендацій щодо безпеки]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-6 | ПЕРЕВІРКА ФУНКЦІЙ БЕЗПЕКИ ТА ПРИВАТНОСТІ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-6(a) | SI-6(a)[1] | організація визначає функції безпеки та приватності | |
| SI-6(a)[2] | перевіряти правильність роботи визначених організацією функцій безпеки та приватності | |
| SI-6(b) | SI-6(b)[1] | SI-6(b)[1][1] | організація визначає системні перехідні стани |
| SI-6(b)[1][2] | організація визначає частоту, з якою виконують перевірку |
| SI-6(b)[2] | виконувати перевірку (один або кілька): | |
| SI-6(b)[2]{1} | визначених організацією системних перехідних станів |
| SI-6(b)[2]{2} | за командою користувача з відповідними повноваженнями |
| SI-6(b)[2]{3] | з визначеною організацією частотою |
| SI-6(c) | SI-6(c)[1] | SI-6(c)[1]{1} | організація визначає персонал |
| SI-6(c)[1]{2} | організація визначає посадових осіб |
| SI-6(c)[2] | повідомляти визначений організацією: | |
| SI-6(c)[2]{1} | персонал про невдалі перевірки безпеки та приватності |
| SI-6(c)[2]{2} | посадові особи про невдалі перевірки безпеки та приватності |
| SI-6(d) | SI-6(d)[1] | визначені організацією альтернативні дії, коли виявляються аномалії. | |
| SI-6(d)[2] | коли виявляються аномалії (один або кілька): | |
| SI-6(d)[2]{1} | вимкнути систему |
| SI-6(d)[2]{2} | перезапустити систему |
| SI-6(d)[2]{3} | виконати визначені організацією альтернативні дії |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки функції безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; попередження, повідомлення про невдалі тести перевірки безпеки; перелік станів переходу системи, що вимагають перевірки функціональності безпеки; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за перевірку функцій безпеки; організаційний персонал, що впроваджує, експлуатує та підтримує інформаційну систему; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для перевірки функції захисту; автоматизовані механізми, що підтримують та, або реалізують можливість перевірки функції безпеки]. | | | |

|  |  |
| --- | --- |
| SI-6(1) | ПЕРЕВІРКА БЕЗПЕКИ ТА ФУНКЦІЙ ПРИВАТНОСТІ - СПОВІЩЕННЯ ПРО НЕУСПІШНЕ ПРОХОДЖЕННЯ ТЕСТІВ З БЕЗПЕКИ |
|  | [Вилучено: Включено до SI-6]. |

|  |  |  |
| --- | --- | --- |
| SI-6(2) | ПЕРЕВІРКА БЕЗПЕКИ ТА ФУНКЦІЙ ПРИВАТНОСТІ - АВТОМАТИЗОВАНА ПІДТРИМКА РОЗПОДІЛЕНОГО ТЕСТУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-6(2)[1] | впровадити автоматизовані механізми для підтримки управління розподіленого тестування функцій безпеки та приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки функції безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за перевірку функцій безпеки; організаційний персонал, що впроваджує, експлуатує та підтримує інформаційну систему; адміністратори системи, мережі; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для перевірки функції захисту; автоматизовані механізми, що підтримують та, або впроваджують управління розподіленим тестуванням безпеки]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-6(3) | ПЕРЕВІРКА БЕЗПЕКИ ТА ФУНКЦІЙ ПРИВАТНОСТІ - ПОВІДОМЛЕННЯ ПРО РЕЗУЛЬТАТИ ПЕРЕВІРКИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-6(3)[1] | SI-6(3)[1]{1} | організація визначає персонал |
| SI-6(3)[1]{2} | організація визначає посадові особи |
| SI-6(3)[2] | повідомляти про результати перевірки функцій безпеки та приватності визначений організацією: | |
| SI-6(3)[2]{1} | персонал |
| SI-6(3)[2]{2} | посадових осіб |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки функції безпеки; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи результатів перевірки функції захисту; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, який відповідає за перевірку функцій безпеки; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для звітування про результати перевірки функції захисту; автоматизовані механізми, що підтримують та, або впроваджують звітування про результати перевірки функцій безпеки]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-7 | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-7[1] | SI-7[1][1] | організація визначає програмне забезпечення, щодо якого необхідно впровадити інструменти перевірки цілісності для виявлення несанкціонованих змін |
| SI-7[1][2] | організація визначає вбудоване програмне забезпечення, щодо якого необхідно впровадити інструменти перевірки цілісності для виявлення несанкціонованих змін |
| SI-7[1][3] | організація визначає інформацію, щодо якої необхідно впровадити інструменти перевірки цілісності для виявлення несанкціонованих змін |
| SI-7[2] | впровадити інструменти перевірки цілісності для виявлення несанкціонованих змін визначеного організацією: | |
| SI-7[2][1] | програмного забезпечення, |
| SI-7[2][2] | вбудованого програмного забезпечення |
| SI-7[2][3] | Інформації. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються цілісності програмного забезпечення, вбудованого програмного забезпечення та інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи, генеровані, ініційовані засобами перевірки цілісності щодо несанкціонованих змін програмного забезпечення, вбудованого програмного забезпечення та інформації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації]. | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SI-7(1) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ЦІЛІСНОСТІ | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | |
| SI-7(1)[1] | SI-7(1)[1][1] | SI-7(1)[1][1][1] | організація визначає програмне забезпечення | |
| SI-7(1)[1][1][2] | організація визначає вбудоване програмне забезпечення | |
| SI-7(1)[1][1][3] | організація визначає інформацію | |
| SI-7(1)[1][2] | SI-7(1)[1][2]{1} | організація визначає перехідні стани, що стосуються безпеки | |
| SI-7(1)[1][2]{2} | організація визначає перехідні події, що стосуються безпеки | |
| SI-7(1)[1][3] | організація визначає частоту, з якою | | |
| SI-7(1)[2] | SI-7(1)[2][1] | виконати перевірку цілісності визначеного організацією програмного забезпечення (один або більше): | | |
| SI-7(1)[2][1][1] | під час запуску | |
| SI-7(1)[2][1][2] | SI-7(1)[2][1][2]{1} | під час визначених організацією перехідних станів, що стосуються безпеки |
| SI-7(1)[2][1][2]{3} | під час визначених організацією перехідних подій, що стосуються безпеки |
| SI-7(1)[2][1][3] | визначена організацією частота | |
| SI-7(1)[2][2] | виконати перевірку цілісності визначеного організацією вбудованого програмного забезпечення (один або більше): | | |
| SI-7(1)[2][2][1] | під час запуску | |
| SI-7(1)[2][2][2] | SI-7(1)[2][2][2]{1} | під час визначених організацією перехідних станів, що стосуються безпеки; |
| SI-7(1)[2][2][2]{3} | під час визначених організацією перехідних подій, що стосуються безпеки |
| SI-7(1)[2][2][3] | визначена організацією частота | |
| SI-7(1)[2][3] | виконати перевірку цілісності визначеної організацією інформації (один або більше): | | |
| SI-7(1)[2][3][1] | під час запуску | |
| SI-7(1)[2][3][2] | SI-7(1)[2][3][2]{1} | під час визначених організацією перехідних станів, що стосуються безпеки |
| SI-7(1)[2][3][2]{3} | під час визначених організацією перехідних подій, що стосуються безпеки; |
| SI-7(1)[2][3][3] | визначена організацією частота | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканування цілісності; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації]. | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-7(2) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АВТОМАТИЧНІ СПОВІЩЕННЯ ПРО ПОРУШЕННЯ ЦІЛІСНОСТІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-7(2)[1] | SI-7(2)[1]{1} | організація визначає персонал |
| SI-7(2)[1]{2} | організація визначає посадові особи |
| SI-7(2)[2] | впровадити автоматизовані інструменти, які надсилають повідомлення до визначеного організацією: | |
| SI-7(2)[2]{1} | персоналу після виявлення розбіжностей під час перевірки цілісності |
| SI-7(2)[2]{2} | посадових осіб після виявлення розбіжностей під час перевірки цілісності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудоване програмне забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканування цілісності; автоматизовані інструменти, що підтримують попередження та повідомлення про порушення в цілісності; попередження, повідомлення, що надаються при виявленні розбіжностей під час перевірки цілісності; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що забезпечують повідомлення про невідповідність цілісності]. | | |

|  |  |  |
| --- | --- | --- |
| SI-7(3) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ІНСТРУМЕНТИ ЦІЛІСНОСТІ З ЦЕНТРАЛІЗОВАНИМ УПРАВЛІННЯМ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-7(3)[1] | впровадити інструменти перевірки цілісності з централізованим управлінням |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудоване програмне забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканування цілісності; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за центральне управління засобами перевірки цілісності; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують центральне управління засобами перевірки цілісності]. | |

|  |  |
| --- | --- |
| SI-7(4) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ – ПАКУВАННЯ З ІНДИКАЦІЄЮ ОЗНАК ЇЇ НЕСАНКЦІОНОВАНОГО РОЗКРИТТЯ |
|  | [Вилучено: Включено до SA-12]. |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-7(5) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АВТОМАТИЧНІ ВІДПОВІДІ ПРО ПОРУШЕННЯ ЦІЛІСНОСТІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-7(5)[1] | організація визначає захисні заходи | |
| SI-7(5)[2] | автоматично (один або більше): | |
| SI-7(5)[2]{1} | вимкнути систему, коли виявляються порушення цілісності |
| SI-7(5)[2]{2} | перезапустити систему, коли виявляються порушення цілісності |
| SI-7(5)[2]{3} | реалізувати визначені організацією захисні заходи, коли виявляються порушення цілісності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудоване програмне забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканування цілісності; записи перевірок цілісності та відповідей на порушення цілісності; записи інформаційного аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що забезпечують автоматичну реакцію на порушення цілісності; автоматизовані механізми, що підтримують та, або впроваджують гарантії безпеки, що застосовуються при виявленні порушень цілісності]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-7(6) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-7(6)[1] | запровадити криптографічні механізми для виявлення несанкціонованих змін: | |
| SI-7(6)[1][1] | програмного забезпечення |
| SI-7(6)[1][2] | вбудованого програмного забезпечення |
| SI-7(6)[1][3] | інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудоване програмне забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; криптографічні механізми та супутня документація; записи виявлених несанкціонованих змін програмного забезпечення, вбудоване програмне забезпечення та інформації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; криптографічні механізми, що реалізують програмне забезпечення, вбудоване програмне забезпечення та цілісність інформації]. | | |

|  |  |  |
| --- | --- | --- |
| SI-7(7) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ІНТЕГРАЦІЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-7(7)[1] | організація визначає відповідні зміни в системі |
| SI-7(7)[2] | включити виявлення визначених організацією відповідних змін в системі, несанкціонованих змін, у можливості організації реагувати на інциденти. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудоване програмне забезпечення та цілісності інформації; процедури, що стосуються реагування на події; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи реагування на події; записи інформаційного аудиту; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; організаційний персонал, відповідальний за реагування на події].  Перевірка: [ВИБІР: Організаційні процеси для включення виявлення несанкціонованих змін, що стосуються безпеки, до можливостей реагування на аварії; програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або впроваджують включення виявлення несанкціонованих змін, що стосуються безпеки, у можливості реагування на аварії]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-7(8) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АУДИТ ВАЖЛИВИХ ПОДІЙ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-7(8)[1] | SI-7(8)[1][1] | SI-7(8)[1][1]{1} | організація визначає персонал |
| SI-7(8)[1][1]{2} | організація визначає посадові особи |
| SI-7(8)[1][2] | організація визначає інші дії | |
| SI-7(8)[2] | при виявленні потенційного порушення цілісності провести аудит події та ініціювати наступні дії: [вибір (один або більше): | | |
| SI-7(8)[2]{1} | створити запис аудиту | |
| SI-7(8)[2]{2} | сповістити поточного користувача; | |
| SI-7(8)[2]{3} | SI-7(8)[2]{3}{1} | сповістити визначені організацією персонал |
| SI-7(8)[2]{3}{2} | сповістити визначені організацією посадові особи; |
| SI-7(8)[2]{4} | виконати визначені організацією інші дії | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканування цілісності; записи реагування на аварії, перелік змін, що стосуються безпеки, в інформаційній системі; автоматизовані інструменти, що підтримують попередження та сповіщення у разі виявлення несанкціонованих змін безпеки; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або реалізують можливість аудиту потенційних порушень цілісності; автоматизовані механізми, що підтримують та, або впроваджують попередження про потенційні порушення цілісності]. | | | |

|  |  |  |
| --- | --- | --- |
| SI-7(9) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ПРОЦЕСУ ЗАВАНТАЖЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-7(9)[1] | організація визначає системні компоненти, щодо яких необхідно перевіряти цілісність процесу завантаження |
| SI-7(9)[2] | перевіряти цілісність процесу завантаження визначених організацією системних компонент |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; засоби перевірки цілісності та відповідна документація; документація; записи сканувань перевірки цілісності; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; розробник системи].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або впроваджують перевірку цілісності процесу завантаження]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-7(10) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ЗАХИСТ ЗАВАНТАЖУВАЛЬНОГО ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-7(10)[1] | SI-7(10)[1][1] | організація визначає заходи безпеки для захисту цілісності завантажувального вбудованого програмного забезпечення |
| SI-7(10)[1][2] | організація визначає компоненти системи, щодо яких реалізують визначені організацією заходи безпеки |
| SI-7(10)[2] | реалізувати визначені організацією заходи безпеки для захисту цілісності завантажувального вбудованого програмного забезпечення визначених організацією компонент системи | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканувань перевірки цілісності; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми підтримки та, або реалізації захисту цілісності завантажувального програмного забезпечення; захисні механізми, що забезпечують захист цілісності завантажувального програмного забезпечення]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-7(11) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ОБМЕЖЕНЕ СЕРЕДОВИЩЕ З ОБМЕЖЕНИМИ ПРИВІЛЕЯМИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-7(11)[1] | організація визначає програмне забезпечення, встановлене користувачем | |
| SI-7(11)[2] | вимагати, щоб визначене організацією програмне забезпечення, встановлене користувачем, виконувалося в обмеженому: | |
| SI-7(11)[2]{1} | фізичному середовищі з обмеженими правами |
| SI-7(11)[2]{2} | віртуальному середовищі з обмеженими правами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або реалізують виконання програмного забезпечення в обмеженому середовищі (фізичному та, або віртуальному); автоматизовані механізми, що підтримують та, або реалізують обмежені привілеї в обмеженому середовищі]. | | |

|  |  |  |
| --- | --- | --- |
| SI-7(12) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ЦІЛІСНОСТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-7(12)[1] | організація визначає програмне забезпечення, встановлене користувачем |
| SI-7(12)[2] | вимагати перевірки цілісності визначеного організацією програмного забезпечення, встановленого користувачем перед виконанням |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи про перевірку цілісності; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або здійснюють перевірку цілісності встановленого користувачем програмного забезпечення перед виконанням]. | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SI-7(13) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ВИКОНАННЯ КОДУ В ЗАХИЩЕНИХ СЕРЕДОВИЩАХ | | | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | | | |
| SI-7(13)[1] | SI-7(13)[1][1] | | організація визначає персонал | | | | |
| SI-7(13)[1][2] | | організація визначає посадову особу | | | | |
| SI-7(13)[2] | дозволяти виконання: | | | | | | |
| SI-7(13)[2]{1} | двійкового коду тільки в обмежених: | | | | | |
| SI-7(13)[2]{1}{1} | | фізичних середовищах і з явним схваленням визначеного організацією: | | | |
| SI-7(13)[2]{1}{1}{1} | персоналу, коли такий код (один або кілька): | | |
| SI-7(13)[2]{1}{1}{1}(a) | отриманий з джерел: | |
| SI-7(13)[2]{1}{1}{1}(a){1} | з обмеженими гарантіями |
| SI-7(13)[2]{1}{1}{1}(a){2} | без гарантій |
| SI-7(13)[2]{1}{1}{1}(b) | без надання вихідного коду | |
| SI-7(13)[2]{1}{1}{2} | посадовими особами, коли такий код: | | |
| SI-7(13)[2]{1}{1}{2}(a) | отриманий з джерел: | |
| SI-7(13)[2]{1}{1}{2}(a){1} | з обмеженими гарантіями |
| SI-7(13)[2]{1}{1}{2}(a){2} | без гарантій |
| SI-7(13)[2]{1}{1}{2}(b) | без надання вихідного коду | |
| SI-7(13)[2]{1}{2} | | віртуальних машин | | | |
| SI-7(13)[2]{1}{2}{1} | персоналу, коли такий код (один або кілька): | | |
| SI-7(13)[2]{1}{2}{1}(a) | отриманий з джерел: | |
| SI-7(13)[2]{1}{2}{1}(a){1} | з обмеженими гарантіями |
| SI-7(13)[2]{1}{2}{1}(a){2} | без гарантій |
| SI-7(13)[2]{1}{2}{1}(b) | без надання вихідного коду | |
| SI-7(13)[2]{1}{2}{2} | посадовими особами, коли такий код: | | |
| SI-7(13)[2]{1}{2}{2}(a) | отриманий з джерел: | |
| SI-7(13)[2]{1}{2}{2}(a){1} | з обмеженими гарантіями |
| SI-7(13)[2]{1}{2}{2}(a){2} | без гарантій |
| SI-7(13)[2]{1}{2}{2}(b) | без надання вихідного коду | |
| SI-7(13)[2]{2} | машинно-виконуваного коду тільки в обмежених: | | | | | |
|  | SI-7(13)[2]{2}{1} | | фізичних середовищах і з явним схваленням визначеного організацією: | | | |
| SI-7(13)[2]{2}{1}{1} | персоналу, коли такий код (один або кілька): | | |
| SI-7(13)[2]{2}{1}{1}(a) | отриманий з джерел: | |
| SI-7(13)[2]{2}{1}{1}(a){1} | з обмеженими гарантіями |
| SI-7(13)[2]{2}{1}{1}(a){2} | без гарантій |
| SI-7(13)[2]{2}{1}{1}(b) | без надання вихідного коду | |
| SI-7(13)[2]{2}{1}{2} | посадовими особами, коли такий код: | | |
|  | отриманий з джерел: | |
| SI-7(13)[2]{2}{1}{2}(a){1} | з обмеженими гарантіями |
| SI-7(13)[2]{2}{1}{2}(a){2} | без гарантій |
| SI-7(13)[2]{2}{1}{2}(b) | без надання вихідного коду | |
| SI-7(13)[2]{2}{2} | | віртуальних машин | | | |
| SI-7(13)[2]{2}{2}{1} | персоналу, коли такий код (один або кілька): | | |
| SI-7(13)[2]{2}{2}{1}(a) | отриманий з джерел: | |
| SI-7(13)[2]{2}{2}{1}(a){1} | з обмеженими гарантіями |
| SI-7(13)[2]{2}{2}{1}(a){2} | без гарантій |
| SI-7(13)[2]{2}{2}{1}(b) | без надання вихідного коду | |
| SI-7(13)[2]{2}{2}{2} | посадовими особами, коли такий код: | | |
| SI-7(13)[2]{2}{2}{2}(a) | отриманий з джерел: | |
| SI-7(13)[2]{2}{2}{2}(a){1} | з обмеженими гарантіями |
| SI-7(13)[2]{2}{2}{2}(a){2} | без гарантій |
| SI-7(13)[2]{2}{2}{2}(b) | без надання вихідного коду. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи затвердження для виконання двійкового та машинно-виконуваного коду; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або впроваджують дозволи на виконання двійкового або машинно-виконуваного коду]. | | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SI-7(14) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ДВІЙКОВИЙ АБО МАШИННОВИКОНУВАНИЙ КОД | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SI-7(14)(a) | заборонити використання: | | | | |
| SI-7(14)(a){1} | двійкового або з джерел: | | | |
| SI-7(14)(a){1}[1] | SI-7(14)(a){1}[1]{1} | | з обмеженою гарантією |
| SI-7(14)(a){1}[1]{2} | | без гарантій |
| SI-7(14)(a){1}[2] | без надання вихідного коду | | |
| SI-7(14)(a){2} | машинно-виконуваного коду | | | |
| SI-7(14)(a){2}[1] | SI-7(14)(a){2}[1]{1} | з обмеженою гарантією | |
| SI-7(14)(a){2}[1]{2} | без гарантій | |
| SI-7(14)(a){2}[2] | без надання вихідного коду | | |
| SI-7(14)(b) | Забезпечити винятки до вимог вихідного коду лише для: | | | | |
| SI-7(14)(b)[1] | SI-7(14)(b)[1]{1} | переконливих завдань | | |
| SI-7(14)(b)[1]{2} | переконливих операційних вимог | | |
| SI-7(14)(b)[2] | за погодженням з уповноваженим службовцем | | | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи затвердження для виконання двійкового та машинно-виконуваного коду; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; уповноважена посадова особа; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують заборону на виконання двійкового або машинно-виконуваного коду]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-7(15) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АВТЕНТИФІКАЦІЯ КОДУ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-7(15)[1] | SI-7(15)[1]{1} | організація визначає програмне забезпечення |
| SI-7(15)[1]{2} | організація визначає компоненти вбудованого програмного забезпечення |
| SI-7(15)[2] | запровадити криптографічні механізми для автентифікації визначеного організацією: | |
| SI-7(15)[2]{1} | програмного забезпечення перед його встановленням |
| SI-7(15)[2]{2} | компоненти вбудованого програмного забезпечення перед його встановленням |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; криптографічні механізми та супутня документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Криптографічні механізми, що перевіряють автентичність програмного забезпечення, вбудованого програмного забезпечення перед установкою]. | | |

|  |  |  |
| --- | --- | --- |
| SI-7(16) | ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ТЕРМІН ВИКОНАННЯ ПРОЦЕСУ БЕЗ НАГЛЯДУ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-7(16)[1] | організація визначає період часу, який не має перевищувати виконання процесів без нагляду |
| SI-7(16)[2] | заборонити виконання процесів без нагляду впродовж більш ніж визначений організацією період часу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються цілісності програмного забезпечення та інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або впроваджують обмеження часу на виконання процесу без нагляду]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-8 | ЗАХИСТ ВІД СПАМУ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-8(a) | впровадити механізми захисту від спаму в: | | |
| SI-8(a)[1] | точках входу системи, щоб: | |
| SI-8(a)[1][1] | виявляти небажані повідомлення |
| SI-8(a)[1][2] | протидіяти небажаним повідомленням |
| SI-8(a)[2] | точках виходу системи, щоб: | |
| SI-8(a)[2][1] | виявляти небажані повідомлення |
| SI-8(a)[2][2] | протидіяти небажаним повідомленням |
| SI-8(b) | оновлювати механізми захисту від спаму, коли доступні нові механізми відповідно до: | | |
| SI-8(b)[1] | організаційної політики | |
| SI-8(b)[2] | процедур управління конфігурацією | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; політика та процедури управління конфігурацією (CM-1); процедури, що стосуються захисту від спаму; механізми захисту від спаму; записи оновлення захисту від спаму; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за захист від спаму; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для впровадження захисту від спаму; автоматизовані механізми, що підтримують та, або впроваджують захист від спаму]. | | | |

|  |  |  |
| --- | --- | --- |
| SI-8(1) | ЗАХИСТ ВІД СПАМУ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-8(1)[1] | централізовано управляти механізмами захисту від спаму |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від спаму; механізми захисту від спаму; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за захист від спаму; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі].  Перевірка: [ВИБІР: Організаційні процеси для централізованого управління захистом від спаму; автоматизовані механізми підтримки та, або впровадження централізованого управління захистом від спаму]. | |

|  |  |  |
| --- | --- | --- |
| SI-8(2) | ЗАХИСТ ВІД СПАМУ - АВТОМАТИЧНІ ОНОВЛЕННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-8(2)[1] | автоматично оновлювати механізми захисту від спаму |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від спаму; механізми захисту від спаму; записи оновлення захисту від спаму; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за захист від спаму; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для захисту від спаму; автоматизовані механізми, що підтримують та, або впроваджують автоматичне оновлення механізмів захисту від спаму]. | |

|  |  |  |
| --- | --- | --- |
| SI-8(3) | ЗАХИСТ ВІД СПАМУ - БЕЗПЕРЕРВНЕ НАВЧАННЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-8(3)[1] | запровадити механізми захисту від спаму з можливістю навчання для більш ефективного визначення законного трафіку зв'язку |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від спаму; механізми захисту від спаму; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за захист від спаму; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для захисту від спаму; автоматизовані механізми, що підтримують та, або впроваджують механізми захисту від спаму з можливістю навчання]. | |

|  |  |
| --- | --- |
| SI-9 | ОБМЕЖЕННЯ НА ВВЕДЕННЯ ІНФОРМАЦІЇ |
|  | [Вилучено: включено до AC-2, AC-3, AC-5, AC-6]. |

|  |  |  |
| --- | --- | --- |
| SI-10 | ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-10[1] | організація визначає інформацію |
| SI-10[2] | перевіряти дійсність визначеної організацією введеної інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; політика та процедури контролю доступу; політика та процедури розподілу обов'язків; процедури, що стосуються перевірки введення інформації; документація на автоматизовані засоби та програми для перевірки достовірності інформації; перелік введених даних, що вимагають перевірки дійсності; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перевірку введення інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують перевірку дійсності на вході інформації]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-10(1) | ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - МОЖЛИВІСТЬ РУЧНОГО ПЕРЕВИЗНАЧЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-10(1)(a) | SI-10(1)(a)[1] | організація визначає входи щодо яких необхідно забезпечити можливість ручного перевизначення для вхідної перевірки |
| SI-10(1)(a)[2] | забезпечити можливість ручного перевизначення для вхідної перевірки визначених організацією входів |
| SI-10(1)(b) | SI-10(1)(b)[1] | організація визначає уповноважені особи |
| SI-10(1)(b)[2] | обмежити використання можливостей ручного перевизначення лише для визначених організацією уповноважених осіб |
| SI-10(1)(c) | перевіряє використання можливостей ручного перевизначення | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; політика та процедури контролю доступу; політика та процедури розподілу обов'язків; процедури, що стосуються перевірки введення інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перевірку введення інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для використання можливостей ручного перевизначення; автоматизовані механізми, що підтримують та, або впроваджують можливість ручного перевизначення для перевірки вхідних даних; автоматизовані механізми, що підтримують та, або здійснюють аудит використання можливостей ручного перевизначення]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-10(2) | ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ПЕРЕГЛЯД ТА УСУНЕННЯ ПОМИЛОК | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-10(2)[1] | визначити організацією період часу, за який необхідно переглядати та усувати помилки перевірки вводу інформації | |
| SI-10(2)[2] | помилки перевірки вводу інформації в межах визначеного організацією періоду часу: | |
| SI-10(2)[2][1] | переглядати |
| SI-10(2)[2][2] | усувати |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; політика та процедури контролю доступу; політика та процедури розподілу обов'язків; процедури, що стосуються перевірки введення інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; переглядати записи помилок перевірки введення інформації та результатів вирішення; журнали або записи помилок перевірки введення інформації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перевірку введення інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі].  Перевірка: [ВИБІР: Організаційні процеси для перегляду та вирішення помилок перевірки вхідних даних; автоматизовані механізми, що підтримують та, або впроваджують перевірку та вирішення помилок перевірки вхідних даних]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-10(3) | ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ПЕРЕДБАЧУВАНА ПОВЕДІНКА | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-10(3)[1] | Перевіряти, що при отриманні недійсних вхідних даних система поводиться: | |
| SI-10(3)[1][1] | передбачуваним способом |
| SI-10(3)[1][2] | документованим способом |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки введення інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перевірку введення інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують передбачувану поведінку при отриманні недійсних входів]. | | |

|  |  |  |
| --- | --- | --- |
| SI-10(4) | ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ЧАСОВІ ВЗАЄМОДІЇ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-10(4)[1] | враховувати часові взаємодії між компонентами системи при визначенні доречних відповідей для невідповідних вхідних даних |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки введення інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перевірку введення інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для визначення відповідних реакцій на недійсні введені дані; автоматизовані механізми, що підтримують та, або реалізують відповіді на недійсні дані]. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-10(5) | ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ОБМЕЖЕННЯ ВХІДНИХ ДАНИХ ДОВІРЕНИМИ ДЖЕРЕЛАМИ І ЗАТВЕРДЖЕНИМИ ФОРМАТАМИ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-10(5)[1] | SI-10(5)[1][1] | організація визначає довірені джерела | |
| SI-10(5)[1][2] | організація визначає формати | |
| SI-10(5)[2] | обмежити використання вхідних даних лише (один або більше): | | |
| SI-10(5)[2]{1} | | визначеними організацією довіреними джерелами |
| SI-10(5)[2{2}] | | визначеними організацією форматами |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки введення інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік надійних джерел для введення інформації; перелік прийнятних форматів обмежень на введення; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перевірку введення інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для обмеження введення інформації; автоматизовані механізми, що підтримують та, або впроваджують обмеження вводу інформації]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-11 | ОБРОБКА ПОМИЛОК | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-11(a) | створити повідомлення про помилки, які надають інформацію, необхідну для реалізації виправних дій, без виявлення інформації, яка може бути використана | | |
| SI-11(b) | SI-11(b)[1] | SI-11(b)[1]{1} | організація визначає персонал |
| SI-11(b)[1]{2} | організація визначає посадові особи |
| SI-11(b)[2] | показувати повідомлення про помилки лише визначеним організацією: | |
| SI-11(b)[2]{1} | персоналу |
| SI-11(b)[2]{2} | посадовим особам |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються обробки помилок інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація, що забезпечує структуру, зміст повідомлень про помилки; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перевірку введення інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для обробки помилок; автоматизовані механізми, що підтримують та, або реалізують обробку помилок; автоматизовані механізми підтримки та, або реалізації управління повідомленнями про помилки]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-12 | УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-12[1] | управляти інформацією всередині системи відповідно до: | |
| SI-12[1][1] | чинного законодавства |
| SI-12[1][2] | виконавчих наказів |
| SI-12[1][3] | директив |
| SI-12[1][4] | правил |
| SI-12[1][5] | політик |
| SI-12[1][6] | стандартів |
| SI-12[1][7] | керівних принципів |
| SI-12[1][8] | експлуатаційних вимог |
| SI-12[2] | зберігати інформацію всередині системи відповідно до: | |
| SI-12[2][1] | чинного законодавства |
| SI-12[2][2] | виконавчих наказів |
| SI-12[2][3] | директив |
| SI-12[2][4] | правил |
| SI-12[2][5] | політик |
| SI-12[2][6] | стандартів |
| SI-12[2][7] | керівних принципів |
| SI-12[2][8] | експлуатаційних вимог |
| SI-12[3] | виводити інформацію з системи відповідно до: | |
| SI-12[3][1] | чинного законодавства |
| SI-12[3][2] | виконавчих наказів, |
| SI-12[3][3] | директив |
| SI-12[3][4] | правил, |
| SI-12[3][5] | політик |
| SI-12[3][6] | стандартів, |
| SI-12[3][7] | керівних принципів |
| SI-12[3][8] | експлуатаційних вимог |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; федеральні закони, розпорядження, директиви, політика, положення, стандарти та експлуатаційні вимоги, що застосовуються до обробки та зберігання інформації; політика та процедури захисту засобів масової інформації; процедури, що стосуються обробки та збереження вихідних даних інформаційної системи; записи про збереження інформації, інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за обробку та збереження інформації; організаційний персонал, який відповідає за інформаційну безпеку, адміністратори мережі].  Перевірка: [ВИБІР: Організаційні процеси для обробки та збереження інформації; автоматизовані механізми, що підтримують та, або впроваджують обробку та збереження інформації]. | | |

|  |  |  |
| --- | --- | --- |
| SI-12(1) | УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ - ОБМЕЖЕННЯ ЕЛЕМЕНТІВ ПЕРСОНАЛЬНИХ ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-12(1)[1] | організація визначає елементи, до яких обмежують обробку персональних даних в життєвому циклі |
| SI-12(1)[2] | Обмежити обробку персональних даних в життєвому циклі інформації до визначених організацією елементів, визначених в ході оцінки ризику приватності. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; федеральні закони, розпорядження, директиви, політика, положення, стандарти та експлуатаційні вимоги, що застосовуються до обробки та зберігання інформації; політика та процедури захисту засобів масової інформації; процедури, що стосуються обробки та збереження вихідних даних інформаційної системи; записи про збереження інформації, інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за обробку та збереження інформації; організаційний персонал, який відповідає за інформаційну безпеку, адміністратори мережі].  Перевірка: [ВИБІР: Організаційні процеси для обробки та збереження інформації; автоматизовані механізми, що підтримують та, або впроваджують обробку та збереження інформації]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-12(2) | УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ - МІНІМІЗАЦІЯ ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ТЕСТУВАННЯ, НАВЧАННЯ ТА ДОСЛІДЖЕННІ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-12(2)[1] | організація визначає методи | |
| SI-12(2)[2] | використовувати визначені організацією методи для мінімізації використання персональних даних для | |
| SI-12(2)[2]{1} | досліджень, відповідно до оцінки ризику приватності |
| SI-12(2)[2]{2} | тестування, відповідно до оцінки ризику приватності |
| SI-12(2)[2]{3} | навчання, відповідно до оцінки ризику приватності |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; федеральні закони, розпорядження, директиви, політика, положення, стандарти та експлуатаційні вимоги, що застосовуються до обробки та зберігання інформації; політика та процедури захисту засобів масової інформації; процедури, що стосуються обробки та збереження вихідних даних інформаційної системи; записи про збереження інформації, інші відповідні документи чи записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за обробку та збереження інформації; організаційний персонал, який відповідає за інформаційну безпеку, адміністратори мережі].  Перевірка: [ВИБІР: Організаційні процеси для обробки та збереження інформації; автоматизовані механізми, що підтримують та, або впроваджують обробку та збереження інформації]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-13 | ПЕРЕДБАЧУВАНЕ ЗАПОБІГАННЯ ЗБОЇВ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-13(a) | SI-13(a)[1] | організація визначає компоненти системи. для яких необхідно визначити середній час до збою в певних середовищах роботи | |
| SI-13(a)[2] | визначити середній час до збою (MTTF) для визначеної організацією компоненти системи в певних середовищах роботи | |
| SI-13(b) | SI-13(b)[1] | організація визначає критерії заміни | |
| SI-13(b)[2] | надати: | |
| SI-13(b)[2][1] | замінні компоненти системи резервними компонентами відповідно до визначених організацією критеріїв заміни |
| SI-13(b)[2][2] | засоби для заміни активних компонентів резервними компонентами відповідно до визначених організацією критеріїв заміни |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБЕРІТЬ З: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання збоїв; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік критеріїв заміщення MTTF; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБЕРІТЬ З: Організаційний персонал, відповідальний за визначення та діяльність MTTF; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; організаційний персонал, відповідальний за планування на випадок непередбачених ситуацій].  Перевірка: [ВИБЕРІТЬ З: Організаційні процеси для управління MTTF]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-13(1) | ЗАПОБІГАННЯ ПЕРЕДБАЧУВАНИХ ЗБОЇВ - ВІДПОВІДАЛЬНІСТЬ ЗА ПЕРЕДАЧУ ФУНКЦІЙ КОМПОНЕНТІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-13(1)[1] | SI-13(1)[1]{1} | організація визначає частину |
| SI-13(1)[1]{2} | організація визначає відсоток |
| SI-13(1)[2] | знімати з експлуатації системні компоненти шляхом передачі функцій на резервні компоненти не пізніше, визначеної організацією: | |
| SI-13(1)[2]{1} | частиною середнього часу до збоїв |
| SI-13(1)[2]{2} | відсоток середнього часу до збоїв |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання відмов; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за діяльність MTTF; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; організаційний персонал, відповідальний за планування на випадок непередбачених ситуацій].  Перевірка: [ВИБІР: Організаційні процеси для управління MTTF; автоматизовані механізми, що підтримують та, або реалізують передачу відповідальності за компоненти]. | | |

|  |  |
| --- | --- |
| SI-13(2) | ЗАПОБІГАННЯ ПЕРЕДБАЧУВАНИХ ЗБОЇВ - ТЕРМІН ВИКОНАННЯ ПРОЦЕСУ БЕЗ НАГЛЯДУ |
|  | [Вилучено: включено до SI-7 (16)]. |

|  |  |  |
| --- | --- | --- |
| SI-13(3) | ЗАПОБІГАННЯ ПЕРЕДБАЧУВАНИХ ЗБОЇВ - РУЧНА ПЕРЕДАЧА ФУНКЦІЙ КОМПОНЕНТІВ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-13(3)[1] | організація визначає відсоток від середнього часу до збоїв |
| SI-13(3)[2] | вручну ініціювати передачу функцій між активними та резервними компонентами системи, коли використання активного компонента досягає визначеного організацією відсотку від середнього часу до збоїв |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання відмов; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за діяльність MTTF; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; організаційний персонал, відповідальний за планування на випадок непередбачених ситуацій].  Перевірка: [ВИБІР: Організаційні процеси для управління MTTF та проведення ручного перенесення між активними та резервними компонентами]. | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SI-13(4) | ЗАПОБІГАННЯ ПЕРЕДБАЧУВАНИХ ЗБОЇВ - ВСТАНОВЛЕННЯ РЕЗЕРВНИХ КОМПОНЕНТІВ ТА ОПОВІЩЕННЯ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SI-13(4)[1] | якщо виявлено збої компонентів системи: | | | | |
| SI-13(4)[1](a) | SI-13(4)[1](a)[1] | | організація визначає період часу для встановлення резервних компонентів | |
| SI-13(4)[1](a)[2] | | переконатися, що резервні компоненти успішно та прозоро встановлені в межах визначеного організацією періоду часу | |
| SI-13(4)[1](b) | SI-13(4)[1](b)[1] | SI-13(4)[1](b)[1][1] | | організація визначає сигнал |
| SI-13(4)[1](b)[1][2] | | організація визначає дію |
| SI-13(4)[1](b)[2] | SI-13(4)[1](b)[2]{1} | | активувати визначений організацією сигнал (та, або) |
| SI-13(4)[1](b)[2]{2} | | автоматично вимкнути систему (та, або) |
| SI-13(4)[1](b)[2]{3} | | виконати визначену організацією дію |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання відмов; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік дій, які слід вжити після виявлення несправності компонента інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за діяльність MTTF; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; організаційний персонал, відповідальний за планування на випадок непередбачених ситуацій].  Перевірка: [ВИБІР: Організаційні процеси для управління MTTF; автоматизовані механізми, що підтримують та, або впроваджують прозорий монтаж резервних компонентів; автоматизовані механізми, що підтримують та, або реалізують аварійні сигнали або вимкнення системи у разі виявлення несправностей компонентів]. | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-13(5) | ЗАПОБІГАННЯ ПЕРЕДБАЧУВАНИХ ЗБОЇВ - МОЖЛИВІСТЬ АВАРІЙНОГО ПЕРЕМИКАННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-13(5)[1] | організація визначає можливість аварійного перемикання | |
| SI-13(5)[2] | забезпечити: | |
| SI-13(5)[2]{1} | в режимі реального часу визначену організацією можливість аварійного перемикання для системи |
| SI-13(5)[2]{2} | близько до реального часу визначену організацією можливість аварійного перемикання для системи |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання відмов; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; документація, що описує можливість відмови, передбачена для інформаційної системи; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за можливість відмови; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; організаційний персонал, відповідальний за планування на випадок непередбачених ситуацій].  Перевірка: [ВИБІР: Організаційні процеси для управління відмовостійкими можливостями; автоматизовані механізми, що підтримують та, або реалізують можливість відмови]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-14 | НЕСТІЙКІСТЬ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-14[1] | SI-14[1][1] | організація визначає компоненти системи | |
| SI-14[1][2] | організація визначає компоненти служби | |
| SI-14[1][3] | організація визначає частоту | |
| SI-14[2] | реалізувати нестійкі визначені організацією: | | |
| SI-14[2][1] | компоненти системи, які ініціюються в відомих станах і завершуються (один або кілька): | |
| SI-14[2][1]{1} | після закінчення сеансу використання |
| SI-14[2][1]{2} | періодично з визначеною організацією частотою |
| SI-14[2][2] | служби, які ініціюються в відомих станах і завершуються (один або кілька): після закінчення сеансу використання, періодично з визначеною організацією частотою | |
| SI-14[2][2]{1} | після закінчення сеансу використання |
| SI-14[2][2]{2} | Періодично, з визначеною організацією частотою |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються непостійності компонентів інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за непостійність; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують ініціацію та завершення роботи нестійких компонентів]. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-14(1) | НЕСТІЙКІСТЬ - ОНОВЛЕННЯ З НАДІЙНИХ ДЖЕРЕЛ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-14(1)[1] | організація визначає довірені джерела | | |
| SI-14(1)[2] | отримувати | | |
| SI-14(1)[2][1] | програмне забезпечення, що використовуються під час оновлення: | |
| SI-14(1)[2][1][1] | компонента системи з визначених організацією довірених джерел |
| SI-14(1)[2][1][2] | служби з визначених організацією довірених джерел |
| SI-14(1)[2][2] | дані, що використовуються під час оновлення: | |
| SI-14(1)[2][2][1] | компонента системи з визначених організацією довірених джерел |
| SI-14(1)[2][2][2] | служби з визначених організацією довірених джерел |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються непостійності компонентів інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за отримання оновлення компонентів та послуг із надійних джерел; організаційний персонал, який відповідає за інформаційну безпеку].  Перевірка: [ВИБІР: Організаційні процеси для визначення та отримання оновлення компонентів та послуг із надійних джерел; автоматизовані механізми, що підтримують та, або впроваджують оновлення компонентів та послуг]. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-15 | ФІЛЬТРАЦІЯ ВИХІДНИХ ДАНИХ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-15[1] | SI-15[1]{1} | організація визначає програмні продукти та, або |
| SI-15[1]{2} | організація визначає програмні додатки |
| SI-15[2] | перевіряти інформацію, що виходить з визначених організацією(один або кілька): | |
| SI-15[2]{1} | програмних продуктів, щоб переконатися, що інформація відповідає очікуваному змісту |
| SI-15[2]{2} | додатків, щоб переконатися, що інформація відповідає очікуваному змісту. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються фільтрації вихідної інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перевірку виводу інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для перевірки виводу інформації; автоматизовані механізми, що підтримують та, або здійснюють перевірку виводу інформації]. | | |

|  |  |  |
| --- | --- | --- |
| SI-15(1) | ФІЛЬТРАЦІЯ ВИХІДНИХ ДАНИХ - ОБМЕЖЕННЯ РОЗПОВСЮДЖЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-15(1)[1] | організація визначає елементи |
| SI-15(1)[2] | обмежити розповсюдження персональних даних на визначені організацією елементи, які визначені при оцінці ризику приватності та узгоджені з уповноваженими цілями |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються фільтрації вихідної інформації; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за перевірку виводу інформації; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процеси для перевірки виводу інформації; автоматизовані механізми, що підтримують та, або здійснюють перевірку виводу інформації]. | |

|  |  |  |
| --- | --- | --- |
| SI-16 | ЗАХИСТ ПАМ'ЯТІ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-16[1] | організація визначає заходи безпеки для захисту системної пам'яті від несанкціонованого виконуваного коду |
| SI-16[2] | виконати визначені організацією заходи безпеки для захисту системної пам'яті від несанкціонованого виконуваного коду |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають пам’ять інформаційної системи від несанкціонованого виконання коду; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за захист пам'яті; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують захисні засоби для захисту пам’яті інформаційної системи від несанкціонованого виконання коду]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-17 | ВІДМОВОСТІЙКІ ПРОЦЕДУРИ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-17[1] | SI-17[1][1] | організація визначає відмовостійкі процедури |
| SI-17[1][2] | організація визначає умови виявлення несправностей |
| SI-17[2] | виконати визначені організацією відмовостійкі процедури, коли настають визначені організацією умови виявлення несправностей | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають пам’ять інформаційної системи від несанкціонованого виконання коду; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-18 | ВИДАЛЕННЯ ІНФОРМАЦІЇ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-18[1] | SI-18[1]{1} | організація визначає методи | |
| SI-18[1]{2} | організація визначає заходи | |
| SI-18[2] | використовує визначені організацією: | | |
| SI-18[2]{1} | методи для: | |
| SI-18[2]{1}{1} | утилізації інформації |
| SI-18[2]{1}{2} | знищення інформації |
| SI-18[2]{1}{3} | стирання інформації |
| SI-18[2]{2} | заходи для: | |
| SI-18[2]{1}{1} | утилізації інформації |
| SI-18[2]{1}{2} | знищення інформації |
| SI-18[2]{1}{3} | стирання інформації |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають пам’ять інформаційної системи від несанкціонованого видалення інформації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту]. | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| SI-19 | ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ | | | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | | | |
| SI-19(a) | SI-19(a){1} | при зборі персональних даних, перевіряти протягом життєвого циклу інформації: | | | |
| SI-19(a){1}[1] | точність інформації | | |
| SI-19(a){1}[2] | релевантність інформації | | |
| SI-19(a){1}[3] | своєчасність інформації | | |
| SI-19(a){1}[4] | критичність інформації | | |
| SI-19(a){1}[5] | повноту інформації | | |
| SI-19(a){1}[6] | де-ідентифікацію інформації | | |
| SI-19(a){2} | створенні персональних даних, перевіряти на: | | | |
| SI-19(a){2}[1] | точність інформації | | |
| SI-19(a){2}[2] | релевантність інформації | | |
| SI-19(a){2}[3] | своєчасність інформації | | |
| SI-19(a){2}[4] | критичність інформації | | |
| SI-19(a){2}[5] | повноту інформації | | |
| SI-19(a){2}[6] | де-ідентифікацію інформації | | |
| SI-19(b) | SI-19(b)[1] | організація визначає частота | | | |
| SI-19(b)[2] | SI-19(b)[2][1] | перевіряти, якщо це необхідно з визначеною організацією частотою та протягом всього життєвого циклу інформації: | | |
| SI-19(b)[2][1](1) | SI-19(b)[2][1](1){1} | неточні персональні дані |
| SI-19(b)[2][1](1){2} | застарілі персональні дані |
| SI-19(b)[2][1](2) | персональні дані з невірно визначеною критичністю | |
| SI-19(b)[2][1](3) | невірно де-ідентифіковані персональні дані | |
| SI-19(b)[2][2] | виправляти, якщо це необхідно з визначеною організацією частотою та протягом всього життєвого циклу інформації: | | |
| SI-19(b)[2][2](1) | SI-19(b)[2][2](1){1} | неточні персональні дані |
| SI-19(b)[2][2](1){2} | застарілі персональні дані |
| SI-19(b)[2][2](2) | персональні дані з невірно визначеною критичністю | |
| SI-19(b)[2][2](3) | невірно де-ідентифіковані персональні дані. | |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; стратегія постійного моніторингу; перелік засобів безпеки, що захищають пам’ять інформаційної системи від несанкціонованого видалення інформації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; засоби перевірки цілісності інформації;]. | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-19(1) | ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - ОНОВЛЕННЯ ТА КОРЕКЦІЯ ПЕРСОНАЛЬНИХ ДАНИХ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-19(1)[1] | впровадити технічні засоби управління для корекції персональних даних, що використовуються в: | | |
| SI-19(1)[1][1] | організаційних програмах та які є: | |
| SI-19(1)[1][1]{1} | неточними |
| SI-19(1)[1][1]{2} | застарілими |
| SI-19(1)[1][1]{3} | невірно визначеними щодо своєї критичності |
| SI-19(1)[1][1]{4} | неправильно де-ідентифіковані |
| SI-19(1)[1][2] | організаційних системах: | |
| SI-19(1)[1][2]{1} | неточними |
| SI-19(1)[1][2]{2} | застарілими |
| SI-19(1)[1][2]{3} | невірно визначеними щодо своєї критичності |
| SI-19(1)[1][2]{4} | неправильно де-ідентифіковані |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; стратегія постійного моніторингу; перелік засобів безпеки, що захищають пам’ять інформаційної системи від несанкціонованого видалення інформації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; технічні засоби управління для корекції персональних даних; засоби перевірки цілісності інформації;]. | | | |

|  |  |  |
| --- | --- | --- |
| SI-19(2) | ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - МІТКИ (ТЕГИ) ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-19(2)[1] | використовувати мітки даних для автоматичного відстеження персональних даних впродовж життєвого циклу інформації в організаційних системах |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; стратегія постійного моніторингу; перелік засобів безпеки, що захищають пам’ять інформаційної системи від несанкціонованого видалення інформації; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми використання міток (тегів) даних]. | |

|  |  |  |
| --- | --- | --- |
| SI-19(3) | ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - ЗБІР ПЕРСОНАЛЬНИХ ДАНИХ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-19(3)[1] | проводити збір персональних даних безпосередньо від фізичних осіб |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають дані в інформаційній системі; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми збору персональних даних; заходи для підтвердження точності та актуальності персональних даних]. | |

|  |  |  |
| --- | --- | --- |
| SI-20 | ДЕ-ІДЕНТИФІКАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-20[1] | видаляти персональні дані з наборів даних |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають дані в інформаційній системі; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми видалення персональних даних]. | |

|  |  |  |
| --- | --- | --- |
| SI-20(1) | ДЕ-ІДЕНТИФІКАЦІЯ - ЗБІР | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-20(1)[1] | де-ідентифікувати набір даних після збору, не збираючи персональні дані. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають дані в інформаційній системі; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми видалення персональних даних]. | |

|  |  |  |
| --- | --- | --- |
| SI-20(2) | ДЕ-ІДЕНТИФІКАЦІЯ - АРХІВАЦІЯ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-20(2)[1] | уникати архівування елементів персональних даних, якщо ці елементи в наборі даних не будуть потрібні після архівування набору даних |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають дані в інформаційній системі; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми видалення персональних даних]. | |

|  |  |  |
| --- | --- | --- |
| SI-20(3) | ДЕ-ІДЕНТИФІКАЦІЯ - РЕЛІЗ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-20(3)[1] | видаляти елементи персональних даних з набору даних перед його випуском (публікацією), якщо ці елементи в наборі даних не повинні бути частиною даних, що публікуються. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають дані в інформаційній системі; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми видалення персональних даних]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-20(4) | ДЕ-ІДЕНТИФІКАЦІЯ - ВИДАЛЕННЯ, МАСКУВАННЯ, ШИФРУВАННЯ, ХЕШУВАННЯ АБО ЗАМІНА ПРЯМИХ ІДЕНТИФІКАТОРІВ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-20(4)[1] | прямі ідентифікатори в наборі даних | |
| SI-20(4)[1]{1} | видаляти |
| SI-20(4)[1]{2} | маскувати |
| SI-20(4)[1]{3} | шифрувати |
| SI-20(4)[1]{4} | хешувати |
| SI-20(4)[1]{5} | замінювати |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають дані в інформаційній системі; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми збору та видалення персональних даних]. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SI-20(5) | ДЕ-ІДЕНТИФІКАЦІЯ - КОНТРОЛЬ СТАТИСТИЧНОГО РОЗКРИТТЯ | | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | | |
| SI-20(5)[1] | управляти: | | |
| SI-20(5)[1][1] | числовими даними, щоб: | |
| SI-20(5)[1][1]{1} | жодна особа не могла бути ідентифікована в результатах аналізу |
| SI-20(5)[1][1]{2} | жодна організація не могла бути ідентифікована в результатах аналізу |
| SI-20(5)[1][2] | таблицями непередбачених обставин, щоб: | |
| SI-20(5)[1][2]{1} | жодна особа не могла бути ідентифікована в результатах аналізу |
| SI-20(5)[1][2]{2} | жодна організація не могла бути ідентифікована в результатах аналізу |
| SI-20(5)[1][3] | статистичними даними, щоб: | |
| SI-20(5)[1][3]{1} | жодна особа не могла бути ідентифікована в результатах аналізу |
| SI-20(5)[1][3]{2} | жодна організація не могла бути ідентифікована в результатах аналізу |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають дані в інформаційній системі; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми збору та видалення персональних даних]. | | | |

|  |  |  |
| --- | --- | --- |
| SI-20(6) | ДЕ-ІДЕНТИФІКАЦІЯ - ДИФЕРЕНЦІЙОВАНА ПРИВАТНІСТЬ | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | |
| SI-20(6)[1] | запобігати розкриттю персональних даних, додаючи недетермінований шум до результатів математичних операцій до отримання результатів |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають дані в інформаційній системі; записи аудиту інформаційної системи; інші відповідні документи або записи].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми збору та видалення персональних даних]. | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-20(7) | ДЕ-ІДЕНТИФІКАЦІЯ - ПЕРЕВІРЕНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-20(7)[1] | виконувати де-ідентифікацію за допомогою: | |
| SI-20(7)[1][1] | перевірених алгоритмів |
| SI-20(7)[1][2] | програмного забезпечення, затвердженого для використання у реалізації алгоритмів. |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають дані в інформаційній системі; записи аудиту інформаційної системи; інші відповідні документи або записи; програмне забезпечення, яке реалізує відповідний алгоритм].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми збору та видалення персональних даних]. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| SI-20(8) | ДЕ-ІДЕНТИФІКАЦІЯ - МОТИВОВАНИЙ ПОРУШНИК | | |
|  | МЕТА ОЦІНКИ:  Визначте, чи: | | |
| SI-20(8)[1] | виконати тест на мотивованого порушника на де-ідентифікованому наборі даних, щоб визначити: | |
| SI-20(8)[1]{1} | чи залишаються присутніми ідентифіковані дані |
| SI-20(8)[1]{2} | або чи можуть дані бути повторно ідентифіковані |
| ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:  Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для інформаційної системи; політики управління даними; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та відповідна документація; перелік засобів безпеки, що захищають дані в інформаційній системі; записи аудиту інформаційної системи; інші відповідні документи або записи; програмне забезпечення, яке реалізує відповідний алгоритм].  Співбесіда: [ВИБІР: Організаційний персонал, відповідальний за процедури захисту; організаційний персонал, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи].  Перевірка: [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми тестування на мотивованого порушника]. | | |