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 2.3-025-24

Том 2

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

Адміністрація Держспецзв'язку
Київ 2024

Додаток А
Том 2

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

I. КЛАС ЗАХОДІВ ЗАХИСТУ АС – УПРАВЛІННЯ ДОСТУПОМ

АС-01	**ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ ДОСТУПОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	АС-01_ODP[01]	**визначено персонал або ролі, на які поширюється політика контролю доступу;**
	АС-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури контролю доступу;**
	АС-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	АС-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами контролю доступу;**
	АС-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика контролю доступу;**
	АС-01_ODP[06]	**визначено події, які вимагають перегляду та оновлення поточної політики контролю доступу;**
	АС-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні процедури контролю доступу;**
	АС-01_ODP[08]	**визначено події, які потребують перегляду та оновлення процедур;**
	АС-01а.[01]	розроблено та задокументовано політику контролю доступу;
	АС-01а.[02]	політика контролю доступу поширюється на **<АС-01_ODP[01] персонал або ролі>**;
	АС-01а.[03]	розроблені та задокументовані процедури контролю доступу для полегшення впровадження політики контролю доступу та пов'язаних з нею заходів захисту;
	АС-01а.[04]	процедури контролю доступу поширюються на **<АС-01_ODP[02] персонал або ролі>**;
	АС-01а.01(а)[01]	політика контролю доступу **<АС-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить мету;
	АС-01а.01(а)[02]	політика контролю доступу **<АС-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить сферу застосування;
	АС-01а.01(а)[03]	політика контролю доступу **<АС-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить ролі;
	АС-01а.01(а)[04]	політика контролю доступу **<АС-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить відповідальність;
	АС-01а.01(а)[05]	політика контролю доступу **<АС-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить зобов’язання керівництва;
	АС-01а.01(а)[06]	політика контролю доступу **<АС-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить координацію між організаційними підрозділами;
	АС-01а.01(а)[07]	політика контролю доступу **<АС-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить систему контролю відповідності;

	AC-01a.01(b)	політика контролю доступу **<AC-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** відповідає чинним законам, виконавчим наказам, директивам, положенням, політикам, стандартам та настановам;
	AC-01b.	**<AC-01_ODP[04] посадова особа>** призначається для управління розробкою, документуванням та розповсюдженням політики та процедур контролю доступу;
	AC-01c.01[01]	переглядається та оновлюється поточна політика контролю доступу **<AC-01_ODP[05] частота>**;
	AC-01c.01[02]	поточну політику контролю доступу переглянуто та оновлено після **<AC-01_ODP[06] подій>**;
	AC-01c.02[01]	переглядаються та оновлюються поточні процедури контролю доступу **<AC-01_ODP[07] частота>**;
	AC-01c.02[02]	поточні процедури контролю доступу переглядаються та оновлюються після **<AC-01_ODP[08] подій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури управління доступом; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за управління доступом; персонал, відповідальний за інформаційну безпеку].	

AC-02	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02_ODP[01]	**визначено передумови та критерії членства в групах і ролях;**
	AC-02_ODP[02]	**визначено атрибути (за необхідності) для кожного облікового запису;**
	AC-02_ODP[03]	**визначено персонал або ролі, необхідні для затвердження запитів на створення облікових записів;**
	AC-02_ODP[04]	**визначено політику, процедури, передумови та критерії створення, активації, зміни, деактивації та видалення облікових записів;**
	AC-02_ODP[05]	**визначено персонал або ролі, які мають бути повідомлені;**
	AC-02_ODP[06]	**визначено період часу, протягом якого адміністратори облікових записів повинні бути повідомлені про те, що облікові записи більше не потрібні;**
	AC-02_ODP[07]	**визначено термін, протягом якого необхідно повідомляти адміністраторів облікових записів про звільнення або переведення користувачів;**
	AC-02_ODP[08]	**визначено період часу, протягом якого необхідно повідомляти адміністраторів облікових записів про зміни у використанні системи або необхідність знати про зміни для окремої особи;**
	AC-02_ODP[09]	**визначено атрибути, необхідні для авторизації доступу до системи (за потреби);**

	AC-02_ODP[10]	**визначено періодичність перегляду облікових записів;**
	AC-02a.[01]	визначено та задокументовано типи облікових записів, дозволених для використання в системі;
	AC-02a.[02]	визначено та задокументовано типи облікових записів, які заборонено використовувати в системі;
	AC-02b	призначені менеджери облікових записів;
	AC-02c	необхідні **<AC-02_ODP[01] умови та критерії>** для членства в групах та ролях;
	AC-02d.01	визначено авторизованих користувачів системи;
	AC-02d.02	вказано приналежність до групи або ролі;
	AC-02d.03[01]	для кожного облікового запису вказуються повноваження доступу (тобто привілеї);
	AC-02d.03[02]	**<AC-02_ODP[02] атрибути (за необхідності)>** вказуються для кожного облікового запису;
	AC-02e	для запитів на створення облікових записів потрібні схвалення від **<AC-02_ODP[03] персоналу або ролей>**;
	AC-02f.[01]	облікові записи створюються відповідно до **<AC-02_ODP[04] політики, процедур, передумов та критеріїв>**;
	AC-02f.[02]	облікові записи активуються відповідно до **<AC-02_ODP[04] політики, процедур, передумов та критеріїв>**;
	AC-02f.[03]	облікові записи змінюються відповідно до **<AC-02_ODP[04] політики, процедур, передумов та критеріїв>**;
	AC-02f.[04]	облікові записи деактивуються відповідно до **<AC-02_ODP[04] політики, процедур, передумов та критеріїв>;**
	AC-02f.[05]	облікові записи видаляються відповідно до **<AC-02_ODP[04] політики, процедур, передумов та критеріїв>;**
	AC-02g	контролюється використання облікових записів;
	AC-02h.01	адміністратори облікових записів та **<AC-02_ODP[05] персонал або ролі>** отримують повідомлення протягом **<AC-02_ODP[06] періоду часу>**, коли облікові записи більше не потрібні;
	AC-02h.02	адміністратори облікових записів та **<AC-02_ODP[05] персонал або ролі>** отримують повідомлення протягом **<AC-02_ODP[07] періоду часу>**, коли користувачі звільнені чи переведені;
	AC-02h.03	адміністратори облікових записів та **<AC-02_ODP[05] персонал або ролі>** отримують повідомлення протягом **<AC-02_ODP[08] періоду часу>**, коли використовуються індивідуальні системи або наявні зміни, які потребують нових знань.
	AC-02i.01	доступ до системи здійснюється на підставі дійсної авторизації доступу;
	AC-02i.02	доступ до системи авторизується на основі передбачуваного використання системи;
	AC-02i.03	доступ до системи авторизовано на основі атрибутів **<AC-02_ODP[09] (за необхідності)>**;

	AC-02j	облікові записи переглядаються на відповідність вимогам управління обліковими записами **<AC-02_ODP[10] частота>**;
	AC-02k.[01]	створено процес повторного випуску облікових даних спільного доступу або групових облікових записів (якщо вони розгорнуті), коли користувачів вилучено з групи;
	AC-02k.[02]	впроваджено процес повторного випуску облікових даних спільного доступу або групових облікових записів (якщо вони розгорнуті), коли користувачів вилучено з групи;
	AC-02l.[01]	процеси управління обліковими записами узгоджуються з процесами звільнення персоналу;
	AC-02l.[02]	процеси управління обліковими записами узгоджуються з процесами переводу персоналу;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; список активних системних облікових записів разом з іменем особи, пов'язаної з кожним обліковим записом; перелік умов для членства в групі та ролі; повідомлення або записи нещодавно переведених, відокремлених або звільнених працівників; список недавно вимкнених облікових записів системи разом з іменем особи, пов'язаної з кожним обліковим записом; записи авторизації доступу; огляди відповідності управління обліковим записом; записи моніторингу системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Управління обліковими записами системи в процесах організації; автоматизовані механізми здійснення управління обліковими записами].	

AC-02(01)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - АВТОМАТИЗОВАНЕ УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(01)_ODP	**визначено автоматизовані механізми, що використовуються для підтримки управління обліковими записами системи;**
	AC-02(01)	управління обліковими записами системи підтримується за допомогою <AC-02(01)_ODP автоматизовані механізми>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи або записи].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами].

AC-02(02)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ВИДАЛЕННЯ ТИМЧАСОВИХ ТА ЕКСТРЕНИХ ОБЛІКОВИХ ЗАПИСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(02) _ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {видаляти; деактивувати};**
	AC-02(02) _ODP[02]	**визначено період часу, після якого автоматично видаляються або деактивуються тимчасові або екстрені облікові записи;**
	AC-02(02)	тимчасові та екстрені облікові записи автоматично **<AC-02(02) _ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** через **<AC-02(02) _ODP[02] період часу>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; сформований перелік тимчасових облікових записів системи, вилучених та / або вимкнених; створений перелік видалених та / або вимкнених екстрених облікових записів системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами].	

AC-02(03)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДЕАКТИВАЦІЯ ОБЛІКОВИХ ЗАПИСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(03)_ODP[01]	**визначено період часу, протягом якого необхідно деактивувати облікові записи;**
	AC-02(03)_ODP[02]	**визначено період часу неактивності, після закінчення якого облікові записи будуть деактивовані;**

	AC-02(03)(a)	облікові записи деактивуються протягом **<AC-02(03)_ODP[01] часового періоду>**, коли термін дії облікових записів минув;
	AC-02(03)(b)	облікові записи деактивуються протягом **<AC-02(03)_ODP[01] часового періоду>**, коли облікові записи більше не пов'язані з користувачем або фізичною особою
	AC-02(03)(c)	облікові записи відключено протягом **<AC-02(03)_ODP[01] часового періоду>**, коли облікові записи порушують політику організації;
	AC-02(03)(d)	облікові записи деактивуються протягом **<AC-02(03)_ODP[01]>**, якщо вони були неактивними протягом **<AC-02(03)_ODP[02]>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; сформований перелік тимчасових облікових записів системи, вилучених та / або вимкнених; створений перелік видалених та / або вимкнених екстрених облікових записів системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами].	

AC-02(04)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДІЇ ПРИ АВТОМАТИЗОВАНОМУ АУДИТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(04)[01]	створення облікового запису автоматично аудитується;
	AC-02(04)[02]	модифікація облікового запису автоматично аудитується;
	AC-02(04)[03]	активація облікового запису автоматично аудитується;
	AC-02(04)[04]	деактивація облікового запису автоматично аудитується;
	AC-02(04)[05]	видалення облікового запису автоматично аудитується.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та супутня документація; повідомлення / сповіщення про створення, модифікацію, активацію, деактивацію та видалення облікових записів; записи аудиту системи; інші відповідні документи або записи].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами].

AC-02(05)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ВИХІД ІЗ СИСТЕМИ ЗА ВІДСУТНОСТІ АКТИВНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(05)_ODP	**визначено часовий період очікуваної бездіяльності або опис, коли потрібно вийти з системи;**
	AC-02(05)	користувачі повинні виходити з системи, коли **<AC-02(05)_ODP період очікуваної бездіяльності або опис часу, коли потрібно вийти з системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; повідомлення про порушення безпеки; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; користувачів, які повинні відповідати політиці виходу з режиму бездіяльності].	

AC-02(06)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДИНАМІЧНЕ УПРАВЛІННЯ ПРИВІЛЕЯМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(06)_ODP	**визначено можливості динамічного управління привілеями;**
	AC-02(06)	реалізовано **<AC-02(06)_ODP можливості динамічного управління привілеями>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік можливостей управління динамічними привілеями системи; записи аудиту системи; інші відповідні доку-	

	менти або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: система або механізм що реалізує можливості динамічного управління привілеями].

AC-02(07)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - СХЕМИ, ЗАСНОВАНІ НА РОЛЯХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(07)_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {схема доступу на основі ролей; схема доступу на основі атрибутів};**
	AC-02(07)(a)	облікові записи привілейованих користувачів створюються та адмініструються відповідно до **<AC-02(07)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**;
	AC-02(07)(b)	проводиться моніторинг призначення привілейованих ролей або атрибутів;
	AC-02(07)(c)	відстежуються зміни ролей або атрибутів;
	AC-02(07)(d)	доступ скасовується, коли призначені привілейовані ролі більше не потрібні.0
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік привілейованих облікових записів користувачів та відповідної ролі в системі; записи про вжиті дії, коли привілейоване призначення ролей більше не присвоюється; записи аудиту системи; звіти про відстеження та моніторинг; записи моніторингу системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами; автоматизовані механізми моніторингу призначень привілейованих ролей].	

AC-02(08)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДИНАМІЧНЕ УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(08)_ODP	**визначено облікові записи системи, які динамічно створюються, активуються, управляються та деактивуються;**
	AC-02(08)[01]	**<AC-02(08)_ODP облікові записи системи>** створюються динамічно;
	AC-02(08)[02]	**<AC-02(08)_ODP облікові записи системи>** активуються динамічно;
	AC-02(08)[03]	**<AC-02(08)_ODP облікові записи системи>** активуються динамічно;
	AC-02(08)[04]	**<AC-02(08)_ODP облікові записи системи>** деактивуються динамічно;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік облікових записів системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організаційний, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами]	

AC-02(09)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ОБМЕЖЕННЯ НА ВИКОРИСТАННЯ СПІЛЬНИХ ТА ГРУПОВИХ ОБЛІКОВИХ ЗАПИСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(09)_ODP	**визначено умови створення спільних та групових облікових записів;**
	AC-02(09)	використання спільних та групових облікових записів дозволено лише за умови дотримання **<AC-02(09)_ODP умов>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та супутня документація; сформований перелік спільних та групових облікових записів системb та пов'язаної з ними ролі; записи аудиту системи; інші відповідні документи або записи].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні та мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують управління спільними та груповими обліковими записами].

AC-02(10)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ЗМІНА ДАНИХ СПІЛЬНИХ І ГРУПОВИХ ОБЛІКОВИХ ЗАПИСІВ**
	[Вилучено: включено до AC-02(k)].

AC-02(11)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - УМОВИ ВИКОРИСТАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(11)_ODP[01]	**визначено обставини та/або умови використання визначених облікових записів системи;**
	AC-02(11)_ODP[02]	**визначені облікові записи системи, що підлягають виконанню обставин та/або умов використання;**
	AC-02(11)	**<AC-02(11)_ODP[01] обставини та/або умови використання>** для **<AC-02(11)_ODP[02] облікових записів системи>** застосовуються.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та супутня документація; сформований перелік облікових записів системи та пов'язані з ними призначення обставин використання та / або умов використання; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами].	

AC-02(12)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - МОНІТОРИНГ НЕТИПОВОГО ВИКОРИСТАННЯ ОБЛІКОВИХ ЗАПИСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(12)_ODP[01]	**визначено обставини та/або умови використання, для яких необхідно здійснювати моніторинг обліко-**

		вих записів системи;
	AC-02(12)_ODP[02]	**визначено персонал або ролі, яким належить повідомляти про визначені обставини та/або умови використання;**
	AC-02(12)(a)	облікові записи системи відстежуються на предмет **<AC-02(12)_ODP[01] обставини та/або умови використання>**;
	AC-02(12)(b)	про визначені обставини та/або умови використання системних облікових записів повідомляється <**AC-02(12)_ODP[02] персонал або ролі>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи моніторингу системи; записи аудиту системи; спостереження аудиту та звіти про моніторинг; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами].	

AC-02(13)	**УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДЕАКТИВАЦІЯ ОБЛІКОВИХ ЗАПИСІВ ОСІБ З ВИСОКИМ РІВНЕМ РИЗИКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-02(13)_ODP[01]	**визначено період часу, протягом якого необхідно деактивувати облікові записи фізичних осіб, які становлять значний ризик;**
	AC-02(13)_ODP[02]	**визначено значні ризики, що призводять до деактивації облікових записів;**
	AC-02(13)	облікові записи користувачів деактивуються протягом **<AC-02(13)_ODP[01] періоду часу>** з моменту виявлення **<AC-02(13)_ODP[02] значних ризиків>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та супутня документація; сформований список відключених облікових записів системи; перелік діяльності користувачів, що становлять значний ризик для організаціъ; записи аудиту системи; інші відповідні документи	

	чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління обліковими записами; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції управління обліковими записами].

AC-03	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ**	
	МЕТА ОЦІНКИ: Визначте, чи	
	AC-03	затверджені повноваження на логічний доступ до інформації та ресурсів системи виконуються відповідно до чинних політик(правил) управління доступом.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік затверджених дозволів (привілеїв користувача); записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу].	

AC-03(01)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ОБМЕЖЕНИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ**
	[Вилучено: включено до складу AC-06]

AC-03(02)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ПОДВІЙНА АВТОРИЗАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(02)_ODP	**визначено привілейовані команди та/або інші дії, що потребують подвійної авторизації;**
	AC-03(02)	подвійна авторизація застосовується для **<AC-03(02)_ODP привілейованих команд та/або інших дій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу та подвійної авторизації; план захисту інформації; проєктна до-	

	кументація системи; налаштування конфігурації системи та супутня документація; список привілейованих команд, що потребують подвійної авторизації; перелік дій, що вимагають подвійної авторизації; перелік затверджених дозволів (привілеїв користувача); інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Подвійні механізми авторизації, що реалізують політику контролю доступу].

AC-03(03)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - МАНДАТНЕ УПРАВЛІННЯ ДОСТУПОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(03)_ODP[01]	**визначено мандатну політику контролю доступу, що застосовується до набору охоплених суб'єктів;**
	AC-03(03)_ODP[02]	**визначено мандатну політику контролю доступу, що застосовується до набору охоплених об'єктів;**
	AC-03(03)_ODP[03]	**визначені суб'єкти, яким явно надаються привілеї;**
	AC-03(03)_ODP[04]	**визначено привілеї, які мають бути прямо надані суб'єктам**
	AC-03(03)[01]	**<AC-03(03)_ODP[01] мандатна політика контролю доступу>** застосовується до набору охоплених суб'єктів, зазначених у політиці
	AC-03(03)[02]	**<AC-03(03)_ODP[02] мандатна політика контролю доступу>** застосовується до набору охоплених об'єктів, зазначених у політиці
	AC-03(03)(a)[01]	**<AC-03(03)_ODP[01] мандатна політика контролю доступу>** застосовується одноманітно до всіх суб'єктів системи;
	AC-03(03)(a)[02]	**<AC-03(03)_ODP[02] мандатна політика контролю доступу>** застосовується одноманітно до всіх об'єктів системи;
	AC-03(03)(b)(01)	**<AC-03(03)_ODP[01] мандатна політика контролю доступу>** та **<AC-03(03)_ODP[02] мандатна політика контролю доступу>**, які визначають, що суб'єкт, якому надано доступ до інформації, зобов'язаний не передавати інформацію неавторизованим суб'єктам або об'єктам;
	AC-03(03)(b)(02)	**<AC-03(03)_ODP[01] мандатна політика контролю доступу>** та **<AC-03(03)_ODP[02] мандатна політика**

		контролю доступу>, які визначають, що суб'єкт, якому надано доступ до інформації, обмежений у наданні своїх привілеїв іншим суб'єктам;
	AC-03(03)(b)(03)	**<AC-03(03)_ODP[01] мандатна політика контролю доступу>** та **<AC-03(03)_ODP[02] мандатна політика контролю доступу>**, які визначають, що суб'єкт, якому надано доступ до інформації, не може змінювати один або декілька атрибутів безпеки (визначених політикою) суб'єктів, об'єктів, системи або компонентів системи;
	AC-03(03)(b)(04)	**<AC-03(03)_ODP[01] мандатна політика контролю доступу>** та **<AC-03(03)_ODP[02] мандатна політика контролю доступу>**, які визначають, що суб'єкт, якому надано доступ до інформації, обмежений у виборі атрибутів безпеки та значень атрибутів (визначених політикою), що повинні бути пов'язані з новостворюваними або зміненими об'єктами;
	AC-03(03)(b)(05)	**<AC-03(03)_ODP[01] мандатна політика контролю доступу>** та **<AC-03(03)_ODP[02] мандатна політика контролю доступу>**, які визначають, що суб'єкт, якому надано доступ до інформації, не має права змінювати правила, що регулюють управління доступом;
	AC-03(03)(c)	**<AC-03(03)_ODP[01] мандатна політика контролю доступу>** та **<AC-03(03)_ODP[02] мандатна політика контролю доступу>**, які визначають, що **<AC-03(03)_ODP[03] суб'єктам>** можуть бути явно надані **<AC-03(03)_ODP[04] привілеї>** таким чином, щоб вони не були обмежені будь-якою визначеною підмножиною (або всіма) з наведених вище обмежень.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; правила мандатного контролю доступу; процедури щодо забезпечення доступу; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік предметів та об'єктів (тобто користувачів та ресурсів), які потребують виконання обов'язкових політик контролю доступу; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують мандатний контроль доступу]	

AC-03(04)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ДИСКРЕЦІЙНЕ УПРАВЛІННЯ ДОСТУПОМ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(04)_ODP[01]	**визначено дискреційну політику управління доступом, яка застосовується до набору охоплених суб'єктів;**
	AC-03(04)_ODP[02]	**визначено дискреційну політику управління доступом, яка застосовується до набору охоплених об'єктів;**
	AC-03(04)[01]	**<AC-03(04)_ODP[01] дискреційна політика управління доступом>** застосовується до набору охоплених суб'єктів, зазначених у політиці;
	AC-03(04)[02]	**<AC-03(04)_ODP[02] дискреційна політика управління доступом>** застосовується до набору охоплених об'єктів, зазначених у політиці;
	AC-03(04)(a)	**<AC-03(04)_ODP[01] дискреційна політика управління доступом>** та **<AC-03(04)_ODP[02] дискреційна політика управління доступом>** застосовуються, коли політика визначає, що суб'єкт, якому надано доступ до інформації, може передавати інформацію будь-яким іншим суб'єктам або об'єктам;
	AC-03(04)(b)	**<AC-03(04)_ODP[01] дискреційна політика управління доступом>** та **<AC-03(04)_ODP[02] дискреційна політика управління доступом>** застосовуються, коли політика визначає, що суб'єкт, якому надано доступ до інформації, може надавати свої привілеї іншим суб'єктам;
	AC-03(04)(c)	**<AC-03(04)_ODP[01] дискреційна політика управління доступом>** та **<AC-03(04)_ODP[02] дискреційна політика управління доступом>** застосовуються, коли політика визначає, що суб'єкт, якому надано доступ до інформації, може змінювати атрибути безпеки суб'єктів, об'єктів, системи або компонентів системи;
	AC-03(04)(d)	**<AC-03(04)_ODP[01] дискреційна політика управління доступом>** та **<AC-03(04)_ODP[02] дискреційна політика управління доступом>** застосовуються там, де політика визначає, що суб'єкт, якому надано доступ до інформації, може вибирати атрибути безпеки, які будуть пов'язані з новоствореними або переглянутими об'єктами;
	AC-03(04)(e)	**<AC-03(04)_ODP[01] дискреційна політика управління доступом>** та **<AC-03(04)_ODP[02] дискреційна політика управління доступом>** застосовуються, коли

		політика визначає, що суб'єкт, якому надано доступ до інформації, може змінювати правила управління доступом.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; дискреційна політика контролю доступу; процедури щодо забезпечення доступу; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік предметів та об'єктів (тобто користувачів та ресурсів), які потребують застосування дискреційних політик контролю доступу; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують дискреційну політику контролю доступу].	

AC-03(05)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ІНФОРМАЦІЯ ЩОДО БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(05)_ODP	**визначено інформацію щодо безпеки, доступ до якої заборонено, за винятком випадків, коли наявні безпечні неробочі стани системи.**
	AC-03(05)	доступ до **<AC-03(05)_ODP інформація щодо безпеки>** заборонено, за винятком випадків, коли наявні безпечні неробочі стани системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що запобігають доступу до інформації, що стосується безпеки, в межах системи].	

AC-03(06)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ЗАХИСТ ІНФОРМАЦІЇ КОРИСТУВАЧА ТА СИСТЕМИ**
	[Вилучено: Включено в MP-04 та SC-28].

AC-03(07)	ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ РОЛЕЙ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(07)_ODP[01]	**визначено ролі, на яких базується управління доступом;**
	AC-03(07)_ODP[02]	**визначено користувачів, уповноважених на прийняття ролей (визначених у AC-03(07)_ODP[01]);**
	AC-03(07)[01]	політика управління доступом на основі ролей застосовується до визначених суб'єктів
	AC-03(07)[02]	політика управління доступом на основі ролей застосовується до визначених об'єктів
	AC-03(07)[03]	доступ контролюється на основі **<AC-03(07)_ODP[01] ролей>** та **<AC-03(07)_ODP[02] користувачів, яким дозволено приймати такі ролі>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; рольові політики контролю доступу; процедури щодо забезпечення доступу; план зпхисту інформації, проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік ролей, користувачів та пов'язаних з ними привілеїв, необхідних для контролю доступу до системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують рольову політику контролю доступу].	

AC-03(08)	ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - АНУЛЮВАННЯ ПРАВ ДОСТУПУ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(08)_ODP	**визначено правила, що регулюють терміни скасування дозволів на доступ;**
	AC-03(08)[01]	здійснюється анулювання прав доступу в результаті зміни атрибутів безпеки суб'єктів на основі **<AC-03(08)_ODP правил>**;
	AC-03(08)[02]	здійснюється анулювання прав доступу в результаті зміни атрибутів безпеки об'єктів на основі <**AC-03(08)_ODP пра-**

		вил>;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; правила, що регулюють скасування дозволів на доступ; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу]	

AC-03(09)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - КЕРОВАНА ПЕРЕДАЧА (ПУБЛІКАЦІЯ) ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(09)_ODP[01])	**визначено зовнішню систему або компонент системи, до якої потрібно надати інформацію;**
	AC-03(09)_ODP[02])	**визначено засоби захисту, які мають бути забезпечені зовнішньою системою або компонентом системи (визначені в AC-03(09)_ODP[01]);**
	AC-03(09)_ODP[03])	**визначено заходи захисту, які використовуються для перевірки доречності інформації, що підлягає оприлюдненню;**
	AC-03(09)(a)	інформація випускається за межі системи, тільки якщо отримуюча <AC-03(09)_ODP[01] система або компонент системи> забезпечує <AC-03(09)_ODP[02] заходи захисту>;
	AC-03(09)(b)	інформація публікується за межами системи, тільки якщо <AC-03(09)_ODP[03] заходи захисту> використовуються для перевірки відповідності інформації, призначеної для публікації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік заходів захисту, що надаються інформаційною системою, яка приймає або її компонентами; список заходів захисту, що підтверджують доречність інформації, призначеної для публікації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за	

	інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу].

AC-03(10)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ПЕРЕГЛЯД АУДИТОМ МЕХАНІЗМІВ КОНТРОЛЮ ДОСТУПУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(10)_ODP[01]	**визначено умови, за яких можна застосовувати перегляд аудитом механізмів автоматизованого управління доступом;**
	AC-03(10)_ODP[02]	**визначено ролі, яким дозволено використовувати перегляд аутом механізмів автоматизованого управління доступом;**
	AC-03(10)	за **<AC-03(10)_ODP[01] умов>** застосовується перегляд аудитом механізмів автоматизованого контролю доступу за допомогою **<AC-03(10)_ODP[02] ролей>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; умови для використання перегляд аудитом автоматизованих механізмів контролю доступу; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу].	

AC-03(11)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ОБМЕЖЕННЯ ДОСТУПУ ДО СПЕЦІАЛЬНОЇ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(11)_ODP	**визначено типи інформації, що потребують обмеженого доступу до сховищ даних;**
	AC-03(11)	обмежено доступ до сховищ даних, що містять **<AC-03(11)_ODP типи інформації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація системи; налаштування конфігурації сис-	

	теми та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу].

AC-03(12)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ВСТАНОВЛЕННЯ ТА ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ЗАСТОСУНКІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(12)_ODP	**визначено програми та функції системи, яким необхідно встановити права доступу;**
	AC-3(12)(a)	у процесі інсталяції програми повинні встановити доступ до таких системних застосунків і функцій системи: <AC-03(12)_ODP програм та функції системи>;
	AC-3(12)(b)	передбачено механізм примусового застосування для запобігання несанкціонованому доступу;
	AC-3(12)(c)	зміни доступу після первинної інсталяції програми схвалено.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу].	

AC-03(13)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ АТРИБУТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(13)_ODP	визначено атрибути для визначення прав доступу;
	AC-03(13)[1]	політика управління доступом на основі атрибутів здійснюється до визначених суб'єктів;

	AC-03(13)[2]	політика управління доступом на основі атрибутів здійснюється до визначених об'єктів;
	AC-03(13)[3]	доступ контролюється на основі **<AC-03(13)_ODP атрибутів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу].	

AC-03(14)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ІНДИВІДУАЛЬНИЙ ДОСТУП**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(14)_ODP[01]	**визначено механізми, що дозволяють фізичним особам мати доступ до елементів їхньої персональної інформації;**
	AC-03(14)_ODP[02]	**визначено елементи інформації, що ідентифікує особу, до якої мають доступ фізичні особи;**
	AC-03(14)	**<AC-03(14)_ODP[01] механізми>** надаються для того, щоб дозволити особам мати доступ до **<AC-03(14)_ODP[02] елементів>** їхньої персональної інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Механізми доступу; політика контролю доступу; процедури, що стосуються забезпечення доступу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; документація щодо доступу до інформації, що ідентифікує особу; записи аудиту системи; план захисту інформації; план забезпечення конфіденційності; оцінка впливу на конфіденційність; висновки та/або звіти з оцінки конфіденційності; інші відповідні документи або записи.]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; юридичний консультант]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції забезпечення доступу; механізми, що дозволяють індивідуальний доступ до інформації, що ідентифі-	

	кує особу].

AC-03(15)	**ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ДИСКРЕЦІЙНИЙ ТА ОБОВ'ЯЗКОВИЙ ДОСТУП**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-03(15)_ODP[01]	**визначено обов'язкову політику контролю доступу, яка застосовується до набору суб'єктів, зазначених у політиці;**
	AC-03(15)_ODP[02]	**визначено обов'язкову політику контролю доступу, яка застосовується до набору об'єктів, зазначених у політиці;**
	AC-03(15)_ODP[03]	**визначено дискреційну політику контролю доступу, яка застосовується до набору суб'єктів, зазначених у політиці;**
	AC-03(15)_ODP[04]	**визначено дискреційну політику контролю доступу, яка застосовується до набору об'єктів, зазначених у політиці;**
	AC-3(15)(a)[01]	**<AC-03(15)_ODP[01] політика обов'язкового контролю доступу>** застосовується до набору охоплених суб'єктів, зазначених у політиці;
	AC-3(15)(a)[02]	**<AC-03(15)_ODP[02] політика обов'язкового контролю доступу>** застосовується до набору охоплених об'єктів, зазначених у політиці;
	AC-3(15)(b)[01]	**<AC-03(15)_ODP[03] дискреційна політика контролю доступу>** застосовується до набору суб'єктів, зазначених у політиці;
	AC-3(15)(b)[02]	**<AC-03(15)_ODP[04] дискреційна політика контролю доступу>** застосовується до набору об'єктів, зазначених у політиці;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління доступом; процедури, що стосуються забезпечення доступу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; перелік суб'єктів та об'єктів (тобто користувачів та ресурсів), що вимагають застосування обов'язкових політик управління доступом; перелік суб'єктів та об'єктів (тобто користувачів та ресурсів), що вимагають застосування дискреційних політик управління доступом; записи аудиту системи; план захисту інформації; інші відповідні документи або записи.].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники систем]. **Перевірка:** [ВИБІР: Механізми реалізації обов'язкової та дискреційної політики контролю доступу].

AC-04	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04_ODP	**визначено політики управління інформаційними потоками всередині системи та між підключеними системами;**
	AC-04	затверджені повноваження застосовуються для контролю потоку інформації всередині системи та між підключеними системами на основі **<AC-04_ODP політики управління інформаційними потоками>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційних потоків; проєктна документація системи; налаштування конфігурації системи та супутня документація; конфігурація базової лінії інформації; перелік дозволів на потік інформації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].	

AC-04(01)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - АТРИБУТИ БЕЗПЕКИ ОБ'ЄКТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(01)_ODP[01]	**визначено атрибути безпеки, які будуть пов'язані з інформацією, джерелом та об'єктами призначення;**
	AC-04(01)_ODP[02]	**визначено атрибути конфіденційності, які будуть пов'язані з інформацією, джерелом та об'єктами призначення;**
	AC-04(01)_ODP[03]	**визначено об'єкти інформації, які будуть пов'язані з атрибутами безпеки;**
	AC-04(01)_ODP[04]	**визначено об'єкти інформації, які будуть пов'язані з**

		атрибутами конфіденційності;
	AC-04(01)_ODP[05]	**визначено джерела об'єктів, які будуть пов'язані з атрибутами безпеки;**
	AC-04(01)_ODP[06]	**визначено джерела об'єктів, які будуть пов'язані з атрибутами конфіденційності;**
	AC-04(01)_ODP[07]	**визначено об'єкти призначення, які будуть пов'язані з атрибутами безпеки;**
	AC-04(01)_ODP[08]	**визначено об'єкти призначення, які будуть пов'язані з атрибутами конфіденційності;**
	AC-04(01)_ODP[09]	**визначено політику управління інформаційними потоками як основу для ухвалення рішень щодо управління потоками;**
	AC-04(01)[01]	**<AC-04(01)_ODP[01] атрибути безпеки>**, пов'язані з **<AC-04(01)_ODP[03] об'єктами інформації>**, **<AC-04(01)_ODP[05] джерела об'єктів>** та **<AC-04(01)_ODP[07] об'єктами призначення>**, використовуються для забезпечення виконання **<AC-04(01)_ODP[09] політик управління інформаційними потоками >** як основи для прийняття рішень щодо управління потоками;
	AC-04(01)[02]	**<AC-04(01)_ODP[02] атрибути конфіденційності>**, пов'язані з **<AC-04(01)_ODP[04] об'єктами інформації>**, **<AC-04(01)_ODP[06] джерела об'єктів>** та **<AC-04(01)_ODP[08] об'єктами призначення>**, використовуються для забезпечення виконання **<AC-04(01)_ODP[09] політик управління інформаційними потоками >** як основи для прийняття рішень щодо управління потоками;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційних потоків; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік атрибутів безпеки та пов'язаних з ними об'єктів інформації, джерела та призначення, що застосовують політику управління інформаційними потоками; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційних потоків].	

AC-04(02)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ДОМЕНИ ОБРОБ-**

	КИ ДАНИХ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(02)_ODP	**визначено політики управління інформаційними потоками, які будуть застосовуватися з використанням захищених доменів обробки;**
	AC-04(02)	захищені домени обробки використовуються для забезпечення дотримання **<AC-04(02)_ODP політики управління інформаційними потоками>** як основи для ухвалення рішень щодо управління потоками.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація системи; архітектура безпеки системи та супутня документація; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку] **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].	

AC-04(03)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ДИНАМІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ ПОТОКОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(03)_ODP	**визначені політики контролю інформаційних потоків, які необхідно впроваджувати;**
	AC-04(03)	Здійснюється динамічне управління потоком інформації на основі **<AC-04(03)_ODP політики управління інформаційними потоками>**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація системи; архітектура безпеки системи та супутня документація; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впро-	

	вадження інформаційного потоку].

AC-04(04)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - УПРАВЛІННЯ ПОТОКОМ ЗАШИФРОВАНОЇ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(04)_ODP[01]	**визначено механізми контролю інформаційних потоків, які унеможливлюють обхід зашифрованої інформації;**
	AC-04(04)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {дешифрування інформації; блокування потоку зашифрованої інформації; завершення сеансів зв'язку що намагаються передавати зашифровану інформацію; <AC-04(04)_ODP[03] визначена організацією процедура або метод>};**
	AC-04(04)_ODP[03]	**визначено організацією процедуру або метод, що використовується для запобігання обходу зашифрованої інформації через механізми контролю інформаційних потоків (якщо вибрано);**
	AC-04(04)	зашифрована інформація не може обійти **<AC-04(04)_ODP[01] механізми контролю потоку інформації>** за допомогою **<AC-04(04)_ODP[02] ОБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].	

AC-04(05)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ВБУДОВУВАННЯ ТИПІВ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(05)_ODP	**визначеного обмеження, які слід застосовувати щодо вбудовування типів даних в інші типи даних;**

	AC-04(05)	**<AC-04(05)_ODP обмеження>** накладаються на вбудовування типів даних у інші типи даних.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік обмежень, які мають бути застосовані щодо вбудовування типів даних в інші типи даних; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що впроваджують політику реалізації інформаційного потоку].	

AC-04(06)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - МЕТАДАНІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(06)_ODP	**визначено метадані, які слід використовувати як засіб управління інформаційним потоком;**
	AC-04(06)	інформаційна система здійснює управління інформаційним потоком на основі **<AC-04(06)_ODP метадані>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; типи метаданих, що застосовуються для забезпечення прийняття рішень щодо управління інформаційним потоком; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику забезпечення впровадження інформаційного потоку].	

AC-04(07)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - МЕХАНІЗМИ ОДНОСТОРОННЬОГО ПОТОКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(07)	односторонні інформаційні потоки забезпечуються за допомогою апаратних механізмів управління потоками.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління інформаційними потоками; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; апаратні механізми системи та пов'язані з ними конфігурації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Апаратні механізми, що реалізують політику застосування інформаційного потоку]

AC-04(08)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ФІЛЬТРИ ПОЛІТИКИ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(08) _ODP[01]	**визначено фільтри політики безпеки, які будуть використовуватися як основа для забезпечення керування інформаційними потоками;**
	AC-04(08) _ODP[02]	**визначено фільтри політики конфіденційності, які будуть використовуватися як основа для забезпечення керування інформаційними потоками;**
	AC-04(08) _ODP[03]	**визначено інформаційні потоки, для яких контроль здійснюється за допомогою фільтрів безпеки;**
	AC-04(08) _ODP[04]	**визначено інформаційні потоки, для яких контроль здійснюється за допомогою фільтрів конфіденційнсоті;**
	AC-04(08) _ODP[05]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<блокування; зміна; карантин};**
	AC-04(08) _ODP[06]	**визначено політику безпеки, яка визначає дії, що мають бути виконані після помилки обробки фільтра;**
	AC-04(08) _ODP[07]	**визначено політику конфіденційності, яка визначає дії, що мають бути виконані після помилки обробки фільтра;**
	AC-04(08)(a)[01]	управління інформаційними потоками здійснюється за допомогою **<AC-04(08) _ODP[01] фільтр політики безпеки>** як основи для прийняття рішень щодо управління потоками для **<AC-04(08) _ODP[03] інформаційних потоків>;**

	AC-04(08)(a)[01]	контроль інформаційних потоків здійснюється за допомогою **<AC-04(08) _ODP[02] фільтр політики конфіденційності>** як основи для прийняття рішень щодо контролю потоків для **<AC-04(08) _ODP[04] інформаційних потоків>;**
	AC-04(08)(b)	**<AC-04(08)_ODP[05] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** дані після помилки обробки фільтра відповідно до **<AC-04(08)_ODP[06] політики безпеки>; <AC-04(08)_ODP[05] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** дані після збою обробки фільтра відповідно до **<AC-04(08)_ODP[07] політики конфіденційності>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік фільтрів політик безпеки, що регулюють рішення щодо управління потоком; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Адміністратори системи / мережі; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].	

AC-04(09)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПЕРЕВІРКИ, ЩО ПРОВОДИТЬ ПЕРСОНАЛ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(09)_ODP[01]	**визначено інформаційні потоки, які потребують використання перевірку персоналом;**
	AC-04(09)_ODP[02]	**визначено умови, за яких використання перевірки персоналом на інформаційні потоки має бути обов'язковим;**
	AC-04(09)	перевірка персоналом використовуються для **<AC-04(09)_ODP[01] інформаційних потоків>** за **<AC-04(09)_ODP[02] умов>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи перевірки людиною щодо інформаційних потоків; перелік умов, що потребують перевірки людиною на інформаційні потоки; записи аудиту системи; інші відповідні документи чи записи].	

	Співбесіда: [ВИБІР: Адміністратори системи / мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за виконання потоку інформації; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що застосовують використання перевірку персоналом].

AC-04(10)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - АКТИВАЦІЯ ТА ДЕАКТИВАЦІЯ ФІЛЬТРІВ ПОЛІТИКИ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(10) _ODP[01]	**визначено фільтри політики безпеки, які привілейовані адміністратори можуть активувати та деактивувати;**
	AC-04(10) _ODP[02]	**визначено фільтри політики конфіденційності, які привілейовані адміністратори можуть активувати та деактивувати;**
	AC-04(10) _ODP[03]	**визначено умови, за яких привілейовані адміністратори можуть активувати та деактивувати фільтри політики безпеки;**
	AC-04(10) _ODP[04]	**визначено умови, за яких привілейовані адміністратори можуть активувати та деактивувати фільтри політики конфіденційності;**
	AC-04(10)[01]	привілейованим адміністраторам надано можливість активувати та деактивувати **<AC-04(10) _ODP[01] фільтри безпеки>** за **<AC-04(10) _ODP[03] умов>;**
	AC-04(10)[02]	привілейованим адміністраторам надано можливість активувати та деактивувати **<AC-04(10) _ODP[02] фільтри конфіденційності>** за **<AC-04(10) _ODP[04] умов>;**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; список фільтрів політик безпеки, увімкнутих та вимкнутих привілейованими адміністраторами; записи аудиту системи; інші відповідні документи чи записи] **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за включення / відключення фільтрів політики безпеки; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].	

AC-04(11)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - КОНФІГУРАЦІЯ ФІЛЬТРІВ ПОЛІТИКИ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: **Визначити, чи:**	
	AC-04(11)_ODP[01]	**визначено фільтри політики безпеки, які привілейовані адміністратори можуть налаштовувати для підтримки різних політик безпеки та конфіденційності;**
	AC-04(11)_ODP[02]	**визначено фільтри політики конфіденційності, які привілейовані адміністратори можуть налаштовувати для підтримки різних політик безпеки та конфіденційності;**
	AC-04(11)[01]	привілейованим адміністраторам надано можливість налаштовувати **<AC-04(11)_ODP[01] фільтри політики безпеки>** для підтримки різних політик безпеки або конфіденційності;
	AC-04(11)[02]	привілейованим адміністраторам надано можливість налаштовувати **<AC-04(11)_ODP[02] фільтри політики конфіденційності>** для підтримки різних політик безпеки або конфіденційності;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік фільтрів політик безпеки; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за налаштування фільтрів політики безпеки; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].	

AC-04(12)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ІДЕНТИФІКАТОРИ ТИПУ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(12)_ODP	**визначено ідентифікатори типів даних, які будуть використовуватися для перевірки даних, необхідних для ухвалення рішень щодо інформаційних потоків;**

	AC-04(12)	при передачі інформації між різними доменами безпеки, **<AC-04(12)_ODP ідентифікатори типів даних>** використовуються для перевірки даних, необхідних для ухвалення рішень щодо інформаційних потоків.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік ідентифікаторів типу даних; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Адміністратори системи / мережі; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].	

AC-04(13)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ДЕКОМПОЗИЦІЯ НА ВІДПОВІДНІ ПОЛІТИЦІ СУБКОМПОНЕНТИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(13)_ODP	**визначено субкомпоненти політики, на які слід розкласти інформацію для подання до механізмів реалізації політики;**
	AC-04(13)	при передачі інформації між різними доменами безпеки інформація розкладається на **<AC-04(13)_ODP субкомпоненти політики>** для подання механізмам забезпечення дотримання політики.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Адміністратори системи / мережі; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].	

AC-04(14)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ОБМЕЖЕННЯ ФІЛЬТРА ПОЛІТИКИ БЕЗПЕКИ**
	МЕТА ОЦІНКИ: Визначити, чи:

	AC-04(14)_ODP[01]	**визначено фільтри політики безпеки, які вимагають повного переліку форматів, що обмежують структуру та зміст даних;**
	AC-04(14)_ODP[02]	**визначено фільтри політики конфіденційності, які вимагають повного переліку форматів, що обмежують структуру та зміст даних;**
	AC-04(14)[01]	при передачі інформації між різними захищеними доменами, реалізовані **<AC-04(14)_ODP[01] фільтри політики безпеки>** вимагають повністю перелічених форматів, які обмежують структуру та вміст даних;
	AC-04(14)[02]	при передачі інформації між різними захищеними доменами, реалізовані **<AC-04(14)_ODP[01] фільтри політики конфіденційності>** вимагають повністю перелічених форматів, які обмежують структуру та вміст даних;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік фільтрів політик безпеки; перелік фільтрів політики щодо вмісту даних; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Адміністратори системи / мережі; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].	

AC-04(15)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОЇ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(15)_ODP[01]	**визначено несанкціоновану інформацію, яку потрібно виявляти;**
	AC-04(15)_ODP[02]	**визначено політику безпеки, яка вимагає заборонити передачу несанкціонованої інформації між різними доменами безпеки (якщо вибрано);**
	AC-04(15)_ODP[03]	**визначено політику конфіденційності, яка вимагає заборонити передачу визначеної організацією несанкціонованої інформації між різними доменами безпеки (якщо вибрано);**
	AC-04(15)[01]	при передачі інформації між різними доменами безпеки інформація перевіряється на наявність **<AC-**

		04(15)_ODP[01] несанкціонованої інформації>;
	AC-04(15)[02]	при передачі інформації між різними доменами безпеки забороняється передача **<AC-04(15)_ODP[01] несанкціонованої інформації>** відповідно до **<AC-04(15)_ODP[02] політики безпеки>**;
	AC-04(15)[03]	при передачі інформації між різними доменами безпеки забороняється передача **<AC-04(15)_ODP[01] несанкціонованої інформації>** відповідно до **<AC-04(15)_ODP[02] політики конфіденційності>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік несанкціонованих типів інформації та пов'язаної з ними інформації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].	

AC-04(16)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПЕРЕДАЧА ІНФОРМАЦІЇ ПРО ВЗАЄМОПОВ'ЯЗАНІ СИСТЕМИ**
	[Вилучено: Включено в AC-04]

AC-04(17)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - АВТЕНТИФІКАЦІЯ ДОМЕНУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(17)_ODP	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {організація, система, програми, служби, індивід};**
	AC-04(17)	для передачі інформації пункти відправлення та призначення унікально ідентифікуються та аутентифікуються за допомогою <**AC-04(17)_ODP ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік несанкціонованих типів інформації та пов'язаної з ними інформа-	

	ції; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику впровадження інформаційного потоку].

AC-04(18)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПРИВ'ЯЗКА АТРИБУТУ БЕЗПЕКИ**
	[Вилучено: Включено в AC-16]

AC-04(19)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПЕРЕВІРКА МЕТАДАНИХ**	
	МЕТА ОЦІНКИ: Визначте, чи	
	AC-04(19)_ODP[01]	**визначено фільтри політики безпеки, які буде застосовано до метаданих (якщо вибрано);**
	AC-04(19)_ODP[02]	**визначено фільтри політики конфіденційності, які буде застосовано до метаданих (якщо вибрано);**
	AC-04(19)[01]	при передачі інформації між різними доменами безпеки, **<AC-04(19)_ODP[01] фільтри політики безпеки>** реалізовано на метаданих;
	AC-04(19)[02]	при передачі інформації між різними доменами безпеки, **<AC-04(19)_ODP[02] фільтри політики конфіденційності>** реалізовано на метаданих.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика посилення інформаційного потоку; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік критеріїв фільтрації політик безпеки, застосованих до метаданих та корисних навантажень даних; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за виконання потоку інформації; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення інформаційного потоку].	

AC-04(20)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ЗАТВЕРДЖЕНІ РІШЕННЯ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(20)_ODP[01]	**визначені рішення про схвалені конфігурації для керування потоками інформації через захищені домени;**
	AC-04(20)_ODP[02]	**визначено інформацію, якою потрібно керувати, коли вона проходить через захищені домени;**
	AC-04(20)	**<AC-04(20)_ODP[01] рішення>** використовуються для контролю потоку **<AC-04(20)_ODP[02] інформації>** між захищеними доменами.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика посилення інформаційного потоку; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік рішень у затверджених конфігураціях; затверджені базові лінії конфігурації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за виконання потоку інформації; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення функціонування потоку інформації].	

AC-04(21)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ФІЗИЧНЕ ТА ЛОГІЧНЕ ВІДДІЛЕННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(21)_ODP[01]	**визначено механізми та/або методи, що використовуються для логічного розділення інформаційних потоків (якщо вибрано);**
	AC-04(21)_ODP[02]	**визначено механізми та/або методи, що використовуються для фізичного розділення інформаційних потоків (якщо вибрано);**
	AC-04(21)_ODP[03]	**визначено необхідні поділи за типами інформації;**
	AC-04(21)[01]	інформаційні потоки логічно розділені за допомогою **<AC-04(21)_ODP[01] механізмів та/або методів>** для виконання **<AC-04(21)_ODP[03] необхідних розділень>;**
	AC-04(21)[02]	інформаційні потоки фізично розділені за допомогою **<AC-04(21)_ODP[02] механізмів та/або методів>** для

		виконання **<AC-04(21)_ODP[03] необхідних розділень>;**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика посилення інформаційного потоку; політики управління потоками інформації; процедури щодо посилення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік необхідного поділу інформаційних потоків за типами інформації; перелік механізмів та / або заходів, використовуваних для логічного або фізичного поділу інформаційних потоків; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації відповідальний за забезпечення потоку інформації; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення функціонування потоку інформації]	

AC-04(22)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ЄДИНИЙ ДОСТУП**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(22)	доступ забезпечується з одного пристрою до обчислювальних платформ, застосунків або даних, що розташовуються в декількох різних захищених доменах, одночасно запобігаючи передачі інформації між різними захищеними доменами.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури розв'язання питань розподілу відповідальності та розподілу обов'язків; налаштування конфігурації системи та супутня документація; перелік підрозділів відповідальності та розподілу обов'язків; авторизація доступу до системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення відповідних підрозділів та розподілу обов'язків; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику розділення обов'язків]	

AC-04(23)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - МОДИФІКОВАНА ІНФОРМАЦІЯ, ЯКА НЕ ПІДЛЯГАЄ ОПРИЛЮДНЕННЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(23)_ODP	**визначено дію модифікації, що застосовується до інформації, яка не підлягає оприлюдненню;**

	AC-04(23)	при передачі інформації між доменами безпеки інформація, що не підлягає оприлюдненню, модифікується шляхом реалізації **<AC-04(23)_ODP дія модифікації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту інформаційних потоків; процедури, що стосуються захисту інформаційних потоків; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформаці; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за забезпечення інформаційних потоків; системні/мережеві адміністратори; окремі співробітники організації з відповідальністю за безпеку інформацію]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції захисту інформаційних потоків]	

AC-04(24)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ВНУТРІШНІЙ НОРМАЛІЗОВАНИЙ ФОРМАТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(24)[1]	при передачі інформації між різними доменами безпеки вхідні дані розбираються у внутрішній, нормалізований формат**;**
	AC-04(24)[2]	при передачі інформації між різними доменами безпеки дані регенеруються, щоб відповідати їхній специфікації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту інформаційних потоків; процедури, що стосуються захисту інформаційних потоків; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформаці; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за забезпечення інформаційних потоків; системні/мережеві адміністратори; окремі співробітники організації з відповідальністю за безпеку інформацію]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції захисту інформаційних потоків]	

AC-04(25)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ОЧИЩЕННЯ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(25)_ODP[01]	вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {доставка шкідливого коду, керування

		та контроль шкідливого коду, доповнення шкідливого коду та даних, закодованих стеганографією; витік конфіденційної інформації};
	AC-04(25)_ODP[02]	визначено політику очищення даних;
	AC-04(25)	при передачі інформації між різними доменами безпеки, дані очищаються для мінімізації **<AC-04(25)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** відповідно до <**AC-04(25)_ODP[02] політики**>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту інформаційних потоків; процедури, що стосуються захисту інформаційних потоків; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформаці; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за забезпечення інформаційних потоків; системні/мережеві адміністратори; окремі співробітники організації з відповідальністю за безпеку інформацію]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції захисту інформаційних потоків]	

AC-04(26)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ДІЇ З ФІЛЬТРАЦІЇ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(26)[01]	при передачі інформації між різними доменами безпеки дії з фільтрації вмісту фіксуються і перевіряються;
	AC-04(26)[02]	при передачі інформації між різними доменами безпеки, результати для інформації, що фільтрується, записуються і перевіряються.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту інформаційних потоків; процедури, що стосуються захисту інформаційних потоків; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформаці; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за забезпечення інформаційних потоків; системні/мережеві адміністратори; окремі співробітники організації з відповідальністю за безпеку інформацію]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції захисту інформаційних потоків, механізми, що реалізують фільтрацію контенту; механізми запису та аудиту фільтрації контенту]	

AC-04(27)	УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - НАДЛИШКОВІ/НЕЗАЛЕЖНІ ФІЛЬТРУЮЧІ МЕХАНІЗМИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(27)	під час передачі інформації між системами безпеки впроваджені рішення для фільтрації контенту забезпечують надлишкові та незалежні механізми фільтрації для кожного типу даних.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту інформаційних потоків; процедури, що стосуються захисту інформаційних потоків; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформаці; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за забезпечення інформаційних потоків; системні/мережеві адміністратори; окремі співробітники організації з відповідальністю за безпеку інформацію]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції захисту інформаційних потоків]	

AC-04(28)	УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ЛІНІЙНІ ФІЛЬТРУВАЛЬНІ КАНАЛИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(28)	при передачі інформації між доменами безпеки реалізовано лінійний конвеєр фільтрації контенту, який забезпечується дискретними та обов'язковими засобами контролю доступу
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту інформаційних потоків; процедури, що стосуються захисту інформаційних потоків; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформаці; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за забезпечення інформаційних потоків; системні/мережеві адміністратори; окремі співробітники організації з відповідальністю за безпеку інформацію]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції захисту інформаційних потоків, механізми, що реалізують лінійні фільтри вмісту]	

AC-04(29)	УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ФІЛЬТР МЕХАНІЗМІВ ОРКЕСТРОВКИ
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	AC-04(29)_ODP	**визначено політику щодо дій з фільтрації контенту;**
	AC-04(29)(a)	при передачі інформації між доменами безпеки використовуються механізми оркестрування фільтрації контенту, які гарантують, що механізми фільтрації контенту успішно завершать виконання без помилок;
	AC-04(29)(b)[01]	при передачі інформації між доменами безпеки використовуються механізми оркестрування фільтрації контенту, які гарантують, що дії з фільтрації контенту відбуваються в правильному порядку;
	AC-04(29)(b)[02]	при передачі інформації між доменами безпеки використовуються механізми оркестрування фільтрації контенту, які гарантують, що дії з фільтрації контенту відповідають **<AC-04(29)_ODP політиці>**. .
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту інформаційних потоків; процедури, що стосуються захисту інформаційних потоків; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформаці; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за забезпечення інформаційних потоків; системні/мережеві адміністратори; окремі співробітники організації з відповідальністю за безпеку інформацію]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції захисту інформаційних потоків, механізми, що реалізують механізми оркестрування контент-фільтрів]	

AC-04(30)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - МЕХАНІЗМИ ФІЛЬТРАЦІЇ З ВИКОРИСТАННЯМ КІЛЬКОХ ПРОЦЕСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(30)	при передачі інформації між доменами безпеки реалізовані механізми контент-фільтрації з використанням декількох процесів.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту інформаційних потоків; процедури, що стосуються захисту інформаційних потоків; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформаці; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за забезпечення інформаційних потоків; системні/мережеві адміністратори; окремі співробітники організації з відповідальністю за безпеку інформацію]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції захисту інформаційних потоків; механізми, що реалізують фільтрацію контенту]

AC-04(31)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ЗАПОБІГАННЯ СПРОБАМ ПЕРЕДАЧІ ВМІСТУ, ЯКИЙ НЕ ПРОЙШОВ ПЕРЕВІРКУ ФІЛЬТРАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(31)	при передачі інформації між різними доменами безпеки запобігається передача вмісту який не пройшов фільрацію.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту інформаційних потоків; процедури, що стосуються захисту інформаційних потоків; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформаці; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за забезпечення інформаційних потоків; системні/мережеві адміністратори; окремі співробітники організації з відповідальністю за безпеку інформацію]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції захисту інформаційних потоків;]	

AC-04(32)	**УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ВИМОГИ ДО ПРОЦЕСУ ПЕРЕДАЧІ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-04(32)[a]	при передачі інформації між різними доменами безпеки процес, який передає інформацію між конвеєрами фільрації, не фільтрує вміст повідомлень;
	AC-04(32)[b]	при передачі інформації між різними доменами безпеки процес, який передає інформацію між конвеєрами фільрації, перевіряє метадані фільтрації;

	AC-04(32)[c]	при передачі інформації між різними доменами безпеки процес, який передає інформацію між конвеєрами фільрації, гарантує, що вміст з метаданими фільтрації успішно пройшов фільтрацію;
	AC-04(32)[d]	при передачі інформації між різними доменами безпеки процес, який передає інформацію між конвеєрами фільрації, передає вміст до цільового конвеєра фільтрів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту інформаційних потоків; процедури, що стосуються захисту інформаційних потоків; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформаці; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за забезпечення інформаційних потоків; системні/мережеві адміністратори; окремі співробітники організації з відповідальністю за безпеку інформацію]. **Перевірка:** [ВИБІР: Механізми, що реалізують функції захисту інформаційних потоків; механізми, що реалізують фільтрацію контенту;]	

AC-05	**РОЗМЕЖУВАННЯ ОБОВ'ЯЗКІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-05_ODP	**визначено обов'язки осіб, які потребують розмежування;**
	AC-05[a]	**<AC-05_ODP обов'язки осіб>** визначені та задокументовані;
	AC-05[b]	визначено права авторизації доступу до системи для підтримки розмежування обов'язків.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури розв'язання питань розподілу відповідальності та розмежування обов'язків; налаштування конфігурації системи та супутня документація; перелік розподілу відповідальності та обов'язків; авторизація доступу до системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення відповідних підрозділів відповідальності та розподілу обов'язків; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику розподілу обов'язків].	

AC-06	МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ	
	МЕТА ОЦІНКИ: Визначте, чи	
	AC-06	застосовується принцип мінімалізації повноважень, який дозволяє користувачам (або процесам, що діють від імені користувачів) здійснювати лише такі авторизовані звернення, які необхідні для виконання поставлених завдань організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; перелік призначених дозволів доступу (привілеїв користувача); налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення мінімізація повноважень, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують мінімізацію повноважень].	

AC-06(01)	МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - АВТОРИЗОВАНИЙ ДОСТУП ДО ФУНКЦІЙ БЕЗПЕКИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-06(01)_ODP[01]	**визначені особи або ролі з авторизованим доступом до функцій безпеки та інформації, що має відношення до безпеки;**
	AC-06(01)_ODP[02]	**визначені функції безпеки (розгорнуті в апаратному забезпеченні) для авторизованого доступу;**
	AC-06(01)_ODP[03]	**визначені функції безпеки (розгорнуті в програмному забезпеченні) для авторизованого доступу;**
	AC-06(01)_ODP[04]	**визначені функції безпеки (розгорнуті в мікропрограмному забезпеченні) для авторизованого доступу;**
	AC-06(01)_ODP[05]	**визначено інформацію, важливу для забезпечення безпеки, для авторизованого доступу;**
	AC-06(01)(a)[01]	авторизовано доступ для **<AC-06(01)_ODP[01] осіб та ролей>** до **<AC-06(01)_ODP[02] функцій безпеки (розгорнуті на апаратному забезпеченні)>**;
	AC-06(01)(a)[02]	авторизовано доступ для **<AC-06(01)_ODP[01] осіб та ролей>** до **<AC-06(01)_ODP[03] функцій безпеки (роз-**

		горнуті на програмному забезпеченні)>;
	AC-06(01)(a)[03]	авторизовано доступ для **<AC-06(01)_ODP[01] осіб та ролей>** до **<AC-06(01)_ODP[04] функцій безпеки (розгорнуті на мікропрограмному забезпеченні)>**;
	AC-06(01)(b)	авторизовано доступ для **<AC-06(01)_ODP[01] осіб та ролей>** до <AC-06(01)_ODP[05] інформації>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; перелік функцій безпеки (розгорнутих в апаратному, програмному та мікропрограмному забезпеченні) та інформації, що стосується безпеки, доступ до якої має бути недвозначно авторизований; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень].	

AC-06(02)	**МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - НЕПРИВІЛЕЙОВАНИЙ ДОСТУП ДО НЕЗАХИЩЕНИХ ФУНКЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-06(02)_ODP	**визначені функції безпеки або інформація, що стосується безпеки**
	AC-06(02)	користувачі облікових записів (або ролей) системи з доступом до **<AC-06(02)_ODP функцій безпеки або інформації, що стосується безпеки>**, повинні використовувати непривілейовані облікові записи або ролі під час доступу до незахищених функцій
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; перелік функцій безпеки, що генеруються системою, або інформації про підвищену безпеку, призначеної для облікових записів або ролей системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення найменших пільг, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори].	

	Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень].

AC-06(03)	**МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - МЕРЕЖЕВИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ КОМАНД**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-06(03)_ODP[01]	**визначено привілейовані команди**
	AC-06(03)_ODP[02]	**визначено невідкладні операційні потреби, що вимагають мережевого доступу до привілейованих команд;**
	AC-06(03)[01]	мережевий доступ до **<AC-06(03)_ODP[01] привілейованих команд>** авторизовано лише для **<AC-06(03)_ODP[02] нагальних оперативних потреб>**;
	AC-06(03)[02]	обґрунтування авторизації мережевого доступу до привілейованих команд задокументовано в плані захисту інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; план захисту інформації; налаштування конфігурації системи та супутня документація; записи аудиту системи; перелік операційних потреб для авторизації доступу до мережі до привілейованих команд; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень].	

AC-06(04)	**МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - РОЗДІЛЬНІ ДОМЕНИ ОБРОБКИ**	
	МЕТА ОЦІНКИ: Визначте, чи	
	AC-06(04)	надаються окремі домени обробки для більш тонкого розподілу повноважень користувачів
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень].

AC-06(05)	**МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ПРИВІЛЕЙОВАНІ ОБЛІКОВІ ЗАПИСИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-06(05)_ODP	**визначено персонал або ролі, яким мають бути обмежені привілейовані облікові записи в системі;**
	AC-06(05)	привілейовані облікові записи в системі обмежено **<AC-06(05)_ODP персонал або ролі>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; перелік визначених привілейованих облікових записів системи; перелі адміністраторів системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень].	

AC-06(06)	**МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ПРИВІЛЕЙОВАНИЙ ДОСТУП КОРИСТУВАЧАМИ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-06(06)	привілейований доступ до системи для користувачів, які не є членами організації, заборонено.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; список привілейованих облікових записів системи; перелік користувачів, які не є членами організації; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення міні-	

	мізації повноважень, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що забороняють привілейований доступ до інформаційної системи].

AC-06(07)	**МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ПЕРЕГЛЯД ПОВНОВАЖЕНЬ КОРИСТУВАЧА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-06(07)_ODP[01]	**визначено частоту перегляду повноважень, призначених ролям або класам користувачів;**
	AC-06(07)_ODP[02]	**визначено ролі або класи користувачів, яким призначено повноваження ;**
	AC-06(07)(a)	повноваження, призначені <**AC-06(07)_ODP[02] ролям і класам**>, переглядаються з <**AC-06(07)_ODP[01] частотою**> для перевірки необхідності таких повноважень;
	AC-06(07)(b)	привілеї перепризначаються або знімаються, якщо це необхідно, для правильного відображення місії організації та потреб.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; список ролей або класів користувачів та призначених привілеїв системи; проєктна документація системи; налаштування конфігурації системи та супутня документація; перевірка відповідності повноважень, призначених ролям, класів або користувачам; записи про видалення або перепризначення повноважень для ролей або класів користувачів; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перегляд мінімізації повноважень, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують перегляд прав користувачів].	

AC-06(08)	**МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - РІВНІ ПРИВІЛЕЇВ ДЛЯ ВИКОНАННЯ КОДУ**
	МЕТА ОЦІНКИ: Визначити, чи:

	AC-06(08)_ODP	**визначено програмне забезпечення, яке не повинно виконуватися з вищими рівнями привілеїв, ніж у користувачів, які виконують це програмне забезпечення;**
	AC-06(08)	**<AC-06(08)_ODP програмне забезпечення>** заборонено виконувати з вищими рівнями привілеїв, ніж у користувачів, які виконують це програмне забезпечення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; перелік програмного забезпечення, яке не повинно виконуватись на вищих рівнях привілеїв, ніж мають користувачі, що виконують програмне забезпечення; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень для виконання програмного забезпечення].	

AC-06(09)	**МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - АУДИТ ВИКОРИСТАННЯ ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ**
	МЕТА ОЦІНКИ: Визначити, чи: **AC-06(09)** проводиться аудит виконання привілейованих функцій **ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:** **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік функцій, що підлягають аудиту; перелік подій, що підлягають аудиту; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перегляд мінімізації повноважень, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми аудиту виконання функцій мінімізації повноважень].

AC-06(10)	**МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ЗАБОРОНА НЕПРИВІЛЕЙОВАНИМ КОРИСТУВАЧАМ ВИКОНУВАТИ ПРИВІЛЕЙОВАНІ ФУНКЦІЇ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-06(10)	непривілейовані користувачі не можуть виконувати привілейовані функції.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються мінімізації повноважень; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік привілейованих функцій та пов'язаних з ними привілейованих облікових записів системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення мінімізації повноважень, необхідних для виконання визначених завдань; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції мінімізації повноважень для непривілейованих користувачів].	

AC-07	**НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-07_ODP[01]	**визначається кількість послідовних неуспішних спроб входу користувача, дозволених протягом певного періоду часу;**
	AC-07_ODP[02]	**визначено період часу, яким обмежується кількість послідовних неуспішних спроб входу користувача;**
	AC-07_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {заблокувати обліковий запис або вузол на <AC-07_ODP[04] період часу>; заблокувати обліковий запис або вузол до зняття адміністратором; затримати наступний запит на вхід за <AC-07_ODP[05] алгоритмом затримки>; повідомити системного адміністратора; виконати іншу <AC-07_ODP[06] дію>};**
	AC-07_ODP[04]	**період часу, на який буде заблоковано обліковий запис або вузол (якщо вибрано);**
	AC-07_ODP[05]	**визначено алгоритм затримки наступного запиту на вхід (якщо вибрано);**
	AC-07_ODP[06]	**інша дія, яка буде виконана після перевищення максимальної кількості невдалих спроб (якщо вибрано);**
	AC-07(a)	застосовано обмеження на **<AC-07_ODP[01] кількість>** послідовних неуспішних спроб входу користувача протягом

		<AC-07_ODP[02] періоду часу>;
	AC-07(b)	автоматично **<AC-07_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**, коли перевищено максимальну кількість невдалих спроб.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури вирішення невдалих спроб входу; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за безпеку інформації; розробники системи; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для невдалих спроб входу].	

AC-07(01)	**НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - АВТОМАТИЧНЕ БЛОКУВАННЯ ОБЛІКОВОГО ЗАПИСУ**
	[Вилучено: Включено в AC-07]

AC-07(02)	**НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - ОЧИЩЕННЯ АБО СТИРАННЯ МОБІЛЬНОГО ПРИСТРОЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-07(02)_ODP[01]	**визначено мобільні пристрої, які підлягають очищенню або стиранню інформації;**
	AC-07(02)_ODP[02]	**визначено вимоги та методи очищення чи стирання інформації з мобільних пристроїв**
	AC-07(02)_ODP[03]	**визначається кількість послідовних невдалих спроб входу в систему до того, як інформація буде очищена або стерта з мобільних пристроїв;**
	AC-07(02)	інформація очищується або стирається з **<AC-07(02)_ODP[01] мобільних пристроїв>** на основі **<AC-07(02)_ODP[02] вимог або методів очищення або стирання>** після **<AC-07(02)_ODP[03 кількість>** послідовних, невдалих спроб входу на пристрій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури вирішення невдалих спроб входу на мобільні пристрої; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік мобільних пристроїв, які потрібно очистити або стерти після визначених організацією послідовних,	

	невдалих спроб входу для пристрою; перелік вимог чи методів очищення або стирання мобільних пристроїв; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для невдалих спроб входу пристрою].

AC-07(03)	**НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - ОБМЕЖЕННЯ НА СПРОБИ БІОМЕТРИЧНОГО ВХОДУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-07(03)_ODP	**визначено кількість невдалих спроб входу за допомогою біометрики**
	AC-07(03)	обмежно **<AC-07(03)_ODP кількість>** невдалих спроб входу за допомогою біометрики.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури вирішення невдалих спроб входу за допомогою біометрики; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для невдалих спроб входу за допомогою біометрики].	

AC-07(04)	**НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - ВИКОРИСТАННЯ АЛЬТЕРНАТИВНОГО ФАКТОРА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-07(04)_ODP[01]	**визначено фактори автентифікації, які дозволено використовувати, але які відрізняються від основних факторів автентифікації;**
	AC-07(04)_ODP[02]	**визначено кількість послідовних, недійсних спроб входу через використання альтернативних факторів;**
	AC-07(04)_ODP[03]	**визначено період часу, протягом якого користувач може спробувати увійти через альтернативні фактори;**
	AC-07(04)(a)	**<AC-07(04)_ODP[01] фактори автентифікації>**, які відрізняються від основних факторів автентифікації, дозволяється використовувати після перевищення кількості визначених організацією послідовних невдалих спроб входу;

	AC-07(04)(b)	введено обмеження на **<AC-07(04)_ODP[02]>** послідовних невдализ спроб входу через використання користувачем альтернативних факторів протягом **<AC-07(04)_ODP[03] періоду часу>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для невдалих спроб входу].	

AC-08	**ПОПЕРЕДЖЕННЯ ПРО ВИКОРИСТАННЯ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-08_ODP[01]	**визначається сповіщення або банер про використання системи, який система буде показувати користувачам перед наданням доступу до системи;**
	AC-08_ODP[02]	визначено умови використання системи, які система відображатиме перед наданням подальшого доступу;
	AC-08(a)	**<AC-08_ODP[01] повідомлення про використання системи>** відображається користувачам перед наданням доступу до системи, яке містить повідомлення про конфіденційність і безпеку, що відповідають чинним законам, нормативним документам, наказам, директивам, політикам, правилам, стандартам і керівним принципам;
	AC-08(a)[01]	у повідомленні про використання системи зазначено, що користувачі отримують доступ до урядової системи;
	AC-08(a)[02]	у повідомленні про використання системи зазначено, що використання системи може контролюватися, реєструватися та підлягати аудиту;
	AC-08(a)[03]	у повідомленні про використання системи зазначено, що несанкціоноване використання системи заборонено і тягне за собою кримінальну та цивільну відповідальність;
	AC-08(a)[04]	у повідомленні про використання системи зазначено, що використання системи означає згоду на моніторинг і запис дій;
	AC-08(b)	сповіщення або банер залишається на екрані до тих пір, поки користувачі не визнають умови використання та не приймуть явні дії для входу в систему або подальшого доступу до неї;
	AC-08(c)[01]	для загальнодоступних систем інформація про використання системи **<AC-08_ODP[02] умови>** відображається перед наданням подальшого доступу до загальнодоступної системи;
	AC-08(c)[02]	для загальнодоступних систем відображаються будь-які посилання на моніторинг, запис або аудит, які узгоджуються з положеннями про конфіденційність таких систем, що зазвичай забороняють ці

		види діяльності;
	AC-08(c)[03]	для загальнодоступних систем додається опис авторизованого використання системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політики конфіденційності та безпеки, процедури щодо сповіщення про використання системи; підтвердження про використання систем сповіщеннями або банерами; записи аудиту системи; підтвердження користувачем отримання сповіщення або банера; проєктна документація системи; налаштування конфігурації системи та супутня документація; використання системами повідомлень про сповіщення; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за надання юридичних консультацій; розробники системи] **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують сповіщення про використання системи].	

AC-09	**СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП)**	
	МЕТА ОЦІНКИ: Визначте, чи	
	AC-09	система повідомляє користувача при успішному вході (доступі) до системи про дату та час останнього входу (доступу).
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо попереднього повідомлення про вхід; проєктна документація системи; налаштування конфігурації системи та супутня документація; повідомлення про використання системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для повідомлення про попередній вхід до системи].	

AC-09(01)	**СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) - НЕВДАЛІ СПРОБИ ВХОДУ ДО СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначте, чи	
	AC-09(01)	система сповіщає користувача після успішного входу / доступу про кількість невдалих спроб входу / доступу з моменту останнього успішного входу / доступу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо попере-	

	нього повідомлення про вхід; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для попереднього повідомлення про вхід].

AC-09(02)	**СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) - УСПІШНІ ТА НЕВДАЛІ СПРОБИ ВХОДУ ДО СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-09(02)_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {успішних спроб доступу/входу; невдалих спроб входу/доступу; обидва варіанти};**
	AC-09(02)_ODP[02]	**визначається період часу, протягом якого система повідомляє користувача про кількість успішних спроб входу в систему, невдалих спроб входу або про обидва випадки;**
	AC-09(02)	після успішного входу в систему користувач отримує повідомлення про кількість **<AC-09(02)_ODP[01] ЗНАЧЕННЯ ВИБРАНОГО ПАРАМЕТРА>** протягом **<AC-09(02)_ODP[02] періоду часу>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо повідомлення про попередній вхід; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для повідомлення про попередній вхід].	

AC-09(03)	**СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) - ПОВІДОМЛЕННЯ ПРО ЗМІНИ В ОБЛІКОВОМУ ЗАПИСІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-09(03)_ODP[01]	**визначено зміни характеристик або параметрів, пов'язаних із безпекою облікового запису користувача, які потребують сповіщення;**

	AC-09(03)_ODP[02]	**визначено період часу, протягом якого система повідомляє користувача про зміни характеристик або параметрів, пов'язаних із безпекою облікового запису користувача;**
	AC-09(03)	після успішного входу користувач отримує повідомлення про зміни **<AC-09(03)_ODP[01] характеристик або параметрів, пов'язаних із безпекою>** протягом **<AC-09(03)_ODP[02] періоду часу>**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо попереднього повідомлення про вхід; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для повідомлення про попередній вхід].	

AC-09(04)	**СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) – ДОДАТКОВА ІНФОРМАЦІЯ ПРО ВХІД**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-09(04)_ODP	**визначено додаткову інформацію, про яку слід повідомити користувача;**
	AC-09(04)	після успішного входу користувач отримує повідомлення **<AC-09(04)_ODP додаткова інформація>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо попереднього повідомлення про вхід; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для повідомлення про попередній вхід].	

AC-10	**УПРАВЛІННЯ ПАРАЛЕЛЬНОЮ СЕСІЄЮ**
	МЕТА ОЦІНКИ: Визначити, чи:

	AC-10_ODP[01]	**визначено облікові записи та/або типи облікових записів, для яких є обмеження кількості одночасних сеансів;**
	AC-10_ODP[02]	**визначено кількість одночасних сеансів, дозволених для кожного облікового запису та/або типу облікового запису;**
	AC-10	кількість одночасних сеансів для кожного **<AC-10_ODP[01] облікового запису та/або типів облікових записів>** обмежена **<AC-10_ODP[02] кількість>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються паралельного контролю сеансу; проєктна документація системи; налаштування конфігурації системи та супутня документація; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику контролю доступу для паралельного контролю сеансу].	

AC-11	**БЛОКУВАННЯ ПРИСТРОЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-11_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {ініціювання блокування пристрою після <AC-11_ODP[02] періоду неактивності>; вимога до користувача ініціювати блокування пристрою перед тим, як залишити систему без нагляду};**
	AC-11_ODP[02]	**часовий проміжок бездіяльності, після якого ініціюється блокування пристрою (якщо вибрано);**
	AC-11(a)	подальший доступ до системи заборонено за допомогою **<AC-11_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**;
	AC-11(b)	блокування пристрою зберігається доти, доки користувач не відновить доступ за допомогою встановлених процедур ідентифікації та автентифікації**.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо блокування сеансу; процедури щодо ідентифікації та автентифікації; проєктна документація системи; налаштування конфігурації системи та супутня документація; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують політику контролю	

	доступу для блокування сеансу].

AC-11(01)	БЛОКУВАННЯ ПРИСТРОЮ - ПРИХОВАНІ ДИСПЛЕЇ	
	МЕТА ОЦІНКИ: Визначте, чи	
	AC-11(01)	система приховує (через блокування сеансу) інформацію, попередньо видиму на дисплеї, загальнодоступним зображенням.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо блокування сеансу; екран дисплея з активованим блокуванням сеансу; проектна документація системи; налаштування конфігурації системи та супутня документація; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Механізми блокування сеансу системи]	

AC-12	ПРИПИНЕННЯ СЕАНСУ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-12_ODP	**визначено умови або події, що вимагають припинення сеансу;**
	AC-12	сеанс користувача автоматично завершується після виконання **<AC-12_ODP умов або подій>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються припинення сеансу; проектна документація системи; налаштування конфігурації системи та супутня документація; перелік умов або подій, які вимагають відключення сеансу; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують припинення сеансу користувача].	

AC-12(01)	ПРИПИНЕННЯ СЕАНСУ - ІНІЦІЙОВАНЕ КОРИСТУВАЧЕМ БЛОКУВАННЯ
	МЕТА ОЦІНКИ: Визначити, чи:

	AC-12(01)_ODP	**визначено інформаційні ресурси, для яких необхідна можливість припинення сеансів зв'язку за ініціативою користувача;**
	AC-12(01)	для сеансів зв'язку, ініційованих користувачем, передбачено можливість виходу з системи щоразу, коли автентифікація використовується для отримання доступу до **<AC-12(01)_ODP інформаційних ресурсів>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються припинення сеансу; повідомлення виходу користувача; проектна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Механізми блокування сеансу системи].	

AC-12(02)	**ПРИПИНЕННЯ СЕАНСУ - ПОВІДОМЛЕННЯ ПРО ПРИПИНЕННЯ СЕАНСУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-12(02)	користувачам буде показано явне повідомлення про завершення сеансу автентифікованого зв'язку.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються припинення сеансу; повідомлення виходу користувача; проектна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Механізми блокування сеансу системи].	

AC-12(03)	**ПРИПИНЕННЯ СЕАНСУ - ЗАСТЕРЕЖНЕ ПОВІДОМЛЕННЯ ПРО ТЕ, ЩО ЧАС СЕСІЇ ДОБІГАЄ КІНЦЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-12(03)_ODP	**визначено час до кінця сесії для відображення користувачам;**
	AC-12(03)	виводиться явне повідомлення користувачам про те, що сеанс завершиться у **<AC-12(03)_ODP час>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються	

	припинення сеансу; повідомлення виходу користувача; проектна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Механізми блокування сеансу системи].

AC-13	**НАГЛЯД ТА ОГЛЯД - УПРАВЛІННЯ ДОСТУПОМ**
	[Вилучено: включено в AC-02 та AU-06].

AC-14	**ДОЗВОЛЕНІ ДІЇ БЕЗ ІДЕНТИФІКАЦІЇ АБО АВТЕНТИФІКАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-14_ODP	**визначено дії користувача, які можуть бути виконані в системі без ідентифікації або автентифікації;**
	AC-14(a)	визначено <**AC-14_ODP дії користувача>**, які можуть бути виконані в системі без ідентифікації або автентифікації, що відповідають місії та функціям організації;
	AC-14(b)[01]	дії користувачів, які не потребують ідентифікації або автентифікації, задокументовані в плані захисту інформації;
	AC-14(a)[02]	обґрунтування дій користувачів, які не потребують ідентифікації або автентифікації, надається в плані захисту інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури вирішення дозволених дій без ідентифікації чи автентифікації; налаштування конфігурації системи та супутня документація; план захисту інформації; перелік дій користувача, які можна виконати без ідентифікації чи автентифікації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]	

AC-14(01)	**ДОЗВОЛЕНІ ДІЇ БЕЗ ІДЕНТИФІКАЦІЇ АБО АВТЕНТИФІКАЦІЇ - НЕОБХІДНЕ ВИКОРИСТАННЯ**
	[Вилучено: включено до AC-14].

AC-15	**АВТОМАТИЗОВАНЕ МАРКУВАННЯ**
	[Вилучено: включено до MP-03].

AC-16	АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-16_ODP[01]	**визначено типи атрибутів безпеки, які мають бути пов'язані зі значеннями атрибутів безпеки для інформації, що зберігається, обробляється та/або передається;**
	AC-16_ODP[02]	**визначено типи атрибутів конфіденційності, які мають бути пов'язані зі значеннями атрибутів конфіденційності для інформації, що зберігається, обробляється та/або передається;**
	AC-16_ODP[03]	**визначено значення атрибутів безпеки для типів атрибутів безпеки;**
	AC-16_ODP[04]	визначено значення атрибутів конфіденційності для типів атрибутів конфіденційності;
	AC-16_ODP[05]	**визначено системи, для яких мають бути встановлені дозволені атрибути безпеки;**
	AC-16_ODP[06]	**визначено системи, для яких мають бути встановлені дозволені атрибути конфіденційності;**
	AC-16_ODP[07]	**визначено атрибути безпеки, визначені як частина AC-16(a), які дозволені для систем;**
	AC-16_ODP[08]	**визначено атрибути конфіденційності, визначені як частина AC-16(a), які дозволені для систем;**
	AC-16_ODP[09]	**визначено значення атрибутів або діапазони для встановлених атрибутів;**
	AC-16_ODP[10]	**визначено частоту, з якою слід переглядати атрибути безпеки на предмет відповідності;**
	AC-16_ODP[11]	**визначено частоту, з якою слід переглядати атрибути конфіденційності на предмет відповідності;**
	AC-16(a)[01]	надано засоби для асоціювання **<AC-16_ODP[01] типів атрибутів безпеки>** зі **<AC-16_ODP[03] значеннями атрибутів безпеки>** для інформації, що зберігається, обробляється та/або передається
	AC-16(a)[02]	надано засоби для асоціювання **<AC-16_ODP[02] типів атрибутів конфіденційності>** зі **<AC-16_ODP[04] значеннями атрибутів конфіденційності>** для інформації, що зберігається, обробляється та/або передається
	AC-16(b)[01]	виникають зв’язки з атрибутами;
	AC-16(b)[02]	зв’язки атрибутів зберігаються разом з інформацією;
	AC-16(c)[01]	на основі атрибутів, визначених у **AC-16_ODP[01]** для **<AC-16_ODP[05] систем>**, встановлюються наступні дозволені атрибути безпеки: **<AC-16_ODP[07] атрибути безпеки>**;
	AC-16(c)[02]	на основі атрибутів, визначених у **AC-16_ODP[02]** для **<AC-16_ODP[06] систем>**, встановлюються наступні дозволені атрибути приватності: **<AC-16_ODP[08] атрибути конфіденційності >**;

	AC-16(d)	визначено наступні допустимі значення або діапазони атрибутів для кожного з встановлених атрибутів: **<AC-16_ODP[09] значення або діапазони атрибутів>**;
	AC-16(e)	проводиться аудит змін до атрибутів;
	AC-16(f)[01]	**<AC-16_ODP[07] атрибути безпеки>** перевіряються на відповідність **<AC-16_ODP[10] частота>**;
	AC-16(f)[02]	**<AC-16_ODP[08] атрибути конфіденційності>** перевіряються на відповідність **<AC-16_ODP[11] частота>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, пов'язані з асоціацією атрибутів безпеки з інформацією, що зберігається, обробляється та передається; проектна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Спроможність організації підтримувати асоціацію атрибутів безпеки з інформацією, що зберігається, обробляється та передається].	

AC-16(01)	**АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ДИНАМІЧНЕ ПОВ'ЯЗАННЯ АТРИБУТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-16(01)_ODP[01]	**визначено суб'єкти, з якими атрибути безпеки повинні динамічно пов'язуватися при створенні та комбінуванні інформації;**
	AC-16(01)_ODP[02]	**визначено об'єкти, з якими атрибути безпеки повинні динамічно пов'язуватися при створенні та комбінуванні інформації;**
	AC-16(01)_ODP[03]	**визначені суб'єкти, з якими атрибути конфіденційності повинні динамічно пов'язуватися при створенні та комбінуванні інформації;**
	AC-16(01)_ODP[04]	**визначені об'єкти, з якими атрибути конфіденційності повинні динамічно пов'язуватися при створенні та комбінуванні інформації;**
	AC-16(01)_ODP[05]	**визначено політики безпеки, що вимагають динамічного пов'язування атрибутів безпеки з суб'єктами та об'єктами;**
	AC-16(01)_ODP[06]	**визначено політики конфіденційності, що вимагають динамічного пов'язування атрибутів безпеки з суб'єктами та об'єктами;**

	AC-16(01)[01]	атрибути безпеки динамічно пов'язуються з **<AC-16(01)_ODP[01] суб'єктами>** відповідно до наведених нижче політик безпеки під час створення та комбінування інформації: **<AC-16(01)_ODP[05] політики безпеки>**;
	AC-16(01)[02]	атрибути безпеки динамічно пов'язуються з **<AC-16(01)_ODP[02] об'єктами>** відповідно до наведених нижче політик безпеки під час створення та комбінування інформації: **<AC-16(01)_ODP[05] політики безпеки>**;
	AC-16(01)[03]	атрибути конфіденційності динамічно пов'язуються з **<AC-16(01)_ODP[03] суб'єктами>** відповідно до наведених нижче політик конфіденційності під час створення та комбінування інформації: **<AC-16(01)_ODP[06] політики конфіденційності>**;
	AC-16(01)[04]	атрибути конфіденційності динамічно пов'язуються з **<AC-16(01)_ODP[04] об'єктами>** відповідно до наведених нижче політик конфіденційності під час створення та комбінування інформації: **<AC-16(01)_ODP[06] політики конфіденційності>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на динамічне пов'язування атрибутів безпеки з інформацією; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують динамічну асоціацію атрибутів безпеки з інформацією].	

AC-16(02)	**АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ЗМІНА ЗНАЧЕНЬ АТРИБУТІВ АВТОРИЗОВАНИМИ ОСОБАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-16(02)[01]	уповноважені особи (або процеси, що діють від імені осіб) мають можливість визначати або змінювати значення пов'язаних з ними атрибутів безпеки;
	AC-16(02)[02]	уповноважені особи (або процеси, що діють від імені осіб) мають можливість визначати або змінювати значення пов'язаних з ними атрибутів конфіденційності;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на зміну значень атрибутів безпеки; проєктна документація системи; налаштування конфігурації системи та супутня документація; список осіб, уповноважених змі-	

	нювати атрибути безпеки; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за зміну значень атрибутів безпеки; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що дозволяють змінювати значення атрибутів безпеки].

AC-16(03)	**АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПІДТРИМКА СИСТЕМОЮ ПОВ'ЯЗАННЯ АТРИБУТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-16(03)_ODP[01]	**визначено атрибути безпеки, які потребують підтримки асоціацій та цілісності;**
	AC-16(03)_ODP[02]	**визначено атрибути конфіденційності, які потребують підтримки асоціації та цілісності;**
	AC-16(03)_ODP[03]	**визначено суб'єкти, які потребують об'єднання та збереження цілісності атрибутів безпеки, що належать до таких суб'єктів;**
	AC-16(03)_ODP[04]	**визначено об'єкти, які потребують об'єднання та збереження цілісності атрибутів безпеки, що належать до таких об'єктів;**
	AC-16(03)_ODP[05]	**визначено суб'єктів, які потребують об'єднання та збереження цілісності атрибутів конфіденційності щодо таких суб'єктів;**
	AC-16(03)_ODP[06]	**визначено об'єктів, які потребують об'єднання та збереження цілісності атрибутів конфіденційності щодо таких об'єктів;**
	AC-16(03)[01]	підтримується зв'язок та цілісність **<AC-16(03)_ODP[01] атрибутів безпеки>** з **<AC-16(03)_ODP[03] суб'єктами>;**
	AC-16(03)[02]	підтримується зв'язок та цілісність **<AC-16(03)_ODP[01] атрибутів безпеки>** з **<AC-16(03)_ODP[04] об'єктами>;**
	AC-16(03)[03]	підтримується зв'язок та цілісність **<AC-16(03)_ODP[02] атрибутів конфіденційності>** з **<AC-16(03)_ODP[05] суб'єктами>;**
	AC-16(03)[04]	підтримується зв'язок та цілісність **<AC-16(03)_ODP[02] атрибутів конфіденційності>** з **<AC-16(03)_ODP[06] об'єктами>;**

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо об'єднання атрибутів безпеки до інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захист інформації; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують об'єднання та цілісність атрибутів безпеки з інформацією].

AC-16(04)	**АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПОВ'ЯЗАННЯ АТРИБУТІВ АВТОРИЗОВАНИМИ ОСОБАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-16(04)_ODP[01]	**визначено атрибути безпеки, які пов'язуються з суб'єктами уповноваженими особами (або процесами, що діють від імені осіб);**
	AC-16(04)_ODP[02]	**визначено атрибути безпеки, які пов'язуються з об'єктами уповноваженими особами (або процесами, що діють від імені осіб);**
	AC-16(04)_ODP[03]	**визначено атрибути конфіденційності, які пов'язуються з суб'єктами уповноваженими особами (або процесами, що діють від імені осіб);**
	AC-16(04)_ODP[04]	**визначено атрибути конфіденційності, які пов'язуються з об'єктами уповноваженими особами (або процесами, що діють від імені осіб);**
	AC-16(04)_ODP[05]	**визначено суб'єкти, що потребують пов'язання атрибутів безпеки з уповноваженими особами (або процесами, що діють від імені осіб);**
	AC-16(04)_ODP[06]	**визначено об'єкти, що потребують пов'язання атрибутів безпеки з уповноваженими особами (або процесами, що діють від імені осіб);**
	AC-16(04)_ODP[07]	**визначено суб'єкти, що потребують пов'язання атрибутів конфіденційності з уповноваженими особами (або процесами, що діють від імені осіб);**
	AC-16(04)_ODP[08]	**визначено об'єкти, що потребують пов'язання атрибутів конфіденційності з уповноваженими особами (або процесами, що діють від імені осіб);**
	AC-16(04)[01]	уповноважені особи (або процеси, що діють від імені осіб) мають можливість пов'язувати **<AC-16(04)_ODP[01] атрибути безпеки>** з **<AC-16(04)_ODP[05] суб'єктами>**;
	AC-16(04)[02]	уповноважені особи (або процеси, що діють від імені осіб) мають можливість пов'язувати **<AC-16(04)_ODP[02] атрибути безпеки>** з **<AC-16(04)_ODP[06] об'єктами>**;
	AC-16(04)[03]	уповноважені особи (або процеси, що діють від імені осіб) мають можливість пов'язувати **<AC-16(04)_ODP[03] атрибути конфіденційності>** з **<AC-16(04)_ODP[07]**

		суб'єктами>;
	AC-16(04)[04]	уповноважені особи (або процеси, що діють від імені осіб) мають можливість пов'язувати **<AC-16(04)_ODP[04] атрибути конфіденційності>** з **<AC-16(04)_ODP[08] об'єктами>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури стосовно об'єднання атрибутів безпеки з інформацією; проєктна документація системи; налаштування конфігурації системи та супутня документація; список користувачів, уповноважених асоціювати атрибути безпеки до інформації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за асоціацію атрибутів безпеки до інформації; персонал організації, відповідальний за інформаційну безпеку; розробники системи] **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують об'єднання атрибутів безпеки з інформацією користувачами].	

AC-16(05)	**АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ВІДОБРАЖЕННЯ АТРИБУТІВ НА ПРИСТРОЯХ ВИВЕДЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-16(05)_ODP[01]	**для кожного об'єкта, який система передає на пристрої виведення, визначено спеціальні інструкції щодо поширення, обробки чи розподілу, які мають використовуватися;**
	AC-16(05)_ODP[02]	**визначено стандартні угоди про ідентифікацію атрибутів безпеки та конфіденційності, які повинні відображатися в зручній для читання формі на кожному об'єкті, який система передає на пристрої виводу;**
	AC-16(05)[01]	атрибути безпеки відображаються у формі, зручній для читання людиною, на кожному об'єкті, який система передає на пристрої виводу для ідентифікації **<AC-16(05)_ODP[01] інструкцій>** з використанням **<AC-16(05)_ODP[02] угод про іменування>**;
	AC-16(05)[02]	атрибути конфіденційності відображаються у формі, зручній для читання людиною, на кожному об'єкті, який система передає на пристрої виводу для ідентифікації **<AC-16(05)_ODP[01] інструкцій>** з використанням **<AC-16(05)_ODP[02] угод про іменування>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються відображення атрибутів безпеки у зручній для людини формі; спеціальні інструкції щодо розповсюдження, поводження чи поширення; типи зрозумілих для людини, ідентифікованих організацією стандартних угод про іменування; проєктна документація системи; налаштування конфігурації системи та супутня докумен-	

	тація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за безпеку інформації; розробники системи]. **Перевірка:** [ВИБІР: Пристрої виведення системи, що відображають атрибути захисту у читаному для людини вигляді на кожному об'єкті].

AC-16(06)	**АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПІДТРИМКА ПОВ'ЯЗАННЯ АТРИБУТІВ ОРГАНІЗАЦІЄЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-16(06)_ODP[01]	**визначено атрибути безпеки, які будуть пов'язані з суб'єктами;**
	AC-16(06)_ODP[02]	**визначено атрибути безпеки, які будуть пов'язані з об'єктами;**
	AC-16(06)_ODP[03]	**визначено атрибути конфіденційності, які будуть пов'язані з суб'єктами;**
	AC-16(06)_ODP[04]	**визначено атрибути конфіденційності, які будуть пов'язані з об'єктами;**
	AC-16(06)_ODP[05]	**визначені суб'єкти, які будуть пов'язані з атрибутами безпеки;**
	AC-16(06)_ODP[06]	**визначені об'єкти, які будуть пов'язані з атрибутами безпеки;**
	AC-16(06)_ODP[07]	**визначені суб'єкти, які будуть пов'язані з атрибутами конфіденційності;**
	AC-16(06)_ODP[08]	**визначені об'єкти, які будуть пов'язані з атрибутами конфіденційності;**
	AC-16(06)_ODP[09]	**політики безпеки, які вимагають від персоналу пов'язувати та підтримувати зв'язок атрибутів безпеки та конфіденційності з суб'єктами та об'єктами;**
	AC-16(06)_ODP[10]	**політики конфіденційності, які вимагають від персоналу пов'язувати та підтримувати зв'язок атрибутів безпеки та конфіденційності з суб'єктами та об'єктами;**
	AC-16(06)[01]	персонал зобов'язаний пов'язувати та підтримувати зв'язок <**AC-16(06)_ODP[01] атрибутів безпеки**> з <**AC-16(06)_ODP[05] суб'єктами**> відповідно до <**AC-16(06)_ODP[09] політик безпеки**>;

	AC-16(06)[02]	персонал зобов'язаний пов'язувати та підтримувати зв'язок **<AC-16(06)_ODP[02] атрибутів безпеки>** з **<AC-16(06)_ODP[06] об'єктами>** відповідно до **<AC-16(06)_ODP[09] політик безпеки>**;
	AC-16(06)[03]	персонал зобов'язаний пов'язувати та підтримувати зв'язок **<AC-16(06)_ODP[03] атрибутів конфіденційності>** з **<AC-16(06)_ODP[07] суб'єктами>** відповідно до **<AC-16(06)_ODP[10] політик безпеки**>;
	AC-16(06)[04]	персонал зобов'язаний пов'язувати та підтримувати зв'язок **<AC-16(06)_ODP[04] атрибутів конфіденційності>** з **<AC-16(06)_ODP[08] об'єктами>** відповідно до **<AC-16(06)_ODP[10] політик безпеки>;**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, пов'язані з об'єднанням атрибутів безпеки з суб'єктами та об'єктами; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за асоціацію та підтримку асоціації атрибутів безпеки з суб'єктами та об'єктами; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують асоціації атрибутів безпеки з суб'єктами та об'єктами].	

AC-16(07)	**АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПОСЛІДОВНА ІНТЕРПРЕТАЦІЯ АТРИБУТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-16(07)[01]	забезпечується послідовна інтерпретація атрибутів безпеки, що передаються між розподіленими компонентами системи.
	AC-16(07)[02]	забезпечується послідовна інтерпретація атрибутів конфіденційності, що передаються між розподіленими компонентами системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються послідовної інтерпретації атрибутів безпеки, що передаються між компонентами розподіленої системи; процедури щодо забезпечення доступу; процедури щодо забезпечення інформаційного потоку; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення послідовної інтерпретації атрибутів безпеки, які використовуються в діях щодо забезпечення доступу і забезпечення потоку інформації; персонал організації, відповідальний за інформаційну безпеку; розробники системи].	

	Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу та забезпечення інформаційного потоку].

AC-16(08)	**АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ТЕХНІКИ ТА ТЕХНОЛОГІЇ ПОВ'ЯЗАННЯ АТРИБУТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-16(08)_ODP[01]	**визначено методи та технології, які необхідно застосувати для пов'язання інформації з атрибутами безпеки;**
	AC-16(08)_ODP[02]	**визначено методи та технології, які необхідно застосувати для пов'язання інформації з атрибутами конфіденційності;**
	AC-16(08)[01]	**<AC-16(08)_ODP[01] методи та технології>** застосовуються для пов'язування атрибутів безпеки з інформацією;
	AC-16(08)[02]	**<AC-16(08)_ODP[02] методи та технології>** застосовуються для пов'язування атрибутів конфіденційності з інформацією;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, пов'язані з об'єднанням атрибутів безпеки з інформацією; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за асоціацію атрибутів безпеки з інформацією; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують методи або технології, що асоціюють атрибути безпеки з інформацією].	

AC-16(09)	**АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПЕРЕПРИЗНАЧЕННЯ АТРИБУТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-16(09)_ODP[01]	**визначено техніки або процедури, що використовуються для перепризначення атрибутів безпеки;**
	AC-16(09)_ODP[02]	**визначено техніки або процедури, що використовуються для перепризначення атрибутів конфіденційності;**
	AC-16(09)[01]	атрибути безпеки, пов'язані з інформацією, перепризна-

		чаються за допомогою **<AC-16(09)_ODP[01] техніки або процедури>**;
	AC-16(09)[02]	атрибути конфіденційності, пов'язані з інформацією, перепризначаються за допомогою **<AC-16(09)_ODP[01] техніки або процедури>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на перерозподіл атрибутів безпеки інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перерозподіл об'єднання атрибутів безпеки до інформації; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують методи або процедури перерозподілу об'єднання атрибутів безпеки до інформації].	

AC-16(10)	**АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - КОНФІГУРАЦІЯ АТРИБУТІВ УПОВНОВАЖЕНИМИ ОСОБАМИ**	
	МЕТА ОЦІНКИ: Визначте, чи.	
	AC-16(10)[01]	уповноваженим особам надається можливість визначати або змінювати тип і значення атрибутів безпеки, доступних для пов'язання з суб'єктами та об'єктами;
	AC-16(10)[02]	уповноваженим особам надається можливість визначати або змінювати тип і значення атрибутів конфіденційності, доступних для пов'язання з суб'єктами та об'єктами;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на налаштування атрибутів безпеки уповноваженими особами; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення або зміну атрибутів безпеки, пов'язаних з інформацією; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість визначення або зміни атрибутів безпеки].	

AC-17	**ВІДДАЛЕНИЙ ДОСТУП**
	МЕТА ОЦІНКИ: Визначити, чи:

	AC-17(a)[01]	для кожного типу дозволеного віддаленого доступу встановлені та задокументовані обмеження на використання;
	AC-17(a)[02]	для кожного типу дозволеного віддаленого доступу встановлені та задокументовані вимоги до конфігурації/підключення;
	AC-17(a)[03]	для кожного типу дозволеного віддаленого доступу встановлені та задокументовані рекомендації;
	AC-17(b)	кожен тип віддаленого доступу до системи авторизується перед тим, як дозволити такі підключення
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання віддаленого доступу (включаючи обмеження); план управління конфігурацією; план захисту інформації; налаштування конфігурації системи та супутня документація; авторизація віддаленого доступу; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління з'єднаннями віддаленого доступу; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Можливість віддаленого доступу до системи].	

AC-17(01)	**ВІДДАЛЕНИЙ ДОСТУП - АВТОМАТИЗОВАНИЙ МОНІТОРИНГ ТА УПРАВЛІННЯ**	
	МЕТА ОЦІНКИ: Визначте, чи:	
	AC-17(01)[01]	проводиться моніторинг методами віддаленого доступу
	AC-17(01)[02]	проводиться управління методами віддаленого доступу
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на віддалений доступ до системи; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; записи моніторингу системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми моніторингу та контролю методів віддаленого доступу].	

AC-17(02)	**ВІДДАЛЕНИЙ ДОСТУП - ЗАХИСТ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ЗА ДОПОМОГОЮ ШИФРУВАННЯ**

	МЕТА ОЦІНКИ: Визначте, чи інформаційна система	
	AC-17(02)	запроваджено криптографічні механізми для захисту конфіденційності та цілісності сесій віддаленого доступу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика контролю доступу; процедури, спрямовані на віддалений доступ до системи; проєктна документація системи; налаштування конфігурації системи та супутня документація; криптографічні механізми та пов'язана з ними документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Криптографічні механізми, що захищають конфіденційність та цілісність сесій віддаленого доступу].	

AC-17(03)	**ВІДДАЛЕНИЙ ДОСТУП - КЕРОВАНІ ТОЧКИ КОНТРОЛЮ ДОСТУПУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-17(03)	віддалений доступ маршрутизується через авторизовані та керовані точки контролю доступу до мережі
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на віддалений доступ до системи; проєктна документація системи; перелік усіх керованих точок контролю доступу до мережі; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що здійснюють маршрутизацію всього віддаленого доступу через керовані точки контролю доступу до мережі].	

AC-17(04)	**ВІДДАЛЕНИЙ ДОСТУП - ПРИВІЛЕЙОВАНІ КОМАНДИ ТА ДОСТУП**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-17(04)_ODP[01]	**визначено потреби, що потребують виконання привілейованих команд за допомогою віддаленого доступу;**

	AC-17(04)_ODP[02]	**визначено потреби, що вимагають доступу до інформації, що стосується безпеки, за допомогою віддаленого доступу;**
	AC-17(04)(a)[01]	виконання привілейованих команд за допомогою віддаленого доступу дозволено лише для наступних потреб: **<AC-17(04)_ODP[01] потреби >**;
	AC-17(04)(a)[02]	доступ до інформації, важливої для безпеки, за допомогою віддаленого доступу дозволяється лише для наступних потреб: **<AC-17(04)_ODP[02] потреби >**;
	AC-17(04)(b)	обґрунтування віддаленого доступу задокументовано в плані захисту інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на віддалений доступ до системи; налаштування конфігурації системи та супутня документація; план захисту інформації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують управління віддаленим доступом].	

AC-17(05)	**ВІДДАЛЕНИЙ ДОСТУП - МОНІТОРИНГ ДЛЯ НЕАВТОРИЗОВАНИХ ПІДКЛЮЧЕНЬ**
	[Вилучено: Включено в CI-04].

AC-17(06)	**ВІДДАЛЕНИЙ ДОСТУП - ЗАХИСТ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-17(06)	інформація про механізми віддаленого доступу захищена від неавторизованого використання та розкриття.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються віддаленого доступу до системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за впровадження або моніторинг віддаленого доступу до системи; користувачі системи, що володіють знаннями про механізми віддаленого доступу; персонал організації, відповідальний за інформаційну безпеку].	

AC-17(07)	ВІДДАЛЕНИЙ ДОСТУП - ДОДАТКОВИЙ ЗАХИСТ ДЛЯ ДОСТУПУ ДО ФУНКЦІЙ БЕЗПЕКИ
	[Вилучено: Включено в AC-03(10)].

AC-17(08)	ВІДДАЛЕНИЙ ДОСТУП - ДЕАКТИВАЦІЯ НЕЗАХИЩЕНИХ ПРОТОКОЛІВ МЕРЕЖІ
	[Вилучено: Включено в CM-07].

AC-17(09)	ВІДДАЛЕНИЙ ДОСТУП - ВІДКЛЮЧЕННЯ АБО ДЕАКТИВАЦІЯ ДОСТУПУ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-17(09)_ODP	**визначено період часу, протягом якого потрібно відключити або деактивувати віддалений доступ до системи;**
	AC-17(09)	передбачена можливість відключення або деактивації віддаленого доступу до системи протягом **<AC-17(09)_ODP періоду часу>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо відключення або дезактивації віддаленого доступу до системи; проєктна документація системи; налаштування конфігурації системи та супутня документація; план захисту інформації, записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість відключення або дезактивації віддаленого доступу до системи].	

AC-17(10)	ВІДДАЛЕНИЙ ДОСТУП - (10) АВТЕНТИФІКАЦІЯ ВІДДАЛЕНИХ КОМАНД	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-17(10)_ODP[01]	**визначено механізми, реалізовані для автентифікації віддалених команд;**
	AC-17(10)_ODP[02]	**визначено віддалені команди, які мають бути автентифіковані механізмами;**
	AC-17(10)	визначені **<AC-17(10)_ODP[01] механізми>** атентифіку-

		ють визначені **<AC-17(10)_ODP[02] віддалені команди>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо відключення або дезактивації віддаленого доступу до системи; проєктна документація системи; налаштування конфігурації системи та супутня документація; план захисту інформації, записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Механізми, що реалізують автентифікацію віддалених команд].	

AC-18	**БЕЗДРОТОВИЙ ДОСТУП**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-18(a)[01]	встановлено обмеження на використання щодо здійснення бездротового доступу
	AC-18(a)[02]	встановлено вимоги до конфігурації або підключення щодо здійснення бездротового доступу
	AC-18(a)[03]	встановлено рекомендації щодо здійснення бездротового доступу
	AC-18(b)	авторизується бездротовий доступ до системи перед тим, як дозволяти такі з'єднання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання бездротового доступу (включаючи обмеження); план управління конфігурацією; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; авторизація бездротового доступу; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління бездротовими з'єднаннями; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Можливість управління бездротовим доступом до системи].	

AC-18(01)	**БЕЗДРОТОВИЙ ДОСТУП - АВТЕНТИФІКАЦІЯ ТА ШИФРУВАННЯ**
	МЕТА ОЦІНКИ: Визначте, чи інформаційна система:

	AC-18(01)_ODP	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {користувачі; пристрої};**
	AC-18(01)[01]	бездротовий доступ до системи захищено за допомогою автентифікації **<AC-18(01)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**;
	AC-18(01)[02]	бездротовий доступ до системи захищений за допомогою шифрування.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання бездротового зв'язку (включаючи обмеження); проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні, мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують захист бездротового доступу до системи].	

AC-18(02)	**БЕЗДРОТОВИЙ ДОСТУП - МОНІТОРИНГ НЕАВТОРИЗОВАНИХ ПІДКЛЮЧЕНЬ**
	[Вилучено: Включено в SI-04].

AC-18(03)	**БЕЗДРОТОВИЙ ДОСТУП - ВІДКЛЮЧЕННЯ БЕЗДРОТОВОЇ МЕРЕЖІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-18(03)	відключено, у разі відсутності необхідності у використанні, вбудовані в компоненти системи можливості бездротових мереж до їх виклику та розгортання
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання бездротового зв'язку (включаючи обмеження); проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми управління відключенням можливостей бездротової мережі, внутрішньо вбудованими в компоненти системи].	

AC-18(04)	БЕЗДРОТОВИЙ ДОСТУП - ОБМЕЖЕННЯ НАЛАШТУВАННЯ КОРИСТУВАЧАМИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-18(04)[01]	встановлено користувачів, яким дозволено самостійно налаштовувати можливості бездротової мережі;
	AC-18(04)[02]	явно авторизуються визначені користувачі, яким дозволено самостійно налаштовувати можливості бездротової мережі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання бездротового зв'язку (включаючи обмеження); проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що дозволяють незалежне налаштування користувачем можливостей бездротової мережі].	

AC-18(05)	БЕЗДРОТОВИЙ ДОСТУП - АНТЕНИ ТА РІВЕНЬ ПОТУЖНОСТІ ПЕРЕДАЧІ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-18(05)[01]	вибирано такі радіо антени, які зменшують ймовірність того, що корисні сигнали можуть прийматися за межами контрольованих організацією меж;
	AC-18(05)[02]	калібруються рівні потужності передачі, щоб зменшити ймовірність того, що корисні сигнали можуть прийматися за контрольованими організацією межами.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на реалізацію та використання бездротового зв'язку (включаючи обмеження); проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Можливість бездротового доступу, що захищає корисні сигнали від несанкціонованого доступу за межами контрольованих організацією меж].	

AC-19	КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-19(a)[01]	встановлено вимоги до конфігурації мобільних пристроїв, що контролюються організацією, в тому числі, коли такі пристрої перебувають за межами контрольованої території;
	AC-19(a)[02]	встановлюються вимоги до підключення для мобільних пристроїв, що контролюються організацією, в тому числі, коли такі пристрої знаходяться за межами контрольованої території;
	AC-19(a)[03]	розроблено рекомендації щодо впровадження для мобільних пристроїв, які контролюються організацією, в тому числі, коли такі пристрої перебувають за межами контрольованої території;
	AC-19(b)	авторизовано підключення мобільних пристроїв до систем організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на контроль доступу для використання мобільних пристроїв (включаючи обмеження); план управління конфігурацією; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; дозволи на підключення мобільних пристроїв до систем організації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, що використовує мобільні пристрої для доступу до організаційних інформаційних систем; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Можливість контролю доступу, що дозволяє авторизувати з'єднання мобільних пристроїв з системами організації].	

AC-19(01)	КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ВИКОРИСТАННЯ ПИСЬМОВИХ ТА ПОРТАТИВНИЙ ПРИСТРОЇВ ДЛЯ ЗБЕРІГАННЯ ДАНИХ
	[Вилучено: Включено в MP-07].

AC-19(02)	КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ПОРТАТИВНИХ ПРИСТРОЇВ ЗБЕРІГАННЯ ДАНИХ
	[Вилучено: Включено в MP-07].

AC-19(03)	КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ВИКОРИСТАННЯ ПОРТАТИВНИХ ПРИСТРОЇВ ЗБЕРІГАННЯ ДАНИХ З НЕІДЕНТИФІКОВАНИМ ВЛАСНИКОМ	
	[Вилучено: Включено в MP-07].	

AC-19(04)	КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ОБМЕЖЕННЯ ДЛЯ ЗАСЕКРЕЧЕНОЇ ІНФОРМАЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-19(04)_ODP[01]	**визначено посадових осіб із захисту інформації, відповідальних за огляд та перевірку захищених мобільних пристроїв та інформації, що зберігається на цих пристроях;**
	AC-19(04)_ODP[02]	**визначено політики безпеки, що обмежують підключення захищених мобільних пристроїв до засекречених систем;**
	AC-19(04)(a)	використання незахищених мобільних пристроїв на об'єктах, що містять системи, які обробляють, зберігають або передають секретну інформацію, заборонено, за винятком випадків, коли на це є спеціальний дозвіл уповноваженої посадової особи;
	AC-19(04)(b)(01)	заборона підключення незахищених мобільних пристроїв до систем з обмеженим доступом застосовується до осіб, яким уповноважена посадова особа дозволила використовувати незахищені мобільні пристрої на об'єктах, що містять системи, які обробляють, зберігають або передають інформацію з обмеженим доступом;
	AC-19(04)(b)(02)	дозвіл уповноваженої посадової особи на підключення незахищених мобільних пристроїв до незахищених систем вимагається від осіб, яким дозволено використовувати незахищені мобільні пристрої на об'єктах, що містять системи, які обробляють, зберігають або передають інформацію з обмеженим доступом;
	AC-19(04)(b)(03)	заборона використання внутрішніх або зовнішніх модемів чи бездротових інтерфейсів у складі незахищених мобільних пристроїв поширюється на осіб, яким уповноваженою посадовою особою дозволено використовувати незахищені мобільні пристрої під час виконання службових обов'язків, а також на осіб, які не мають права на використання таких пристроїв
	AC-19(04)(b)(04)[01]	вибірковий огляд та перевірка незахищених мобільних

		пристроїв та інформації, що зберігається на них, **<AC-19(04)_ODP[01] посадовими особами>** є обов'язковими;
	AC-19(04)(b)(04)[02]	дотримання політики обробки інцидентів застосовується у разі виявлення секретної інформації під час випадкового огляду та перевірки незахищених мобільних пристроїв;
	AC-19(04)(c)	підключення захищенихмобільних пристроїв до засекречених систем обмежено відповідно до **<AC-19(04)_ODP[02] політики безпеки>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; політика поводження з інцидентами; процедури, спрямовані на контроль доступу для мобільних пристроїв; проєктна документація системи; налаштування конфігурації системи та супутня документація; доказова документація щодо випадкових перевірок та оглядів мобільних пристроїв; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за випадкові огляди або перевірки мобільних пристроїв; персонал організації, що використовує мобільні пристрої в приміщеннях, які призначені для обробки, зберігання або передачі секретної інформації ; персонал організації, відповідальний за реагування на інциденти; системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що забороняють використовувати внутрішні або зовнішні модеми або бездротові інтерфейси з мобільними пристроями].	

AC-19(05)	**КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ПОВНЕ ШИФРУВАННЯ ПРИСТРОЇВ ТА СХОВИЩ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-19(05)_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {повне шифрування пристроїв; шифрування сховищ інформації};**
	AC-19(05)_ODP[02]	**визначено мобільні пристрої, на яких слід використовувати шифрування;**
	AC-19(05)	**<AC-19(05)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРІВ>** використовується для захисту конфіденційності та цілісності інформації на **<AC-19(05)_ODP[02] мобільних пристроях>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, спрямовані на контроль доступу для мобільних пристроїв; проєктна документація системи; налаштування конфігурації системи та супутня документація; механізм шифрування і пов'язана з ним конфігураційна документація; записи аудиту системи; інші	

	відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за контроль доступу для мобільних пристроїв; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Механізми шифрування, що захищають конфіденційність та цілісність інформації на мобільних пристроях].

AC-20	**ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-20_ODP[01]	**вибрано одне або більше з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {встановити <AC-20_ODP[02] умови та положення>; визначити <AC-20_ODP[03] заходи захисту>}**
	AC-20_ODP[02]	**визначено умови та положення, що відповідають довірчим відносинам, встановленим з іншими організаціями, які володіють, експлуатують та/або обслуговують зовнішні системи (якщо вибрано);**
	AC-20_ODP[03]	**визначено заходи захисту, які мають бути застосовані до зовнішніх систем відповідно до довірчих відносин, встановлених з іншими організаціями, що володіють, експлуатують та/або обслуговують зовнішні системи (якщо обрано);**
	AC-20_ODP[04]	**визначено типи зовнішніх систем, заборонених до використання;**
	AC-20(04)(a)[01]	**<AC-20_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** узгоджується(ються) з довірчими відносинами, встановленими з іншими організаціями, які володіють, експлуатують та/або обслуговують зовнішні системи, що дозволяє уповноваженим особам отримувати доступ до системи із зовнішніх систем (якщо це застосовно);
	AC-20(04)(a)[02]	**<AC-20_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** відповідає(ють) довірчим відносинам, встановленим з іншими організаціями, які володіють, експлуатують та/або підтримують зовнішні системи, що дозволяє уповноваженим особам обробляти, зберігати або передавати інформацію, за допомогою зовнішніх систем (якщо це застосовно);
	AC-20(04)(b)	заборонено використання **<AC-20_ODP[04] заборонені типи зовнішніх систем>** (якщо застосовно).
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо використання зовнішніх систем; зовнішні системи та умови; перелік типів програм, дос-	

	тупних із зовнішніх систем; категоризація максимальної безпеки для інформації, що обробляється, зберігається або передається у зовнішніх системах; налаштування конфігурації системи та супутня документація; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення умов та обставин використання зовнішніх систем для доступу до систем організації; системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку] **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують умови використання зовнішніх систем].

AC-20(01)	**ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ОБМЕЖЕННЯ НА АВТОРИЗОВАНЕ ВИКОРИСТАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-20(01)(a)	Авторизовані особи мають право використовувати зовнішню систему для доступу до системи або для обробки, зберігання чи передачі інформації, що контролюється організацією, лише після перевірки виконання заходів безпеки та конфіденційності, зазначених у політиці безпеки та конфіденційності організації, а також планах безпеки та конфіденційності (якщо такі застосовуються);
	AC-20(01)(b)	Авторизовані особи мають право використовувати зовнішню систему для доступу до системи або для обробки, зберігання чи передачі інформації, що контролюється організацією, лише після збереження погоджених угод про підключення або обробку системи з структурою організації, на якій розміщена зовнішня система.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються використання зовнішніх систем; план захисту інформації; угоди про підключення або обробку систем; документи з управління облікового запису; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують обмеження на використання зовнішніх систем].	

AC-20(02)	**ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ПЕРЕНОСНІ ПРИСТРОЇ ЗБЕРІГАННЯ ДАНИХ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-20(02)_ODP	**визначено обмеження на використання авторизованими особами портативних носіїв інформації у зовнішніх системах;**
	AC-20(02)	використання портативних пристроїв носіїв інформації уповноваженими особами обмежено у зовнішніх системах за допомогою **<AC-20(02)_ODP обмеження >.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо використання зовнішніх систем; план захисту інформації; налаштування конфігурації системи та супутня документація; угоди про підключення або роботу з системами; документи з управління обліковими записами; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обмеження або заборону використання носіїв інформації у зовнішніх інформаційних системах; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують обмеження на використання портативних носіїв інформації].	

AC-20(03)	**ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - СИСТЕМИ ТА КОМПОНЕНТИ, ЩО НЕ ЗНАХОДЯТЬСЯ У ВЛАСНОСТІ ОРГАНІЗАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-20(03)_ODP	**визначено обмеження на використання систем або компонентів систем, що не належать організації, для обробки, зберігання або передачі інформації організації;**
	AC-20(03)	використання систем або компонентів систем, що не належать організації, для обробки, зберігання або передачі інформації, що належить організації, обмежується за допомогою **<AC-20(03)_ODP обмеження>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо використання зовнішніх систем; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; угоди про підключення або обробку системи; документи з управління рахунками; записи аудиту системи, інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обмеження або заборону використання систем, компонентів системи чи пристроїв, що не належать	

	до організації; системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують обмеження щодо використання систем, компонентів систем або пристроїв не організації].

AC-20(04)	**ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ПРИСТРОЇ ДЛЯ ЗБЕРІГАННЯ ДАНИХ, ЯКІ МОЖУТЬ МАТИ ДОСТУП ДО МЕРЕЖІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-20(03)_ODP	**визначано мережеві носії інформації, які можуть мати доступ до мережі;**
	AC-20(03)	заборонено використовувати **<AC-20(03)_ODP мережеві носії інформації>** у зовнішніх системах.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються використання мережевих носіїві інформації даних у зовнішніх інформаційних системах; план захисту інформації, проєктна документація системи; налаштування конфігурації системи та супутня документація; угоди про підключення або роботу з системою; перелік мережевих доступних носіїв інформації, заборонених до використання у зовнішніх системах; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за заборону використання мережевих носіїі інформації у зовнішніх системах; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що забороняють використовувати мережеві носіїі інформації у зовнішніх системах].	

AC-20(05)	**ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ПОРТАТИВНІ ПРИСТРОЇ ДЛЯ ЗБЕРІГАННЯ ДАНИХ – ЗАБОРОНА ВИКОРИСТАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-20(05)	використання уповноваженими особами зовнішніх носіїв інформації, підконтрольних організації, на зовнішніх системах заборонено.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються використання зовнішніх носіїв інформації у зовнішніх інформаційних системах; план захисту інформації, проєктна документація системи; налаштування конфі-	

	гурації системи та супутня документація; угоди про підключення або роботу з системою; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за заборону використання портативних пристроїв зберігання даних у зовнішніх системах; системні / мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку].

AC-21	**РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-21_ODP[01]	**визначені обставини обміну інформацією, за яких користувач повинен на власний розсуд визначати, чи відповідають повноваження доступу, надані партнеру з обміну, обмеженням доступу та використання інформації;**
	AC-21_ODP[02]	**визначено автоматизовані механізми або ручні процеси, які допомагають користувачам у ухваленні рішень щодо обміну інформацією та співпраці;**
	AC-21(a)	авторизованим користувачам дозволено визначати, чи відповідають повноваження доступу, призначені партнеру з обміну, обмеженням доступу та використання інформації для **<AC-21_ODP[01] обставин обміну інформацією>;**
	AC-21(b)	**<AC-21_ODP[02] автоматизовані механізми>** використовуються для допомоги користувачам у прийнятті рішень щодо обміну інформацією та співпраці.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо співпраці з користувачами та обміну інформацією (включаючи обмеження); проєктна документація системи; налаштування конфігурації системи та супутня документація; список користувачів, уповноважених приймати рішення щодо обміну та співпраці; перелік обставин обміну інформацією, що вимагає обачності від користувача; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за прийняття рішень щодо обміну та співпраці; системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми або ручний процес, що реалізує авторизацію доступу, що підтримує рішення щодо обміну інформацією та співпраці користувачів].	

AC-21(01)	**РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ - АВТОМАТИЧНА ПІДТРИМКА УХВАЛЕННЯ РІШЕНЬ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-21(01)_ODP	**визначено автоматизовані механізми, що застосовуються для забезпечення виконання рішень про спільний доступ до інформації авторизованими користувачами;**
	AC-21(01)	**<AC-21(01)_ODP автоматизовані механізми>** використовуються для забезпечення виконання рішень щодо обміну інформацією уповноваженими користувачами на основі дозволів доступу партнерів з обміну та обмежень доступу до інформації, що підлягає обміну.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються взаємодії з користувачами та обміну інформацією (включаючи обмеження); проєктна документація системи; налаштування системи та супутня документація; список користувачів, уповноважених приймати рішення щодо обміну та співпраці; перелік обставин обміну інформацією, які вимагають розсуду користувача; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Системні або мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують авторизацію доступу, що підтримують рішення щодо обміну інформацією та співпраці користувачів].	

AC-21(02)	**РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ - ПОШУК І ПЕРЕВІРКА ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-21(02)_ODP	**визначено обмеження щодо обміну інформацією;**
	AC-21(02)	впроваджено сервіси пошуку та перевірки інформації, які застосовують е **<AC-21(02)_ODP обмеження>** щодо обміну інформацією.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються взаємодії з користувачами та обміну інформацією (включаючи обмеження); проєктна документація системи; налаштування системи та супутня документація; сформований перелік обмежень доступу щодо інформації, яку потрібно передавати; записи щодо пошуку та перевірки інформації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу до служб пошуку та перевірки систем; системні або мережеві адміністрато-	

	ри; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Служби пошуку та перевірки системи, що застосовують обмеження щодо обміну інформацією].

AC-22	**ПУБЛІЧНО ДОСТУПНИЙ КОНТЕНТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-22_ODP	**визначено частоту, з якою слід переглядати вміст загальнодоступної системи на предмет наявності там інформації з обмеженим доступом;**
	AC-22(a)	визначені особи уповноважені на розміщення інформації в загальнодоступній системі;
	AC-22(b)	уповноважені особи проходять навчання, щоб гарантувати, що загальнодоступна інформація не містить інформацію з обмеженим доступом;
	AC-22(c)	запропонований зміст інформації перевіряється до публікації в загальнодоступній системі, щоб гарантувати, що там не міститься інформація з обмеженим доступом;
	AC-22(d)[01]	зміст у загальнодоступній системі перевіряється на наявність інформації з обмеженим доступом з **<AC-22_ODP частотою>**;
	AC-22(d)[02]	інформація з обмеженим доступом видаляється з загальнодоступної системи, якщо її виявлено.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури звернення до загальнодоступного контенту; перелік користувачів, які мають право публікувати загальнодоступний вміст в системах організації; навчальні матеріали та / або записи; записи оглядів загальнодоступної інформації;; журнали аудиту системи; записи про навчання поінформованості з безпеки; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління загальнодоступною інформацією, розміщеною в системах організації; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують управління загальнодоступним контентом].	

AC-23	**ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-23_ODP[01]	**визначено техніки виявлення та попередження витоку даних;**
	AC-23_ODP[02]	**визначено об'єкти зберігання даних**;
	AC-23	**<AC-23_ODP[01] техніки>** використовуються для **<AC-23_ODP[02] об'єктів зберігання даних>** для виявлення та захисту від несанкціонованого інтелектуального аналізу даних.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються методів інтелектуального аналізу даних; процедури, спрямовані на захист об'єктів зберігання даних від інтелектуального аналізу даних; проєктна документація системи; конфігурація системи та супутня документація; журнали аудиту системи; записи аудиту системи; інші відповідні документи чи записи] **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за впровадження методів виявлення та запобігання обробці даних для об'єктів зберігання даних; персонал організації відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують запобігання та виявлення інтелектуального аналізу даних].	

AC-24	**РІШЕННЯ ЩОДО УПРАВЛІННЯ ДОСТУПОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-24_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {встановити процедури; запровадити механізми};**
	AC-24_ODP[02]	**визначено рішення щодо контролю доступу, які застосовуються до кожного запиту щодо доступу до виконання доступу;**
	AC-24	**<AC-24_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ІВ)>** забезпечують застосування **<AC-24_ODP[02] рішення щодо контролю доступу>** до кожного запиту щодо доступу до виконання доступу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури контролю доступу; проєктна документація системи; налаштування системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за встановлення процедур щодо прийняття рішень щодо контролю доступу до системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що застосовують встановлені рішення та процедури контролю доступу].

AC-24(01)	**РІШЕННЯ ЩОДО УПРАВЛІННЯ ДОСТУПОМ - ІНФОРМАЦІЯ ПРО ПЕРЕДАЧУ АВТОРИЗОВАНОГО ДОСТУПУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-24(01)_ODP[01]	**визначено інформацію щодо авторизації доступу, яка передається до систем, які забезпечують ухвалення рішень щодо управління доступом;**
	AC-24(01)_ODP[02]	**визначено заходи безпеки, які слід використовувати, коли інформація про авторизацію передається до систем, що забезпечують виконання рішень щодо управління доступом;**
	AC-24(01)_ODP[03]	**визначено системи, які забезпечують ухвалення рішень щодо управління доступом;**
	AC-24(01)	**<AC-24(01)_ODP[01] інформація щодо авторизації доступу>** передається за допомогою **<AC-24(01)_ODP[02] заходів безпеки>** до **<AC-24(01)_ODP[03] систем>**, які забезпечують ухвалення рішень щодо управління доступом.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні та мережеві адміністратори; персонал організації відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу].	

AC-24(02)	**РІШЕННЯ ЩОДО УПРАВЛІННЯ ДОСТУПОМ - ВІДСУТНІСТЬ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА АБО ПРОЦЕСУ, ЩО ДІЄ ВІД ІМЕНІ КОРИСТУВАЧА**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	AC-24(02)_ODP[01]	**визначено атрибути безпеки, які не охоплюють ідентифікацію користувача або процесу, що діє від імені користувача (якщо вибрано);**
	AC-24(02)_ODP[02]	**визначено атрибути конфіденційності, які не охоплюють ідентифікацію користувача або процесу, що діє від імені користувача (якщо вибрано);**
	AC-24(02)[01]	рішення щодо управління доступом здійснюються на основі **<AC-24(02)_ODP[01] атрибутів безпеки>**, які не охоплюють ідентифікацію користувача або процесу, що діє від імені користувача (якщо вибрано);
	AC-24(02)[02]	рішення щодо управління доступом здійснюються на основі **<AC-24(02)_ODP[02] атрибутів конфіденційності>**, які не охоплюють ідентифікацію користувача або процесу, що діє від імені користувача (якщо вибрано);
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація системи; налаштування системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні та мережеві адміністратори; персонал організації відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу].	

AC-25	**ДИСПЕТЧЕР ДОСТУПУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AC-25_ODP	**визначено політики контролю доступу, для яких реалізовано диспетчер доступу;**
	AC-25	реалізовано диспетчер доступу для **<AC-25_ODP політики контролю доступу>**, який захищений від несанкціонованого доступу, завжди доступний для виклику та досить компактний, щоб бути підданим аналізу й тестуванню, надійність якого може бути гарантована
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури щодо забезпечення доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи	

	чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за забезпечення доступу; системні та мережеві адміністратори; персонал організації відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують функції забезпечення доступу].

II. КЛАС ЗАХОДІВ ЗАХИСТУ АТ – ОБІЗНАНІСТЬ ТА НАВЧАННЯ

АТ-01	**ПОЛІТИКА ТА ПРОЦЕДУРИ ПІДВИЩЕННЯ ОБІЗНАНОСТІ ТА НАВЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	АТ-01_ODP[01]	**визначено персонал або ролі, серед яких має бути поширена політика обізнаності та навчання;**
	АТ-01_ODP[02]	**визначено персонал або ролі, серед яких мають бути поширені процедури, що сприяють реалізації політики підвищення обізнаності;**
	АТ-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	АТ-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами підвищення обізнаності та навчання;**
	АТ-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика інформування;**
	АТ-01_ODP[06]	**визначено події, які потребують перегляду та оновлення поточної політики;**
	АТ-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні процедури;**
	АТ-01_ODP[08]	**визначено події, які потребують перегляду та оновлення поточних процедур;**
	АТ-01(a)[01]	розроблено та задокументовано політику обізнаності та навчання;
	АТ-01(a)[02]	політика обізнаності та навчання поширюється на **<АТ-01_ODP[01] персонал або ролі>**;
	АТ-01(a)[03]	розроблені та задокументовані процедури, що сприяють впровадженню політики обізнаності та навчання і пов'язаних з нею засобів контролю доступу;
	АТ-01(a)[04]	процедури поширюються на **<АТ-01_ODP[02] персонал або ролі>**.
	АТ-01(a)[01](a)[01]	**<АТ-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політика обізнаності та навчання містить мету;
	АТ-01(a)[01](a)[02]	**<АТ-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політика обізнаності та навчання містить сферу застосування;
	АТ-01(a)[01](a)[03]	**<АТ-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політика обізнаності та навчання містить ролі;
	АТ-01(a)[01](a)[04]	**<АТ-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політика обізнаності та навчання містить обов'язки;
	АТ-01(a)[01](a)[05]	**<АТ-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політика обізнаності та навчання містить відповідальність керівництва;
	АТ-01(a)[01](a)[06]	**<АТ-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політика обізнаності та навчання містить координацію між підрозділами організації;
	АТ-01(a)[01](a)[07]	**<АТ-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політика обізнаності та навчання містить систему контролю відповідності;

	AT-01(a)[01](b)	**<AT-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політика обізнаності та навчання відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам;
	AT-01(b)	**<AT-01_ODP[04]** посадова особа> призначається для управління політикою та процедурами підвищення обізнаності та навчання у сфері забезпечення безпеки та конфіденційності.
	AT-01(c)[01][01]	переглядається та оновлюється поточна політика обізнаності та навчання з **<AT-01_ODP[05] частототою>**;
	AT-01(c)[01][02]	переглядається та оновлюється поточна політика обізнаності та навчання після **<AT-01_ODP[06] подій>**;
	AT-01(c)[02][01]	переглядаються та оновлюються поточні процедури обізнаності та навчання з **<AT-01_ODP[07] частототою>**;
	AT-01(c)[02][02]	переглядаються та оновлюються поточні процедури обізнаності та навчання після **<AT-01_ODP[08] подій>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури політики обізнаності та навчання; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику обізнаності та навчання; персонал, відповідальний за інформаційну безпеку].	

AT-02	**НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-02_ODP[01]	**визначено періодичність проведення навчання грамотності з питань безпеки для користувачів системи (в тому числі менеджерів, вищого керівництва та підрядників) після початкового тренінгу;**
	AT-02_ODP[02]	**визначено періодичність проведення навчання грамотності з питань конфіденційності для користувачів системи (в тому числі менеджерів, вищого керівництва та підрядників) після початкового тренінгу;**
	AT-02_ODP[03]	**визначено події, які потребують навчання користувачів системи грамотності з питань безпеки;**
	AT-02_ODP[4]	**визначено події, які потребують навчання користувачів системи грамотності з питань конфіденційності;**
	AT-02_ODP[05]	**визначено методи, які слід застосовувати для підвищення обізнаності користувачів системи щодо безпеки та конфіденційності;**
	AT-02_ODP[06]	**визначено частоту оновлення навчання грамотності та змісту обізнаності;**

	AT-02_ODP[07]	**визначено події після яких необхідне оновлення навчання грамотності та змісту обізнаності;**
	AT-02(a)[01][01]	навчання з грамотності з питань безпеки надається користувачам системи (включаючи менеджерів, керівників вищої ланки та підрядників) як частина початкового навчання для нових користувачів;
	AT-02(a)[01][02]	навчання з грамотності з питань конфіденційності надається користувачам системи (включаючи менеджерів, керівників вищої ланки та підрядників) як частина початкового навчання для нових користувачів;
	AT-02(a)[01][03]	для користувачів системи (включно з менеджерами, вищим керівництвом та підрядниками) проводиться навчання з безпеки з **<AT-02_ODP[01] періодичністю>** після цього;
	AT-02(a)[01][04]	для користувачів системи (включно з менеджерами, вищим керівництвом та підрядниками) проводиться навчання з конфіденційності з **<AT-02_ODP[02] періодичністю>** після цього;
	AT-02(a)[02][01]	тренінги з грамотності з питань безпеки проводяться для користувачів системи (включаючи менеджерів, керівників вищої ланки та підрядників), коли цього вимагають зміни в системі або після **<AT-02_ODP[03] подій>**;
	AT-02(a)[02][02]	тренінги з грамотності з питань конфіденціності проводяться для користувачів системи (включаючи менеджерів, керівників вищої ланки та підрядників), коли цього вимагають зміни в системі або після **<AT-02_ODP[04] подій>**;
	AT-02(b)	**<AT-02_ODP[05] методи>** застосовуються для підвищення обізнаності користувачів системи щодо безпеки та конфіденційності;
	AT-02(c)[01]	оновлюється зміст навчання грамотності та підвищення обізнаності з **<AT-02_ODP[06] частотою>**;
	AT-02(c)[02]	оновлюється зміст навчання грамотності та підвищення обізнаності після **<AT-02_ODP[07] подій>**;
	AT-02(d)	уроки, отримані в результаті внутрішніх або зовнішніх інцидентів або порушень безпеки, включені в методи навчання та підвищення обізнаності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за навчання з підвищення безпеки; персонал організації з обов'язками інформаційної безпеки; персонал органі-	

	зації, що складається із загальної спільноти користувачів системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми управління навчанням з питань безпеки.]

AT-02(01)	**НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - ПРАКТИЧНІ ЗАНЯТТЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-02(01)	передбачені практичні вправи з тренування обізнаності, які імітують інциденти в області безпеки та конфіденційності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який бере участь у навчанні з підвищення безпеки; персонал організації, відповідальний за навчання з підвищення безпеки; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують моделювання кібератак у практичних вправах].	

AT-02(02)	**НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - ВНУТРІШНІ ЗАГРОЗИ**	
	МЕТА ОЦІНКИ: Визначте, чи	
	AT-02(02)[01]	введено до програми навчання вправи з розпізнавання потенційних індикаторів внутрішніх загроз;
	AT-02(02)[02]	введено до програми навчання вправи з виявлення потенційних індикаторів внутрішніх загроз;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який бере участь у навчанні з підвищення безпеки; персонал організації, відповідальний за базове навчання з підвищення безпеки; персонал організації, відповідальний за інформаційну безпеку].	

AT-02(03)	**НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - СОЦІАЛЬНА ІНЖЕНЕРІЯ**

	ТА СОЦІАЛЬНИЙ ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-02(03)[01]	**до програми навчання введено вправи з розпізнавання потенційних та фактичних випадків соціального інжинірингу;**
	AT-02(03)[02]	**до програми навчання введено вправи з повідомлення про потенційні та фактичні випадки соціального інжинірингу;**
	AT-02(03)[03]	**до програми навчання введено вправи з розпізнавання потенційних та фактичних випадків інтелектуального аналізу соціальних даних;**
	AT-02(03)[04]	**до програми навчання введено вправи з повідомлення про потенційні та фактичні випадки інтелектуального аналізу соціальних даних;**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який бере участь у навчанні з підвищення безпеки; персонал організації, відповідальний за базове навчання з підвищення безпеки; персонал організації, відповідальний за інформаційну безпеку].	

AT-02(04)	**НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - ПІДОЗРІЛІ ПОВІДОМЛЕННЯ ТА АНОМАЛЬНА ПОВЕДІНКА СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-02(04)_ODP	**визначено індикатори шкідливого коду;**
	AT-02(04)	навчання грамотності щодо розпізнавання підозрілих повідомлень та аномальної поведінки у системах організації проводиться з використанням **<AT-02(04)_ODP індикаторів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який бере участь у навчанні з підвищення безпеки; персонал організації, відповідальний за базове навчання з підвищення безпеки; персонал організації, відповідальний за інформаційну безпеку].	

AT-02(05)	НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - ВДОСКОНАЛЕНА СТІЙКА ЗАГРОЗА	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-02(05)	забезпечено навчання грамотності щодо стійкої постійної загрози
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який бере участь у навчанні з підвищення безпеки; персонал організації, відповідальний за базове навчання з підвищення безпеки; персонал організації, відповідальний за інформаційну безпеку].	

AT-02(06)	НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - СЕРЕДОВИЩЕ КІБЕРЗАГРОЗ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-02(06)(a)	забезпечено навчання грамотності щодо середовища кіберзагроз
	AT-02(06)(b)	відображається поточна інформація про кіберзагрози в операціях системи
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який бере участь у навчанні з підвищення безпеки; персонал організації, відповідальний за базове навчання з підвищення безпеки; персонал організації, відповідальний за інформаційну безпеку].	

AT-03	РОЛЬОВЕ НАВЧАННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-03_ODP[01]	**визначено ролі та обов'язки для тренінгів з безпеки на основі ролей;**
	AT-03_ODP[02]	**визначено ролі та обов'язки для тренінгів з конфіденційності**

		на основі ролей;
	AT-03_ODP[03]	**визначено частоту проведення тренінгів на основі ролей з безпеки та конфіденційності для призначеного персоналу після початкової підготовки;**
	AT-03_ODP[04]	**визначено частоту оновлення змісту навчання на основі ролей;**
	AT-03_ODP[05]	**визначено події, які потребують оновлення змісту навчання на основі ролей;**
	AT-03(a)[01][01]	навчання з безпеки на основі ролей проводиться для **<AT-03_ODP[01] ролей та обов'язків>** перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків;
	AT-03(a)[01][02]	навчання з конфіденційності на основі ролей проводиться для **<AT-03_ODP[02] ролей та обов'язків>** перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків;
	AT-03(a)[01][03]	навчання з безпеки на основі ролей проводиться для <**AT-03_ODP[01] ролей та обов'язків>** з **<AT-03_ODP[03] частотою>** після цього;
	AT-03(a)[01][04]	навчання з конфіденційності на основі ролей проводиться для **<AT-03_ODP[02] ролей та обов'язків>** з **<AT-03_ODP[03] частотою>** після цього;
	AT-03(a)[02][01]	навчання з питань безпеки на основі ролей проводиться для персоналу, який виконує певні ролі та обов'язки у сфері безпеки, коли цього вимагають зміни в системі;
	AT-03(a)[02][02]	навчання з питань конфіденційності на основі ролей проводиться для персоналу, який виконує певні ролі та обов'язки у сфері безпеки, коли цього вимагають зміни в системі;
	AT-03(b)[01]	оновлюється вміст навчання на основі ролей з **<AT-03_ODP[04] частотою>**;
	AT-03(b)[02]	оновлюється вміст навчання на основі ролей після **<AT-03_ODP[05] подій>**;
	AT-03(c)	інформація отримана з внутрішніх чи зовнішніх інцидентів або порушень безпеки, включається в навчання на основі ролей.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються впровадження тренінгів з безпеки; навчальний план з питань безпеки; навчальні матеріали з безпеки; план захисту інформації; навчальні записи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за навчання безпеки на	

	основі ролей; персонал організації з призначеними обов'язками з безпеки системи]. **Перевірка:** [ВИБІР: автоматизовані механізми управління навчанням безпеки на основі ролей].

AT-03(01)	**РОЛЬОВЕ НАВЧАННЯ - ЗАХОДИ БЕЗПЕКИ РОБОЧОГО СЕРЕДОВИЩА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-03(01)_ODP[01]	**визначено персонал або ролі, які мають бути забезпечені початковим навчанням та підвищенням кваліфікації з питань застосування та експлуатації заходів захисту робочого середовища;**
	AT-03(01)_ODP[02]	**визначено частоту проведення підвищення кваліфікації в галузі операцій та функціонування заходів захисту робочого середовища;**
	AT-03(01)	**<AT-03(01)_ODP[01] персонал або ролі>** забезпечується підвищенням кваліфікації в галузі зайнятості та функціонування заходів захисту робочого середовища з **<AT-03(01)_ODP[02] частотою>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються впровадження тренінгів з безпеки; навчальний план з питань безпеки; навчальні матеріали з безпеки; план захисту інформації; навчальні записи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за навчання безпеки на основі ролей; персонал організації, відповідальний за використання та управління заходами захисту навколишнього середовища].	

AT-03(02)	**РОЛЬОВЕ НАВЧАННЯ - ФІЗИЧНІ ЗАХОДИ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-03(02)_ODP[01]	**визначаено персонал або ролі, які мають бути забезпечені підготовкою з питань застосування та експлуатації заходів фізичної безпеки;**
	AT-03(02)_ODP[02]	**визначаеночастоту проведення підготовки з питань застосування та експлуатації заходів фізичної безпеки;**
	AT-03(02)	**<AT-03(02)_ODP[01] персонал або ролі>** забезпечуються підготовкою з питань застосування та експлуатації заходів

		фізичної безпеки з **<AT-03(02)_ODP[02] частотою>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються впровадження тренінгів з безпеки; навчальний план з питань безпеки; навчальні матеріали з безпеки; план захисту інформації; навчальні записи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за навчання безпеки на основі ролей; персонал організації, відповідальний за використання та керування фізичними засобами безпеки].	

AT-03(03)	**РОЛЬОВЕ НАВЧАННЯ - ПРАКТИЧНІ ЗАНЯТТЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-3(03)[01]	програма навчання включає практичні заняття з безпеки, які мають підкріпити досягнення цілей навчання.
	AT-3(03)[02]	програма навчання включає практичні заняття з конфіденційності, які мають підкріпити досягнення цілей навчання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, спрямовані на реалізацію тренінгу з підвищення рівня безпеки; навчальний план з підвищення обізнаності з безпеки; навчальні матеріали з підвищення безпеки; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за навчання безпеки на основі ролей; персонал організації,, який бере участь у навчанні з підвищення безпеки].	

AT-03(04)	**РОЛЬОВЕ НАВЧАННЯ - ПІДОЗРІЛІ ЗВ'ЯЗКИ ТА АНОМАЛЬНА ПОВЕДІНКА СИСТЕМИ**
	[Вилучено: включено до AT-02(04)].

AT-03(05)	**РОЛЬОВЕ НАВЧАННЯ - ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-03(05)_ODP[01]	**визначено персонал або посади, які мають пройти навчання з використання та управління обробкою персональних даних та контролю прозорості;**

	AT-03(05)_ODP[02]	визначено періодичність проведення навчання з використання та управління обробкою персональних даних та контролю прозорості
	AT-3(05)	<AT-03(05)_ODP[01] персонал або ролі> навчання з <AT-03(05)_ODP[02] частотою> з використання та управління обробкою персональних даних та контролю прозорості;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються впровадження тренінгів з безпеки; навчальний план з питань безпеки; навчальні матеріали з безпеки; план захисту інформації; навчальні записи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за навчання ролі з безпеки; персонал організації, який бере участь у навчанні з підвищення безпеки].	

AT-04	**НАВЧАЛЬНІ ЗАПИСИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-04_ODP	**визначено період зберігання індивідуальних записів про навчання;**
	AT-04(a)[01]	задокументовані індивідуальні навчальні заходи із забезпечення безпеки та конфіденційності інформації, включно з базовою підготовкою з питань безпеки та конфіденційності, а також спеціальною підготовкою з безпеки та конфіденційності;
	AT-04(a)[02]	відстежуються індивідуальні навчальні заходи із забезпечення безпеки та конфіденційності інформації, включно з базовою підготовкою з питань безпеки та конфіденційності, а також спеціальною підготовкою з безпеки та конфіденційності;
	AT-04(b)	індивідуальні записи про навчання зберігаються протягом **<AT-04_ODP період часу>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Поінформованість щодо безпеки та політика навчання; процедури, що стосуються записів навчання з безпеки; обізнаність із безпеки та навчальні записи; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками щодо зберігання записів з безпеки]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують управління записами навчань з безпеки].	

AT-05	**КОНТАКТИ З ГРУПАМИ БЕЗПЕКИ ТА АСОЦІАЦІЯМИ**

	Вилучено: включено в PM-15.

AT-06	**ВІДГУКИ ПРО ПРОВЕДЕНІ НАВЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AT-06_ODP[01]	**визначено частоту надання відгуків щодо результатів навчання в організації;**
	AT-06_ODP[02]	**призначено персонал, якому надаватиметься відгуки щодо результатів навчання в організації;**
	AT-06	відгуки про результати навчання надаються з визначеною **<AT-06_ODP[01] частотою>** до **<AT-06_ODP[02] персоналу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обізнаності та навчання з питань безпеки; процедури, що стосуються записів навчання з безпеки; обізнаність із безпеки та навчальні записи; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками щодо зберігання записів з безпеки]. **Перевірка:** [ВИБІР: Механізми, що підтримують управління записами про тренінги з безпеки].	

III. КЛАС ЗАХОДІВ ЗАХИСТУ AU – АУДИТ ТА ПІДЗВІТНІСТЬ

AU-01	ПОЛІТИКА ТА ПРОЦЕДУРИ АУДИТУ ТА ПІДЗВІТНОСТІ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-01_ODP[01]	**визначено персонал або ролі, до яких має бути доведена політика аудиту та підзвітності;**
	AU-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури аудиту та підзвітності;**
	AU-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	AU-01_ODP[04]	**визначено посадову особу, яка управлятиме політикою та процедурами аудиту та підзвітності;**
	AU-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика аудиту та підзвітності;**
	AU-01_ODP[06]	**визначено події, які потребують перегляду та оновлення поточної політики аудиту та підзвітності;**
	AU-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні процедури аудиту та підзвітності;**
	AU-01_ODP[08]	**визначено події, які потребують перегляду та оновлення поточної процедури аудиту та підзвітності;**
	AU-01(a)[01]	розроблено та задокументовано політику аудиту та підзвітності;
	AU-01(a)[02]	політика аудиту та підзвітності доведена до **<AU-01_ODP[01] персонал або ролі>**;
	AU-01(a)[03]	розроблені та задокументовані процедури аудиту та підзвітності, що сприяють впровадженню політики аудиту та підзвітності, а також відповідні заходи контролю аудиту та підзвітності;
	AU-01(a)[04]	процедури аудиту та підзвітності поширюються на **<AU-01_ODP[02] персонал або ролі>**;
	AU-01(a)[01](a)[01]	**<AU-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики аудиту та підзвітності містить мету;
	AU-01(a)[01](a)[02]	**<AU-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики аудиту та підзвітності містить сферу застосування;

	AU-01(a)[01](a)[03]	**<AU-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики аудиту та підзвітності містить ролі;
	AU-01(a)[01](a)[04]	**<AU-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики аудиту та підзвітності містить обов'язки;
	AU-01(a)[01](a)[05]	**<AU-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики аудиту та підзвітності містить відповідальність керівництва;
	AU-01(a)[01](a)[06]	**<AU-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики аудиту та підзвітності містить координацію між підрозділами організації;
	AU-01(a)[01](a)[07]	**<AU-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики аудиту та підзвітності містить систему контролю відповідності;
	AU-01(a)[01](b)	**<AU-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики аудиту та підзвітності відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам;
	AU-01(b)	**<AU-01_ODP[04] посадова особа>** призначається для управління політикою та процедурами аудиту та підзвітності
	AU-01(c)[01][01]	переглядається та оновлюється поточна політика аудиту та підзвітності з **<AU-01_ODP[05] частота>**;
	AU-01(c)[01][02]	переглядається та оновлюється поточна політика аудиту та підзвітності після **<AU-01_ODP[06] подій>**;
	AU-01(c)[02][01]	переглядається та оновлюється поточні процедури аудиту та підзвітності з **<AU-01_ODP[07] частота>**;
	AU-01(c)[02][02]	переглядається та оновлюється поточні процедури аудиту та підзвітності після **<AU-01_ODP[08] подій>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури аудиту та підзвітності; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику аудиту та підзвітності; персонал, відповідальний за інформаційну безпеку].	

AU-02	**ПОДІЇ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-02_ODP[01]	**визначено типи подій, які система може реєструвати для**

		підтримки функції аудиту;
	AU-02_ODP[02]	**визначено типи подій (підмножина AU-02_ODP[01]) що підлягають аудиту у системі;**
	AU-02_ODP[03]	**визначено частоту або ситуацію, що вимагає проведення аудиту для кожної ідентифікованої події;**
	AU-02_ODP[04]	**частота перегляду та оновлення типів подій, обраних для журналювання;**
	AU-02(a)	**<AU-02_ODP[01] типи подій>**, які система здатна реєструвати, визначено для підтримки функції аудиту;
	AU-02(b)	функція аудиту безпеки координується з іншими підрозділами організації, які вимагають інформації, пов'язаної з аудитом, длдля посилення взаємної підтримки та допомоги у виборі типів подій, що перевіряються;
	AU-02(c)[01]	Типи подій **<AU-02_ODP[02] (підмножина AU-02_ODP[01])>** визначаються для реєстрації у системі;
	AU-02(c)[02]	зазначені типи подій реєструються у системі **<AU-02_ODP[03] частота або ситуація>**;
	AU-02(d)	надається обґрунтування, чому типи подій, що перевіряються, вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов’язаних з безпекою та конфіденційністю
	AU-02(e)	переглядаються та оновлюються типи подій, вибрані для реєстрації, **<AU-02_ODP[04] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика аудиту та підзвітності; процедури вирішення подій аудиту; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; події аудиту системи; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації з обов'язками інформаційної безпеки; системні / мережеві адміністратори]. **Перевірка**: [ВИБІР: Автоматизовані механізми, що реалізують аудит системи].	

AU-02(01)	**ПОДІЇ АУДИТУ - УЗАГАЛЬНЕННЯ ЗАПИСІВ ПРО АУДИТ З ДЕКІЛЬКОХ ДЖЕРЕЛ**
	[Вилучено: Включено в AU-12].

AU-02(02)	ПОДІЇ АУДИТУ - ВИБІР ПОДІЇ АУДИТУ ЗА КОМПОНЕНТАМИ
	[Вилучено: Включено в AU-12].

AU-02(03)	ПОДІЇ АУДИТУ - ПЕРЕГЛЯД ТА ОНОВЛЕННЯ
	[Вилучено: Включено в AU-02].

AU-02(04)	ПОДІЇ АУДИТУ - ПРИВІЛЕЙОВАНІ ФУНКЦІЇ
	[Вилучено: Включено в AC-06(09)].

AU-03	ЗМІСТ ЗАПИСІВ АУДИТУ	
	МЕТА ОЦІНКИ: Визначте, чи:	
	AU-03(a)	записи аудиту містять інформацію, яка встановлює який тип події стався;
	AU-03(b)	записи аудиту містять інформацію, яка встановлює коли подія сталася;
	AU-03(c)	записи аудиту містять інформацію, яка встановлює де відбулася подія;
	AU-03(d)	записи аудиту містять інформацію, яка встановлює джерело події;
	AU-03(e)	записи аудиту містять інформацію, яка встановлює наслідки події;
	AU-03(f)	записи аудиту містять інформацію, яка встановлює результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються змісту записів аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік визначених організацією заходів аудиту; записи аудиту системи; повідомлення про випадки в системі; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації з обов'язками інформаційної безпеки; системні або мережеві адміністратори]. **Перевірка**: [ВИБІР: Автоматизовані механізми, що реалізують аудит системи певних подій].	

AU-03(01)	ЗМІСТ ЗАПИСІВ АУДИТУ - ДОДАТКОВА ІНФОРМАЦІЯ ПРО АУДИТ

	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-03(01)_ODP	**визначено додаткову інформацію, яка має бути включена до записів аудиту;**
	AU-03(01)	сформовані записи аудиту містять наступну **<AU-03(01)_ODP додаткова інформація>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються змісту записів аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік визначених організацією заходів аудиту; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; прсонал організаціїз обов'язками пов'язаними з інформаційною безпекою; системні або мережеві адміністратори; розробники системи]. **Перевірка**: [ВИБІР: Можливість аудиту системи].	

AU-03(02)	**ЗМІСТ ЗАПИСІВ АУДИТУ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ ПЛАНОВАНИМ ЗМІСТОМ ЗАПИСІВ АУДИТУ**
	[Вилучено: Включено до PL-09]

AU-03(03)	**ЗМІСТ ЗАПИСІВ АУДИТУ - ОБМЕЖЕННЯ ЕЛЕМЕНТІВ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-03(03)_ODP	**визначаються елементи, визначені в оцінці ризику конфіденційності;**
	AU-03(03)	інформація, що ідентифікує особу, яка міститься в записах аудиту, обмежується **<AU-03(03)_ODP елементами>**, визначеними в оцінці ризиків конфіденційності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика аудиту та підзвітності; процедури, пов'язані з можливостями зберігання аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; вимоги до зберігання записів аудиту; можливість зберігання записів аудиту для компонентів системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації з обов'язками інформаційної безпеки; системні або	

	мережеві адміністратори; розробники системи]. **Перевірка**: [ВИБІР: Спроможність аудиту системи].

AU-04	**МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-04_ODP	**визначено вимоги до зберігання записів аудиту;**
	AU-04	розподілено ємність для зберігання записів аудиту відповідно до **<AU-04_ODP вимог>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика аудиту та підзвітності; процедури, пов'язані з можливостями зберігання аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; вимоги до зберігання записів аудиту; можливість зберігання записів аудиту для компонентів системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організаціїз обов'язками інформаційної безпеки; системні або мережеві адміністратори; розробники системи]. **Перевірка**: [ВИБІР: Перевірити ємність пам'яті запису та відповідні налаштування конфігурації].	

AU-04(01)	**МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ - ПЕРЕДАЧА ДО АЛЬТЕРНАТИВНОГО СХОВИЩА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-04(01)_ODP	визначено частоту завантаження записів аудиту на іншу систему чи носій інформації, з системи що перевіряється;
	AU-04(01)	записи аудиту вивантажуються на іншу систему або носій інформації, з системи, що перевіряється, з **<AU-04(01)_ODP частотою>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика аудиту та підзвітності; процедури, пов'язані з можливостями зберігання аудиту; процедури, спрямовані на передачу записів аудиту системи до вторинних або альтернативних систем; проєктна документація системи; налаштування конфігурації системи та супутня документація; журнали передач записів аудиту до вторинних або альтернативних систем; записи аудиту системи, передані вторинним системам; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за планування можливостей зберігання аудиту; персонал організації з обов'язками інформаційної без-	

	пеки; системні або мережеві адміністратори]. **Перевірка**: [ВИБІР: Автоматизовані механізми, що підтримують передачу записів аудиту на іншу систему].

AU-05	**РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-05_ODP[01]	**визначено персонал або ролі, які отримують сповіщення про збої в процесі обробки даних аудиту ;**
	AU-05_ODP[02]	**визначено період часу, протягом якого персонал або ролі отримують сповіщення про збої в процесі обробки даних аудиту;**
	AU-05_ODP[03]	**визначено додаткові дії, яких слід вжити у випадку збою в процесі обробки даних аудиту ;**
	AU-05(a)	**<AU-05_ODP[01] персонал або ролі>** отримують сповіщення у разі збою процесу обробки даних аудиту **<AU-05_ODP[02] періоду часу>;**
	AU-05(b)	**<AU-05_ODP[03] додаткові дії>** виконуються у разі збою процесу обробки даних аудиту**.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація системи; план захисту інформації; налаштування конфігурації системи та супутня документація; перелік персоналу, який повинен бути повідомлений у разі відмови обробки даних аудиту; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організаціїз обов'язками інформаційної безпеки; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують відповідь системи на помилки обробки даних аудиту].	

AU-05(01)	**РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-05(01)_ODP[01]	**визначено персонал або ролі, які мають бути попереджені, коли обсяг записів аудиту, що зберігаються, досягає максимуму місткості сховища.**

	AU-05(01)_ODP[02]	**визначено період часу, протягом якого визначений персонал або ролі будуть попереджені;**
	AU-05(01)_ODP[03]	**визначено відсоток максимальної ємності сховища для зберігання журналів аудиту;**
	AU-05(01)	попередження надається **<AU-05(01)_ODP[01] персоналу або ролям>** протягом **<AU-05(01)_ODP[02] періоду часу>**, коли виділений обсяг сховища журналів аудиту досягає **<AU-05(01)_ODP[03] відсотків>** від максимального обсягу сховища журналів аудиту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація системи; план захисту інформації; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації з обов'язками інформаційної безпеки; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують попередження про обмеження зберігання аудиту].	

AU-05(02)	**РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - ТРИВОЖНЕ СПОВІЩЕННЯ В РЕАЛЬНОМУ ЧАСІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-05(02)_ODP[01]	**визначено період реального часу, за який потрібно надсилати сповіщення при виникненні подій збою аудиту (визначених у AU-05(02)_ODP[03]);**
	AU-05(02)_ODP[02]	**визначено персонал або ролі, які мають бути сповіщені при виникненні подій збоїв в аудиті (визначених в AU-05(02)_ODP[03]);**
	AU-05(02)_ODP[03]	**визначено події, пов'язані зі збоями та помилками аудиту;**
	AU-05(02)	протягом **<AU-05(02)_ODP[01] періоду реального часу>** надається сповіщення **<AU-05(02)_ODP[02] персоналу або ролям>**, коли виникають **<AU-05(02)_ODP[03] події>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація системи; план захисту інформації; налаштування конфігурації системи та супутня документація; записи сповіщень або сповіщень у режимі реального часу, коли виникають збої в	

	обробці аудиту; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організаціїз обов'язками інформаційної безпеки; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують попередження аудиту в режимі реального часу, коли відбуваються пошкодження аудиту, визначені організацією].

AU-05(03)	**РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - НАЛАШТУВАННЯ ПОРОГОВОГО ОБСЯГУ ТРАФІКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-05(03)_ODP	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {відхилити; затримати};**
	AU-05(03)[01]	застосовуються налаштовані порогові значення обсягу трафіку комунікаційних мереж, що відображають обмеження на можливості аудиту;
	AU-05(03)[02]	мережевий трафік **<AU-05(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**, якщо обсяг мережевого трафіку перевищує налаштовані порогові значення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація системи; план захисту інформації; налаштування конфігурації системи та супутня документація; конфігурація порогів обсягу трафіку мережевих комунікацій; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Можливість системи, що реалізує налаштовані пороги обсягу трафіку].	

AU-05(04)	**РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - ВИМКНЕННЯ У РАЗІ ВІДМОВИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-05(04)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {повне вимикання системи; часткове вимикання системи; знижений режим роботи з обмеженням доступної/цільової функціональності};**

	AU-05(04)_ODP[02]	**визначено збої аудиту, які спричиняють зміну режиму роботи;**
	AU-05(04)	**<AU-05(04)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** викликається/викликаються у випадку **<AU-05(04)_ODP[02] збоїв аудиту>**, якщо не існує альтернативної можливості ведення аудиту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація системи; план захисту інформації; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Можливість автоматично викликати вимкнення системи або погіршення режиму роботи у випадку збою в обробці даних аудиту].	

AU-05(05)	**РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - МОЖЛИВІСТЬ АЛЬТЕРНАТИВНОГО ЖУРНАЛЮВАННЯ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-05(05)_ODP	**визначено альтернативний функціонал ведення журналу аудиту на випадок збою в роботі основної функції ведення журналу аудиту;**
	AU-05(05)	альтернативна можливість ведення журналу аудиту надається на випадок відмови основної можливості ведення журналу аудиту, який реалізує **<AU-05(05)_ODP визначений альтернативний функціонал ведення журналу аудиту>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на реагування на помилки обробки аудиту; проєктна документація системи; план захисту інформації; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Альтернативна можливість ведення журналу аудиту].	

AU-06	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-06_ODP[01]	**визначено частоту, з якою переглядаються та аналізуються записи аудиту системи;**
	AU-06_ODP[02]	**визначена неналежна або незвична діяльність;**
	AU-06_ODP[03]	**визначено персонал або ролі які отримують результати оглядів та аналізів системних записів;**
	AU-06(a)	записи аудиту системи переглядаються та аналізуються **<AU-06_ODP[01] частота>** для виявлення ознак **<AU-06_ODP[02] неналежної або незвичної діяльності>** та потенційного впливу неналежної або незвичної діяльності;
	AU-06(b)	звіт аудиту відправляється **<AU-06_ODP[03] персоналу або ролям>**;
	AU-06(c)	рівень перевірки, аналізу та звітування записів аудиту в системі коригується у разі зміни ризиків на основі інформації правоохоронних органів, розвідувальної інформації або інших достовірних джерел інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; звіти про результати аудиту; записи про дії, вжиті у відповідь на огляди / аналітичні записи аудиту; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит, аналіз та звітність; персонал організації, відповідальний за інформаційну безпеку].	

AU-06(01)	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - АВТОМАТИЗОВАНА ІНТЕГРАЦІЯ ПРОЦЕСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-06(01)_ODP	**визначено автоматизовані механізми, що використовуються для інтеграції процесів перегляду, аналізу та звітності записів аудиту;**
	AU-06(01)	процеси перегляду, аналізу та звітності інтегровані з використанням **<AU-06(01)_ODP автоматизованих механізмів>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; процедури щодо розслідування та реагування на підозрілі дії; проєктна документація системи; налаштування конфігурації систе-	

	ми та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит, аналіз та звітність; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що інтегрують процеси огляду, аналізу та звітності аудиту].

AU-06(02)	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - АВТОМАТИЗОВАНІ СПОВІЩЕННЯ ПРО ПОРУШЕННЯ БЕЗПЕКУ**
	[Вилучено: Включено до SI-4]

AU-06(03)	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ЗІСТАВЛЯННЯ СХОВИЩ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-06(03)	аналізуються та зіставляються записи аудиту в різних сховищах, задля забезпечення ситуативної обізнаності в масштабах організації
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи в різних сховищах; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит, аналіз та звітність; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують аналіз та кореляцію записів аудиту].	

AU-06(04)	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ЦЕНТРАЛІЗОВАНИЙ ПЕРЕГЛЯД ТА АНАЛІЗ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-06(04)[01]	забезпечино можливість централізованого перегляду та аналізу записів аудиту з декількох компонентів у системі.
	AU-06(04)[02]	впроваджено можливість централізованого перегляду та аналізу записів аудиту з декількох компонентів у системі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосу-	

	ються огляду, аналізу та звітності аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; план захисту інформації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит, аналіз та звітність; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Здатність системи до централізації огляду та аналізу записів аудиту].

AU-06(05)	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ІНТЕГРОВАНИЙ АНАЛІЗ ЗАПИСІВ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-06(05)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {інформація про сканування вразливостей; дані про продуктивність; інформація про моніторинг системи; <AU-06(05)_ODP[02] дані/інформація, зібрана з інших джерел>};**
	AU-06(05)_ODP[02]	**визначено дані/інформацію, зібрані з інших джерел, що підлягають аналізу (якщо вони були обрані);**
	AU-06(05)	аналіз записів аудиту інтегровано з аналізом **<AU-06(05)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**, для подальшого підвищення здатності виявляти неприйнятну або незвичайну діяльність.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; інтегрований аналіз записів аудиту, інформація про сканування вразливості, дані про продуктивність, інформація про моніторинг мережі та супутня документація; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має перевірки аудиту, аналіз та звітність; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість інтегрувати аналіз записів аудиту з аналізом джерел даних або інформації].	

AU-06(06)	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - КОРЕЛЯЦІЯ З ФІЗИЧНИМ МОНІТОРИНГОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-06(06)	інформація з записів аудиту співвідноситься з інформацією,

		отриманою в результаті моніторингу фізичного доступу, для подальшого посилення здатності виявляти підозрілу, невідповідну, незвичну або зловмисну діяльність.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; процедури щодо моніторингу фізичного доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; документація, що надає докази співвіднесеної інформації, отриманої з записів аудите та записів моніторингу фізичного доступу; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має перевірки аудиту, аналіз та звітність; персонал організації, відповідальний за контроль фізичного доступу; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість співвідносити інформацію з записів аудиту з інформацією з моніторингу фізичного доступу].	

AU-06(07)	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ДОЗВОЛЕНІ ДІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-06(07)_ODP	вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {процес системи; роль; користувач};
	AU-06(07)	визначено дозволені дії для кожного **<AU-06(07)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**, пов'язані з переглядом, аналізом та поданням інформації про аудит.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються процесу, ролі та / або дозволених користувачами дій з огляду аудиту, аналізу та звітності; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за аудит, аналіз та звітність; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують дозволені дії щодо огляду, аналізу та звітності інформації аудиту].	

AU-06(08)	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - АНАЛІЗ ПОВНОГО ТЕКСТУ ПРИВІЛЕЙОВАНИХ КОМАНД**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-06(08)	виконується повний аналіз тексту привілейованих команд аудиту у фізично окремому компоненті чи підсистемі або іншій системі, яка може виконувати такий аналіз.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБРАТИ З: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; проєктна документація інформаційної системи; налаштування конфігурації інформаційної системи та супутня документація; інструменти аналізу тексту; документація з аналізу тексту перевірених привілейованих команд; план безпеки; інші відповідні документи чи записи]. **Співбесіда:** [ВИБРАТИ З: Організаційний персонал, який має обов'язки з аудиту, аналізу та звітності; організаційний персонал, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБРАТИ З: Автоматизовані механізми, що реалізують можливість виконувати повний аналіз тексту аудитованих команд привілеїв].

AU-6(9)	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - КОРЕЛЯЦІЯ З ІНФОРМАЦІЄЮ З НЕТЕХНІЧНИХ ДЖЕРЕЛ**	
	МЕТА ОЦІНКИ: Визначте, чи:	
	AU-06(09)	зіставляється інформація з нетехнічних джерел з інформацією аудиту з метою посилення організаційної обізнаності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються огляду, аналізу та звітності аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; документація, що забезпечує докази співвіднесеної інформації, отриманої з записів аудиту та визначених організацією нетехнічних джерел; перелік видів інформації з нетехнічних джерел для співвідношення з інформацією аудиту; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит, аналіз та звітність; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість співвідносити інформацію з нетехнічних джерел].	

AU-06(10)	**ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - РЕГУЛЮВАННЯ РІВНЯ АУДИТУ**
	[Вилучено: Включено до AU-06]

AU-07	**СКОРОЧЕННЯ ЗАПИСІВ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ**
	МЕТА ОЦІНКИ: Визначити, чи:

	AU-07(a)[01]	забезпечено можливість скорочення записів перевірок аудитом та звітів, до рівня що підтримує перевірку, аналіз і звітність аудиту на вимогу та розслідування (постфактум) інцидентів безпеки;
	AU-07(a)[02]	реалізовано можливість скорочення записів перевірок аудитом та звітів, до рівня що підтримує перевірку, аналіз і звітність аудиту на вимогу та розслідування (постфактум) інцидентів безпеки;
	AU-07(b)[01]	забезпечено можливість скорочення записів перевірок аудитом та звітів, які не змінюють оригінальний зміст або час упорядкування записів аудиту;
	AU-07(b)[02]	реалізовано можливість скорочення записів перевірок аудитом та звітів, які не змінюють оригінальний зміст або час упорядкування записів аудиту;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо скорочення аудиту та формування звітів; проєктна документація системи; налаштування конфігурації системи та супутня документація; засоби зменшення аудиту, огляду, аналізу та звітності; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має обов'язки з скорочення аудиту та створенням звітів; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Скорочення аудиту та створення звітів].	

AU-07(01)	**СКОРОЧЕННЯ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ - АВТОМАТИЧНА ОБРОБКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-07(01)_ODP	**визначено поля в записах аудиту, які можна обробляти, сортувати або шукати;**
	AU-7(01)[01]	забезпечити можливість обробки записів аудиту для подій, що представляють інтерес, на основі **<AU-07(01)_ODP полей в записах аудиту>**
	AU-7(01)[02]	реалізувати можливість обробки записів аудиту для подій, що представляють інтерес, на основі **<AU-07(01)_ODP полей в записах аудиту>**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо скорочення аудиту та формування звітів; проєктна документація системи; налаштування конфігурації системи та супутня документація; засоби зменшення аудиту, огляду, аналізу та звітності; критерії (поля) аудиту, що встановлюють події; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має обов'язки з скорочення ауди-	

	ту та створенням звітів; персонал організації, відповідальний за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Скорочення аудиту та створення звітів].

AU-07(02)	**СКОРОЧЕННЯ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ - АВТОМАТИЧНЕ СОРТУВАННЯ ТА ПОШУК**
	[Вилучено: Включено до AU-07(01)]

AU-08	**ПОЗНАЧКА ЧАСУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-08_ODP	**визначено деталізацію вимірювання часу для часових позначок записів аудиту;**
	AU-08(a)	внутрішній системний годинник використовується для створення позначок часу для записів аудиту;
	AU-08(b)	позначки часу застосовуються для записів аудиту, які відповідають **<AU-08_ODP деталізація вимірювання часу>** і які використовують всесвітній координований час, мають фіксоване місцеве зміщення місцевого часу від всесвітнього координованого часу або включають зміщення місцевого часу як частину позначки часу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються генерації часових позначок; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують генерацію часових позначок].	

AU-08(01)	**ПОЗНАЧКА ЧАСУ - СИНХРОНІЗАЦІЯ З АВТОРИТЕТНИМ ДЖЕРЕЛОМ ЧАСУ**
	[Вилучено: Включено до SC-45(01)]

AU-08(02)	**ПОЗНАЧКА ЧАСУ - ВТОРИННЕ АВТОРИТЕТНЕ ДЖЕРЕЛО ЧАСУ**
	[Вилучено: Включено до SC-45(02)]

AU-09	**ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-09_ODP	**визначено персонал або ролі, які мають бути сповіщені при виявленні несанкціонованого доступу, зміни або видалення інформації аудиту;**
	AU-09(a)	інформація про аудит та інструменти журналювання аудиту захищені від несанкціонованого доступу, зміни та видалення;
	AU-09(b)	**<AU-09_ODP персонал або ролі>** отримують сповіщення при виявленні несанкціонованого доступу, зміни або видалення інформації аудиту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист інформації аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація, записи аудиту системи; інструменти аудиту; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують захист інформації аудиту].	

AU-09(01)	**ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - АПАРАТНІ НОСІЇ ІНФОРМАЦІЇ ОДНОРАЗОВОГО ЗАПИСУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-09(01)	журнали аудиту записані на апаратні носії інформації з одноразовим записом.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист інформації аудитц; проєктна документація системи; налаштування апаратних засобів системи; налаштування конфігурації системи та супутня документація; зовнішні носій інформації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Система, що зберігає контрольні журнали.].	

AU-09(02)	**ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ЗБЕРІГАННЯ НА ОКРЕМИХ ФІЗИЧНИХ СИСТЕМАХ АБО КОМПОНЕНТАХ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-09(02)_ODP	**визначено частоту з якою необхідно зберігати записи аудиту;**
	AU-09(02)	зберігати записи аудиту з **<AU-09(02)_ODP частотою>** у репозиторії, який є частиною іншої системи або компонента системи, не частиною системи або компонента системи, який перевіряється.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на захист інформації аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; система або зовішній носій інформації, що зберігають резервні копії записів аудиту системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують резервне копіювання записів аудиту].	

AU-09(03)	**ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - КРИПТОГРАФІЧНИЙ ЗАХИСТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-09(03)	впроваджено криптографічні механізми для захисту цілісності інформації аудиту
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист інформації аудиту; проєктна документація системи; налаштування апаратних засобів системи; налаштування конфігурації системи та супутня документація, записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Криптографічні механізми, що захищають цілісність інформації аудиту та інструментів].	

AU-09(04)	**ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ДОСТУП, ЯКИЙ НАДАЄТЬСЯ ЧЕРЕЗ ЧЛЕНСТВО В ПІДМНОЖИНИ ПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	AU-09(04)_ODP	визначено підмножину привілейованих користувачів;
	AU-09(04)	авторизувати доступ до управління функціональністю аудиту тільки для **<AU-09(04)_ODP підмножини привілейованих користувачів>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист інформації аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація, список привілейованих користувачів з доступом до управління функціями аудиту; авторизація доступу; список контролю доступу; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми управління доступом до функцій аудиту].	

AU-09(05)	**ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ПОДВІЙНА АВТОРИЗАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-09(05)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {переміщення; видалення};**
	AU-09(05)_ODP[02]	**визначено інформацію аудиту, для якої має бути застосована подвійна авторизація;**
	AU-09(05)	подвійна авторизація застосовується для **<AU-09(05)_ODP[01] ВИБІРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** з **<AU-09(05)_ODP[02] інформації аудиту>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист інформації аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують виконання подвійної авторизації].	

AU-09(06)	ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ДОСТУП ТІЛЬКИ ДЛЯ ЧИТАННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-09(06)_ODP	визначено підмножину привілейованих користувачів для яких доступ авторизовано тільки для читання.
	AU-09(06)	авторизувати доступ лише для читання інформації аудиту для **<AU-09(06)_ODP підмножини привілейованих користувачів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист інформації аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація, список привілейованих користувачів із доступом до інформації аудиту лише для читання; авторизація доступу; список контролю доступу; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми управління доступом до інформації аудиту].	

AU-09(07)	ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ЗБЕРІГАННЯ НА КОМПОНЕНТІ ІНШОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-09(07)	інформація про аудит зберігається на компоненті, що працює з іншою операційною системою, ніж система або компонент, який проходить аудит
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; політика та процедури контролю доступу; процедури, спрямовані на захист інформації аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація, список привілейованих користувачів із доступом до інформації аудиту лише для читання; авторизація доступу; список контролю доступу; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аудит та підзвітність; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми управління доступом до інформації аудиту].	

AU-10	НЕСПРОСТОВНІСТЬ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-10_ODP	**визначено дії, на які поширюється принцип неспростовності;**
	AU-10	надаються неспростовні докази того, що особа (або процес, що діє від імені особи) виконала **<AU-10_ODP дії>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо неспростовності; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість неспростовності].	

AU-10(01)	НЕСПРОСТОВНІСТЬ - АСОЦІАЦІЯ ІДЕНТИЧНОСТІ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-10(01)_ODP	**визначено міцність зв'язку між особистістю джерела інформації та інформацією;**
	AU-10(01)(a)	особистість джерела інформації зв'язується з інформацією з **<AU-10(01)_ODP сила зв'язування>**;
	AU-10(01)(b)	впроваджено засоби, якими уповноважені особи можуть визначити особу виробника інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо неспростовності; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість неспростовності].	

AU-10(02)	НЕСПРОСТОВНІСТЬ - РАТИФІКАЦІЯ ПРИВ'ЯЗКИ ІНФОРМАЦІЇ ПРО ІДЕНТИЧНІСТЬ ВИРОБНИКА

	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-10(02)_ODP[01]	**визначено частоту, з якою необхідно підтверджувати прив'язку інформації про ідентичність джерела до інформації;**
	AU-10(02)_ODP[01]	**визначено дії, які мають бути виконані у разі помилки перевірки;**
	AU-10(02)(a)	прив'язка інформації про ідентичність джерела до інформації підтверджується з **<AU-10(02)_ODP[01] частотою>**;
	AU-10(02)(b)	виконуються **<AU-10(02)_ODP[02] дії>** у разі помилки перевірки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо неспростовності; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість неспростовності].	

AU-10(03)	**НЕСПРОСТОВНІСТЬ - ЛАНЦЮЖОК ЗБЕРЕЖЕННЯ ДОКАЗІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-10(03)	підтримується перегляд і випуск ідентичності та повноважень у межах встановленого ланцюжка збереження доказів для всієї переглянутої або оприлюдненої інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо неспростовності; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи оглядів та випусків; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість неспростовності].	

AU-10(04)	**НЕСПРОСТОВНІСТЬ - ВАЛІДАЦІЯ ЗВ'ЯЗКУ ІДЕНТИЧНОСТІ ПЕРЕГЛЯ-**

	ДАЧА ІНФОРМАЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-10(04)_ODP[01]	**визначено домени безпеки, для яких прив'язка особи рецензента інформації до інформації повинна бути підтверджена в точках передачі або видачі;**
	AU-10(04)_ODP[02]	**визначено дії, які мають бути виконані у випадку помилки перевірки;**
	AU-10(04)(a)	прив'язка особистості рецензента інформації до інформації в точках передачі або видачі до її випуску або передачі між **<AU-10(04)_ODP[01] доменами безпеки>** підтверджується**;**
	AU-10(04)(b)	**<AU-10(04)_ODP[02] дії>** виконуються у випадку помилки перевірки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо неспростовності; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи перевірки; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість неспростовності].	

AU-10(05)	**НЕСПРОСТОВНІСТЬ - ЦИФРОВІ ПІДПИСИ**
	[Вилучено: Включено до SI-07]

AU-11	**ЗБЕРЕЖЕННЯ ЗАПИСІВ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-11_ODP	**визначено період часу для зберігання записів аудиту, який узгоджується з політикою зберігання записів;**
	AU-11	записи аудиту зберігаються впродовж **<AU-11_ODP період часу>**, щоб забезпечити підтримку розслідування (постфактум) інцидентів безпеки та конфіденційності, а також відповідати нормативним та вимогам організації щодо збереження даних аудиту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; політика та процедури збереження записів аудиту; план захисту інформації; визначений організацією термін збері-	

	гання записів аудиту; архіви записів аудиту; журнали аудиту; записи аудиту; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за збереження записів аудиту; персонал організації, відповідальний за захист інформації; системні або мережеві адміністратори].

AU-11(01)	**ЗБЕРЕЖЕННЯ ЗАПИСІВ АУДИТУ - ДОВГОСТРОКОВА МОЖЛИВІСТЬ ОТРИМАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-11(01)_ODP	**визначено заходи, необхідні для реалізації довгострокової можливості отримання записів аудиту**
	AU-11(01)	впровадити **<AU-11(01)_ODP заходи>**, щоб гарантувати, що довгострокові записи аудиту, можуть бути отримані.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; політика та процедури збереження записів аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; архіви записів аудиту; журнали аудиту; записи аудиту; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за збереження записів аудиту; персонал організації, відповідальний за захист інформації; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість збереження записів аудиту]**.**	

AU-12	**ГЕНЕРАЦІЯ ДАНИХ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-12_ODP[01]	**визначено компоненти системи, які забезпечують можливість генерації записів аудиту для типів подій (визначених у AU-02_ODP[02]);**
	AU-12_ODP[02]	**визначено персонал або ролі, яким дозволено обирати типи подій, що мають реєструватися певними компонентами системи;**
	AU-12(a)	можливість генерації записів аудиту для типів подій, які система здатна перевіряти (визначених у AU-02_ODP[01]), забезпечується **<AU-12_ODP[01] компонентами системи>**;
	AU-12(b)	**<AU-12_ODP[02] персонал або ролі>** може/можуть вибирати типи подій, які будуть реєструватися певними компонентами системи;

	AU-12(c)	згенеровано записи аудиту для типів подій, визначених у AU-02_ODP[02], які включають вміст записів аудиту, визначений у AU-03.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження: [**ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на створення записів аудиту; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік подій аудиту; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за створення записів аудиту; персонал організації, відповідальний за захист інформації; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість створення записів аудиту].	

AU-12(01)	**ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - ЗАГАЛЬНОСИСТЕМНИЙ ТА СИНХРОНІЗОВАНИЙ ЗА ЧАСОМ ЖУРНАЛУ АУДИТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-12(01)_ODP[01]	**визначено компоненти системи, з яких записи аудиту мають бути зібрані в загальносистемний (логічний або фізичний) журнал аудиту;**
	AU-12(01)_ODP[01]	**визначено рівень взаємозв'язку між мітками часу окремих записів у журналах аудиту;**
	AU-12(01)	записи аудиту з **<AU-12(01)_ODP[01] компонентів системи>** збираються у загальносистемний (логічний або фізичний) журнал аудиту, який синхронізується у часі в межах **<AU-12(01)_ODP[02] рівня взаємозв'язку>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на створення записів аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; загальносистемний журнал аудиту (логічний або фізичний); записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за створення записів аудиту; персонал організації, відповідальний за захист інформації; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість створення записів аудиту].	

AU-12(02)	**ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - СТАНДАРТИЗОВАНІ ФОРМАТИ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	AU-12(02)	створюється загальносистемний (логічний) журнал аудиту, що складається з записів аудиту в стандартизованому форматі
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на створення записів аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; загальносистемний журнал аудиту (логічний або фізичний); записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за створення записів аудиту; персонал організації, відповідальний за захист інформації; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість створення записів аудиту].	

AU-12(03)	**ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - ЗМІНИ, ЩО ВНОСЯТЬ АВТОРИЗОВАНІ ОСОБИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-12(03)_ODP[01]	**визначено осіб або ролі, яким дозволено змінювати аудит компонентів системи;**
	AU-12(03)_ODP[02]	**визначено компоненти системи, на яких має виконуватися аудит;**
	AU-12(03)_ODP[03]	**визначено критерії вибору подій;**
	AU-12(03)_ODP[04]	**визначено часові пороги, в яких мають змінюватися аудит;**
	AU-12(03)[01]	забезпечено можливість **<AU-12(03)_ODP[01] особам або ролям>** змінювати аудит на **<AU-12(03)_ODP[02] компонентах системи>** на основі **<AU-12(03)_ODP[03] обраних критеріїв події>** у межах **<AU-12(03)_ODP[04] часових порогів>**;
	AU-12(03)[02]	реалізовано можливість **<AU-12(03)_ODP[01] особам або ролям>** змінювати аудит на **<AU-12(03)_ODP[02] компонентах системи>** на основі **<AU-12(03)_ODP[03] обраних критеріїв події>** у межах **<AU-12(03)_ODP[04] часових порогів>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на створення записів аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; сформований список осіб або по-	

	сад, уповноважених змінювати аудит, який слід виконувати; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за створення записів аудиту; персонал організації, відповідальний за захист інформації; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість створення записів аудиту].

AU-12(04)	**ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - АУДИТ ЗАПИТІВ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-12(04)[01]	забезпечена можливості аудиту параметрів подій запитів користувачів для наборів даних, що містять персональну ідентифікаційну інформацію.
	AU-12(04)[02]	реалізувана можливості аудиту параметрів подій запитів користувачів для наборів даних, що містять персональну ідентифікаційну інформацію.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, спрямовані на створення записів аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; сформований список осіб або посад, уповноважених змінювати аудит, який слід виконувати; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за створення записів аудиту; персонал організації, відповідальний за захист інформації; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість створення записів аудиту].	

AU-13	**МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-13_ODP[01]	**визначено інформацію з відкритих джерел та/або інформаційні сайти, що підлягають моніторингу на наявність доказів неавторизованого розголошення конфіденційної інформації;**
	AU-13_ODP[02]	**визначено частоту моніторингу інформації з відкритих джерел та/або інформаційних сайтів на наявність доказів неавторизованого розголошення конфіденційної інформації;**
	AU-13_ODP[03]	**визначено персонал або ролі, які мають бути повідомлені в**

		разі виявлення розголошення інформації;
	AU-13_ODP[04]	**визначено додаткові дії, які необхідно вжити у разі виявлення розголошення інформації;**
	AU-13(a)	**<AU-13_ODP[01] інформація з відкритих джерел та/або інформаційні сайти>** відстежуються **<AU-13_ODP[02] частота>** на наявність доказів неавторизованого розголошення конфіденційної інформації;
	AU-13(b)[01]	**<AU-13_ODP[03] персонал або ролі>** буде повідомлено, якщо буде виявлено розголошення інформації;
	AU-13(b)[02]	**<AU-13_ODP[04] додаткові дії>** вживаються, якщо виявлено розголошення інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо моніторингу розкриття інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи моніторингу; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за моніторинг інформації з відкритим кодом та / або інформаційних сайтів; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують моніторинг для розкриття інформації].	

AU-13(01)	**МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ - ВИКОРИСТАННЯ АВТОМАТИЧНИХ ЗАСОБІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-13(01)_ODP	**визначено автоматизовані механізми моніторингу інформації з відкритих джерел та інформаційних сайтів;**
	AU-13(01)	моніторинг інформації з відкритих джерел та інформаційних сайтів здійснюється за допомогою **<AU-13(01)_ODP автоматизовані механізми>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо моніторингу розкриття інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; автоматизовані засоби моніторингу; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за моніторинг розкриття інформації; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують моніторинг для	

	розкриття інформації].

AU-13(02)	МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ - ОГЛЯД САЙТІВ, ЩО ПІДЛЯГАЮТЬ МОНІТОРИНГУ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-13(02)_ODP	визначено частоту з якою проводять огляд відкритих інформаційних сайтів, що підлягають моніторингу
	AU-13(02)	проводиться огляд відкритих інформаційних сайтів, що підлягають моніторингу з **<AU-13(02)_ODP частотою>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо моніторингу розкриття інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; огляди інформаційних сайтів з відкритим кодом, що контролюються; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за моніторинг інформаційних сайтів з відкритим кодом; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують моніторинг для розкриття інформації].	

AU-13(03)	МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ - АВТОРИЗОВАНЕ КОПІЮВАННЯ ІНФОРМАЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-13(03)	застосовуються методи, процеси та інструменти виявлення, щоб визначити, чи не копіюють зовнішні суб'єкти інформацію організації в несанкціонований спосіб.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; план захисту інформації; план забезпечення конфіденційності; процедури моніторингу розкриття інформації; процедури реплікації інформації; проектна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; навчальні ресурси для персоналу щодо розпізнавання несанкціонованого використання інформації організації; інші відповідні документи чи записи.]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за моніторинг несанкціонованого копіювання інформації; персонал організації, відповідальний за безпеку інформації та конфіденційність]. **Перевірка:** [ВИБІР: Інструменти виявлення несанкціонованої копіювання ін-	

	формації].

AU-14	АУДИТ СЕСІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-14_ODP[01]	**визначено користувачів або ролі, які можуть перевіряти вміст сесії користувача;**
	AU-14_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {збору/запису або перегляду/прослуховування};**
	AU-14_ODP[03]	**визначено обставини, за яких вміст сесії користувача може бути перевірено;**
	AU-14(a)[01]	**<AU-14_ODP[01] користувачам або ролям>** надається можливість **<AU-14_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** вмісту сесії користувача за <AU-14_ODP[03] обставин>;
	AU-14(a)[02]	реалізовано можливість для **<AU-14_ODP[01] користувачів або ролей> <AU-14_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** вмісту сесії користувача за **<AU-14_ODP[03] обставин>**;
	AU-14(b)[01]	діяльність з аудиту сесій розробляється після консультацій з юристом та відповідно до чинних законів, розпоряджень, директив, нормативних актів, політик, стандартів та вказівок;
	AU-14(b)[02]	діяльність з аудиту сесій інтегрується після консультацій з юристом та відповідно до чинних законів, розпоряджень, директив, нормативних актів, політик, стандартів та вказівок;
	AU-14(b)[03]	діяльність з аудиту сесій використовується після консультацій з юристом та відповідно до чинних законів, розпоряджень, директив, нормативних актів, політик, стандартів та вказівок;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо аудиту сесії користувача; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість аудиту сесій користувача].	

AU-14(01)	АУДИТ СЕСІЇ - СИСТЕМА ЗАПУСКУ
	МЕТА ОЦІНКИ: Визначити, чи:

	AU-14(01)	аудит сесії при запуску системи автоматично ініціюється
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо аудиту сесій користувача; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість аудиту сесій користувача].	

AU-14(02)	**АУДИТ СЕСІЇ - ЗАХОПЛЕННЯ ТА ЗАПИС ІНФОРМАЦІЇ**
	[Вилучено: Включено до AU-14]

AU-14(03)	**АУДИТ СЕСІЇ - ВІДДАЛЕНИЙ ПЕРЕГЛЯД ТА ПРОСЛУХОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-14(03)[01]	забезпечується можливість для авторизованих користувачів віддалено переглядати та прослуховувати вміст, пов'язаний із встановленою сесією користувача, в режимі реального часу;
	AU-14(03)[02]	реалізовано можливість для авторизованих користувачів віддалено переглядати та прослуховувати вміст, пов'язаний із встановленою сесією користувача, в режимі реального часу;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури щодо аудиту сесії користувача; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість аудиту сеансів користувача].	

AU-15	**АЛЬТЕРНАТИВНА МОЖЛИВІСТЬ АУДИТУ**
	[Вилучено: Включено до AU-05(05)]

AU-16	**МІЖОРГАНІЗАЦІЙНИЙ АУДИТ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-16_ODP[01]	**визначено методи для координації інформації серед зовнішніх організацій, коли інформація аудиту передається через (за) межі організації (системи);**
	AU-16_ODP[02]	**визначено інформацію для координації інформації серед зовнішніх організацій, коли інформація аудиту передається через (за) межі організації (системи);;**
	AU-16	організація використовує **<AU-16_ODP[01] методи>** для координації **<AU-16_ODP[02] інформації>** серед зовнішніх організацій, коли інформація аудиту передається через (за) межі організації (системи).
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються методів координації інформації аудиту серед зовнішніх організацій; проєктна документація системи; налаштування конфігурації системи та супутня документація; методи координації інформації аудиту серед зовнішніх організацій; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за координацію інформації аудиту серед зовнішніх організацій; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують міжорганізаційний аудит (якщо застосовується)].	

AU-16(01)	**МІЖОРГАНІЗАЦІЙНИЙ АУДИТ - ЗБЕРЕЖЕННЯ ІДЕНТИЧНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-16(01)	вимагається, щоб ідентичність особистості зберігалася в міжорганізаційних журналах аудиту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури розв'язання питань міжорганізаційного аудиту; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за міжорганізаційний аудит; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що впроваджують міжорганізаційний аудит (якщо застосовується)].	

AU-16(02)	**МІЖОРГАНІЗАЦІЙНИЙ АУДИТ - ОБМІН ІНФОРМАЦІЄЮ АУДИТУ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-16(02)_ODP[01]	**визначено організації до яких надають інформацію про міжорганізаційний аудит**
	AU-16(02)_ODP[02]	**визначено міжорганізаційну угоду про розподіл.**
	AU-16(02)	надати інформацію про міжорганізаційний аудит до **<AU-16(02)_ODP[01] організацій>** організацією на основі **<AU-16(02)_ODP[02] угоди про розподіл>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; процедури, що стосуються міжорганізаційного обміну інформацією аудиту; міжорганізаційні угоди про обмін; угоди про обмін даними; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обмін інформацією міжорганізаційного аудиту; персонал організації, відповідальний за інформаційну безпеку].	

AU-16(03)	**МІЖОРГАНІЗАЦІЙНИЙ АУДИТ - РОЗМЕЖУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	AU-16(03)_ODP	**визначено заходи для розмежування окремих осіб від інформації аудиту, що передається в межах організації;**
	AU-16(03)	<AU-16(03)_ODP заходи> впроваджуються для того, щоб розмежування окремих осіб від інформації аудиту, що передається в межах організації;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика аудиту та підзвітності; план захисту інформації; план забезпечення конфіденційності; процедури, що стосуються міжорганізаційного обміну інформацією аудиту; політика та/або процедури щодо деідентифікації PII; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; інші відповідні документи або записи.]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обмін інформацією міжорганізаційного аудиту; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Механізми реалізації розмежування].	

IV. КЛАС ЗАХОДІВ ЗАХИСТУ СА – ОЦІНЮВАННЯ, АКРЕДИТАЦІЯ ТА МОНІТОРИНГ

CA-01	**ПОЛІТИКА І ПРОЦЕДУРИ ОЦІНЮВАННЯ, АКРЕДИТАЦІЯ ТА МОНІТОРИНГ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-01_ODP[01]	**визначено персонал або ролі, серед яких має бути поширена політика оцінювання, авторизації та моніторингу;**
	CA-01_ODP[02]	**визначено персонал або ролі, серед яких мають бути поширені процедури оцінювання, авторизації та моніторингу;**
	CA-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	CA-01_ODP[04]	**визначено посадову особу, яка управлятиме розробкою, документуванням і розповсюдженням політики та процедур оцінювання, авторизації та моніторингу;**
	CA-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика оцінювання, авторизації та моніторингу;**
	CA-01_ODP[06]	**визначено події, які потребують перегляду та оновлення поточної політики оцінки, авторизації та моніторингу;**
	CA-01_ODP[07]	**визначено частоту, з якою переглядається та оновлюється поточні процедури оцінювання, авторизації та моніторингу;**
	CA-01_ODP[08]	**визначено події, які потребують перегляду та оновлення поточні процедури оцінки, авторизації та моніторингу;**
	CA-01(a)[01]	розроблено та задокументовано політику оцінювання, авторизації та моніторингу;
	CA-01(a)[02]	політика оцінювання, авторизації та моніторингу поширюється серед **<CA-01_ODP[01] персоналу або ролей>**;
	CA-01(a)[03]	розроблені та задокументовані процедури оцінювання, авторизації та моніторингу, що сприяють впровадженню політики оцінювання, авторизації та моніторингу, а також пов'язані з ними засоби контролю оцінювання, авторизації та моніторингу;
	CA-01(a)[04]	процедури оцінювання, авторизації та моніторингу поширюються серед **<CA-01_ODP[02] персоналу або ролей>**;

	CA-01(a)[01](a)[01]	політика **<CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** оцінювання, авторизації та моніторингу містить мету;
	CA-01(a)[01](a)[02]	політика **<CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** оцінювання, авторизації та моніторингу містить сферу застосування;
	CA-01(a)[01](a)[03]	політика **<CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** оцінювання, авторизації та моніторингу містить ролі;
	CA-01(a)[01](a)[04]	політика **<CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** оцінювання, авторизації та моніторингу містить обов'язки;
	CA-01(a)[01](a)[05]	політика **<CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** оцінювання, авторизації та моніторингу містить відповідальність керівництва;
	CA-01(a)[01](a)[06]	політика **<CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** оцінювання, авторизації та моніторингу містить координацію між підрозділами організації;
	CA-01(a)[01](a)[07]	політика **<CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** оцінювання, авторизації та моніторингу містить систему контролю відповідності;
	CA-01(a)[01](b)	**<CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політика оцінювання, надання дозволів та моніторингу відповідає чинним законам, нормативним документам, наказам, положенням, політиці, стандартам і керівним принципам;
	CA-01(b)	**<CA-01_ODP[04] посадова особа>** призначається для управління розробкою, документуванням та розповсюдженням політики та процедур оцінювання, авторизації та моніторингу;
	CA-01(c)[01][01]	переглядається та оновлюється поточна політика оцінки, авторизації та моніторингу з **<CA-01_ODP[05] частотою>**;
	CA-01(c)[01][02]	переглядається та оновлюється поточна політика оцінки, авторизації та моніторингу після **<CA-01_ODP[06] подій>**;
	CA-01(c)[02][01]	переглядаються та оновлюються поточні процедури оцінки, авторизації та моніторингу з **<CA-01_ODP[07] частотою>**;
	CA-01(c)[02][02]	переглядаються та оновлюються поточні процедури оцінки, авторизації та моніторингу після **<CA-01_ODP[07] подій>**;

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури оцінювання, авторизації та моніторингу; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику оцінювання, авторизації та моніторингу; персонал, відповідальний за інформаційну безпеку].

CA-02	**ОЦІНЮВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-02_ODP[01]	**визначено частоту, з якою слід оцінювати засоби контролю в системі та середовищі її функціонування;**
	CA-02_ODP[02]	**визначені особи або ролі, яким мають бути надані результати оцінювання з безпеки;**
	CA-02(a)	обрано відповідного оцінювача або команду оцінювачів для проведення оцінювання;
	CA-02(b)[01]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи заходи захисту та посилені заходи, що підлягають оцінюванню.
	CA-02(b)[02]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи процедури оцінювання, які використовуватимуться для визначення ефективності заходів.
	CA-02(b)[03][01]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи середовище оцінювання.
	CA-02(b)[03][02]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи групу оцінювання.
	CA-02(b)[03][03]	розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи ролі й обов'язки з оцінювання.
	CA-02(c)	план оцінки заходів захисту розглядається та затверджується уповноваженою посадовою особою або призначеним представником перед проведенням оцінки;
	CA-02(d)[01]	заходи захисту оцінюються в системі та середовищі її функціонування **<CA-02_ODP[01] частота оцінки>**, щоб визначити, наскільки коректно реалізовані заходи захисту, чи працюють вони за призначенням і чи дають бажаний результат щодо дотримання встановлених вимог до безпеки;
	CA-02(d)[02]	заходи захисту оцінюються в системі та середовищі її функціонування **<CA-02_ODP[01] частота оцінки>**, щоб визначити, наскільки коректно реалізовані заходи захисту, чи працюють вони за призначенням і чи дають бажаний результат щодо дотримання встановлених вимог до конфіденційності;

	CA-02(e)	готується звіт оцінювання , який документує результати оцінювання;
	CA-02(f)	результати оцінювання з безпеки надаються **<CA-02_ODP[02] особам або ролям>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури щодо планування оцінки безпеки; процедури, що стосуються оцінок безпеки; план оцінки безпеки; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за оцінку безпеки; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують оцінку безпеки, розробку плану оцінки безпеки та / або звітність про оцінку безпеки].	

CA-02(01)	**ОЦІНЮВАННЯ - НЕЗАЛЕЖНІ ЕКСПЕРТИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-02(01)	для проведення контрольних оцінок залучаються незалежні експерти або групи експертів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури, що стосуються оцінок безпеки; пакет дозволів на безпеку (включаючи план захисту інформації, план оцінки безпеки, звіт про оцінку безпеки, план дій та основні етапи, заяву про авторизацію); інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за оцінку безпеки; персонал організації, відповідальний за інформаційну безпеку].	

CA-02(02)	**ОЦІНЮВАННЯ - СПЕЦІАЛІЗОВАНІ ОЦІНКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-02(02)_ODP[01]	**визначено частоту, з якою слід включати спеціалізовані оцінки як частину оцінювання безпеки та конфіденційності;**
	CA-02(02)_ODP[02]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {з попередженням; без попередження};**
	CA-02(02)_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {поглиблений моніторинг; сканування уразливостей; тестування на шкідливих користувачів; оцінювання внутрішньої загрози; тестування продуктивності та навантаження; };**
	CA-02(02)_ODP[04]	**визначаються інші форми оцінювання (якщо вони були обрані);**

	CA-02(02)	**<CA-02(02)_ODP[01] періодичність оцінювання> <CA-02(02)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА> <CA-02(02)_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** включаються як частина оцінювання заходів безпеки та конфіденційності;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури, що стосуються оцінок безпеки; план захисту інформації; план оцінки безпеки; звіт про оцінку безпеки; докази оцінки безпеки; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за оцінку безпеки; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують оцінку заходів захисту].	

CA-02(03)	**ОЦІНЮВАННЯ - ЗОВНІШНІ ОРГАНІЗАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-02(03)_ODP[01]	визначено організацію, яка надає результати оцінок заходів захисту інформації та персональних даних
	CA-02(03)_ODP[02]	визначено систему, яка приймає результати оцінок заходів захисту інформації та персональних даних
	CA-02(03)_ODP[03]	визначено вимоги до результатів оцінок заходів захисту інформації та персональних даних
	CA-02(03)	прийняти результати оцінок заходів захисту інформації та персональних даних **<CA-02(03)_ODP[01] організаціями.>**, що надані, на **<CA-02(03)_ODP[02] систему>**, коли оцінювання відповідає **<CA-02(03)_ODP[03] вимогам>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури, що стосуються оцінок безпеки; план захисту інформації; вимоги щодо оцінки безпеки; план оцінки безпеки; звіт про оцінку безпеки; докази оцінки безпеки; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за оцінку безпеки; персонал організації, відповідальний за захист інформації].	

CA-03	**ВЗАЄМОДІЯ СИСТЕМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-03_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {): угоди безпеки взаємозв'язку; договори безпеки обміну інформацією; меморандуми про взаєморозуміння;**

		угоди про рівень обслуговування; угоди користувача; угоди про нерозголошення; <CA-03_ODP[02] тип угоди>};
	CA-03_ODP[02]	**визначено тип угоди, який використовується для схвалення та керування обміном інформацією (якщо вибрано);**
	CA-03_ODP[03]	**визначено частоту, з якою необхідно переглядати та оновлювати угоди;**
	CA-03(a)	обмін інформацією між системою та іншими системами схвалюється та керується за допомогою **<CA-03_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>;**
	CA-03(b)[01]	характеристики інтерфейсу задокументовані як частина кожної угоди про обмін;
	CA-03(b)[02]	вимоги до безпеки задокументовані як частина кожної угоди про обмін;
	CA-03(b)[03]	вимоги щодо конфіденційності задокументовані як частина кожної угоди про обмін;
	CA-03(b)[04]	заходи захисту задокументовані як частина кожної угоди про обмін;
	CA-03(b)[05]	відповідальність за кожну систему задокументована як частина кожної угоди про обмін;
	CA-03(b)[06]	характер переданої інформації документується як частина кожної угоди про обмін;
	CA-03(c)	угоди переглядаються та оновлюються **<CA-03_ODP[03] частота>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються з'єднань системи; політика захисту системи та комунікацій; угоди про безпеку взаємозв'язку системи; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за розробку, впровадження або затвердження угод про взаємозв'язок системи; персонал організації, відповідальний за захист інформації; персонал, що керує системою (системами), на яку поширюється угода про безпеку взаємозв'язку].	

CA-03(01)	**ВЗАЄМОДІЯ СИСТЕМ- НЕЗАХИЩЕНІ З'ЄДНАННЯ СИСТЕМИ**
	[Вилучено: Включено до SC-07(25)].

CA-03(02)	ВЗАЄМОДІЯ СИСТЕМ - ЗАХИЩЕНІ З'ЄДНАННЯ СИСТЕМИ
	[Вилучено: Включено до SC-07(26)].

CA-03(03)	ВЗАЄМОДІЯ СИСТЕМ - НЕСЕКРЕТНІ З'ЄДНАННЯ СИСТЕМИ БЕЗПЕКИ, ЩО НЕ Є НАЦІОНАЛЬНИМИ
	[Вилучено: Включено до SC-07(27)].

CA-03(04)	ВЗАЄМОДІЯ СИСТЕМ - ПІДКЛЮЧЕННЯ ДО ЗАГАЛЬНОДОСТУПНИХ МЕРЕЖ
	[Вилучено: Включено до SC-07(28)].

CA-03(05)	ВЗАЄМОДІЯ СИСТЕМ - ОБМЕЖЕННЯ ЗВ'ЯЗКУ ІЗ ЗОВНІШНІМИ СИСТЕМАМИ
	[Вилучено: Включено до SC-07(05)].

CA-03(06)	ВЗАЄМОДІЯ СИСТЕМ - ПЕРЕДАЧА ДОЗВОЛІВ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-03(06)	особи або системи, які передають дані між системами, що з'єднуються, мають необхідні повноваження (тобто дозволи на запис або привілеї) перед тим, як приймати такі дані.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються з'єднань системи; політика захисту системи та комунікацій; угоди про взаємозв'язок системи; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; звіт про оцінку безпеки; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління з'єднаннями із зовнішніми системами; мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують обмеження на зовнішні підключення до системи].	

CA-03(07)	ВЗАЄМОДІЯ СИСТЕМ - ТРАНЗИТИВНИЙ ОБМІН ІНФОРМАЦІЄЮ
	МЕТА ОЦІНКИ: Визначити, чи:

	CA-03(07)(a)	визначено транзитний обмін інформацією з іншими системами через системи, визначені в CA-03a;
	CA-03(07)(b)	вживаються заходи для забезпечення припинення транзитного обміну інформацією, коли засоби контролю над ідентифікованими транзитними системами не можуть бути перевірені або підтверджені.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються з'єднань системи; політика захисту системи та комунікацій; угоди про взаємозв'язок системи; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; звіт про оцінку безпеки; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління з'єднаннями із зовнішніми системами; мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують обмеження на зовнішні підключення до системи].	

CA-04	**СЕРТИФІКАЦІЯ БЕЗПЕКИ**
	[Вилучено: Включено до CA-02].

CA-05	**ПЛАН УСУНЕННЯ НЕДОЛІКІВ ТА КОНТРОЛЬНІ ПОКАЗНИКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-05_ODP	**визначено частоту оновлення чинного плану усунення недоліків та контрольних показників на основі результатів оцінювання заходів захисту, незалежних аудитів та постійного моніторингу;**
	CA-05(a)	розроблено план усунення недоліків та контрольні показники для системи, та задокументувано заплановані дії організації з коригування, спрямовані на усунення недоліків та зауважень, виявлених під час оцінки заходів захисту, а також на зменшення або усунення відомих вразливостей в системі;
	CA-05(b)	існуючий план оновлюються **<CA-05_ODP частота>** на основі результатів оцінювання заходів, незалежних аудитів та постійного моніторингу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; план захисту інформації; план оцінки безпеки; звіт про оцінку безпеки; докази оцінки безпеки; інші відповідні документи чи записи].	

	Співбесіда: [ВИБІР: Політика оцінювання, авторизації та моніторингу; процедури, що стосуються плану дій та етапів; план оцінки заходів захисту; звіт про оцінку заходів захисту; докази оцінки заходів захисту; план дій та етапи; план захисту інформації; план забезпечення конфіденційності; інші відповідні документи або записи]. **Перевірка:** [ВИБІР: Персонал організації, відповідальний за розробку та реалізацію плану дій та основних етапів; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка:** [ВИБІР: Механізми розробки, впровадження та підтримки плану дій та етапів].

CA-05(01)	**ПЛАН УСУНЕННЯ НЕДОЛІКІВ ТА КОНТРОЛЬНІ ПОКАЗНИКИ - АВТОМАТИЗАЦІЯ ПІДТРИМКИ ЗАДЛЯ ТОЧНОСТІ ТА ВЖИВАНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-05(01)_ODP	визначено автоматизовані механізми, які використовуються для забезпечення точності, актуальності та доступності плану усунення недоліків і основних етапів для системи;
	CA-05(01)	**<CA-05(01)_ODP автоматизовані механізми>** використовуються для забезпечення точності, актуальності та доступності плану усунення недоліків і основних етапів для системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури щодо плану дій та етапів; проєктна документація системи, налаштування конфігурації системи та супутня документація; записи аудиту системи; план дій та етапів; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з планом дій та основних етапів розробки та реалізацією обов'язків; відповідальними за розробку та впровадження; gерсонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми розробки, впровадження та підтримки плану дій та етапів].	

CA-06	**АКРЕДИТАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-06_ODP	**визначено частоту, з якою потрібно оновлювати акредитації;**
	CA-06(a)	призначено старшого керівника, який відповідає за систему;

	CA-06(b)	призначено старшого керівника, відповідального за систему, та будь-які загальні заходи захисту, успадковані системою;
	CA-06(c)[01]	перед початком функціонування системи посадова особа, яка відповідає за систему, акредитує загальні заходи захисту, що успадковані системою;
	CA-06(c)[02]	перед початком функціонування системи посадова особа, яка відповідає за систему, акредитує систему на функціонування за призначенням;
	CA-06(d)	посадова особа, яка акредитує заходи захисту, дозволяє використання цих заходів захисту для успадкування системами організації;
	CA-06(e)	акредитації оновлюються **<CA-06_ODP частота>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури, що стосуються дозволу безпеки; пакет дозволів на безпеку (включаючи план захисту інформації; звіт про оцінку безпеки; план дій та основні етапи; заява про акредитацію); інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за повноваження щодо безпеки; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що полегшують акредитацію та оновлення безпеки].	

CA-06(01)	**АКРЕДИТАЦІЯ - СПІЛЬНА АКРЕДИТАЦІЯ - ОДНА І ТА САМА ОРГАНІЗАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-06(01)[01]	для системи впроваджено спільний процес акредитації;
	CA-06(01)[02]	спільний процес акредитації, який використовується в системі, включає в себе кілька посадових осіб з однієї організації, які надають акредитацію.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика акредитації; процедури, що стосуються дозволу безпеки; пакет дозволів на безпеку (включаючи план захисту інформації; звіт про оцінку безпеки; план дій та основні етапи; заява про акредитаціїю); інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за повноваження щодо безпеки; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що полегшують акредитацію та оновлення безпеки].	

CA-06(02)	АКРЕДИТАЦІЯ - СПІЛЬНА АКРЕДИТАЦІЯ - РІЗНІ ОРГАНІЗАЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-6(02)[01]	для системи впроваджено спільний процес акредитації;
	CA-6(02)[02]	спільний процес акредитації, що використовується в системі, передбачає наявність кількох посадових осіб, які надають акредитації, принаймні одна з яких є посадовою особою з організації, що не належить до організації, яка здійснює акредитацію.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика акредитації; процедури, що стосуються дозволу безпеки; пакет дозволів на безпеку (включаючи план безпеки; звіт про оцінку безпеки; план дій та основні етапи; заява про акредитаціїю); інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за повноваження щодо безпеки; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що полегшують акредитацію та оновлення безпеки].	

CA-07	БЕЗПЕРЕРВНИЙ МОНІТОРИНГ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-07_ODP[01]	**визначено метрики системного рівня, які підлягають моніторингу;**
	CA-07_ODP[02]	**визначено частоту, з якою слід моніторити ефективність заходів захисту;**
	CA-07_ODP[03]	**визначено частоту, з якою слід оцінювати ефективність заходів захисту;**
	CA-07_ODP[04]	**визначено персонал або ролі, яким повідомляється про стан безпеки системи;**
	CA-07_ODP[05]	**визначено частоту, з якою повідомляється про стан безпеки системи;**
	CA-07_ODP[06]	**визначено персонал або ролі, яким повідомляється про стан конфіденційності системи;**
	CA-07_ODP[07]	**визначено частоту, з якою повідомляється про стан конфіденційності системи;**
	CA-07[01]	розроблено стратегію безперервного моніторингу на системному рівні;

	CA-07[02]	безперервний моніторинг на рівні системи здійснюється відповідно до стратегії безперервного моніторингу на рівні організації;
	CA-07(a)	безперервний моніторинг на рівні системи включає встановлення наступних метрик на рівні системи, які підлягають моніторингу: **<CA-07_ODP[01] метрики системного рівня>**;
	CA-07(b)[01]	безперервний моніторинг на рівні системи включає встановлені **<CA-07_ODP[02] частоти>** для моніторингу ефективності заходів захисту;
	CA-07(b)[02]	безперервний моніторинг на рівні системи включає встановлені **<CA-07_ODP[03] частоти>** для оцінки ефективності заходів захисту;
	CA-07(c)	безперервний моніторинг на рівні системи включає поточні контрольні оцінки відповідно до стратегії безперервного моніторингу;
	CA-07(d)	безперервний моніторинг на рівні системи включає постійний моніторинг визначених системою та організацією показників відповідно до стратегії безперервного моніторингу;
	CA-07(e)	безперервний моніторинг на рівні системи включає зіставлення та аналіз інформації, отриманої в результаті оцінювання та моніторингу;
	CA-07(f)	безперервний моніторинг на рівні системи включає в себе дії з реагування на результати аналізу інформації, пов’язаної з безпекою та приватністю;
	CA-07(g)[01]	безперервний моніторинг на рівні системи включає повідомлення про статус безпеки системи для **<CA-07_ODP[04] персоналу або ролей> <CA-07_ODP[05] частота>**;
	CA-07(g)[02]	безперервний моніторинг на рівні системи включає повідомлення про стан конфіденційності системи **<CA-07_ODP[06] персоналу або ролям> <CA-07_ODP[07] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури, спрямовані на постійний моніторинг заходів захисту системи; процедури, спрямовані на управління конфігурацією; план захисту інформації; звіт про оцінку безпеки; план дій та етапи; записи моніторингу системи; записи управління конфігурацією, аналіз впливу на безпеку; звіти про стан; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з постійними обов'язками моніторингу; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Механізми, що здійснюють постійний моніторинг].	

CA-07(01)	БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - НЕЗАЛЕЖНЕ ОЦІНЮВАННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-07(01)	для постійного моніторингу заходів захисту в системі залучаються незалежні експертів або групи з оцінювання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури, спрямовані на постійний моніторинг заходів захисту системи; план захисту інформації; звіт про оцінку безпеки; план дій та етапи; записи моніторингу системи; аналізи впливу на безпеку; звіти про стан; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з постійними обов'язками моніторингу; персонал організації, відповідальний за інформаційну безпеку].	

CA-07(02)	БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - ВИДИ ОЦІНОК
	[Вилучено: Включено до CA-02]

CA-07(03)	БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - АНАЛІЗ ТЕНДЕНЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-7(03)[01]	аналіз тенденцій використовується для визначення того, чи потрібно змінювати реалізацію заходів захисту, які використовуються в процесі безперервного моніторингу, на основі емпіричних даних;
	CA-7(03)[02]	аналіз тенденцій застосовується для того, щоб на основі емпіричних даних визначити, чи потрібно змінювати частоту постійного моніторингу;
	CA-7(03)[03]	аналіз тенденцій застосовується для того, щоб на основі емпіричних даних визначити, чи потрібно змінювати види діяльності, які використовуються в процесі безперервного моніторингу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Стратегія постійного моніторингу; оцінка безпеки та політика авторизації; процедури, спрямовані на постійний моніторинг заходів захисту системи; план захисту інформації; звіт про оцінку безпеки; план дій та етапи; записи моніторингу системи; аналізи впливу на безпеку; звіти про стан; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з постійними обов'язками моніторингу; персонал організації, відповідальний за інформаційну безпеку].	

CA-07(04)	БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - МОНІТОРИНГ РИЗИКУ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-07(04)	моніторинг ризиків є невід'ємною частиною стратегії безперервного моніторингу;
	CA-07(04)(a)	моніторинг ефективності включено до моніторингу ризиків;
	CA-07(04)(b)	моніторинг відповідності включено до моніторингу ризиків;
	CA-07(04)(c)	моніторинг змін включений до моніторингу ризиків.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінювання, авторизації та моніторингу; стратегія безперервного моніторингу на рівні організації; стратегія безперервного моніторингу на рівні системи; процедури, що стосуються безперервного моніторингу заходів захисту системи; звіт про оцінку; план дій та основні етапи; записи моніторингу системи; аналіз впливу; звіти про стан справ; план захисту інформації; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з постійними обов'язками моніторингу; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Механізми підтримки моніторингу ризиків].	

CA-07(05)	БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - УЗГОДЖЕНИЙ АНАЛІЗ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-07(05)_ODP[01]	**визначені дії для підтвердження того, що політики встановлені;**
	CA-07(05)_ODP[02]	**визначені дії для підтвердження того, що впроваджені заходи захисту працюють узгоджено;**
	CA-07(05)[01]	**<CA-07(05)_ODP[01] дії>** використовуються для перевірки того, що політики встановлено;
	CA-07(05)[02]	**<CA-07(05)_ODP[02] дії>** використовуються для перевірки того, що впроваджені заходи захисту працюють узгоджено
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінювання, авторизації та моніторингу; стратегія безперервного моніторингу на рівні організації; стратегія безперервного моні-	

	торингу на рівні системи; процедури, що стосуються безперервного моніторингу заходів захисту системи; звіт про оцінку; план дій та основні етапи; записи моніторингу системи; аналіз впливу на безпеку; звіти про стан справ; план захисту інформації; інші відповідні документи або записи**.**]. **Співбесіда:** [ВИБІР: Персонал організації з постійними обов'язками моніторингу; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Механізми підтримки узгодженого аналізу].

CA-07(06)	**БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - АВТОМАТИЧНА ПІДТРИМКА МОНІТОРИНГУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-07(06)_ODP	**визначено автоматизовані механізми забезпечення точності, актуальності та доступності результатів моніторингу системи;**
	CA-07(06)	<**CA-07(06)_ODP автоматизовані механізми**> використовуються для забезпечення точності, актуальності та доступності результатів моніторингу системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінювання, авторизації та моніторингу; стратегія безперервного моніторингу на рівні організації; стратегія безперервного моніторингу на рівні системи; процедури, що стосуються безперервного моніторингу заходів захисту системи; звіт про оцінку; план дій та основні етапи; записи моніторингу системи; аналіз впливу на безпеку; звіти про стан справ; план захисту інформації; інші відповідні документи або записи**.**]. **Співбесіда:** [ВИБІР: Персонал організації з постійними обов'язками моніторингу; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Механізми підтримки автоматичного аналізу].	

CA-08	**ТЕСТУВАННЯ НА ПРОНИКНЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-08_ODP[01]	визначено частоту з якою проводить тестування на проникнення.
	CA-08_ODP[02]	визначено систему у якій проводить тестування на проникнення
	CA-08	проводиться тестування на проникнення з **<CA-08_ODP[01] частотою>** у **<CA-08_ODP[02] системі>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури, спрямо-	

	вані на тестування на проникнення; план захисту інформації; план оцінки безпеки; звіт про випробування на проникнення; звіт про оцінку безпеки; докази оцінки безпеки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за оцінку безпеки; персонал організації, відповідальний за інформаційну безпеку, системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують тестування на проникнення].

CA-08(01)	**ТЕСТУВАННЯ НА ПРОНИКНЕННЯ - НЕЗАЛЕЖНА КОМАНДА АБО АГЕНТ НА ПРОНИКНЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-08(01)	для проведення тестування на проникнення в систему або компонентів системи залучається незалежний агент або команда з тестування на проникнення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури, спрямовані на тестування на проникнення; план захисту інформації; план оцінки безпеки; звіт про випробування на проникнення; звіт про оцінку безпеки; докази оцінки безпеки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за оцінку безпеки; персонал організації, відповідальний за інформаційну безпеку].	

CA-08(02)	**ТЕСТУВАННЯ НА ПРОНИКНЕННЯ - ЧЕРВОНА КОМАНДА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-08(02)_ODP	**визначено вправи червоної команди для імітації спроби супротивників скомпрометувати системи організації;**
	CA-08(02)	залучити **<CA-08(02)_ODP вправи червоної команди>**, щоб імітувати спроби супротивників скомпрометувати системи організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури, спрямовані на тестування на проникнення; процедури щодо вправ червоної команди; план захисту інформації; план оцінки безпеки; результати вправ червоної команди; звіт про випробування на проникнення; звіт про оцінку безпеки; докази оцінки безпеки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за оцінку безпеки; персонал організації, відповідальний за інформаційну безпеку; системні або ме-	

	режеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують використання вправ червоної команди].

CA-08(03)	**ТЕСТУВАННЯ НА ПРОНИКНЕННЯ - МОЖЛИВОСТІ ПЕРЕВІРКИ НА ПРОНИКНЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-08(03)_ODP[01]	**визначено частоту спроби обійти або зламати заходи захисту, пов'язані з фізичними точками доступу до об'єкта в тестуванні на проникнення**
	CA-08(03)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {з попередженням; без попередження};**
	CA-08(03)	впроваджено процес тестування на проникнення, який включає **<CA-08(03)_ODP[01] частоту>**, **<CA-08(03)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>**, спроби обійти або зламати заходи захисту, пов'язані з фізичними точками доступу до об'єкта
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Оцінка безпеки та політика авторизації; процедури, спрямовані на тестування на проникнення; процедури щодо вправ червоної команди; план захисту інформації; план оцінки безпеки; результати вправ червоної команди; звіт про випробування на проникнення; звіт про оцінку безпеки; докази оцінки безпеки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за оцінку безпеки; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують використання вправ червоної команди].	

CA-09	**ВНУТРІШНІ З'ЄДНАННЯ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-09_ODP[01]	**визначено компоненти системи або класи компонентів, що потребують внутрішніх підключень до системи;**
	CA-09_ODP[02]	**визначено умови, за яких необхідно розірвати внутрішні підключення;**
	CA-09_ODP[03]	**визначено частоту, з якою необхідно переглядати постійну потребу в кожному внутрішньому з'єднанні;**
	CA-09(a)	внутрішні підключення **<CA-09_ODP[01] компонентів системи>**

		до системи є авторизовані;
	CA-09(b)[01]	для кожного внутрішнього з'єднання задокументовані характеристики інтерфейсу;
	CA-09(b)[02]	для кожного внутрішнього з'єднання задокументовані вимоги безпеки;
	CA-09(b)[03]	для кожного внутрішнього з'єднання задокументовані вимоги конфіденційності;
	CA-09(b)[04]	для кожного внутрішнього з'єднання задокументовані характер переданої інформації;
	CA-09(c)	внутрішні з'єднання системи розриваються після виконання **<CA-09_ODP[02] умов>**;
	CA-09(d)	переглядається подальша потреба у кожному внутрішньому з'єднанні **<CA-09_ODP[03] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються з'єднань системи; політика захисту системи та комунікацій; план захисті інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; список компонентів або класів компонентів, дозволених як внутрішні з'єднання системи; звіт про оцінку безпеки; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за розробку, впровадження або дозвіл внутрішніх з'єднань системи; персонал організації, відповідальний за інформаційну безпеку].	

CA-09(01)	**ВНУТРІШНІ З'ЄДНАННЯ СИСТЕМИ - ВІДПОВІДНІСТЬ ПЕРЕВІРКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CA-09(01)[01]	перед встановленням внутрішнього з'єднання виконується перевірка на відповідність вимогам безпеки складових компонентів системи;
	CA-09(01)[02]	перед встановленням внутрішнього з'єднання виконується перевірка на відповідність вимогам конфіденційності складових компонентів системи;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика контролю доступу; процедури, що стосуються з'єднань системи; політика захисту системи та комунікацій; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; список компонентів або класів компонентів, дозволених як внутрішні з'єднання системи; звіт про оцінку безпеки; записи аудиту системи; інші відповідні документи або записи].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за розробку, впровадження або дозвіл внутрішніх з'єднань системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують перевірку відповідності].

V. КЛАС ЗАХОДІВ ЗАХИСТУ СМ – УПРАВЛІННЯ КОНФІГУРАЦІЄЮ

СМ-01	**ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ КОНФІГУРАЦІЄЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	СМ-01_ODP[01]	**визначено персонал або ролі, на яких поширюється політика управління конфігурацією;**
	СМ-01_ODP[02]	**визначено персонал або ролі, на яких поширюється процедури управління конфігурацією;**
	СМ-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	СМ-01_ODP[04]	**визначено посадову особу, яка управляє розробкою, документуванням і розповсюдженням політики та процедур керування конфігурацією;**
	СМ-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика управління конфігурацією;**
	СМ-01_ODP[06]	**визначено події, після яких переглядається та оновлюється поточна політика управління конфігурацією;**
	СМ-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні процедури управління конфігурацією;**
	СМ-01_ODP[08]	**визначено події, після яких переглядаються та оновлюються поточні процедури управління конфігурацією;**
	СМ-01(a)[01]	розроблено та задокументовано політику управління конфігурацією;
	СМ-01(a)[02]	політика управління конфігурацією поширюється на **<СМ-01_ODP[01] персонал або ролі>;**
	СМ-01(a)[03]	розроблені та задокументовані процедури управління , що сприяють реалізації політики управління конфігурацією та пов’язаних з нею заходів управління конфігурацією;
	СМ-01(a)[04]	процедури управління конфігурацією поширюються на **<СМ-01_ODP[02] персонал або ролі>;**
	СМ-01(a)[01](a)[01]	**<СМ-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики управління конфігурацією містить мету;

	CM-01(a)[01](a)[02]	**<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики управління конфігурацією містить сферу застосування;
	CM-01(a)[01](a)[03]	**<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики управління конфігурацією містить ролі;
	CM-01(a)[01](a)[04]	**<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики управління конфігурацією містить обов'язки;
	CM-01(a)[01](a)[05]	**<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики управління конфігурацією містить відповідальність керівництва;
	CM-01(a)[01](a)[06]	**<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики управління конфігурацією містить координацію між підрозділами організації;
	CM-01(a)[01](a)[07]	**<CM-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** політики управління конфігурацією містить систему контролю відповідності;
	CM-01(a)[01](b)	політика управління конфігурацією відповідає чинним законам, нормативним документам, наказам, положенням, політикам, стандартам і керівним принципам;
	CM-01(b)	**<CM-01_ODP[04] посадова особа>** призначається для управління розробкою, документуванням і розповсюдженням політики та процедур керування конфігурацією;
	CM-01(c)[01][01]	переглядається та оновлюється поточна політика управління конфігурацією **<CM-01_ODP[05] частота>;**
	CM-01(c)[01][02]	переглядається та оновлюється поточна політика управління конфігурацією після **<CM-01_ODP[06] події>;**
	CM-01(c)[02][01]	переглядаються та оновлюються поточні процедури управління конфігурацією **<CM-01_ODP[07] частота>;**
	CM-01(c)[02][02]	переглядаються та оновлюються поточні процедури управління конфігурацією після **<CM-01_ODP[08] події>;**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури управління конфігурацією; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику управління конфігурацією; персонал, відповідальний за інформаційну безпеку].	

CM-02	**БАЗОВА КОНФІГУРАЦІЯ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	CM-02_ODP[01]	**визначено частоту перегляду та оновлення базових налаштувань;**
	CM-02_ODP[02]	**визначено обставини, що вимагають перегляду та оновлення базових налаштувань;**
	CM-02(a)[01]	розроблено та задокументовано поточні базові налаштування системи;
	CM-02(a)[02]	поточні базові налаштування системи підтримуються за допомогою заходів конфігурації;
	CM-02(b)[01]	переглядаються та оновлюються базові налаштування системи **<CM-02_ODP[01] частота>;**
	CM-02(b)[02]	переглядаються та оновлюються базові налаштування системи після **<CM-02_ODP[02] подій>;**
	CM-02(b)[03]	переглядаються та оновлюються базові налаштування системи коли встановлюються або модернізуються компоненти системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються базової конфігурації системи; план управління конфігурацією; проєктна документація системи; документація архітектури та конфігурація системи; налаштування конфігурації системи та супутня документація; записи змін заходів захисту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління конфігурацією; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з управління базовими конфігураціями; автоматизовані механізми, що підтримують управління конфігурацією базової конфігурації].	

CM-02(01)	**БАЗОВА КОНФІГУРАЦІЯ - ПЕРЕГЛЯД ТА ОНОВЛЕННЯ**
	[Вилучено: Включено до CM-02].

CM-02(02)	**БАЗОВА КОНФІГУРАЦІЯ - АВТОМАТИЗАЦІЯ ПІДТРИМКИ ЗАДЛЯ ТОЧНОСТІ ТА ВЖИВАНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-02(02)_ODP	**визначено автоматизовані механізми підтримки базової конфігурації системи;**

	CM-02(02)[01]	актуальність базової конфігурації системи підтримується за допомогою **<CM-02(02)_ODP автоматизовані механізми>**;
	CM-02(02)[02]	повнота базової конфігурації системи підтримується за допомогою **<CM-02(02)_ODP автоматизовані механізми>**;
	CM-02(02)[03]	точність базової конфігурації системи підтримується за допомогою **<CM-02(02)_ODP автоматизовані механізми>**;
	CM-02(02)[04]	доступність базової конфігурації системи підтримується за допомогою **<CM-02(02)_ODP автоматизовані механізми>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються базової конфігурації системи; план управління конфігурацією; проєктна документація системи; документація архітектури та конфігурація системи; налаштування конфігурації системи та супутня документація; записи управління зміною конфігурації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління конфігурацією; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з управління базовими конфігураціями; автоматизовані механізми, що реалізують підтримку базової конфігурації].	

CM-02(03)	**БАЗОВА КОНФІГУРАЦІЯ - ЗБЕРІГАННЯ ПОПЕРЕДНІХ ВЕРСІЙ КОНФІГУРАЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-02(03)_ODP	**визначено попередні версії базових конфігурацій системи необхідні для підтримки відкату**
	CM-02(03)	зберігати **<CM-02(03)_ODP попередні версії>** для підтримки відкату
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються базової конфігурації системи; план управління конфігурацією; документація архітектури та конфігурація системи; налаштування конфігурації системи та супутня документація; копії попередніх версій конфігурації системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління конфігурацією; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з управління конфігураціями системи].	

CM-02(04)	БАЗОВА КОНФІГУРАЦІЯ - НЕАВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
	[Вилучено: Включено до CM-07(04)].

CM-02(05)	БАЗОВА КОНФІГУРАЦІЯ - АВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
	[Вилучено: Включено до CM-07(05)].

CM-02(06)	БАЗОВА КОНФІГУРАЦІЯ - РОЗРОБКА ТА СЕРЕДОВИЩЕ ТЕСТУВАННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-02(06)[01]	підтримується базова конфігурація для розробки системи, які керуються окремо від робочої базової конфігурації.
	CM-02(06)[02]	підтримується базова конфігурація для розробки тестових середовищ, які керуються окремо від робочої базової конфігурації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються базової конфігурації системи; план управління конфігурацією; проєктна документація системи; документація архітектури та конфігурації системи; налаштування конфігурації системи та супутня документація; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління конфігурацією; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з управління базовими конфігураціями; автоматизовані механізми, що реалізують окремі базові конфігурації для середовищ розробки, тестування та експлуатації].	

CM-02(07)	БАЗОВА КОНФІГУРАЦІЯ - КОНФІГУРАЦІЯ СИСТЕМ ТА КОМПОНЕНТІВ ДЛЯ СФЕР З ВИСОКИМ РИЗИКОМ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-02(07)_ODP[01]	**визначено системи або компоненти систем, які мають видаватися особам, що перебувають у місцях зі значним ризиком;**
	CM-02(07)_ODP[01]	**визначено конфігурації систем або компонентів си-**

		стем, що видаються у місцях зі значним ризиком;
	CM-02(07)_ODP[01]	**визначено заходи безпеки, які мають застосовуватися після повернення осіб з поїздки;**
	CM-02(07)(a)	**<CM-02(07)_ODP[01] системи або компоненти системи>** з **<CM-02(07)_ODP[02] конфігураціями>** видаються особам, що перебувають у місцях, які організація вважає, становлять значний ризик;
	CM-02(07)(b)	**<CM-02(07)_ODP[03] заходи безпеки>** застосовуються до систем або компонентів системи, коли особи повертаються з поїздки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика управління конфігурацією; план управління конфігурацією; процедури, що стосуються базової конфігурації системи; процедури щодо встановлення та оновлення компонентів системи; документація архітектури та конфігурація системи; налаштування конфігурації системи та супутня документація; записи оглядів та оновлень базової лінії конфігурації системи; установки або оновлення компонентів системи та пов'язані з ними записи; записи змін заходів захисту; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління конфігурацією; Персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації управління конфігураціями базової лінії].	

CM-03	**УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-03_ODP[01]	**визначено період часу, протягом якого зберігатимуться записи про зміни конфігурації;**
	CM-03_ODP[02]	**визначено елементи управління змінами конфігурації, відповідальні за координацію та нагляд за діяльністю з управління змінами;**
	CM-03_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<CM-03_ODP[04] частота>; коли <CM-03_ODP[05] умови>};**
	CM-03_ODP[04]	**визначено частоту, з якою викликаються елементи управління змінами конфігурації (якщо вибрано);**
	CM-03_ODP[05]	**визначено умови, за яких викликаються елементи управління змінами конфігурації (якщо вибрано);**

	CM-03(a)	визначено та задокументовано типи змін до системи, які контролюються конфігурацією;
	CM-03(b)[01]	розглядаються запропоновані зміни в конфігурації, що контролюються системою;
	CM-03(b)[02]	запропоновані зміни в конфігурації, що контролюються системою, схвалюються або відхиляються з урахуванням аналізу наслідків безпеки;
	CM-03(c)	рішення про зміну конфігурації системи документуються;
	CM-03(d)	впроваджуються схвалені зміни до конфігурації в систему;
	CM-03(e)	записи про зміни конфігурації у системі зберігаються протягом **<період часу CM-03_ODP[01]>;**
	CM-03(f)[01]	здійснюється моніторинг дій, пов'язаних зі змінами конфігурації системи;
	CM-03(f)[02]	здійснюється аналіз дій, пов'язаних зі змінами конфігурації системи;
	CM-03(g)[01]	діяльність з управління змінами конфігурації координується та контролюється **<CM-03_ODP[02] елемент управління>;**
	CM-03(g)[02]	елемент управління зміною конфігурації викликається **<CM-03_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на управління зміною конфігурації системи; план управління конфігурацією; документація архітектури системи та конфігурації; план захисту інформації; записи контролю; записи аудиту системи; звіти про контроль аудиту та перегляд змін; порядок денний з контролю за зміною конфігурації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління зміною конфігурації; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; члени ради управління змінами чи подібні]. **Перевірка:** [ВИБІР: Процеси організації управління зміною конфігурації; автоматизовані механізми, що реалізують контроль зміни конфігурації].	

CM-03(01)	**УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - АВТОМАТИЗОВАНЕ ДОКУМЕНТУВАННЯ, ПОВІДОМЛЕННЯ ТА ЗАБОРОНА ВНЕСЕННЯ ЗМІН**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-03(01)_ODP[01]	**визначено механізми, що використовуються для ав-**

		томатизації управління змінами конфігурації
	CM-03(01)_ODP[02]	**визначені уповноважені органи, про які необхідно повідомляти та узгоджувати пропоновані зміни в системі;**
	CM-03(01)_ODP[03]	**визначено період часу, після якого слід виділяти зміни, які не були схвалені або відхилені;**
	CM-03(01)_ODP[04]	**визначено персонал, який буде повідомлений про завершення затверджених змін;**
	CM-03(01)(a)	**<CM-03(01)_ODP[01] автоматизовані механізми>** використовуються для документування запропонованих змін до системи;
	CM-03(01)(b)	**<CM-03(01)_ODP[01] автоматизовані механізми>** використовуються для повідомлення **<CM-03(01)_ODP[02] уповноважені органи>** про запропоновані зміни в системі та запиту на затвердження змін;
	CM-03(01)(c)	**<CM-03(01)_ODP[01] автоматизовані механізми>** використовуються для виділення запропонованих змін до системи, які не були схвалені або відхилені протягом **<CM-03(01)_ODP[03] період часу>**;
	CM-03(01)(d)	**<CM-03(01)_ODP[01] автоматизовані механізми>** використовуються для заборони внесення змін до системи до отримання відповідних погоджень;
	CM-03(01)(e)	**<CM-03(01)_ODP[01] автоматизовані механізми>** використовуються для документування всіх змін в системі;
	CM-03(01)(f)	**<CM-03(01)_ODP[01] автоматизовані механізми>** використовуються для повідомлення **<CM-03(01)_ODP[04] персоналу>** про завершення погоджених змін у системі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на управління зміною конфігурації системи; план управління конфігурацією; проєктна документація системи; документація архітектури системи та конфігурації; автоматизовані механізми управління конфігурацією; налаштування конфігурації системи та супутня документація; записи контролю; записи аудиту системи; зміни запитів на затвердження; зміни затверджень; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління зміною конфігурації; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації управління зміною конфігурації; автоматизовані механізми, що реалізують керування зміною конфігурації].	

CM-03(02)	УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - ТЕСТУВАННЯ, ВАЛІДАЦІЯ ТА ДОКУМЕНТУВАННЯ ЗМІН	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-03(02)[01]	зміни в системі тестуються перед повним впровадженням змін;
	CM-03(02)[02]	зміни в системі перевіряються перед повним впровадженням змін;
	CM-03(02)[03]	зміни в системі документуються перед повним впровадженням змін.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; план управління конфігурацією; процедури, спрямовані на управління зміною конфігурації системи; проєктна документація системи; документація архітектури та конфігурація системи; налаштування конфігурації системи та супутня документація; тестові записи; записи перевірок; записи контролю; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління зміною конфігурації; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації управління зміною конфігурації; автоматизовані механізми підтримки та / або впровадження тестування, перевірки та документування змін системи].	

CM-03(03)	УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - АВТОМАТИЗОВАНА РЕАЛІЗАЦІЯ ЗМІН	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-03(03)_ODP	**визначено автоматизовані механізми для внесення змін та розгортання оновленого базового плану по всій встановленій базі;**
	CM-03(03)[01]	зміни до поточного базового плану системи реалізуються за допомогою **<CM-03(03)_ODP автоматизовані механізми>**;
	CM-03(03)[02]	оновлений базовий план розгортається по всій встановленій базі за допомогою **<CM-03(03)_ODP автоматизовані механізми>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політика управління конфігурацією; план управління конфігурацією; процедури, спрямовані на управління зміною конфігурації системи; проєктна документація системи; документація архітектури системи та конфігурації; автоматизовані механізми управління конфігурацією; записи контролю; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління зміною конфігурації; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації управління зміною конфігурації; автоматизовані механізми впровадження змін до поточної базової конфігурації системи].

CM-03(04)	**УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - ПРЕДСТАВНИК БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-03(04)_ODP[01]	**визначено представника з безпеки, який має бути членом елементу керування змінами конфігурації;**
	CM-03(04)_ODP[02]	**визначено представника з конфіденційності, який має бути членом елементу керування змінами конфігурації;**
	CM-03(04)_ODP[03]	**визначено елемент керування змінами конфігурації, членами якого мають бути представники безпеки та конфіденційності;**
	CM-03(04)[01]	**<CM-03(04)_ODP[01] представники безпеки>** повинні бути членами **<CM-03(04)_ODP[03] елемента керування змінами конфігурації>**;
	CM-03(04)[02]	**<CM-03(04)_ODP[02] представники конфіденційності>** повинні бути членами **<CM-03(04)_ODP[03] елемента керування змінами конфігурації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на управління зміною конфігурації системи; план управління конфігурацією; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління зміною конфігурації; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації управління зміною конфігурації].	

CM-03(05)	**УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - АВТОМАТИЧНЕ РЕАГУВАННЯ БЕЗПЕКИ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	CM-03(05)_ODP	**визначено реагування безпеки, які мають бути застосовані автоматично;**
	CM-03(05)	**<CM-03(05)_ODP реагування безпеки>** автоматично застосовуються, якщо базова конфігурація системи змінюється несанкціонованим чином.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на управління зміною конфігурації системи; план управління конфігурацією; план захисту інформації; проєктна документація системи; документація архітектури системи та конфігурації; налаштування конфігурації системи та супутня документація; попередження або сповіщення про несанкціоновані зміни базової конфігурації; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління зміною конфігурації; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації з управління зміною конфігурації; автоматизовані механізми, що реалізують відповіді безпеки на зміни в базових конфігураціях].	

CM-03(06)	**УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - УПРАВЛІННЯ ЗАСОБАМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-03(06)_ODP	**визначено заходи захисту;**
	CM-03(06)	криптографічні механізми, які використовуються для забезпечення відповідних заходів захисту перебувають під управлінням конфігурацією **<CM-03(06)_ODP заходи захисту>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на управління зміною конфігурації системи; план управління конфігурацією; план захисту інформації; проєктна документація системи; документація архітектури системи та конфігурації; налаштування конфігурації системи та супутня документація; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління зміною конфігурації; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з управління зміною конфігурації; криптографічні механізми, що реалізують гарантії безпеки організації] .	

CM-03(07)	УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - ПЕРЕГЛЯД ЗМІН У СИСТЕМІ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-03(07)_ODP[01]	**визначено частоту, з якою необхідно переглядати зміни;**
	CM-03(07)_ODP[02]	**визначено обставини, за яких зміни мають бути переглянуті;**
	CM-03(07)	зміни в системі переглядаються <**CM-03(07)_ODP[01] частота**> або за <**CM-03(07)_ODP[02] обставин**>, щоб визначити, чи відбулися неавторизовані зміни.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури контролю змін конфігурації системи; план управління конфігурацією; записи контролю змін; документація з архітектури та конфігурації системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інвентаризація компонентів системи; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління змінами конфігурації; персонал організації, відповідальний за безпеку; системні/мережеві адміністратори; члени ради з управління змінами або подібні до них.]. **Перевірка:** [ВИБІР: Процеси управління змінами конфігурації в організації; механізми, що реалізують аудит записів про зміни].	

CM-03(08)	УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - ЗАПОБІГАННЯ ЧИ ОБМЕЖЕННЯ ЗМІН КОНФІГУРАЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-03(08)_ODP	**визначено обставини, за яких зміни мають бути запобіжені або обмежені;**
	CM-03(08)	зміни конфігурації системи запобігають або обмежують за <**CM-03(08)_ODP обставин**>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури контролю змін конфігурації системи; план управління конфігурацією; записи контролю змін; документація з архітектури та конфігурації системи; налаштування конфігурації системи та відповідна документація; інвентаризація компонентів системи; план захисту інформації; інші відповідні документи або записи].	

CM-04	АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-04[01]	аналізуються зміни в системі, щоб визначити потенційну загрозу безпеці перед реалізацією змін
	CM-04[02]	аналізуються зміни в системі, щоб визначити потенційну загрозу конфіденційності перед реалізацією змін
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на аналіз впливу на безпеку щодо змін в системі; план управління конфігурацією; документація щодо аналізу впливу на безпеку; інструменти аналізу та пов'язані з ними результати; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аналіз впливу на безпеку; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації для аналізу впливу на безпеку].	

CM-04(01)	АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ - ВІДОКРЕМЛЕНІ ВИПРОБУВАЛЬНІ СЕРЕДОВИЩА	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-04(01)[01]	зміни в системі аналізуються в окремому тестовому середовищі перед впровадженням в операційному середовищі;
	CM-04(01)[02]	зміни в системі аналізуються на предмет впливу на безпеку через недоліки;
	CM-04(01)[03]	зміни в системі аналізуються на предмет впливу на конфіденційність через недоліки;
	CM-04(01)[04]	зміни в системі аналізуються на предмет впливу на безпеку через слабкості;
	CM-04(01)[05]	зміни в системі аналізуються на предмет впливу на конфіденційність через слабкості;
	CM-04(01)[06]	зміни в системі аналізуються на предмет впливу на безпеку через несумістність;
	CM-04(01)[07]	зміни в системі аналізуються на предмет впливу на конфіденційність через несумістність;
	CM-04(01)[08]	зміни в системі аналізуються на предмет впливу на безпеку

		через навмисне спричинення шкоди;
	CM-04(01)[09]	зміни в системі аналізуються на предмет впливу на конфіденційність через навмисне спричинення шкоди;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на аналіз впливу на безпеку щодо змін в системі; план управління конфігурацією; документація щодо аналізу впливу на безпеку; інструменти аналізу та пов'язані з ними виходи на проєктну документацію системи; документація архітектури та конфігурація системи; записи контролю змін; записи аудиту системи; документальне підтвердження окремих випробувальних та експлуатаційних середовищ; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аналіз впливу на безпеку; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації для аналізу впливу на безпеку; автоматизовані механізми, що підтримують та / або здійснюють аналіз впливу змін на безпеку].	

CM-04(02)	**АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ - ВЕРИФІКАЦІЯ ФУНКЦІЙ БЕЗПЕКИ ТА ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-04(02)[01]	заходи захисту, на які було здійснено вплив, реалізовані правильно з точки зору відповідності вимогам безпеки системи після внесення змін до системи;
	CM-04(02)[02]	заходи захисту, на які було здійснено вплив, реалізовані правильно з точки зору відповідності вимогам конфіденційності системи після внесення змін до системи;
	CM-04(02)[03]	заходи захисту, на які було здійснено вплив, функціонують належним чином з точки зору відповідності вимогам безпеки системи після внесення змін до системи;
	CM-04(02)[04]	заходи захисту, на які було здійснено вплив, функціонують належним чином з точки зору відповідності вимогам конфіденційності системи після внесення змін до системи;
	CM-04(02)[05]	заходи захисту, на які було здійснено вплив, дають бажаний результат з точки зору відповідності вимогам безпеки системи після внесення змін до системи;
	CM-04(02)[06]	заходи захисту, на які було здійснено вплив, дають бажаний результат з точки зору відповідності вимогам конфіденційності системи після внесення змін до системи;

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на аналіз впливу на безпеку щодо змін в системі; план управління конфігурацією; документація щодо аналізу впливу на безпеку; інструменти аналізу та пов'язані з ними результати; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аналіз впливу на безпеку; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації для аналізу впливу на безпеку; автоматизовані механізми, що підтримують та / або реалізують перевірку функцій безпеки].

СМ-05	**ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	СМ-05[01]	визначені та задокументовані фізичні обмеження доступу, пов'язані зі змінами в системі;
	СМ-05[02]	затверджені фізичні обмеження доступу, пов'язані зі змінами в системі;
	СМ-05[03]	застосовуються фізичні обмеження доступу, пов'язані зі змінами в системі;
	СМ-05[04]	визначені та задокументовані логічні обмеження доступу, пов'язані зі змінами в системі;
	СМ-05[05]	затверджені логічні обмеження доступу, пов'язані зі змінами в системі;
	СМ-05[06]	застосовуються логічні обмеження доступу, пов'язані зі змінами в системі;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до системи; план управління конфігурацією; проєктна документація системи; документація архітектури та конфігурація системи; налаштування конфігурації системи та супутня документація; логічні схвалення доступу; затвердження фізичного доступу; доступ до облікових даних; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками логічного контролю доступу; персонал організації з обов'язками фізичного контролю доступу; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори].	

	Перевірка: [ВИБІР: Процеси організації для управління обмеженнями доступу для зміни; автоматизовані механізми підтримки / реалізації / забезпечення обмежень доступу, пов'язаних зі змінами в системі].

CM-05(01)	**ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - АУДИТ І ЗДІЙСНЕННЯ АВТОМАТИЧНОГО ДОСТУПУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-05(01)_ODP	**визначено механізми, що використовуються для автоматизації застосування обмежень доступу;**
	CM-05(01)(a)	обмеження доступу до змін застосовуються за допомогою **<CM-05(01)_ODP автоматизованих механізмів>**;
	CM-05(01)(b)	автоматично формуються записи аудиту для виконаних дій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до системи; проєктна документація системи; документація архітектури та конфігурація системи; налаштування конфігурації системи та супутня документація; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для управління обмеженнями доступу для зміни; автоматизовані механізми, що здійснюють виконання обмежень доступу для змін до системи; автоматизовані механізми, що підтримують аудит дій з примусового виконання].	

CM-05(02)	**ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ПЕРЕГЛЯД ЗМІН У СИСТЕМІ**
	[Вилучено: перенесено до CM-03(07)].

CM-05(03)	**ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ПІДПИСАНІ КОМПОНЕНТИ**
	[Вилучено: перенесено до CM-14].

CM-05(04)	**ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ПОДВІЙНА АВТОРИЗАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-05(04)_ODP[01]	**визначено компоненти системи, що потребують**

		подвійної авторизації для внесення змін;
	CM-05(04)_ODP[02]	**визначено інформацію на рівні системи, що потребують подвійної авторизації для внесення змін;**
	CM-05(04)[01]	запроваджено подвійну авторизацію для внесення змін до **<CM-05(04)_ODP[01] компонентів системи>;**
	CM-05(04)[02]	запроваджено подвійну авторизацію для внесення змін до **<CM-05(04)_ODP[02] інформації>;**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до системи; план управління конфігурацією; план захисту інформації; проєктна документація системи; документація архітектури системи та конфігурації; налаштування конфігурації системи та супутня документація; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з подвійними обов'язками щодо виконання дозволу на впровадження змін системи; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації для управління обмеженнями доступу для зміни; автоматизовані механізми, що реалізують подвійне виконання авторизації].	

CM-05(05)	**ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ОБМЕЖЕННЯ ПОВНОВАЖЕНЬ ДЛЯ ВИРОБНИЦТВА ТА ЕКСПЛУАТАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-05(05)_ODP[01]	**визначено частоту перегляду повноважень;**
	CM-05(05)_ODP[02]	**визначено частоту переоцінення повноважень;**
	CM-05(05)(a)[01]	повноваження для зміни компонентів системи у виробничому або операційному середовищі обмежені;
	CM-05(05)(a)[02]	повноваження для зміни інформації, пов'язаної із системою у виробничому або операційному середовищі обмежені;
	CM-05(05)(b)[01]	переглядаються повноваження **<CM-05(05)_ODP[01] частота>**;
	CM-05(05)(b)[02]	переоцінюються повноваження **<CM-05(05)_ODP[02] частота>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури вирі-	

	шення обмежень доступу для змін до системи; план управління конфігурацією; план захисту інформації; проєктна документація системи; документація архітектури системи та конфігурації; налаштування конфігурації системи та супутня документація; огляди привілеїв користувачів; повторне підтвердження прав користувачів; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за безпеку інформації; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з управління обмеженнями доступу для зміни; автоматизовані механізми, що підтримують та / або реалізують обмеження доступу для змін].

CM-05(06)	**ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ОБМЕЖЕННЯ ПОВНОВАЖЕНЬ ДЛЯ БІБЛІОТЕК**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-05(06)	обмежено повноваження для зміни програмного забезпечення, яке перебуває в бібліотеках програмного забезпечення
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури вирішення обмежень доступу для змін до системи; план управління конфігурацією; проєктна документація системи; документація архітектури та конфігурації системи; налаштування конфігурації системи та супутня документація; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за безпеку інформації; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з управління обмеженнями доступу для зміни; автоматизовані механізми, що підтримують та / або реалізують обмеження доступу для змін].	

CM-05(07)	**ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - АВТОМАТИЧНЕ ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ**
	[Вилучено: включено до SI-07].

CM-06	**НАЛАШТУВАННЯ КОНФІГУРАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-06_ODP[01]	**визначено загальні безпечні конфігурації для встановлення та документування параметрів конфігурації компонентів, які застосовуються в системі;**

	CM-06_ODP[02]	**визначено компоненти системи, для яких необхідно затвердити відхилення;**
	CM-06_ODP[03]	**визначені експлуатаційні вимоги, що вимагають затвердження відхилень;**
	CM-6(a)	налаштування конфігурації, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам, встановлені та задокументовані для компонентів, що застосовуються в системі з використанням **<CM-06_ODP[01] безпечні конфігурації>**;
	CM-6(b)	реалізовано установки конфігурації, задокументовані в CM-06a;
	CM-6(c)[01]	будь-які відхилення від встановлених параметрів конфігурації для **<CM-06_ODP[02] компонентів системи>** визначаються та документуються на основі **<CM-06_ODP[03] експлуатаційних вимог>**;
	CM-6(c)[02]	будь-які відхилення від встановлених налаштувань конфігурації для **<CM-06_ODP[02] компонентів системи>** затверджуються;
	CM-6(d)[01]	зміни в налаштуваннях конфігурації відстежуються відповідно до політики та процедур організації;
	CM-6(d)[02]	зміни налаштувань конфігурації керуються відповідно до політики та процедур організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на налаштування конфігурації системи; план управління конфігурацією; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; контрольні списки налаштувань безпеки; докази, що підтверджують затверджені відхилення від встановлених параметрів конфігурації; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління конфігурацією безпеки; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з управління налаштуваннями конфігурації; автоматизовані механізми, що реалізують, контролюють та / або керують налаштуваннями конфігурації системи; автоматизовані механізми, що ідентифікують та / або документують відхилення від встановлених параметрів конфігурації].	

CM-06(01)	**НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - АВТОМАТИЗОВАНЕ УПРАВЛІННЯ, ЗАСТОСУВАННЯ ТА ВЕРИФІКАЦІЯ**
	МЕТА ОЦІНКИ: Визначити, чи:

	CM-06(01)_ODP[01]	**визначено компоненти системи, для яких можна керувати, застосовувати та перевіряти налаштування конфігурації;**
	CM-06(01)_ODP[02]	**визначено автоматизовані механізми керування налаштуваннями конфігурації;**
	CM-06(01)_ODP[03]	**визначено автоматизовані механізми застосування налаштувань конфігурації;**
	CM-06(01)_ODP[04]	**визначено автоматизовані механізми перевірки налаштувань конфігурації;**
	CM-06(01)[01]	налаштування конфігурації для **<CM-06(01)_ODP[01] компонентів системи>** керуються за допомогою **<CM-06(01)_ODP[02] автоматизованих механізмів>**;
	CM-06(01)[02]	налаштування конфігурації для **<CM-06(01)_ODP[01] компонентів системи>** застосовуються за допомогою **<CM-06(01)_ODP[03] автоматизованих механізмів>**;
	CM-06(01)[03]	налаштування конфігурації для **<CM-06(01)_ODP[01] компонентів системи>** перевіряються за допомогою **<CM-06(01)_ODP[04] автоматизованих механізмів>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на налаштування конфігурації системи; план управління конфігурацією; проєктна документація системи; налаштування конфігурації системи та супутня документація; контрольні списки налаштувань безпеки; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління конфігурацією безпеки; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації з управління налаштуваннями конфігурації; автоматизовані механізми, реалізовані для централізованого управління, застосування та перевірки параметрів конфігурації системи].	

CM-06(02)	**НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - РЕАГУВАННЯ НА НЕСАНКЦІОНОВАНІ ЗМІНИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-06(02)_ODP[01]	**визначені дії, яких слід вжити у випадку неавторизованої зміни;**
	CM-06(02)_ODP[02]	**визначено параметри конфігурації, які вимагають дій у разі неавторизованої зміни;**

	CM-06(02)	**<CM-06(02)_ODP[01] дії>** виконуються у відповідь на неавторизовані зміни в **<CM-06(02)_ODP[02] параметри конфігурації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на налаштування конфігурації системи; план управління конфігурацією; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; попередження або сповіщення про несанкціоновані зміни в налаштуваннях конфігурації системи; задокументовані відповіді на несанкціоновані зміни в налаштуваннях конфігурації системи; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління конфігурацією безпеки; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з реагування на несанкціоновані зміни в налаштуваннях конфігурації системи; автоматизовані механізми, що підтримують та / або реалізують гарантії безпеки для реагування на несанкціоновані зміни].	

CM- 06(03)	**НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ ЗМІН**
	[Вилучено: Включено до SI-07]

CM-06(04)	**НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - ДЕМОНСТРАЦІЯ ВІДПОВІДНОСТІ**
	[Вилучено: Включено до CM-04]

CM-07	**МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-07_ODP[01]	**визначено основні функції системи, необхідні для виконання місії;**
	CM-07_ODP[02]	**визначено функції, які необхідно заборонити або обмежити;**
	CM-07_ODP[03]	**визначено системні порти, які необхідно заборонити або обмежити;**
	CM-07_ODP[04]	**визначено протоколи, які необхідно заборонити або обмежити;**

	CM-07_ODP[05]	**визначено програмне забезпечення, яке необхідно заборонити або обмежити;**
	CM-07_ODP[06]	**визначено служби, які необхідно заборонити або обмежити;**
	CM-07(a)	система налаштована на забезпечення лише **<CM-07_ODP[01] основні функції системи >**;
	CM-07(b)[01]	використання **<CM-07_ODP[02] функцій>** заборонено або обмежено;
	CM-07(b)[02]	використання **<CM-07_ODP[03] порти>** заборонено або обмежено;
	CM-07(b)[03]	використання **<CM-07_ODP[04] протоколи>** заборонено або обмежено;
	CM-07(b)[04]	використання **<CM-07_ODP[05] програмне забезпечення>** заборонено або обмежено;
	CM-07(b)[05]	використання **<CM-07_ODP[06] служби>** заборонено або обмежено;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; план управління конфігурацією; процедури, що стосуються найменшої функціональності в системі; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; контрольні списки налаштувань безпеки; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками управління конфігурацією безпеки; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації, що забороняють або обмежують функції, порти, протоколи та / або послуги; автоматизовані механізми, що реалізують обмеження або заборону функцій, портів, протоколів та / або послуг].	

CM-07(01)	**МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ПЕРІОДИЧНИЙ ПЕРЕГЛЯД**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-07(01)_ODP[01]	**визначено частоту, з якою слід переглядати систему для виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг;**
	CM-07(01)_ODP[02]	**визначено функції, які слід вимкнути, якщо вони вважаються непотрібними або незахищеними;**

	CM-07(01)_ODP[03]	**визначено порти, які слід вимкнути, якщо вони вважаються непотрібними або незахищеними;**
	CM-07(01)_ODP[04]	**визначено протоколи, які слід вимкнути, якщо вони вважаються непотрібними або незахищеними;**
	CM-07(01)_ODP[05]	**визначено послуги, які слід вимкнути, якщо вони вважаються непотрібними або незахищеними;**
	CM-07(01)(a)	система переглядається **<CM-07(01)_ODP[01] частота>** для виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг;
	CM-07(01)(b)[01]	**<CM-07(01)_ODP[02] функції>**, які вважаються непотрібними та/або незахищеними, вимкнено;
	CM-07(01)(b)[02]	**<CM-07(01)_ODP[03] порти>**, які вважаються непотрібними та/або незахищеними, вимкнено;
	CM-07(01)(b)[03]	**<CM-07(01)_ODP[04] протоколи>**, які вважаються непотрібними та/або незахищеними, вимкнено;
	CM-07(01)(b)[04]	**<CM-07(01)_ODP[05] послуги>**, які вважаються непотрібними та/або незахищеними, вимкнено;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються найменшої функціональності в системі; план управління конфігурацією; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; контрольні списки налаштувань безпеки; задокументовані огляди функцій, портів, протоколів та / або послуг; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перегляд функцій, портів, протоколів та послуг системи; персонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з огляду або відключення незахищених функцій, портів, протоколів та / або послуг; автоматизовані механізми, що реалізують огляд та відключення незахищених функцій, портів, протоколів та / або послуг].	

CM-07(02)	**МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ЗАБОРОНА ВИКОНАННЯ ПРОГРАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-07(02)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<CM-07(02)_ODP[02] політики, правил поведінки та/або угод про доступ щодо викори-**

		стання програмного забезпечення та обмежень>; правила, що встановлюють терміни та умови використання програмного забезпечення};
	CM-07(02)_ODP[02]	**визначені політики, правил поведінки та/або угод про доступ щодо використання програмного забезпечення та обмежень (якщо вибрано);**
	CM-07(02)	виконання програми заборонено відповідно до **<CM-07(02)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються найменшої функціональності в системі; план управління конфігурацією; план захисту інформації; проєктна документація системи; специфікації щодо запобігання виконанню програм; налаштування конфігурації системи та супутня документація; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за безпеку інформації; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації з, що перешкоджають виконанню програми в системі; процеси організації використання програмного забезпечення та обмеження; автоматизовані механізми, що запобігають виконанню програми в системі; автоматизовані механізми, що підтримують та / або реалізують використання та обмеження програм].	

CM-07(03)	**МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ВІДПОВІДНІСТЬ РЕЄСТРАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-07(03)_ODP	**визначено вимоги до реєстрації функцій, портів, протоколів та сервісів;**
	CM-07(03)	**<CM-07(03)_ODP вимоги до реєстрації>** дотримано.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються найменшої функціональності в системі; план управління конфігурацією; план захисту інформації; налаштування конфігурації системи та супутня документація; перевірки аудиту та дотримання відповідності; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за безпеку інформації; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації, що забезпечують відповідність вимогам реєстрації для функцій, портів, протоколів та / або послуг; автоматизовані	

	механізми, що реалізують відповідність вимогам реєстрації для функцій, портів, протоколів та / або послуг].

CM-07(04)	**МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - НЕАВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - ЧОРНИЙ СПИСОК**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-07(04)_ODP[01]	**визначено програмне забезпечення, яке не має дозволу на виконання в системі;**
	CM-07(04)_ODP[02]	**визначено частоту, з якою слід переглядати та оновлювати список неавторизованих програм;**
	CM-07(04)(a)	визначено **<CM-07(04)_ODP[01] програмне забезпечення>;**
	CM-07(04)(b)	політика "дозволу всього, за винятком деяких" застосовується для заборони виконання неавторизованих програм у системі;
	CM-07(04)(c)	переглядається та оновлюється список неавторизованих програм **<CM-07(04)_ODP[02] частота>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються найменшої функціональності в системі; план управління конфігурацією; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік програм, які не мають права виконувати в системі; контрольні списки налаштувань безпеки; перегляд та оновлення записів, пов'язаних зі списком програм, що не мають дозволу; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за виявлення програмного забезпечення, яке не має права виконуватися в системі; gерсонал організації, відповідальний за інформаційну безпеку; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси ідентифікації, перегляду та оновлення програм, які не мають права виконуватися в системі; процес реалізації чорного списку; автоматизовані механізми підтримки та / або впровадження чорного списку].	

CM-07(05)	**МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - АВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ – БІЛИЙ СПИСОК**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-07(05)_ODP[01]	**визначено програмне забезпечення, яке авторизовано**

		для виконання в системі;
	CM-07(05)_ODP[02]	**визначено частоту перегляду та оновлення списку авторизованих програм;**
	CM-07(05)(a)	визначено **<CM-07(05)_ODP[01] програмне забезпечення>;**
	CM-07(05)(b)	політика "заборонити все, дозволити за винятком" застосовуэться, щоб дозволити виконання авторизованих програм у системі;
	CM-07(05)(c)	переглядається та оновлюється список авторизованих програм **<CM-07(05)_ODP[02] частота>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються найменшої функціональності в системі; план управління конфігурацією; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік програм, дозволених до виконання в системі; контрольні списки налаштувань безпеки; перегляд та оновлення записів, пов'язаних із переліком авторизованих програм; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення програмного забезпечення, дозволеного до виконання в системі; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеис ідентифікації, перегляду та оновлення програм, дозволених до виконання в системі; процеси реалізації білого списку; автоматизовані механізми, що реалізують білий список].	

CM-07(06)	**МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ЗАМКНУТІ СЕРЕДОВИЩА З ОБМЕЖЕНИМИ ПРИВІЛЕЯМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-07(06)_ODP	**визначено встановлене користувачем програмне забезпечення, яке потрібно виконувати в обмеженому середовищі**;
	CM-07(06)	<**CM-07(06)_ODP програмне забезпечення, встановлене користувачем**> має виконуватися в обмеженому середовищі фізичної або віртуальної машини з обмеженими привілеями.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються найменш функціональних можливостей системи; план управління конфігурацією; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; список або запис програмного забезпечен-	

	ня, необхідного для виконання в обмеженому середовищі; інвентаризація компонентів системи; загальні контрольні списки безпечної конфігурації; записи аудиту системи; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за ідентифікацію та/або управління встановленим користувачем програмним забезпеченням та пов'язаними з ним привілеями; персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори]. **Перевірка:** [ВИБІР: Процес ідентифікації встановленого користувачем програмного забезпечення, необхідного для виконання в обмеженому середовищі; механізми підтримки та/або реалізації обмеження встановленого користувачем програмного забезпечення фізичним або віртуальним машинним середовищем; механізми підтримки та/або реалізації обмежень привілеїв для встановленого користувачем програмного забезпечення.].

CM-07(07)	**МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ВИКОНУВАНИЙ КОД У ЗАХИЩЕНОМУ СЕРЕДОВИЩІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-07(07)_ODP	**визначено персонал або ролі для явного дозволу на виконання двійкового або машинно-виконуваного коду;**
	CM-07(07)	виконання двійкового або машинного коду дозволено лише в обмеженому середовищі фізичної або віртуальної машини;
	CM-07(07)(a)	виконання двійкового або машинного коду, отриманого з джерел з обмеженою гарантією або без неї, дозволяється лише з явного дозволу **<CM-07(07)_ODP персонал або ролі>;**
	CM-07(07)(b)	виконання двійкового або машинного коду без надання вихідного коду дозволяється лише з явного дозволу <**CM-07(07)_ODP персонал або ролі**>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються найменш функціональних можливостей системи; план управління конфігурацією; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; список або записи двійкового або машинного коду; інвентаризація компонентів системи; загальні контрольні списки безпечної конфігурації; записи аудиту системи; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за затвердження виконання двійкового або машинного коду; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління програмним забезпеченням; адміністратори системи/мережі; розробники системи].	

	Перевірка: [ВИБІР: Процес затвердження виконання двійкового або машинного коду; процес обмеження виконання двійкового або машинного коду фізичним або віртуальним машинним середовищем; механізми, що підтримують та/або реалізують обмеження виконання двійкового або машинного коду фізичним або віртуальним машинним середовищем.].

CM-07(08)	**МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - БІНАРНИЙ АБО МАШИННИЙ ВИКОНУВАНИЙ КОД**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-07(08)(a)	використання двійкового або машинного коду заборонено, якщо він походить з джерел з обмеженою гарантією або без неї, або без надання вихідного коду;
	CM-07(08)(b)[01]	винятки із заборони на використання двійкового або машинного коду з джерел з обмеженою гарантією або без неї, або без надання вихідного коду допускаються лише для обов'язкових місій або оперативних вимог;
	CM-07(08)(b)[02]	винятки із заборони на використання двійкового або машинного коду з джерел з обмеженою гарантією або без неї, або без надання вихідного коду допускаються лише у разі погодження з уповноваженою посадовою особою;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються найменш функціональних можливостей системи; план управління конфігурацією; план захисту інформації; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; список або записи двійкового або машинного коду; інвентаризація компонентів системи; загальні контрольні списки безпечної конфігурації; записи аудиту системи; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за визначення місій та експлуатаційних вимог; посадова особа, відповідальна за систему; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління програмним забезпеченням; системні/мережеві адміністратори]. **Перевірка:** [ВИБІР: Процес затвердження виконання двійкового або машинного коду; Механізми, що підтримують та/або реалізують обмеження виконання двійкового або машинного коду фізичним або віртуальним машинним середовищем.].	

CM-07(09)	**МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ЗАБОРОНА ВИКОРИСТАННЯ НЕАВТОРИЗОВАНОГО ОБЛАДНАННЯ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	CM-07(09)_ODP[01]	**визначено апаратні компоненти, дозволені для використання в системі;**
	CM-07(09)_ODP[02	**визначено періодичність перегляду та оновлення переліку дозволених апаратних компонентів;**
	CM-07(09)(a)	ідентифіковано <**CM-07(09)_ODP[01] апаратні компоненти**>;
	CM-07(09)(b)	використання або підключення несанкціонованих апаратних компонентів заборонено;
	CM-07(09)(c)	список дозволених апаратних компонентів переглядається та оновлюється з <**CM-07(09)_ODP[02] частота**>;.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; політика та процедури підключення до мережі; план управління конфігурацією; план захисту інформації; проектна документація системи; інвентаризація компонентів системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління обладнанням системи; персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори]. **Перевірка:** [ВИБІР: Процес погодження виконання двійкового або машинного коду; механізми підтримки та/або реалізації заборони на використання двійкового або машинного коду].	

CM-08	**ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-08_ODP[01]	**визначено інформацію, яка вважається необхідною для досягнення ефективної підзвітності компонентів системи;**
	CM-08_ODP[02]	**визначено частоту перегляду та оновлення опису компонентів системи;**
	CM-08(a)[01]	розроблено та задокументовано процес інвентаризації компонентів системи, який точно описує поточну систему;
	CM-08(a)[02]	розроблено та задокументовано процес інвентаризації компонентів системи, якийохоплює всі компоненти в межах акредитації системи;
	CM-08(a)[03]	розроблено та задокументовано процес інвентаризації компонентів системи, який не включає повторний облік компонентів

		або компонентів, будь-якої іншої системи;
	CM-08(a)[04]	розроблено та задокументовано процес інвентаризації компонентів системи, який визначає рівень деталізації, який є необхідним для відстеження та звітування;
	CM-08(a)[05]	розроблено та задокументовано процес інвентаризації компонентів системи, який включає **<CM-08_ODP[01] інформацію>;**
	CM-08(b)	переглядається та оновлюється опис компонентів системи **<CM-08_ODP[02] частота>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів системи; план управління конфігурацією; план захисту інформації; записи інвентаризації системи; огляди запасів та оновлення записів; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інвентаризацію компонентів системи; персонал організації з обов'язками інформаційної безпеки; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси розробки та документування інвентаризації компонентів системи; автоматизовані механізми, що підтримують та / або реалізують інвентаризацію компонентів системи].	

CM-08(01)	**ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ОНОВЛЕННЯ ПІД ЧАС ВСТАНОВЛЕННЯ ТА ВИДАЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-08(01)[01]	інвентаризація компонентів системи оновлюється в рамках інсталяцій компонентів системи;
	CM-08(01)[02]	інвентаризація компонентів системи оновлюється в рамках видалення компонентів системи;
	CM-08(01)[03]	інвентаризація компонентів системи оновлюється в рамках оновлення компонентів системи;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів системи; план управління конфігурацією; план захисту інформації; записи інвентаризації системи; огляди запасів та оновлення записів; записи про встановлення компонентів; записи про видалення компонентів; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за оновлення інвентаризації компонентів системи; персонал організаціїз обов'язками інформаційної безпеки; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з оновлення опису компонентів систе-	

	ми; автоматизовані механізми, що реалізують оновлення інвентаризації компонентів системи].

CM-08(02)	**ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - АВТОМАТИЗОВАНА ПІДТРИМКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-08(02)_ODP[01]	**визначено автоматизовані механізми підтримки актуальності інвентаризації компонентів системи;**
	CM-08(02)_ODP[02]	**визначено автоматизовані механізми підтримки повноти інвентаризації компонентів системи;**
	CM-08(02)_ODP[03]	**визначено автоматизовані механізми підтримки точності інвентаризації компонентів системи;**
	CM-08(02)_ODP[04]	**визначено автоматизовані механізми підтримки доступності інвентаризації компонентів системи;**
	CM-08(02)[01]	**<CM-08(02)_ODP[01] автоматизовані механізми>** використовуються для підтримки актуальності інвентаризації компонентів системи;
	CM-08(02)[02]	**<CM-08(02)_ODP[02] автоматизовані механізми>** використовуються для підтримки повноти інвентаризації компонентів системи;
	CM-08(02)[03]	**<CM-08(02)_ODP[03] автоматизовані механізми>** використовуються для підтримки точності інвентаризації компонентів системи;
	CM-08(02)[04]	**<CM-08(02)_ODP[04] автоматизовані механізми>** використовуються для підтримки доступності інвентаризації компонентів системи;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; план управління конфігурацією; процедури, що стосуються інвентаризації компонентів системи; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи інвентаризації системи; записи контролю змін; записи технічного обслуговування систем; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління автоматизованими механізмами, що реалізують інвентаризацію компонентів системи; персонал організаціїз обов'язками інформаційної безпеки; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Процеси з ведення інвентаризації компонентів системи; автоматизовані механізми реалізації інвентаризації компонентів системи].	

CM-08(03)	ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ КОМПОНЕНТІВ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-08(03)_ODP[01]	**визначено автоматизовані механізми, що використовуються для виявлення наявності несанкціонованого обладнання в системі;**
	CM-08(03)_ODP[02]	**визначено автоматизовані механізми, що використовуються для виявлення наявності несанкціонованого програмного забезпечення в системі;**
	CM-08(03)_ODP[03]	**визначено автоматизовані механізми, що використовуються для виявлення наявності несанкціонованих мікропрограмних компонентів в системі;**
	CM-08(03)_ODP[04]	**визначено частоту, з якою використовуються автоматизовані механізми для виявлення присутності несанкціонованих компонентів системи в системі;**
	CM-08(03)_ODP[05]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {відключення доступу до мережі такими компонентами; ізолювати компоненти; повідомити <CM-08(03)_ODP[06] персонал або ролі>};**
	CM-08(03)_ODP[06]	**визначено персонал або ролі, які мають бути повідомлені при виявленні несанкціонованих компонентів (якщо вибрано);**
	CM-08(03)(a)[01]	наявність несанкціонованого обладнання в системі виявляється за допомогою **<CM-08(03)_ODP[01] автоматизованих механізмів> <CM-08(03)_ODP[04] частота>;**
	CM-08(03)(a)[02]	наявність несанкціонованого програмного забезпечення в системі виявляється за допомогою **<CM-08(03)_ODP[02] автоматизованих механізмів> <CM-08(03)_ODP[04] частота>;**
	CM-08(03)(a)[03]	наявність несанкціонованих мікропрограмних компонентів в системі виявляється за допомогою **<CM-08(03)_ODP[03] автоматизованих механізмів> <CM-08(03)_ODP[04] частота>;**
	CM-08(03)(b)[01]	**<CM-08(03)_ODP[05] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** приймаються при виявленні несанкціонованого обладнання;
	CM-08(03)(b)[02]	**<CM-08(03)_ODP[05] ВИБРАНЕ ЗНАЧЕННЯ ПА-**

		РАМЕТРА(ів)> приймаються при виявленні несанкціонованого програмного забезпечення;
	СМ-08(03)(b)[03]	**<СМ-08(03)_ODP[05] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** приймаються при виявленні несанкціонованих мікропрограмних компонентів;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів системи; план управління конфігурацією; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи інвентаризації системи; оповіщення або сповіщення про несанкціоновані компоненти в системі; записи моніторингу системи; записи контролю змін; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління автоматизованими механізмами, що реалізують виявлення несанкціонованих компонентів системи; персонал організаціїз обов'язками інформаційної безпеки; системні або мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації з виявлення несанкціонованих компонентів системи; автоматизовані механізми, що реалізують виявлення несанкціонованих компонентів системи].	

СМ-08(04)	**ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ІНФОРМАЦІЯ ПРО ПІДЗВІТНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	СМ-08(04)_ODP	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {ім'я; позиція; роль};**
	СМ-08(04)	впровадженно в інвентаризацію компонентів системи засіб для ідентифікації **<СМ-08(04)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** осіб, відповідальних і підзвітних за управління цими компонентами.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів системи; план управління конфігурацією; план захисту інформації; записи інвентаризації системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління запасами компонентів системи; персонал організаціїз обов'язками інформаційної безпеки; системні або мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з ведення інвентаризації компонентів системи; автоматизовані механізми реалізації інвентаризації компонентів системи].	

CM-08(05)	ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ВИКЛЮЧЕННЯ ДУБЛЮВАННЯ КОМПОНЕНТІВ ОБЛІКУ
	[Вилучено: перенесено до CM-08].

CM-08(06)	ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ПЕРЕВІРЕНІ НАЛАШТУВАННЯ ТА ЗАТВЕРДЖЕНІ ВІДХИЛЕННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-08(06)[01]	включено перевірені налаштування компонентів до поточних розгорнутих конфігурацій в інвентаризаційний облік компонентів системи;
	CM-08(06)[02]	включено будь-які затверджені відхилення до поточних розгорнутих конфігурацій в інвентаризаційний облік компонентів системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів системи; план управління конфігурацією; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи інвентаризації системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління запасами та оцінкою компонентів системи; персонал організаціїз обов'язками інформаційної безпеки; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з ведення інвентаризації компонентів системи; автоматизовані механізми реалізації інвентаризації компонентів системи].	

CM-08(07)	ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ЦЕНТРАЛІЗОВАНЕ СХОВИЩЕ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-8(07)	впроваджено централізоване сховище для інвентаризаційного обліку компонентів системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів системи; план управління конфігурацією; проєктна документація системи; сховище інвентаризації системи; записи інвентаризації системи; інші відповідні документи чи записи].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за управління компонентами системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують інвентаризацію компонентів системи в централізованому сховищі].

CM-08(08)	**ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - АВТОМАТИЗОВАНЕ ВІДСТЕЖЕННЯ МІСЦЯ РОЗТАШУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-08(08)_ODP	**визначено автоматизовані механізми відстеження компонентів;**
	CM-08(08)	використовуються **<CM-08(08)_ODP автоматизовані механізми>** для підтримки відстеження компонентів системи за географічним розташуванням
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються інвентаризації компонентів системи; план управління конфігурацією; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи інвентаризації системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління компонентами системи; персонал організаціїз обов'язками інформаційної безпеки; системні / мережеві адміністратори; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують інвентаризацію компонентів системи; автоматизовані механізми, що підтримують відстеження компонентів системи за географічним розташуванням].	

CM-08(09)	**ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ПРИЗНАЧЕННЯ КОМПОНЕНТІВ СИСТЕМАМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-08(09)_ODP	**визначено персонал або ролі, від яких слід отримувати підтвердження;**
	CM-08(09)(a)	компоненти системи призначаються системі;
	CM-08(09)(b)	отримано підтвердження призначення компонента від **<CM-08(09)_ODP персонал або ролі>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що сто-	

	суються інвентаризації компонентів системи; план управління конфігурацією; план захисту інформації; проєктна документація системи; підтвердження призначень компонентів системи; записи інвентаризації системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління запасами компонентів системи; власник системи; персонал організації з обов'язками інформаційної безпеки; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з присвоєння компонентів системам; процеси організації з підтвердження призначення компонентів системам; автоматизовані механізми, що здійснюють віднесення придбаних компонентів до системи; автоматизовані механізми, що реалізують підтвердження віднесення придбаних компонентів до системи].

CM-09	**ПЛАН УПРАВЛІННЯ КОНФІГУРАЦІЄЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-09_ODP	**визначено персонал або ролі для розгляду та затвердження плану управління конфігурацією;**
	CM-09[01]	розроблено та задокументовано план управління конфігурацією системи;
	CM-09[01]	реалізовано план управління конфігурацією системи;
	CM-09(a)[01]	план управління конфігурацією описує ролі;
	CM-09(a)[02]	план управління конфігурацією описує відповідальність;
	CM-09(a)[03]	план управління конфігурацією описує процеси та процедури управління конфігурацією;
	CM-09(b)[01]	план управління конфігурацією встановлює процес ідентифікації елементів конфігурації протягом всього життєвого циклу розробки системи;
	CM-09(b)[02]	план управління конфігурацією встановлює процес управління конфігурацією елементів;
	CM-09(c)[01]	план управління конфігурацією визначає елементи конфігурації системи;
	CM-09(c)[02]	план управління конфігурацією розміщує елементи конфігурації під управлінням конфігурацією;
	CM-09(d)	план управління конфігурацією розглянуто та затверджено **<CM-09_ODP персонал або ролі>**;

	CM-09(e)[01]	план управління конфігурацією захищений від несанкціонованого розкриття;
	CM-09(e)[02]	план управління конфігурацією захищений від несанкціонованої модифікації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на планування управління конфігурацією; план управління конфігурацією; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за розробку плану управління конфігурацією; персонал організації, відповідальний за впровадження та управління процесами, визначеними в плані управління конфігурацією; персонал організації, відповідальний за захист плану управління конфігурацією; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з розробки та документування плану управління конфігурацією; процеси організації з ідентифікації та управління елементами конфігурації; процеси організації із захисту плану управління конфігурацією; автоматизовані механізми, що реалізують план управління конфігурацією; автоматизовані механізми управління елементами конфігурації; автоматизовані механізми захисту плану управління конфігурацією].	

CM-09(01)	**ПЛАН УПРАВЛІННЯ КОНФІГУРАЦІЄЮ - ВСТАНОВЛЕННЯ ВІДПОВІДАЛЬНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-09(01)	встановлено відповідальність за реалізацію процесу управління конфігурацією персоналу, який безпосередньо не бере участь у розробці системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури вирішення відповідальності за розробку процесів управління конфігурацією; план управління конфігурацією; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за розвиток процесів управління конфігурацією; персонал організації, відповідальний за інформаційну безпеку].	

CM-10	**ОБМЕЖЕННЯ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**
	МЕТА ОЦІНКИ: Визначити, чи:

	CM-10(a)	програмне забезпечення та супутня документація використовуються відповідно до договірних угод та законів про авторські права;
	CM-10(b)	використання програмного забезпечення та пов'язаної з ним документації, захищеної ліцензіями, відстежується для контролю за копіюванням та розповсюдженням;
	CM-10(c)	використання технології однорангового обміну файлами контролюється та документується, щоб гарантувати, що одноранговий обмін файлами не використовується для несанкціонованого розповсюдження, відображення, виконання або відтворення програмного забезпечення, захищеного авторським правом.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, спрямовані на обмеження використання програмного забезпечення; план управління конфігурацією; план захисту інформації; договори програмного забезпечення та закони про авторські права; документація на ліцензії; перелік обмежень щодо використання програмного забезпечення; звіти про відстеження ліцензій на програмне забезпечення; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори; персонал організації, що працює, використовує та / або підтримує систему; персонал організаціїз обов'язками управління ліцензіями на програмне забезпечення]. **Перевірка:** [ВИБІР: Процеси організації з відстеження використання програмного забезпечення, захищеного кількісними ліцензіями; процеси організації з контролю / документування використання технологій спільного використання однорангових файлів; автоматизовані механізми, що реалізують відстеження ліцензій на програмне забезпечення; автоматизовані механізми, що реалізують та контролюють використання технологій спільного використання однорангових файлів].	

CM-10(01)	**ОБМЕЖЕННЯ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ - ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ З ВІДКРИТИМ ВИХІДНИМ КОДОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-10(01)_ODP	**визначено обмеження на використання програмного забезпечення з відкритим вихідним кодом**
	CM-10(01)	встановлено <**CM-10(01)_ODP обмеження**> на використання програмного забезпечення з відкритим вихідним кодом.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури вирішення обмежень щодо використання програмного забезпечення з відкритим кодом; план управління конфігурацією; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за встановлення та	

	виконання обмежень щодо використання програмного забезпечення з відкритим кодом; персонал організації з обов'язками інформаційної безпеки; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації з обмеження використання програмного забезпечення з відкритим кодом; автоматизовані механізми, що реалізують обмеження на використання програмного забезпечення з відкритим кодом].

CM-11	**ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-11_ODP[01]	**визначено правила (політики), що регулюють встановлення програмного забезпечення користувачами;**
	CM-11_ODP[02]	**визначено методи, що використовуються для забезпечення дотримання правил (політик) встановлення програмного забезпечення;**
	CM-11_ODP[03]	**визначено частоту, з якою слід контролювати відповідність правил (політик);**
	CM-11(a)	встановлено **<CM-11_ODP[01] правила (політики)>**, що регулюють встановлення програмного забезпечення користувачами;
	CM-11(b)	правила (політики) встановлення програмного забезпечення застосовуються за допомогою **<CM-11_ODP[02] методів>**;
	CM-11(c)	дотримання **<CM-11_ODP[01] політик>** контролюється **<CM-11_ODP[03] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури звернення до встановленого користувачем програмного забезпечення; план управління конфігурацією; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік правил, що регулюють встановлене користувачем програмне забезпечення; записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи; стратегія постійного моніторингу]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління програмним забезпеченням, встановленим користувачем; персонал організації, що працює, використовує та / або підтримує систему; персонал організації, що здійснює контроль за дотриманням користувачем встановленої політики; персонал організації, відповідальний за інформаційну безпеку; системні / мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації, що керують встановленим користувачем програмним забезпеченням в системі; автоматизовані механізми забезпечення правил / методів управління встановленням програмного забезпечення користувачами; автоматизовані механізми контролю за дотриманням політики].	

CM-11(01)	ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - ПОПЕРЕДЖЕННЯ ПРО НЕСАНКЦІОНОВАНУ ІНСТАЛЯЦІЮ
	[Вилучено: Включено до CM-08(03)].

CM-11(02)	ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - ВСТАНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ПРИВІЛЕЙОВАНИМ СТАТУСОМ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-11(02)	встановлювати програмне забезпечення дозволено користувачеві лише при наявності привілейованого статусу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури звернення до встановленого користувачем програмного забезпечення; план управління конфігурацією; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та супутня документація; оповіщення / сповіщення про несанкціоновану інсталяцію програмного забезпечення; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління програмним забезпеченням, встановле користувачем; персонал організації, що працює, використовує та / або підтримує інформаційну систему]. **Перевірка:** [ВИБІР: Процеси організації, що керують встановленим користувачем програмним забезпеченням в системі; автоматизовані механізми заборони встановлення програмного забезпечення без привілейованого статусу].	

CM-11(03)	ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - АВТОМАТИЧНЕ ВИКОНАННЯ І МОНІТОРИНГ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-11(03)_ODP[01]	**визначено автоматизовані механізми для забезпечення дотримання політик виконання програмного забезпечення;**
	CM-11(03)_ODP[02]	**визначено автоматизовані механізми для забезпечення дотримання політик контролю програмного забезпечення;**
	CM-11(03)[01]	дотримання політик виконання програмного забезпечення забезпечується за допомогою <**CM-11(03)_ODP[01] автоматизованих механізмів>**;

	CM-11(03)[02]	дотримання політик контролю програмного забезпечення контролюється за допомогою **<CM-11(03)_ODP[02] автоматизованих механізмів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються встановленого користувачем програмного забезпечення; план управління конфігурацією; план захисту інформації; проектна документація системи; налаштування конфігурації системи та відповідна документація; перелік правил, що регулюють встановлене користувачем програмне забезпечення; записи моніторингу системи; записи аудиту системи; стратегія безперервного моніторингу; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління програмним забезпеченням, встановленим користувачами; персонал організації, який експлуатує, використовує та/або обслуговує систему; персонал організації, який контролює дотримання політики щодо програмного забезпечення, встановленого користувачами; персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації, що регулюють встановлення користувачами програмного забезпечення в системі; автоматизовані механізми забезпечення дотримання політик щодо встановлення програмного забезпечення користувачами; автоматизовані механізми контролю за дотриманням політик.].	

CM-12	**РОЗТАШУВАННЯ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-12_ODP	**визначено інформацію, місцезнаходження якої має бути визначено та задокументовано;**
	CM-12(a)[01]	місцезнаходження **<CM-12_ODP інформація>** визначено та задокументовано;
	CM-12(a)[02]	визначено та задокументовано конкретні компоненти системи, на яких обробляється **<CM-12_ODP інформація>**;
	CM-12(a)[03]	визначено та задокументовано конкретні компоненти системи, на яких зберігається **<CM-12_ODP інформація>**;
	CM-12(b)[01]	визначено та задокументовано користувачів, які мають доступ до системи та компонентів системи, де обробляється **<CM-12_ODP інформація>**;
	CM-12(b)[02]	визначено та задокументовано користувачів, які мають доступ до системи та компонентів системи, де зберігається **<CM-12_ODP інформація>**;

	CM-12(c)[01]	задокументовано зміни розташування (наприклад, системи або компонентів системи), де обробляється **<CM-12_ODP інформація>**;
	CM-12(c)[02]	задокументовано зміни розташування (наприклад, системи або компонентів системи), де зберігається **<CM-12_ODP інформація>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління розташуванням інформації; план захисту інформації; проєктна документація системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління розташуванням інформації; персонал організації, що працює, використовує та / або підтримує систему]. **Перевірка:** [ВИБІР: Процеси організації, що керують розташуванням інформації]	

CM-12(01)	**РОЗТАШУВАННЯ ІНФОРМАЦІЇ - АВТОМАТИЗОВАНІ ІНСТРУМЕНТИ ПІДТРИМКИ РОЗТАШУВАННЯ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-12(01)_ODP[01]	**інформація визначена за типом;**
	CM-12(01)_ODP[02]	**визначено компоненти системи, де знаходиться інформація;**
	CM-12(01)	автоматизовані інструменти використовуються для ідентифікації **<CM-12(01)_ODP[01] інформації за типом>** на **<CM-12(01)_ODP[02] компонентах системи>**, щоб забезпечити впровадження належних заходів захисту щодо інформації про організацію і персональних даних.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління розташуванням інформації; план захисту інформації; проєктна документація системи; записи аудиту системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління розташуванням інформації; персонал організації, що працює, використовує та / або підтримує систему]. **Перевірка:** [ВИБІР: Процеси організації, що керують розташуванням інформації]	

CM-13	**ВІДОБРАЖЕННЯ ДІЙ ДАНИХ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	CM-13	розроблено та задокументовано карту дій з даними системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури ідентифікації та документування місцезнаходження інформації; процедури мапування даних; план управління конфігурацією; план захисту інформації; план забезпечення конфіденційності; проектна документація системи; документація з інвентаризації; документація з мапування даних; записи контролю змін; інвентаризація компонентів системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління розміщенням інформації; персонал організації, відповідальний за мапування даних; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; системні/мережеві адміністратори; системні розробники]. **Перевірка:** [ВИБІР: Процеси організації, що визначають місцезнаходження інформації; механізми, що підтримують або впроваджують мапування дій з даними]	

CM-14	**ПІДПИСАНІ КОМПОНЕНТИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CM-14_ODP[01]	**визначено програмне забезпечення, яке потребує перевірки сертифікату з цифровим підписом перед встановленням;**
	CM-14_ODP[02]	**визначено мікропрограмні компоненти, які потребує перевірки сертифікату з цифровим підписом перед встановленням;**
	CM-14[01]	інсталяція <**CM-14_ODP[01] програмне забезпечення**> попередньо запобігається, якщо не буде перевірено, що програмне забезпечення було підписано цифровим підписом за допомогою сертифіката, визнаного та затвердженого організацією;
	CM-14[02]	інсталяція <**CM-14_ODP[02] мікропрограмні компоненти** > попередньо запобігається, якщо не буде перевірено, що мікропрограмні компоненти були підписані цифровим підписом за допомогою сертифіката, визнаного та затвердженого організацією;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика управління конфігурацією; процедури, що стосуються сертифікатів з цифровим підписом для компонентів програмного забезпечення та мікропрограмного забезпечення; план управління конфігурацією; план безпеки системи; проектна документація системи; записи контролю змін;	

	інвентаризація компонентів системи; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку сертифікатів з цифровим підписом для встановлення програмного забезпечення та мікропрограмних компонентів; персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори; системні розробники]. **Перевірка:** [ВИБІР: Процеси організації, що регулюють розміщення інформації; механізми, що забезпечують дотримання політик і методів управління розміщенням інформації; автоматизовані засоби, що підтримують або реалізують цифрові підписи для компонентів програмного забезпечення та мікропрограмного забезпечення; автоматизовані засоби, що підтримують або реалізують перевірку цифрових підписів при встановленні програмного забезпечення та мікропрограмного забезпечення.]

VI. КЛАС ЗАХОДІВ ЗАХИСТУ CP – ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ

CP-01	ПОЛІТИКА ТА ПРОЦЕДУРИ ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-01_ODP[01]	**визначено персонал або посади, на які поширюється політика планування безперервної роботи на випадок надзвичайних ситуацій;**
	CP-01_ODP[02]	**визначено персонал або посади, на які поширюється процедури планування безперервної роботи на випадок надзвичайних ситуацій;**
	CP-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	CP-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами планування безперервної роботи на випадок надзвичайних ситуацій;**
	CP-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика;**
	CP-01_ODP[06]	**визначено події, після яких переглядається та оновлюється поточна політика;**
	CP-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні процедури;**
	CP-01_ODP[08]	**визначено події, після яких переглядаються та оновлюються поточні процедури;**
	CP-01(a)[01]	розроблено та задокументовано політику планування безперервної роботи на випадок надзвичайних ситуацій;
	CP-01(a)[02]	політика планування безперервної роботи на випадок надзвичайних ситуацій поширюється на **<CP-01_ODP[01] персонал або посади>**;
	CP-01(a)[03]	розроблені та задокументовані процедури планування безперервної роботи на випадок надзвичайних ситуацій, що сприяють впровадженню політики планування безперервної роботи на випадок надзвичайних ситуацій та пов'язаних з нею заходів захисту на випадок надзвичайних ситуацій;

	CP-01(a)[04]	процедури планування безперервної роботи на випадок надзвичайних ситуацій поширюються на **<CP-01_ODP[02] персонал або посади>**;
	CP-01(a)[01](a)[01]	політика планування безперервної роботи на випадок надзвичайних ситуацій **<CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить мету;
	CP-01(a)[01](a)[02]	політика планування безперервної роботи на випадок надзвичайних ситуацій **<CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить сферу застосування;
	CP-01(a)[01](a)[03]	політика планування безперервної роботи на випадок надзвичайних ситуацій **<CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить ролі;
	CP-01(a)[01](a)[04]	політика планування безперервної роботи на випадок надзвичайних ситуацій **<CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить обов'язки;
	CP-01(a)[01](a)[05]	політика планування безперервної роботи на випадок надзвичайних ситуацій **<CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить відповідальність керівництва;
	CP-01(a)[01](a)[06]	політика планування безперервної роботи на випадок надзвичайних ситуацій **<CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить координацію між підрозділами організації;
	CP-01(a)[01](a)[07]	політика планування безперервної роботи на випадок надзвичайних ситуацій **<CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить систему контролю відповідності;
	CP-01(a)[01](b)	**<CP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика планування безперервної роботи на випадок надзвичайних ситуацій відповідає чинним законам, виконавчим розпорядженням, директивам, положенням, політикам, стандартам і керівним принципам;
	CP-01(b)	**<CP-01_ODP[04] посадова особа>** призначається для управління , документуванням та розповсюдженням політики та процедур планування безперервної роботи на випадок надзвичайних ситуацій;
	CP-01(c)[01][01]	переглядається та оновлюється поточна політика планування безперервної роботи на випадок надзвичайних ситуацій **<CP-01_ODP[05] частота>**;
	CP-01(c)[01][02]	переглядається та оновлюється поточна політика планування безперервної роботи на випадок надзвичайних ситуацій після **<CP-01_ODP[06] подій>**;

	CP-01(c)[02][01]	переглядаються та оновлюються поточні процедури планування безперервної роботи на випадок надзвичайних ситуацій **<CP-01_ODP[07] частота>**;
	CP-01(c)[02][02]	переглядаються та оновлюються поточні процедури планування безперервної роботи на випадок надзвичайних ситуацій після **<CP-01_ODP[08] подій>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики та процедури планування безперервної роботи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику планування безперервної роботи; персонал, відповідальний за інформаційну безпеку].	

CP-02	**ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-02_ODP[01]	**визначено персонал або ролі для перегляду плану забезпечення безперервної роботи у надзвичайних ситуаціях;**
	CP-02_ODP[02]	**визначено персонал або ролі для затвердження плану забезпечення безперервної роботи у надзвичайних ситуаціях;**
	CP-02_ODP[03]	**визначено ключовий резервний персонал (ідентифікований за іменами та/або за ролями), якому поширюються копії плану забезпечення безперервної роботи на випадок надзвичайних ситуацій;**
	CP-02_ODP[04]	**визначено ключові елементи, на які поширюються копії плану забезпечення безперервної роботи на випадок надзвичайних ситуацій;**
	CP-02_ODP[05]	**визначено періодичність перегляду плану забезпечення безперервної роботи у надзвичайних ситуаціях;**
	CP-02_ODP[06]	**визначено ключовий резервний персонал (ідентифікований за іменами та/або ролями), якому необхідно повідомити про зміни;**
	CP-02_ODP[07]	**визначено ключові елементи організації, і які необхідно повідомити про зміни;**
	CP-02(a)[01]	розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який визначає основні завдання, функції та пов'язані з ними вимоги щодо безперервної роботи;

	CP-02(a)[02][01]	розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який забезпечує цілі;
	CP-02(a)[02][02]	розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який забезпечує пріорітети;
	CP-02(a)[02][03]	розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який забезпечує відповідні показники;
	CP-02(a)[03][01]	розроблено план забезпечення безперервної роботи на випадок надзвичайних ситуацій для системи, в якому визначено ролі;
	CP-02(a)[03][02]	розроблено план забезпечення безперервної роботи на випадок надзвичайних ситуацій для системи, в якому визначено обов'язки;
	CP-02(a)[03][03]	розроблено план забезпечення безперервної роботи на випадок надзвичайних ситуацій для системи, в якому визначено відповідальних осіб з контактною інформацією;
	CP-02(a)[04]	розроблено план забезпечення безперервної роботи на випадок непередбачених обставин для системи, який спрямований на підтримку основних завдань і функції, попри системні збої, компрометації або помилки;
	CP-02(a)[05]	розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який спрямований на повне відновлення функціонування системи без погіршення запланованих і реалізованих заходів захисту інформації та персональних даних;
	CP-02(a)[06]	розроблено план забезпечення безперервної роботи на випадок надзвичайних ситуацій для системи, який вирішує питання обміну інформацією про надзвичайні ситуації;
	CP-02(a)[07][01]	розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який переглядається **<CP-02_ODP[01] персоналом або ролями>**;
	CP-02(a)[07][02]	розроблено план забезпечення безперервної роботи у надзвичайних ситуаціях для системи, який затверджено **<CP-02_ODP[02] персоналом або ролями>**;
	CP-02(b)[01]	копії плану забезпечення безперервної роботи на випадок надзвичайних ситуацій розповсюджуються серед **<CP-02_ODP[03] персоналу>**;
	CP-02(b)[02]	копії плану забезпечення безперервної роботи на випадок надзвичайних ситуацій розповсюджуються серед **<CP-02_ODP[04] елементів>**;
	CP-02(c)	діяльність з планування безперервної роботи координується з діяльністю із заходами по усуненню інцидентів;

	CP-02(d)	переглядається план забезпечення безперервної роботи у надзвичайних ситуаціях для системи <**CP-02_ODP[05] частота**>;
	CP-02(e)[01]	план забезпечення безперервної роботи на випадок надзвичайних ситуацій оновлюється з урахуванням змін в організації, системі або середовищі функціонування;
	CP-02(e)[02]	план забезпечення безперервної роботи на випадок надзвичайних ситуацій оновлюється для вирішення проблем, що виникають під час впровадження, виконання або тестування плану дій на випадок надзвичайних ситуацій;
	CP-02(f)[01]	зміни в плані забезпечення безперервної роботи на випадок надзвичайних ситуацій повідомляються <**CP-02_ODP[06] персоналу**>;
	CP-02(f)[02]	зміни в плані забезпечення безперервної роботи на випадок надзвичайних ситуацій повідомляються <**CP-02_ODP[07] елементам**>;
	CP-02(g)[01]	уроки, отримані під час тестування планів забезпечення безперервної роботи у надзвичайних ситуаціях або фактичних дій у надзвичайних ситуаціях, включаються в навчання;
	CP-02(g)[02]	уроки, отримані під час тестування планів забезпечення безперервної роботи у надзвичайних ситуаціях або фактичних дій у надзвичайних ситуаціях, включаються в тестування;
	CP-02(h)[01]	план забезпечення безперервної роботи у надзвичайних ситуаціях захищений від несанкціонованого доступу;
	CP-02(h)[02]	план забезпечення безперервної роботи у надзвичайних ситуаціях захищений від несанкціонованих змін;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для системи; резервний план; план захисту інформації; докази оглядів та оновлень плану забезпечення безперервної роботи у надзвичайних ситуаціях; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал, відповідальний за планування надзвичайних ситуацій та виконання плану; персонал, який несе відповідальність за вирішення інцидентів; персонал, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси розробки, огляду, оновлення та захисту плану забезпечення безперервної роботи у надзвичайних ситуаціях; автоматизовані механізми розробки, перегляду, оновлення та / або захисту плану забезпечення безперервної роботи в надзвичайних ситуацій].	

CP-02(01)	**ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - КООРДИНАЦІЯ З ПОВ'ЯЗАНИМИ ПЛАНАМИ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	СР-02(01)	розробка плану забезпечення безперервної роботи у надзвичайних ситуаціях координується зі структурними підрозділами, які відповідають за розробку та реалізацію пов'язаних планів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження: [**ВИБІР: Політика забезпечення безперервної роботи на випадок надзвичайних ситуацій; процедури, що стосуються забезпечення безперервної роботи під час надзвичайних операцій для системи; план на випадок надзвичайних ситуацій; бізнес-плани на випадок надзвичайних ситуацій; плани аварійного відновлення; плани безперервності операцій; плани комунікацій у кризових ситуаціях; плани критичної інфраструктури; план реагування на кіберінциденти; плани реагування на внутрішні загрози; плани на випадок надзвичайних ситуацій, пов'язаних із діями зловмисників; план забезпечення безпеки системи; інші відповідні документи чи записи.]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування надзвичайних ситуацій та виконання плану; персонал організації, відповідальний за інформаційну безпеку; персонал, відповідальний за пов'язані плани].	

СР-02(02)	**ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ПЛАНУВАННЯ РЕСУРСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	СР-02(02)[01]	планування ресурсів здійснюється таким чином, щоб забезпечити необхідний потенціал для обробки інформації під час відновлення функціонування системи;
	СР-02(02)[02]	планування ресурсів здійснюється таким чином, щоб забезпечити необхідний потенціал для комунікацій під час відновлення функціонування системи;
	СР-02(02)[03]	планування ресурсів здійснюється таким чином, щоб забезпечити необхідний потенціал для підтримки середовища під час відновлення функціонування системи;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для системи; резервний план; документи з планування потенціалу; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування надзвичайних ситуацій та виконання плану; персонал організації, відповідальний за інформаційну безпеку].	

CP-02(03)	ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ВІДНОВЛЕННЯ КРИТИЧНИХ ФУНКЦІЙ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-02(03)_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {усі; істотні};**
	CP-02(03)_ODP[02]	**визначено період часу активації плану забезпечення безперервної роботи на випадок надзвичайних ситуацій, протягом якого необхідно відновити місію та бізнес-функції;**
	CP-02(03)	відновлення **<CP-02(03)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** місії та бізнес-функцій передбачається впродовж **<CP-02(03)_ODP[02] періоду часу>** з моменту активації плану забезпечення безперервної роботи на випадок надзвичайних ситуаціях.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування дій у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для системи; резервний план; план захисту інформації; оцінка впливу на бізнес; інші пов'язані плани; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування надзвичайних ситуацій та виконання плану; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації з відновлення місій та функцій].	

CP-02(04)	ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ВІДНОВЛЕННЯ ВСІХ ФУНКЦІЙ
	[Вилучено: включено до CP-02(03)].

CP-02(05)	ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - БЕЗПЕРЕРВНІСТЬ ВИКОНАННЯ КРИТИЧНИХ ФУНКЦІЙ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-02(05)_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {усі; основні};**
	CP-02(05)[01]	планується безперервність виконання критичних функцій **<CP-02(05)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** з мінімальною втратою або без втрати безперервності роботи;

	CP-02(05)[02]	безперервність підтримується до повного відновлення системи на місцях первинної обробки та/або зберігання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, що стосуються забезпечення безперервної роботи в надзвичайних ситуацій для системи; резервний план; оцінка впливу на бізнес; угоди про первинну обробку; угоди про первинне зберігання; альтернативні угоди про обробку; альтернативні угоди про місце зберігання; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану забезпечення безперервної роботи на випадок надзвичайних ситуацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування надзвичайних ситуацій та виконання плану; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації з продовження місій та ділових функцій].	

CP-02(06)	**ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - МІСЦЯ АЛЬТЕРНАТИВНОЇ ОБРОБКИ ТА ЗБЕРІГАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-02(06)_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {усі; основні};**
	CP-02(06)[01]	планується перенесення виконання критичних функцій **<CP-02(06) _ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** в альтернативні місця обробки та/або зберігання з мінімальною втратою або без втрати безперервності роботи;
	CP-02(06)[02]	підтримується безперервність роботи під час відновлення системи на первинних майданчиках обробки та/або зберігання
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для системи; резервний план; оцінка впливу на організацію; альтернативні угоди про обробку сайтів; альтернативні угоди про місце зберігання; документація тестування плану забезпечення безперервної роботи на випадок надзвичайних ситуацій; результати випробувань плану забезпечення безперервної роботи на випадок надзвичайних ситуацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування надзвичайних ситуацій та виконання плану; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для передачі основних місій та бізнес-	

	функцій на альтернативні місця для обробки / зберігання].

CP-02(07)	**ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - КООРДИНАЦІЯ З ПРОВАЙДЕРАМИ ЗОВНІШНІХ ПОСЛУГ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-02(07)	план забезпечення безперервної роботи у надзвичайних ситуаціях узгоджується з планами забезпечення безперервної роботи зовнішніх постачальників послуг, щоб гарантувати, що вимоги щодо забезпечення безперервної роботи у надзвичайних ситуаціях можуть бути виконані.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для системи; резервний план; плани зовнішніх дій; постачальники послуг; договори про рівень обслуговування; план захисту інформації; вимоги до плану забезпечення безперервної роботи у надзвичайних ситуаціях; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування надзвичайних ситуацій та виконання плану; зовнішні постачальники послуг; персонал організації, відповідальний за інформаційну безпеку].	

CP-02(08)	**ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ВИЗНАЧЕННЯ КРИТИЧНИХ АКТИВІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-02(08)_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {усі; основні};**
	CP-02(08)	визначити критичні активи системи, що підтримують критичні функції **<CP-02(08)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, що стосуються операцій з надзвичайних ситуацій для системи; резервний план; оцінка впливу на організацію; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування надзвичайних ситуацій та виконання плану; персонал організації, відповідальний за інформаційну безпеку].	

CP-03	НАВЧАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-03_ODP[01]	**визначено період часу, протягом якого необхідно провести тренінг з підготовки до дій в умовах надзвичайних ситуацій після прийняття на себе ролі або відповідальності в умовах надзвичайних ситуацій;**
	CP-03_ODP[02]	**визначено частоту проведення тренінгів для користувачів системи, які виконують непередбачувану роль або несуть відповідальність;**
	CP-03_ODP[03]	**визначено частоту, з якою необхідно переглядати та оновлювати зміст тренувань на випадок надзвичайних ситуацій;**
	CP-03_ODP[04]	**визначено події, які потребують перегляду та оновлення тренувань на випадок надзвичайних ситуацій;**
	CP-03(a)[01]	підготовка на випадок надзвичайних ситуацій надається користувачам системи відповідно до призначених ролей та обов'язків протягом **<CP-03_ODP[01] періоду часу>** з моменту прийняття на себе надзвичайної ролі або обов'язку;
	CP-03(a)[02]	навчання на випадок надзвичайних ситуацій проводиться для користувачів системи відповідно до призначених ролей та обов'язків, якщо цього вимагають зміни в системі;
	CP-03(a)[03]	користувачам системи надається навчання на випадок надзвичайних ситуацій відповідно до призначених ролей та обов'язків <**CP-03_ODP[02] частота>**;
	CP-03(b)[01]	переглядається та оновлюється зміст тренувань за планом реагування на надзвичайні ситуації **<CP-03_ODP[03] частота>**;
	CP-03(b)[02]	зміст тренувань за планом реагування на надзвичайні ситуації переглядається та оновлюється після наступних **<CP-03_ODP[04] події>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, що стосуються навчання у надзвичайних ситуаціях; резервний план; навчальна програма з надзвичайних ситуацій; навчальний матеріал з надзвичайних ситуацій; план захисту інформації; записи про навчання у надзвичайних ситуаціях; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який займається плануванням, реалізацією плану та навчанням; персонал організації, відповідальний за інформаційну безпеку].	

	Перевірка: [ВИБІР: Процеси організації для навчання у надзвичайних ситуаціях].

CP-03(01)	**НАВЧАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ - ЗІМІТОВАНІ ПОДІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-03(01)	впроваджено моделювання подій в навчанні, щоб забезпечити ефективне реагування персоналу на кризові ситуації
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, що стосуються навчання у надзвичайних ситуаціях; резервний план; навчальна програма з надзвичайних ситуацій; навчальний матеріал з надзвичайних ситуацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який займається плануванням, реалізацією плану та навчанням; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для навчання у надзвичайних ситуаціях; автоматизовані механізми моделювання подій у надзвичайних ситуаціях].	

CP-03(02)	**НАВЧАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ - АВТОМАТИЗОВАНІ НАВЧАЛЬНІ СЕРЕДОВИЩА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-03(02)	впроваджено автоматизовані механізми, щоб забезпечити більш досконале та реалістичне середовище навчання
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, що стосуються навчання у надзвичайних ситуаціях; резервний план; навчальна програма з надзвичайних ситуацій; навчальний матеріал з надзвичайних ситуацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який займається плануванням, реалізацією плану та навчанням; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для навчання у надзвичайних ситуаціях; автоматизовані механізми моделювання подій у надзвичайних ситуаціях].	

CP-04	**ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	CP-04_ODP[01]	**визначено частоту тестування плану забезпечення безперервної роботи у надзвичайних ситуаціях для системи;**
	CP-04_ODP[02]	**визначено тести для визначення ефективності плану забезпечення безперервної роботи у надзвичайних ситуаціях;**
	CP-04_ODP[03]	**визначені тести для визначення готовності до виконання плану забезпечення безперервної роботи у надзвичайних ситуаціях;**
	CP-04(a)[01]	тестується план забезпечення безперервної роботи у надзвичайних ситуаціях для системи **<CP-04_ODP[01] частота>**;
	CP-04(a)[02]	**<CP-04_ODP[02] тести>** використовуються для визначення ефективності плану;
	CP-04(a)[03]	**<CP-04_ODP[03] тести>** використовуються для визначення готовності до виконання плану;
	CP-04(b)	переглядаються результати тестування плану забезпечення безперервної роботи у надзвичайних ситуаціях;
	CP-04(c)	за необхідності ініціюються коригувальні дії.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, спрямовані на тестування плану забезпечення безперервної роботи на випадок надзвичайних ситуацій, резервний план; план захисту інформації; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану забезпечення безперервної роботи на випадок надзвичайних ситуацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за тестування плану забезпечення безперервної роботи на випадок надзвичайних ситуацій, перегляд або реагування на тести плану забезпечення безперервної роботи на випадок надзвичайних дій; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для тестування плану на випадок надзвичайних дій; автоматизовані механізми, що підтримують тестування плану дій та / або тестування плану на випадок надзвичайних ситуацій].	

CP-04(01)	**ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - КООРДИНАЦІЯ З ПОВ'ЯЗАНИМ ПЛАНАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-04(01)	координується тестування плану забезпечення безперервної роботи та відновлення функціонування з підрозділами організації, що від-

		повідають за реалізацію пов'язаних планів
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування дій у надзвичайних ситуаціях; політика реагування на інциденти; процедури, спрямовані на тестування плану дій на випадок дій у надзвичайних ситуаціях, документація тестування плану дій на випадок надзвичайних ситуацій; резервний план; плани безперервності роботи; плани відновлення після аварій; критичні інфраструктурні плани; плани реагування на кіберінциденти; плани надзвичайних ситуацій для виконуючих обов'язки; план захисту інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками тестування плану на випадок надзвичайних ситуацій; персонал організації; персонал, відповідальний за плани; персонал організації, відповідальний за інформаційну безпеку].	

CP-04(02)	**ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - АЛЬТЕРНАТИВНА ПЛАТФОРМА ТЕСТУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-04(02)(a)	план забезпечення безперервної роботи у надзвичайних ситуаціях тестується на альтернативній платформі для ознайомлення персоналу з об'єктом та наявними ресурсами;
	CP-04(02)(b)	план забезпечення безперервної роботи у надзвичайних ситуаціях тестується на альтернативній платформі для оцінки можливостей альтернативної платформи;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, спрямовані на тестування плану забезпечення безперервної роботи на випадок надзвичайних ситуаціях, резервний план; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану забезпечення безперервної роботи на випадок надзвичайних ситуацій; альтернативні угоди про обробку сайтів; угоди про рівень обслуговування; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування надзвичайних ситуацій та виконання плану; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка: [**ВИБІР: Процеси організації для тестування плану забезпечення безперервної роботи на випадок надзвичайних ситуаціях; автоматизовані механізми, що підтримують план на випадок надзвичайних ситуацій та / або тестування плану на випадок надзвичайних ситуацій].	

CP-04(03)	**ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - АВТОМАТИЧНЕ ТЕСТУВАННЯ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-04(03)_ODP	**визначено автоматизовані механізми тестування планів забезпечення безперервної роботи у надзвичайних ситуаціях;**
	CP-04(03)	план забезпечення безперервної роботи на випадок надзвичайних ситуацій тестується за допомогою **<CP-04(03)_ODP автоматизованих механізмів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури, спрямовані на тестування плану забезпечення безперервної роботи на випадок надзвичайних ситуацій, резервний план; автоматизовані механізми, що підтримують тестування плану забезпечення безперервної роботи; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану забезпечення безперервної роботи на випадок надзвичайних ситуацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за тестування плану забезпечення безперервної роботи на випадок надзвичайних ситуацій; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для тестування плану забезпечення безперервної роботи; автоматизовані механізми, що підтримують тестування плану на випадок надзвичайних ситуацій].	

CP-04(04)	**ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ПОВНЕ ВІДНОВЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-04(04)[01]	включено повне відновлення системи до відомого стану як частину тестування плану забезпечення безперервної роботи та відновлення функціонування
	CP-04(04)[02]	включено повне повернення системи до відомого стану як частину тестування плану забезпечення безперервної роботи та відновлення функціонування
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури щодо відновлення та відтворення системи; резервний план; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану забезпечення безперервної роботи на випадок надзвичайних ситуацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками тестування плану на випадок надзвичайних ситуацій; персонал організації, відповідальний за відновлення та відтворення системи; персонал організації, відповідальний за інфор-	

	маційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для тестування плану забезпечення безперервної роботи у надзвичайних ситуаціях; автоматизовані механізми, що підтримують тестування плану забезпечення безперервної роботи у надзвичайних ситуація; автоматизовані механізми підтримки відновлення та відтворення системи].

CP-04(05)	**ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - САМОВИКЛИК**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-04(05)_ODP[01]	**визначено механізми, що застосовуються для порушення та негативного впливу на систему або на компонент системи;**
	CP-04(05)_ODP[02]	**визначено систему або компонент системи, до яких застосовуються механізми порушення та негативного впливу**
	CP-04(05)	**<CP-04(05)_ODP[01] механізми>** застосовуються для порушення та негативного впливу на **<CP-04(05)_ODP[02] систему або компонент системи>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури щодо відновлення та відтворення системи; резервний план; документація про випробування на випадок надзвичайних ситуацій; результати випробувань плану забезпечення безперервної роботи на випадок надзвичайних ситуацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками тестування плану забезпечення безперервної роботи на випадок надзвичайних ситуацій; персонал організації, відповідальний за відновлення та відтворення системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для тестування планів забезпечення безперервної роботи у надзвичайних ситуаціях; механізми, що підтримують тестування планів забезпечення безперервної роботи у надзвичайних ситуаціях].	

CP-05	**ОНОВЛЕННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ**
	[Вилучено: Включено до CP-02].

CP-06	**АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-06(a)[01]	створено альтернативне місце зберігання;
	CP-06(a)[02]	створення альтернативного місця зберігання включає в себе необхідні угоди, що дозволяють зберігати та видавати інформацію резервного копіювання системи;
	CP-06(b)	в альтернативному місці зберігання впроваджені заходи захисту, аналогічні заходам захисту основної локації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних місць зберігання; резервний план; альтернативні угоди про місце зберігання; угоди про первинне зберігання; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має план забезпечення безперервної роботи у надзвичайних ситуаціях, чергує обов'язки на місці зберігання; персонал організації, відповідальний за відновлення системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації зберігання та отримання резервної інформації системи на альтернативному місці зберігання; автоматизовані механізми, що підтримують та / або реалізують зберігання та пошук резервної копії системи на альтернативному місці зберігання].	

CP-06(01)	**АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ - ВІДДІЛЕННЯ ВІД ПЕРВИННОГО СХОВИЩА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-06(01)	визначено альтернативне місце зберігання, яке відокремлено від основного місця зберігання, щоб зменшити сприйнятливість до тих самих загроз.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних місць зберігання; резервний план; альтернативне місце зберігання; альтернативні угоди про місце зберігання; угоди про первинне зберігання; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має план забезпечення безперервної роботи у надзвичайних ситуаціях, чергує обов'язки на місці зберігання; персонал організації, відповідальний за відновлення системи; персонал організації, відповідальний за інформаційну безпеку].	

CP-06(02)	АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ - ЧАС ВІДНОВЛЕННЯ ТА ВСТАНОВЛЕННЯ ЦІЛЕЙ ВІДНОВЛЕННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-06(02)[01]	налаштувати альтернативне місце зберігання для полегшення операцій відновлення відповідно до часу відновлення;
	CP-06(02)[02]	налаштувати альтернативне місце зберігання для полегшення операцій відновлення відповідно до встановлених цілей відновлення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних місць зберігання; резервний план; альтернативе місце зберігання; альтернативні угоди про місце зберігання; альтернативні конфігурації місця зберігання; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації з обов'язками тестування плану на випадок надзвичайних ситуацій; персонал організації, відповідальний за тестування пов'язаних планів; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для тестування плану забезпечення безперервної роботи на випадок надзвичайних ситуаціях; автоматизовані механізми, що підтримують цілі відновлення часу / точок].	

CP-06(03)	АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ - ДОСТУПНІСТЬ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-06(03)[01]	визначено потенційні проблеми доступності для альтернативного місця зберігання в разі збоїв або стихійних лих по всьому регіоні;
	CP-06(03)[02]	в загальних рисах окреслено дії щодо пом'якшення наслідків
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних місць зберігання; резервний план; альтернативне місце зберігання; перелік можливих проблем із доступністю до альтернативного місця зберігання; дії щодо пом'якшення наслідків проблем із доступністю до альтернативного місця зберігання; оцінки ризиків організації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має план забезпечення безперервної роботи у надзвичайних ситуаціях, чергує обов'язки на місці зберігання; персонал організації, відповідальний за відновлення системи; персонал органі-	

	зації, відповідальний за інформаційну безпеку].

CP-07	**АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК РОБОТИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-07_ODP[01]	**визначені операції системи для основних завдань і функцій;**
	CP-07_ODP[02]	**визначено період часу, відповідно термінам відновлення та встановленим цілям відновлення;**
	CP-07(a)	альтернативний майданчик для роботи, включно з необхідними угодами, які дозволяють передачу та відновлення **<CP-07_ODP[01] операцій системи>** для виконання основних завдань та функцій, створюється протягом **<CP-07_ODP[02] періоду часу>**, коли можливості основного майданчика недоступні;
	CP-07(b)[01]	обладнання та прилади, необхідні для передачі, доступні на альтернативному місці роботи або якщо укладені контракти на підтримку доставки на це місце протягом **<CP-07_ODP[02] періоду часу>** для передачі;
	CP-07(b)[02]	обладнання та прилади, необхідні для відновлення, доступні на альтернативному місці роботи або якщо укладені контракти на підтримку доставки на це місце протягом **<CP-07_ODP[02] періоду часу>** для передачі;
	CP-07(c)	впроваджено на альтернативному майданчику роботи заходи захисту, еквівалентні тим, що впровадженні на основному майданчику.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних місць обробки; резервний план; угоди про альтернативні місця роботи; угоди про основні місця роботи; запасне обладнання та прилади на альтернативній ділянці роботи; договори на обладнання та постачання; угоди про рівень обслуговування; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування надзвичайних ситуацій та / або альтернативну організацію майданчика; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Персонал організації з відновлення на альтернативному місці; автоматизовані механізми, що підтримують та / або реалізують відновлення на альтернативному місці].	

CP-07(01)	**АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ВІДДІЛЕННЯ ВІД ОСНОВНОГО МАЙДАНЧИКА**

	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-07(01)	визначено альтернативний майданчик для роботи, який відокремлений від основного майданчика, з метою зменшення сприйнятливості до тих самих загроз
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних майданчиків роботи; резервний план; альтернативне місце роботи; угоди про альтернативні місця роботи; угоди про основні місця роботи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має план забезпечення безперервної роботи у надзвичайних ситуаціях, чергує обов'язки по обробці місця; персонал організації, відповідальний за відновлення системи; персонал організації, відповідальний за інформаційну безпеку].	

CP-07(02)	**АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ДОСТУПНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-07(02)[01]	визначено потенційні проблеми доступності для альтернативного майданчика для роботи в разі збоїв або катастрофи по всьому регіону
	CP-07(02)[02]	окреслено чіткі заходи щодо пом'якшення наслідків
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних місць роботи; резервний план; альтернативе місце роботи; угоди про альтернативні місця роботи; угоди про основні місця роботи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має план забезпечення безперервної роботи у надзвичайних ситуаціях, чергує обов'язки по обробці місця; персонал організації, відповідальний за відновлення системи; персонал організації, відповідальний за інформаційну безпеку].	

CP-07(03)	**АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ПРІОРИТЕТ ОБСЛУГОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-07(03)	розроблено угоди про альтернативний майданчик для роботи, які містять положення щодо пріоритету обслуговування відповідно до вимог стосовно доступності (включно з вимогами щодо часу відно-

		влення).
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних місць роботи; резервний план; угоди про альтернативні місця роботи; угоди про рівень обслуговування; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має план забезпечення безперервної роботи у надзвичайних ситуаціях, чергує обов'язки у місці обробки; персонал організації, відповідальний за відновлення системи; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за придбання / договірні угоди].	

CP-07(04)	**АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ПІДГОТОВКА ДЛЯ ВИКОРИСТАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-07(04)	підготовлено альтернативний майданчик для роботи таким чином, щоб майданчик був готовий до використання як оперативний майданчик, що підтримує виконання основних завдань та функцій
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних місць роботи; резервний план; альтернативний майданчик роботи; угоди про альтернативні місця роботи; конфігурація альтернативного робочого місця; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який має план забезпечення безперервної роботи у надзвичайних ситуаціях, чергує обов'язки по обробці місця; персонал організації, відповідальний за відновлення системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують відновлення на альтернативному робочому місці].	

CP-07(05)	**АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ЕКВІВАЛЕНТНІ ЗАХОДИ БЕЗПЕКИ ІНФОРМАЦІЇ**
	[Вилучено: Включено до CP-07]

CP-07(06)	**АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - НЕЗДАТНІСТЬ ПОВЕРНУТИСЯ НА ОСНОВНИЙ МАЙДАНЧИК**
	МЕТА ОЦІНКИ: Визначити, чи:

	CP-07(06)[01]	розроблено план до обставин, які виключають повернення на основне місце роботи;
	CP-07(06)[02]	підготувалися до обставин, які виключають повернення на основне місце роботи;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження: [**ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних місць роботи; резервний план; альтернативний майданчик роботи; угоди про альтернативні місця роботи; конфігурація альтернативного робочого місця; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за відновлення системи; персонал організації, відповідальний за інформаційну безпеку].	

CP-08	**КОМУНІКАЦІЙНІ ПОСЛУГИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-08_ODP[01]	**визначено операції системи, які необхідно відновити для виконання основних завдань та функцій;**
	CP-08_ODP[02]	**визначено період часу, протягом якого необхідно відновити основні завдання та функції, коли основні комунікаційні можливості недоступні;**
	CP-08	альтернативні комунікаційні послуги, включно з необхідними угодами, що дозволяють відновити **<CP-08_ODP[01] операції системи>**, створюються для основних завдань та функцій протягом **<CP-08_ODP[02] періоду часу>**, коли основні комунікаційні можливості недоступні на основному або альтернативному місцях роботи або зберігання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних комунікаційних послуг; резервний план; основні та альтернативні угоди про послуги з комунікації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за план забезпечення безперервної роботи у надзвичайних ситуацій; персонал організації, відповідальний за відновлення системи; персонал організаціїз обов'язками інформаційної безпеки; персонал організації, відповідальний за придбання / договірні угоди]. **Перевірка:** [ВИБІР: Автоматизовані механізми підтримки комунікацій].	

CP-08(01)	**КОМУНІКАЦІЙНІ ПОСЛУГИ - ПРІОРИТЕТ ПОСТАЧАННЯ ПОСЛУГ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-08(01)(a)[01]	розроблено угоди про надання основних комунікаційних послуг, які містять пріоритетні положення про надання послуг відповідно до вимог щодо доступності (включно з вимогами щодо часу відновлення);
	CP-08(01)(a)[02]	розроблено альтернативні угоди про надання комунікаційних послуг, які містять положення про пріоритетність надання послуг відповідно до вимог доступності (включно з вимогами щодо часу відновлення);
	CP-08(01)(b)	надсилається запит про пріоритети комунікаційних послуг для всіх комунікаційних послуг, що використовуються для забезпечення безперервності роботи, якщо основні та/або альтернативні комунікаційні послуги надаються загальним оператором.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до основних та альтернативних комунікаційних послуг; резервний план; первинні та альтернативні угоди про послуги з телекомунікацій; пріоритетна документація щодо послуг зв'язку; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обов'язки щодо плану забезпечення безперервної роботи у надзвичайних ситуаціях; персонал організації, відповідальний за відновлення системи; персонал організації з обов'язками інформаційної безпеки; персонал організації, відповідальний за придбання / договірні угоди]. **Перевірка:** [ВИБІР: Автоматизовані механізми підтримки комунікацій].	

CP-08(02)	**КОМУНІКАЦІЙНІ ПОСЛУГИ - ЄДИНІ ТОЧКИ ВІДМОВИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-08(02)	отримано альтернативні комунікаційні послуги з метою зменшення ймовірності спільного використання єдиної точки відмови з основними комунікаційними послугами.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до основних та альтернативних комунікаційних послуг; резервний план; основні та альтернативні угоди про послуги з комунікацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обов'язки щодо плану забезпечення безперервної роботи у надзвичайних ситуаціях; персонал	

	організації, відповідальний за відновлення системи; основні та альтернативні постачальники послуг зв'язку; персонал організації, відповідальний за інформаційну безпеку].

CP-08(03)	**КОМУНІКАЦІЙНІ ПОСЛУГИ - ВІДДІЛЕННЯ ОСНОВНИХ ТА АЛЬТЕРНАТИВНИХ ПРОВАЙДЕРІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-08(03)	отримуються альтернативні комунікаційні послуги від постачальників, які відокремлені від основних постачальників послуг, щоб зменшити сприйнятливості до тих самих загроз.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до основних та альтернативних комунікаційних послуг; резервний план; основні та альтернативні угоди про послуги з комунікацій; альтернативне місце постачальника послуг зв'язку; сайт провайдера первинних комунікаційних послуг; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обов'язки щодо плану забезпечення безперервної роботи у надзвичайних ситуаціях; персонал організації, відповідальний за відновлення системи; первинні та альтернативні постачальники послуг зв'язку; персонал організації, відповідальний за інформаційну безпеку].	

CP-08(04)	**КОМУНІКАЦІЙНІ ПОСЛУГИ - ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ПОСТАЧАЛЬНИКА КОМУНІКАЦІЙНИХ ПОСЛУГ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-08(04)_ODP[01]	**визначено частоту, з якою постачальники послуг повинні надавати свідчення про тестування планів забезпечення безперервної роботи;**
	CP-08(04)_ODP[02]	**визначено частоту, з якою постачальники послуг повинні надавати свідчення про тренування з планів забезпечення безперервної роботи;**
	CP-08(04)(a)[01]	постачальники основних комунікаційних послуг зобов'язані мати плани забезпечення безперервної роботи;
	CP-08(04)(a)[02]	постачальники альтернативних комунікаційних послуг зобов'язані мати плани забезпечення безперервної роботи;
	CP-08(04)(b)	переглядаються плани забезпечення безперервної роботи постачальників комунікаційних послуг для забезпечення

		відповідності планам забезпечення безперервної роботи організації;
	CP-08(04)(c)[01]	отримано свідчення про тестування планів забезпечення безперервної роботи **<CP-08(04)_ODP[01] частота>**.
	CP-08(04)(c)[02]	отримано свідчення про тренування з планів забезпечення безперервної роботи <**CP-08(04)_ODP[02] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до основних та альтернативних комунікаційних послуг; резервний план; основні та альтернативні угоди про послуги з комунікацій; альтернативне місце постачальника послуг зв'язку; сайт провайдера первинних комунікаційних послуг; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обов'язки щодо плану забезпечення безперервної роботи у надзвичайних ситуаціях; персонал організації, відповідальний за відновлення системи; первинні та альтернативні постачальники послуг зв'язку; персонал організації, відповідальний за інформаційну безпеку].	

CP-08(05)	**КОМУНІКАЦІЙНІ ПОСЛУГИ - ТЕСТУВАННЯ АЛЬТЕРНАТИВНИХ КОМУНІКАЦІЙНИХ ПОСЛУГ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-08(05)_ODP	визначено частоту з якою необхідно тестувати надання альтернативних комунікаційних послуг;
	CP-08(05)	тестування надання альтернативних комунікаційних послуг з **<CP-08(05)_ODP частотою>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування забезпечення безперервної роботи у надзвичайних ситуаціях; процедури звернення до альтернативних комунікаційних послуг; резервний план; докази тестування альтернативних комунікаційних послуг; альтернативні угоди про послуги з комунікацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування на випадок надзвичайних ситуацій, виконання плану та тестування; альтернативні постачальники послуг; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують тестування альтернативних комунікаційних послуг].	

CP-09	**РЕЗЕРВНЕ КОПІЮВАННЯ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-09_ODP[01]	**визначено компоненти системи, для яких необхідно проводити резервне копіювання інформації користувачів;**
	CP-09_ODP[02]	**визначено частоту, з якою слід проводити резервне копіювання інформації користувача відповідно до часу відновлення та цілей відновлення;**
	CP-09_ODP[03]	**визначено частоту проведення резервного копіювання інформації системи, що відповідає завдань відновлення і встановлених цілей відновлення;**
	CP-09_ODP[04]	**визначено частоту, з якою слід проводити резервне копіювання документації системи відповідно до часу відновлення та цілей точки відновлення;**
	CP-09(a)	резервне копіювання інформації користувача, що міститься в **<CP-09_ODP[01] компонентах системи>**, здійснюється **<CP-09_ODP[02] частота>**;
	CP-09(b)	виконується резервне копіювання інформації системи, що міститься в системі **<CP-09_ODP[03] частота>**;
	CP-09(c)	створюються резервні копії документації системи, включаючи документацію, пов'язану з безпекою та конфіденційністю **<CP-09_ODP[04] частота>**;
	CP-09(d)[01]	конфіденційність резервних копій інформації захищена;
	CP-09(d)[02]	цілісність резервних копій інформації захищена;
	CP-09(d)[03]	доступність резервних копій інформації захищена.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання системи; резервний план; резервне місце (місця) зберігання; журнали або записи резервного копіювання системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за резервне копіювання системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для проведення резервних копій систем; автоматизовані механізми підтримки та / або реалізації резервних копій систем].	

CP-09(01)	**РЕЗЕРВНЕ КОПІЮВАННЯ - ВИПРОБУВАННЯ НА НАДІЙНІСТЬ ТА ЦІЛІСНІСТЬ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	CP-09(01)_ODP[01]	**визначено частоту тестування на надійність носіїв резервних копій інформації;**
	CP-09(01)_ODP[02]	**визначено частоту тестування на цілісність носіїв резервних копій інформації;**
	CP-09(01)[01]	носії резервних копій інформації тестується **<CP-09(01)_ODP[01] частота>** для перевірки надійності;
	CP-09(01)[02]	носії резервних копій інформації тестується **<CP-09(01)_ODP[02] частота>** для перевірки цілісності;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання системи; резервний план; результати тестування резервної копії системи; документація на випробування плану забезпечення безперервної роботи у надзвичайних ситуаціях; результати випробувань плану забезпечення безперервної роботи у надзвичайних ситуаціях; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за резервне копіювання системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для проведення резервних копій систем; автоматизовані механізми підтримки та / або реалізації резервних копій систем].	

CP-09(02)	**РЕЗЕРВНЕ КОПІЮВАННЯ - ТЕСТУВАННЯ ВІДНОВЛЕННЯ З ВИКОРИСТАННЯМ ЗРАЗКІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-09(02)	використовується зразок резервної копії інформації при відновленні вибраних функцій системи як частину тестування плану забезпечення безперервної роботи та відновлення функціонування
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання системи; резервний план; результати тестування резервної копії системи; документація на випробування плану забезпечення безперервної роботи на випадок непередбачених ситуацій; результати випробувань плану забезпечення безперервної роботи на випадок непередбачених ситуацій; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за резервне копіювання системи; персонал організації, який відповідає за планування на випадок непередбачених ситуацій / тестування плану забезпечення безперервної роботи на випадок непередбачених ситуацій; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для проведення резервних копій сис-	

	тем; автоматизовані механізми підтримки та / або реалізації резервних копій систем].

CP-09(03)	**РЕЗЕРВНЕ КОПІЮВАННЯ - ВІДОКРЕМЛЕНЕ СХОВИЩЕ КРИТИЧНОЇ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-09(03)_ODP	**визначено критичного системного програмного забезпечення та іншої інформації, пов'язаної з безпекою яке має зберігатися в окремому сховищі або у вогнетривкому контейнері;**
	CP-09(03)	резервні копії **<CP-09(03)_ODP критичного системного програмного забезпечення та іншої інформації, пов'язаної з безпекою>** зберігаються в окремому сховищі або у вогнетривкому контейнері, не пов'язаному з системою.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання системи; резервний план; резервне місце (місця) зберігання; конфігурації резервної копії системи та супутня документація; журнали або записи резервного копіювання системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування на випадок надзвичайних ситуацій та виконання плану; персонал організації, відповідальний за резервне копіювання системи; персонал організації, який відповідає за інформаційну безпеку].	

CP-09(04)	**РЕЗЕРВНЕ КОПІЮВАННЯ - ЗАХИСТ ВІД НЕАВТОРИЗОВАНИХ МОДИФІКАЦІЙ**
	[Вилучено: Включено до CP-09].

CP-09(05)	**РЕЗЕРВНЕ КОПІЮВАННЯ - ПЕРЕДАЧА НА АЛЬТЕРНАТИВНЕ СХОВИЩЕ ЗБЕРІГАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-09(05)_ODP[01]	**визначено період часу, що відповідає часу відновлення та цілям відновлення;**
	CP-09(05)_ODP[02]	**визначено швидкість передачі даних, що відповідає часу відновлення та цілям відновлення;**
	CP-09(05)[01]	інформація резервної копії системи передається до альтернативного сховища протягом **<CP-09(05)_ODP[01] періоду часу>**;

	CP-09(05)[02]	інформація резервної копії системи передається до альтернативного сховища з **<CP-09(05)_ODP[02] швидкість передачі >**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання системи; резервний план; журнали або записи резервного копіювання системи; докази про резервне копіювання системи, переданої на альтернативне місце зберігання; альтернативні угоди про місця зберігання; інші відповідні документи або записи] **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за резервне копіювання системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для передачі резервних копій системи на альтернативне місце зберігання; автоматизовані механізми підтримки та / або реалізації резервних копій систем; автоматизовані механізми, що підтримують та / або реалізують передачу інформації до альтернативного місця зберігання].	

CP-09(06)	**РЕЗЕРВНЕ КОПІЮВАННЯ - НАДЛИШКОВА ВТОРИННА СИСТЕМА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-09(06)[01]	резервне копіювання системи здійснюється шляхом підтримки надлишкової вторинної системи, яка не пов'язана з первинною системою;
	CP-09(06)[02]	резервне копіювання системи здійснюється шляхом підтримки резервної вторинної системи, яка може бути активована без втрати інформації або порушення роботи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання системи; резервний план; результати тестування резервної копії системи; результати випробувань плану забезпечення безперервної роботи на випадок непередбачених ситуацій; документація на випробування плану на випадок непередбачених ситуацій; резервна вторинна система для резервного копіювання системи; розташування надлишкових вторинних систем резервного копіювання; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за резервне копіювання системи; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за надлишкову вторинну систему]. **Перевірка:** [ВИБІР: Процеси організації для підтримки надлишкових вторинних систем; автоматизовані механізми підтримки та / або реалізації резервних копій систем; автоматизовані механізми, що підтримують та / або реалізують передачу інформації до резервної вторинної системи].	

CP-09(07)	**РЕЗЕРВНЕ КОПІЮВАННЯ - ПОДВІЙНА АВТОРИЗАЦІЯ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-09(07)_ODP	**визначено резервну інформацію, для якої необхідно застосувати подвійну авторизацію з метою видалення або знищення;**
	CP-09(07)	застосовано подвійну авторизацію для видалення або знищення **<CP-09(07)_ODP резервної інформації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання системи; резервний план; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік подвійних повноважень або правил авторизації; журнали або записи видалення або знищення резервної інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за резервне копіювання системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують подвійну авторизацію; автоматизовані механізми підтримки та / або реалізації видалення / знищення резервної інформації].	

CP-09(08)	**РЕЗЕРВНЕ КОПІЮВАННЯ - КРИПТОГРАФІЧНИЙ ЗАХИСТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-09(08)_ODP	**визначено резервні копії інформації для захисту від несанкціонованого розкриття та змін;**
	CP-09(08)	реалізовано криптографічні механізми для запобігання несанкціонованому розкриттю та зміні **<CP-09(08)_ODP резервної інформації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання системи; резервний план; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік подвійних повноважень або правил авторизації; журнали або записи видалення або знищення резервної інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за резервне копіювання системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують подвійну авторизацію; автоматизовані механізми підтримки та / або реалізації видалення / знищення резервної інформації].	

CP-10	ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-10_ODP[01]	**визначено період часу для відновлення, часу та цілям відновлення системи;**
	CP-10_ODP[02]	**визначено період часу для відтворення, часу та цілям відновлення системи;**
	CP-10[01]	відновлення системи до відомого стану забезпечується протягом **<CP-10_ODP[01] часу>** після збою, компрометації або помилки;
	CP-10[02]	відтворення системи до відомого стану забезпечується протягом **<CP-10_ODP[02] часу>** після збою, компрометації або помилки;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються резервного копіювання системи; резервний план; результати тестування резервної копії системи; результати випробувань плану забезпечення безперервної роботи на випадок непередбачених ситуацій; документація на випробування плану на випадок непередбачених ситуацій; резервна вторинна система для резервного копіювання системи; розташування надлишкових вторинних систем резервного копіювання; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за планування, відновлення та / або відновлення; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації, що реалізують операції з відновлення та відновлення системи; автоматизовані механізми, що підтримують та / або впроваджують операції з відновлення та відтворення системи].	

CP-10(01)	ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ
	[Вилучено: Включено до CP-04].

CP-10(02)	ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ВІДНОВЛЕННЯ ТРАНЗАКЦІЙ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-10(02)	реалізовано відновлення транзакцій для систем, що базуються на транзакціях
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури відновлення та відтворення системи; резервний план; проєктна	

	документація системи; налаштування конфігурації системи та відповідна документація; документація на випробування плану на випадок непередбачених ситуацій; результати випробувань плану забезпечення безперервної роботи на випадок непередбачених ситуацій; записи відновлення транзакцій системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за відновлення транзакцій; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість відновлення транзакцій].

CP-10(03)	**ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - КОМПЕНСАЦІЙНІ ЗАХОДИ ЗАХИСТУ**
	[Вилучено: Переадресовано через процедури адаптації].

CP-10(04)	**ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ВІДНОВЛЕННЯ В МЕЖАХ ЧАСОВОГО ПЕРІОДУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-10(04)_ODP	**визначено період часу відновлення, протягом якого компоненти системи відновлюються до відомого, робочого стану;**
	CP-10(04)	забезпечено можливість відновлення компонентів системи протягом **<CP-10(04)_ODP період часу відновлення>** з інформації управління конфігурацією та захищеною цілісністю, яка описує відомий робочий стан компонентів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури відновлення та відтворення системи; резервний план; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація на випробування плану на випадок непередбачених ситуацій результати випробувань плану на випадок непередбачених ситуацій; докази операцій з відновлення та відтворення системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за відновлення та відтворення системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують відновлення / відтворення інформації системи].	

CP-10(05)	**ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ЗДАТНІСТЬ ВІДМОВОСТІЙКОСТІ**

	[Вилучено: Включено до SI-13].

CP-10(06)	**ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ЗАХИСТ КОМПОНЕНТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-10(06)	забезпечино захист компонентів системи, які використовуються для резервного відновлення та відтворення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури відновлення та відтворення системи; резервний план; проєктна документація системи; налаштування конфігурації системи та відповідна документація; дані логічного доступу; облікові дані фізичного доступу; записи авторизації логічного доступу; записи фізичних дозволів доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за відновлення та відтворення системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для захисту апаратного забезпечення, прошивки та програмного забезпечення для резервного копіювання та відновлення; автоматизовані механізми, що підтримують і / або здійснюють захист резервного копіювання та відновлення апаратних засобів, програмно-апаратних та програмних]].	

CP-11	**АЛЬТЕРНАТИВНІ ПРОТОКОЛИ ЗВ'ЯЗКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-11_ODP	**організація визначає альтернативні протоколи зв'язку для підтримки збереження безперервності функціонування**
	CP-11	організація забезпечує можливість застосування **<CP-11_ODP альтернативних протоколів зв'язку>** для підтримки збереження безперервності функціонування
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР:Політика планування на випадок непередбачених ситуацій; процедури, що стосуються альтернативних протоколів зв'язку; резервний план; план безперервності операцій; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік альтернативних протоколів зв'язку, що підтримують безперервність операцій; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування на випадок надзвичайних ситуацій та виконання плану; персонал організації з безперервні-	

	стю оперативного планування та відповідальності за виконання плану; персонал організації який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР:Автоматизовані механізми, що використовують альтернативні протоколи зв'язку].

CP-12	**БЕЗПЕЧНИЙ РЕЖИМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-12_ODP[01]	визначено умови, за яких організація вводить безпечний режим роботи;
	CP-12_ODP[02]	визначено обмеження в безпечному режимі роботи;
	CP-12	при виявлені **<CP-12_ODP[01] умови>**, вводиться безпечний режим роботи з **<CP-12_ODP[02] обмеженням>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються безпечного режиму роботи системи; резервний план; проєктна документація системи; налаштування конфігурації системи та відповідна документація; посібники з адміністрування системи; посібники з експлуатації системи; посібники з встановлення системи; протоколи випробувань на випадок непередбачених ситуацій; записи про обробку інцидентів; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують безпечний режим роботи].	

CP-13	**АЛЬТЕРНАТИВНІ МЕХАНІЗМИ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	CP-13_ODP[01]	**визначені альтернативні або додаткові механізми безпеки;**
	CP-13_ODP[02]	**визначені функції безпеки;**
	CP-13	**<CP-13_ODP[01] альтернативні або додаткові механізми безпеки>** використовуються для реалізації **<CP-13_ODP[02] функцій безпеки>**, коли основні засоби реалізації функцій безпеки недоступні або скомпрометовані.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політика планування на випадок непередбачених ситуацій; процедури, що стосуються альтернативних механізмів безпеки; резервний план; план безперервності операцій; проєктна документація системи; налаштування конфігурації системи та відповідна документація; протоколи випробувань на випадок непередбачених ситуацій; результати випробувань плану на випадок непередбачених ситуацій; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Можливість системи впроваджувати альтернативні механізми безпеки].

VII. КЛАС ЗАХОДІВ ЗАХИСТУ IA – ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

IA-01	ПОЛІТИКА ТА ПРОЦЕДУРИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-01_ODP[01]	**визначено персонал або ролі, на які поширюється політика ідентифікації та автентифікації;**
	IA-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури ідентифікації та автентифікації;**
	IA-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесів; рівень системи};**
	IA-01_ODP[04]	**визначено посадову особу, яка управляє політикою та процедурами ідентифікації та автентифікації;**
	IA-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика ідентифікації та автентифікації;**
	IA-01_ODP[06]	**визначено події, які потребують перегляду та оновлення поточної політики ідентифікації та автентифікації;**
	IA-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні процедури ідентифікації та автентифікації;**
	IA-01_ODP[08]	**визначено події, які потребують перегляду та оновлення процедур ідентифікації та автентифікації;**
	IA-01(a)[01]	розроблено та задокументовано політику ідентифікації та автентифікації;
	IA-01(a)[02]	політика ідентифікації та автентифікації поширюється на **<IA-01_ODP[01] персонал або ролі>**;
	IA-01(a)[03]	розроблені та задокументовані процедури ідентифікації та автентифікації, що сприяють впровадженню політики ідентифікації та автентифікації, а також відповідні заходи ідентифікації та перевірки автентичності;
	IA-01(a)[04]	процедури ідентифікації та автентифікації поширюються на **<IA-01_ODP[02] персонал або ролі>**;
	IA-01(a)[01](a)[01]	**<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політики ідентифікації та автентифікації містить мету;

	IA-01(a)[01](a)[02]	**<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політики ідентифікації та автентифікації містить сферу застосування;
	IA-01(a)[01](a)[03]	**<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політики ідентифікації та автентифікації містить ролі;
	IA-01(a)[01](a)[04]	**<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політики ідентифікації та автентифікації містить обов'язки;
	IA-01(a)[01](a)[05]	**<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політики ідентифікації та автентифікації містить відповідальність керівництва;
	IA-01(a)[01](a)[06]	**<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політики ідентифікації та автентифікації містить координацію між підрозділами організації;
	IA-01(a)[01](a)[07]	**<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політики ідентифікації та автентифікації містить систему контролю відповідності;
	IA-01(a)[01](b)	політика ідентифікації та автентифікації **<IA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** відповідає чинному законодавству, виконавчим розпорядженням, директивам, положенням, політиці, стандартам і керівним принципам;
	IA-01(b)	**<IA-01_ODP[04] посадова особа>** призначається для управління політикою та процедурами ідентифікації та автентифікації;
	IA-01(c)[01][01]	переглядається та оновлюється поточна політика ідентифікації та автентифікації **<IA-01_ODP[05] частота>**;
	IA-01(c)[01][02]	переглядається та оновлюється поточна політика ідентифікації та автентифікації після **<IA-01_ODP[06] подій>**;
	IA-01(c)[02][01]	переглядаються та оновлюються поточні процедури ідентифікації та автентифікації **<IA-01_ODP[07] частота>**;
	IA-01(c)[02][02]	переглядаються та оновлюються поточні процедури ідентифікації та автентифікації після **<IA-01_ODP[08] подій>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури ідентифікації та автентифікації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику ідентифікації та автентифікації; персонал, відповідальний за інформаційну безпеку].	

IA-02	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ)**

	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-02[01]	користувачі унікально ідентифіковані та автентифіковані;
	IA-02[02]	процеси що діють від імені користувачів унікально ідентифіковані та автентифіковані;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; список облікових записів системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; персонал організації, відповідальний за управління обліковими записами; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для однозначної ідентифікації та автентифікації користувачів; автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації].	

IA-02(01)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-02(01)	реалізувано багатофакторну автентифікацію для доступу до привілейованих облікових записів
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; список облікових записів системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, відповідальний за управління обліковими записами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість багатофакторної автентифікації].	

IA-02(02)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ НЕПРИВІЛЕЙОВАНИХ**

	ОБЛІКОВИХ ЗАПИСІВ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-02(02)	реалізовано багатофакторну автентифікацію для доступу до непривілейованих облікових записів
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; перелік облікових записів системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, відповідальний за управління обліковими записами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість багатофакторної автентифікації].	

IA-02(03)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ЛОКАЛЬНИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ**
	[Вилучено: Включено до IA-02(01)].

IA-02(04)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ЛОКАЛЬНИЙ ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ**
	[Вилучено: Включено до IA-02(02)].

IA-02(05)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ІНДИВІДУАЛЬНА АВТЕНТИФІКАЦІЯ З ГРУПОВОЮ АВТЕНТИФІКАЦІЄЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-02(05)	користувачі повинні пройти індивідуальну автентифікацію перед наданням доступу до спільних облікових записів або ресурсів, якщо використовуються спільні облікові записи або автентифікатори.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація	

	системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; перелік облікових записів системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, відповідальний за управління обліковими записами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість автентифікації для групових облікових записів].

IA-02(06)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - МЕРЕЖЕВИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ – ОКРЕМИЙ ПРИСТРІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-02(06)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {локальний; мережевий; віддалений};**
	IA-02(06)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: { привілейовані облікові записи; непривілейовані облікові записи};**
	IA-02(06)_ODP[03]	**визначено вимоги до міцності механізму, який має забезпечуватися окремим від системи пристроєм, що отримує доступ до облікових записів;**
	IA-02(06)(a)	багатофакторна автентифікація реалізована для **<IA-02(06)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** доступу до **<IA-02(06)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** таким чином, що один з факторів забезпечується пристроєм, окремим від системи, який отримує доступ;
	IA-02(06)(b)	реалізовано багатофакторну автентифікацію для **<IA-02(06)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** доступу до **<IA-02(06)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ІВ)>** таким чином, щоб пристрій відповідав **<IA-02(06)_ODP[03] вимогам до міцності механізму>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; перелік облікових записів системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування сис-	

	теми; персонал організації, відповідальний за управління обліковими записами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість автентифікації для групових облікових записів].

IA-02(07)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - МЕРЕЖЕВИЙ ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ – ОКРЕМИЙ ПРИСТРІЙ**
	[Вилучено: Включено до IA-02(01)].

IA-02(08)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ДОСТУП ДО ОБЛІКОВИХ ЗАПИСІВ – СТІЙКІСТЬ ДО ВІДТВОРЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-02(08)_ODP	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {привілейовані облікові записи; непривілейовані облікові записи};**
	IA-02(08)	реалізовано стійкі до повторного відтворення механізми автентифікації для доступу до **<IA-02(08)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; перелік привілейованих облікових записів системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, відповідальний за управління обліковими записами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що підтримують та / або впроваджують стійкі до відтворення механізми автентифікації].	

IA-02(09)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ – СТІЙКІСТЬ ДО ВІДТВОРЕННЯ**
	[Вилучено: Включено до IA-02(08)].

IA-02(10)	ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ЄДИНА ТОЧКА ВХОДУ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-02(10)_ODP	**визначено облікові записи та послуги системи, для яких має бути забезпечена можливість єдиного входу;**
	IA-02(10)	забезпечено можливість єдиного входу для **<IA-02(10)_ODP облікових записів і послуг системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються можливості єдиного входу для облікових записів та послуг системи; процедури, що стосуються ідентифікації та автентифікації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; перелік облікових записів та послуг системи, що вимагають можливості єдиного входу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, відповідальний за управління обліковими записами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що підтримують та / або впроваджують можливість єдиного входу для облікових записів та послуг системи].	

IA-02(11)	ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ВІДДАЛЕНИЙ ДОСТУП - ОКРЕМИЙ ПРИСТРІЙ
	[Вилучено: Включено до IA-02(06)].

IA-02(12)	ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ПРИЙНЯТТЯ ПОВНОВАЖЕНЬ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИСТОЇ ІНФОРМАЦІЇ (PIV CREDENTIALS)	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-02(12)	приймаються та електронним шляхом підтверджуються повноваження облікових даних особистої ідентифікації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи	

	аудиту системи; записи перевірки PIV; докази посвідчення особи PIV; уповноваження PIV; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, відповідальний за управління обліковими записами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують прийняття та перевірку облікових даних PIV].

IA-02(13)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - АВТЕНТИФІКАЦІЯ ПО ЗОВНІШНЬОМУ КАНАЛУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-02(13)_ODP[01]	**визначено механізми зовнішньої автентифікації;**
	IA-02(13)_ODP[02]	**визначено умови, за яких має бути реалізована зовнішня автентифікація;**
	IA-02(13)	**<IA-02(13)_ODP[01] механізми зовнішньої автентифікації>** застосовано за **<IA-02(13)_ODP[02] умов>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; план захисту інформації; процедури, що стосуються ідентифікації та автентифікації користувачів; налаштування конфігурації системи та пов'язана з ними документація; записи аудиту системи; список зовнішніх шляхів автентифікації, що генеруються системою; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за роботу системи; або персонал організації, відповідальний за управління обліковими записами; або персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори; системні розробники]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують можливість зовнішньої автентифікації].	

IA-03	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-03_ODP[01]	**визначені пристрої та/або типи пристроїв, які повинні бути унікально ідентифіковані та автентифіковані перед установкою підключення;**
	IA-03_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {локальний; віддалений; мережевий};**

	IA-03	**<IA-03_ODP[01] пристрої та/або типи пристроїв>** унікально ідентифіковані та автентифіковано перед встановленням підключення **<IA-03_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації пристрою; проєктна документація системи; перелік пристроїв, що вимагають унікальної ідентифікації та автентифікації; звіти про підключення пристрою; налаштування конфігурації системи та відповідна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за ідентифікацію та автентифікацію пристрою; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість ідентифікації та автентифікації пристрою].	

IA-03(01)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - КРИПТОГРАФІЧНА ДВОБІЧНА АВТЕНТИФІКАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-03(01)_ODP[01]	**визначено пристрої та/або типи пристроїв, які потребують використання двобічної автентифікації яка заснована на криптографічних механізмах для автентифікації перед встановленням підключення;**
	IA-03(01)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {локальний; віддалений; мережевий};**
	IA-03(01)	**<IA-03(01)_ODP[01] пристрої та/або типи пристроїв>** автентифікуються перед встановленням підключення **<IA-03(01)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації пристрою; проєктна документація системи; перелік пристроїв, що вимагають унікальної ідентифікації та автентифікації; звіти про підключення пристрою; налаштування конфігурації системи та відповідна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за ідентифікацію та автентифікацію пристрою; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість аутентифікації пристрою; криптографічно засновані двобічні механізми автентифікації].	

IA-03(02)	ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - КРИПТОГРАФІЧНИЙ ДВОБІЧНА МЕРЕЖА АВТЕНТИФІКАЦІЯ
	[Виключено: включено до IA-03(01)].

IA-03(03)	ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - ДИНАМІЧНИЙ РОЗПОДІЛ АДРЕСИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-03(03)_ODP[01]	**визначено інформацію про оренду, яку буде використано для стандартизації динамічного розподілу адрес для пристроїв;**
	IA-03(03)_ODP[02]	**визначено тривалість оренди, яка буде використовуватися для стандартизації динамічного виділення адрес для пристроїв;**
	IA-03(03)(a)[01]	інформація про оренду динамічного розподілу адрес, що призначається пристроям з динамічним розподілом адрес, стандартизована відповідно до **<IA-03(03)_ODP[01] інформація про оренду>**;
	IA-03(03)(a)[02]	тривалість оренди динамічного виділення адреси, що призначається пристроям з динамічним виділенням адреси, стандартизовано відповідно до **<IA-03(03)_ODP[02] тривалість оренди>**;
	IA-03(03)(b)	інформація про оренду перевіряється, коли її призначено пристрою.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації пристрою; проєктна документація системи; налаштування конфігурації системи та відповідна документація; інформація про оренду та тривалості оренди, призначені пристроям; звіти про підключення пристрою; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за ідентифікацію та автентифікацію пристрою; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість ідентифікації та автентифікації пристрою; автоматизовані механізми підтримки та / або реалізації динамічного розподілу адрес; автоматизовані механізми, що підтримують та / або імплантують аудит інформації про оренду].	

IA-03(04)	ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - АТЕСТАЦІЯ

	ПРИСТРОЮ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-03(04)_ODP	**визначено процес управління конфігурацією, який буде використовуватися для ідентифікації та автентифікації пристроїв на основі атестації;**
	IA-03(04)	ідентифікація та автентифікація пристрою виконується на основі атестації за допомогою **<IA-03(04)_ODP процес управління конфігурацією>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації пристрою; процедури, що стосуються управління конфігурацією пристрою; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи управління конфігурацією; записи змін заходів захисту; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за ідентифікацію та автентифікацію пристрою; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість ідентифікації та автентифікації пристрою; автоматизовані механізми підтримки та / або реалізації управління конфігурацією; криптографічні механізми, що підтримують атестацію пристроїв].	

IA-04	**УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-04_ODP[01]	**визначено персонал або ролі, від яких необхідно отримати дозвіл на призначення ідентифікатора;**
	IA-04_ODP[02]	**визначено період часу для запобігання повторному використанню ідентифікаторів;**
	IA-04(a)	управління ідентифікаторами здійснюється шляхом отримання дозволу від **<IA-04_ODP[01] персоналу або ролей>** на призначення ідентифікатора особі, групі, ролі або пристрою;
	IA-04(b)	управління ідентифікаторами здійснюється шляхом вибору ідентифікатора, який ідентифікує окрему особу, групу, ролі або пристрій;
	IA-04(c)	управління ідентифікаторами здійснюється шляхом призначення ідентифікатора особі, групі, ролі або пристрою;

	IA-04(d)	ідентифікатори управляються шляхом запобігання повторному використанню ідентифікаторів впродовж **<IA-04_ODP[02] період часу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік облікових записів системи; перелік ідентифікаторів, що генеруються з фізичних пристроїв контролю доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікаторами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують управління ідентифікаторами].	

IA-04(01)	**УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ЗАБОРОНА ВИКОРИСТАННЯ ІДЕНТИФІКАТОРІВ ОБЛІКОВИХ ЗАПИСІВ ТАКИ САМИХ, ЯК Й ПУБЛІЧНІ ІДЕНТИФІКАТОРИ**
	МЕТА ОЦІНКИ: Визначити, чи:
	IA-04(01) заборонено використання ідентифікаторів облікових записів системи, які збігаються із загальнодоступними ідентифікаторами для індивідуальних облікових записів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікаторами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують управління ідентифікаторами].

IA-04(02)	**УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - АВТОРИЗАЦІЯ СУПЕРВАЙЗЕРА**
	[Виключено: Включено до IA-12(01)].

IA-04(03)	**УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - МНОЖИННІ ФОРМИ СЕРТИФІКАЦІЇ**

	[Виключено: Включено до IA-12(02)].

IA-04(04)	УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ІДЕНТИФІКАЦІЯ СТАТУСУ КОРИСТУВАЧА	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-04(04)_ODP	визначено ознаку, що ідентифікує індивідуальний статус;
	IA-04(04)	управління індивідуальними ідентифікаторами, однозначно ідентифікуючи кожного індивідуума **<IA-04(04)_ODP ознака>**, що ідентифікує індивідуальний статус.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; перелік ознак, що ідентифікують індивідуальний статус; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікаторами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують управління ідентифікаторами].	

IA-04(05)	УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ДИНАМІЧНЕ УПРАВЛІННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-04(05)_ODP	**визначено політику динамічних ідентифікаторів для управління індивідуальними ідентифікаторами;**
	IA-04(05)	індивідуальні ідентифікатори динамічно управляються відповідно до **<IA-04(05)_ODP політика динамічних ідентифікаторів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікаторами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалі-	

	зують управління динамічним ідентифікатором].

IA-04(06)	УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - КРОС-ОРГАНІЗАЦІЙНЕ УПРАВЛІННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-04(06)_ODP	визначено зовнішні організації з якими необхідно здійснювати координацію для крос-організаційного управління ідентифікаторами;
	IA-04(06)	здійснюється координація з **<IA-04(06)_ODP зовнішні організації>** для крос-організаційного управління ідентифікаторами.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікаторами; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують управління ідентифікаторами].	

IA-04(07)	УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ОСОБИСТА РЕЄСТРАЦІЯ
	[Виключено: Включено до IA-12(04)].

IA-04(08)	УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ПОПАРНІ ПСЕВДОНІМНІ ІДЕНТИФІКАТОРИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-04(08)	створено попарні псевдонімні ідентифікатори.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікаторами; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впрова-	

	джують управління ідентифікаторами].

IA-04(09)	УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ПОПАРНІ ПСЕВДОНІМНІ ІДЕНТИФІКАТОРИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-04(09)_ODP	**визначено захищене центральне сховище, яке використовується для зберігання атрибутів для кожної унікально ідентифікованої особи, пристрою або служби;**
	IA-04(09)	атрибути для кожної унікально ідентифікованої особи, пристрою або служби зберігаються у **<IA-04(09)_ODP захищеному центральному сховищі>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; процедури, що стосуються управління обліковими записами; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікаторами; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують управління ідентифікаторами].	

IA-05	УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05_ODP[01]	**визначено період часу для зміни або оновлення автентифікаторів за типом автентифікатора;**
	IA-05_ODP[01]	**визначено події, які викликають зміну або оновлення автентифікаторів;**
	IA-05(a)	управління системними автентифікаторами здійснюється шляхом перевірки, як частини початкового розподілу автентифікатора, особи, групи, ролі або пристрою, який отримує автентифікатор;
	IA-05(b)	управління системними автентифікаторами здійснюється шляхом створення вихідного вмісту автентифікатора для будь-яких автентифікаторів, виданих організацією;
	IA-05(c)	управління системними автентифікаторами здійснюється шляхом забезпечення того, щоб автентифікатори мали достатню стійкість механізму для їх використання за призначенням;

	IA-05(d)	управління системними автентифікаторами здійснюється шляхом створення та реалізація адміністративних процедур для первинного розповсюдження автентифікаторів, для втрачених/скомпрометованих або пошкоджених автентифікаторів, а також для відкликання автентифікаторів;
	IA-05(e)	управління системними автентифікаторами здійснюється шляхом зміни типових автентифікаторів перед першим використанням;
	IA-05(f)	управління системними автентифікаторами здійснюється шляхом зміни/оновлення автентифікаторів у встановлений **<IA-05_ODP[01] період часу>** або коли відбуваються **<IA-05_ODP[02] події>**;
	IA-05(g)	управління системними автентифікаторами здійснюється шляхом захисту вмісту автентифікатора від несанкціонованого розкриття та модифікацій;
	IA-05(h)	управління системними автентифікаторами здійснюється шляхом вимоги до осіб, які використовують пристрої, використовувати спеціальні заходи безпеки для захисту автентифікаторів;
	IA-05(i)	управління системними автентифікаторами здійснюється шляхом вимоги змінювати автентифікатори для облікових записів груп/ролей при зміні членства в цих облікових записах.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікатором; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік типів автентифікатора системи; записи змін заходів захисту, пов'язаних з управлінням автентифікаторами системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління автентифікатором; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості управління автентифікатором].	

IA-05(01)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТЕНТИФІКАЦІЯ НА ОСНОВІ ПАРОЛЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(01)_ODP[01]	**визначено частоту оновлення списку часто використовуваних, очікуваних або скомпрометованих паролів;**
	IA-05(01)_ODP[02]	**визначено склад та правила складності автентифікатора;**
	IA-05(01)(a)	для автентифікації на основі паролів підтримується та оновлюється список часто використовуваних, очікуваних або

		скомпрометованих паролів **<IA-05(01)_ODP[01] частота>**, а також коли є підозра, що паролі організації були скомпрометовані прямо чи опосередковано;
	IA-05(01)(b)	для автентифікації на основі паролів, коли паролі створюються або оновлюються користувачами, паролі перевіряються на відсутність у списку загальновживаних, очікуваних або скомпрометованих паролів в IA-05(01)(a);
	IA-05(01)(c)	для автентифікації на основі паролів, паролі передаються лише криптографічно захищеними каналами;
	IA-05(01)(d)	для автентифікації на основі паролів паролі зберігаються за допомогою затвердженого алгоритму гешування, переважно використовуючи ключову геш-функцію;
	IA-05(01)(e)	для автентифікації на основі пароля після відновлення облікового запису потрібно негайно вибрати новий пароль;
	IA-05(01)(f)	для автентифікації на основі пароля дозволяється вибір користувачем довгих паролів і фраз, що включають пробіли та всі друковані символи;
	IA-05(01)(g)	для автентифікації на основі пароля використовуються автоматизовані інструменти, які допомагають користувачеві у виборі надійних автентифікаторів паролів;
	IA-05(01)(h)	для автентифікації на основі пароля застосовуються **<IA-05(01)_ODP[02] склад та правила складності>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; політика щодо паролів; процедури, що стосуються управління автентифікатором; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; конфігурації паролів та відповідна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління автентифікатором; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують можливість керування автентифікатором на основі паролів].	

IA-05(02)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТЕНТИФІКАЦІЯ НА ОСНОВІ ВІДКРИТОГО КЛЮЧА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(02)(a)(01)	для автентифікації на основі відкритого ключа потрібен авторизований доступ до відповідного закритого ключа;

	IA-05(02)(a)(02)	автентифікована ідентичність прив'язується до облікового запису особи або групи для автентифікації на основі відкритого ключа;
	IA-05(02)(b)(01)	коли використовується інфраструктура відкритих ключів (PKI), сертифікати перевіряються шляхом створення та перевірки шляху сертифікації до прийнятої довіреної прив'язки, включаючи перевірку інформації про статус сертифіката;
	IA-05(02)(b)(02)	коли використовується інфраструктура відкритих ключів (PKI), реалізується локальний кеш даних для підтримки виявлення та перевірки шляху.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікаторами; план захисту інформації; документація з проектування системи; налаштування конфігурації системи та пов'язана з ними документація; записи про підтвердження сертифікації PKI; списки анулювання сертифікації PKI; інші відповідні документи або записи**.**]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління автентифікаторами на основі PKI; персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори; розробники систем]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або впроваджують можливості управління автентифікацією на основі PKI].	

IA-05(03)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ОСОБИСТА АБО ДОВІРЧА АВТЕНТИФІКАЦІЯ ЗОВНІШНЬОЇ СТОРОНИ**
	[Виключено: Включено до IA-12(04)].

IA-05(04)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТОМАТИЗОВАНА ПІДТРИМКА ДЛЯ ВИЗНАЧЕННЯ МІЦНОСТІ ПАРОЛЯ**
	[Виключено: Включено до IA-05(01)].

IA-05(05)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ЗМІНА АВТЕНТИФІКАТОРІВ ДО ДОСТАВКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(05)	розробники та інсталятори компонентів системи зобов'язані надавати унікальні автентифікатори або змінювати автентифікатори за замовчуванням до доставки та встановлення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; план захисту інформації; політика придбання систем та послуг; процедури управління автентифікаторами; процедури інтеграції вимог безпеки в процес придбання; документа-	

	ція щодо придбання; контракти на придбання систем або послуг; інші необхідні документи або записи.]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління автентифікаторами; персонал організації, відповідальний за інформаційну безпеку, придбання та укладання контрактів; розробники системи]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують можливість керування автентифікаторами].

IA-05(06)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ЗАХИСТ АВТЕНТИФІКАТОРІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(06)	автентифікатори захищені відповідно до категорії безпеки інформації, до якої дозволяє доступ використання автентифікатора.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури управління автентифікаторами; документація щодо категоризації безпеки системи; оцінка безпеки засобів захисту автентифікаторів; результати оцінки ризиків; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління автентифікаторами; персонал організації, який впроваджує та/або підтримує захист автентифікаторів; персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують можливості керування автентифікаторами; механізми захисту автентифікаторів].	

IA-05(07)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ВІДСУТНІСТЬ ВБУДОВАНИХ НЕЗАШИФРОВАНИХ СТАТИЧНИХ АВТЕНТИФІКАТОРІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(07)	незашифровані статичні автентифікатори не вбудовуються в застосунки або сценарії доступу та не збережені на функціональній клавіші.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; план захисту інформації; процедури управління автентифікаторами; проектна документація системи; налаштування конфігурації системи та супутня документація; сценарії логічного доступу; огляди коду додатків для виявлення незашифрованих статичних автентифікаторів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління автенти-	

	фікаторами; персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори; розробник системи]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують можливості керування автентифікаторами; механізми, що реалізують автентифікацію в застосунках].

IA-05(08)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - БАГАТОСИСТЕМНІ ОБЛІКОВІ ЗАПИСИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(08)_ODP	**визначено заходи захисту, впроваджені для управління ризиком компрометації через те, що користувачі мають облікові записи в декількох системах.**
	IA-05(08)	**<IA-05(08)_ODP заходи захисту>** впроваджені для управління ризиком компрометації через наявність облікових записів у декількох системах.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікаторами; план захисту інформації; список осіб, що мають облікові записи в декількох системах; список заходів захисту, призначених для управління ризиком компрометації через те, що особи мають облікові записи в декількох системах; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління автентифікаторами; персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або впроваджують гарантії для управління автентифікацією].	

IA-05(09)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - УПРАВЛІННЯ ОБ'ЄДНАННЯМ АВТЕНТИФІКАТОРІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(09)_ODP	**визначено зовнішні організації, які будуть використовуватися для об'єднання автентифікаторів;**
	IA-05(09)	**<IA-05(09)_ODP зовнішні організації>** використовуються для об'єднання автентифікаторів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікаторами; процедури, що стосуються управління обліковими записами; план захисту інформації; угоди про безпеку; інші відповідні	

	документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління автентифікаторами; персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або впроваджують гарантії для управління автентифікацією].

IA-05(10)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ДИНАМІЧНЕ ЗВ'ЯЗУВАННЯ МАНДАТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(10)_ODP	**визначено правила для динамічного зв'язування ідентифікаторів та автентифікаторів;**
	IA-05(10)	ідентифікатори та автентифікатори динамічно зв'язуються за допомогою **<IA-05(10)_ODP правила для динамічного зв'язування >**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; план захисту інформації; проєктна документація системи; автоматизовані механізми, що забезпечують динамічну прив'язку ідентифікаторів та автентифікаторів; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікаторами; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливості управління ідентифікаторами; автоматизовані механізми, що реалізують динамічне забезпечення ідентифікаторів].	

IA-05(11)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТЕНТИФІКАЦІЯ НА ОСНОВІ АПАРАТНИХ ТОКЕНІВ**
	[Вилучено: Включено до IA-02(01), IA-02(02)].

IA-05(12)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ЕФЕКТИВНІСТЬ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(12)_ODP	**визначено вимоги до якості біометрії;**

	IA-05(12)	для біометричної автентифікації використовувати механізми, які задовольняють **<IA-05(12)_ODP вимоги>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікатором; план захисту інформації; проєктна документація системи; автоматизовані механізми, що використовують біометричну автентифікацію для системи; перелік вимог до якості біометричної автентифікації; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління автентифікатором; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують можливість управління автентифікатором на основі біометричних даних].	

IA-05(13)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ЗАКІНЧЕННЯ ТЕРМІНУ КЕШУВАННЯ АВТЕНТИФІКАТОРІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(13)_ODP	**визначено періоду часу після якого необхідно заборонити використання кешованих автентифікаторів**
	IA-05(13)	забороняється використання кешованих автентифікаторів після **<IA-05(13)_ODP періоду часу>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікатором; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління автентифікатором; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості управління автентифікатором].	

IA-05(14)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - УПРАВЛІННЯ ЗМІСТОМ ДОВІРЧИХ СХОВИЩ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(14)	для автентифікації на основі інфраструктури з відкритим ключем використовується загальноорганізаційна методологія управління

		вмістом довірених сховищ інфраструктури відкритого ключа, встановлених на всіх платформах, включно з мережами, операційними системами, браузерами та застосунками.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління автентифікатором; план захисту інформації; методологія організації з управління вмістом довірчих сховищ відкритого ключа на всіх встановлених платформах; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація архітектури безпеки підприємства; документація з архітектури підприємства; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління автентифікатором; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості управління автентифікатором на основі відкритого ключа; автоматизовані механізми, що підтримують та / або впроваджують можливість зберігання довіри відкритого ключа].	

IA-05(15)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ПРОДУКТИ ТА ПОСЛУГИ, ЗАТВЕРДЖЕНІ УПОВНОВАЖЕНИМ ОРГАНОМ**
	МЕТА ОЦІНКИ: Визначити, чи:
	IA-05(15) — використовуються лише схвалені та затверджені уповноваженим органом продукти та послуги.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються управління ідентифікаторами; план захисту інформації; проєктна документація системи; автоматизовані механізми, що забезпечують динамічну прив'язку ідентифікаторів та автентифікаторів; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікацією та автентифікацією; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують можливості управління обліковим записом; автоматизовані механізми, що підтримують та / або реалізують можливості управління ідентифікацією та аутентифікацією для системи].

IA-05(16)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ПЕРЕДАЧА ОСОБИСТОЇ АБО ДОВІРЧОЇ АВТЕНТИФІКАЦІЇ ЗОВНІШНЬОЇ СТОРОНИ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(16)_ODP[01]	**визначено типи та/або конкретні автентифікатори, які будуть передаватися;**
	IA-05(16)_ODP[02]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {особисто; довіреною зовнішньою стороною};**
	IA-05(16)_ODP[03]	**визначено зареєстрований орган, який приймає автентифікатори;**
	IA-05(16)_ODP[04]	**визначено персонал або ролі, які уповноважують передачу автентифікаторів;**
	IA-05(16)	передача **<IA-05(16)_ODP[01] типів та/або конкретних автентифікаторів>** має здійснюватися **<IA-05(16)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** до **<IA-05(16)_ODP[03] зареєстрований орган >** з дозволу **<IA-05(16)_ODP[04] персоналу або ролей>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та аутентифікації; процедури, що стосуються управління ідентифікаторами; план захисту інформації; проєктна документація систем; автоматизовані механізми, що забезпечують динамічну прив'язку ідентифікаторів та автентифікатор; настройки конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікацією та автентифікацією; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості управління обліковим записом; автоматизовані механізми, що підтримують та / або реалізують можливості управління ідентифікацією та аутентифікацією для системи].	

IA-05(17)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТОМАТИЗОВАНІ ЗАСОБИ ВИЯВЛЕННЯ АТАК ІЗ ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ АВТЕНТИФІКАТОРІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(17)	використовуються механізми виявлення атак із використанням штучно виготовлених артефактів для біометричних автентифікаторів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та аутентифікації; процедури, що стосуються управління ідентифікаторами; план захисту інформації; проєктна до-	

	кументація систем; автоматизовані механізми, що забезпечують динамічну прив'язку ідентифікаторів і автентифікатор; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікацією та автентифікацією; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості управління обліковим записом; автоматизовані механізми, що підтримують та / або реалізують можливості управління ідентифікацією та аутентифікацією для системи].

IA-05(18)	**УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - МЕНЕДЖЕР ПАРОЛІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-05(18)_ODP[01]	**визначено менеджери паролів, які використовуються для створення та керування паролями;**
	IA-05(18)_ODP[02]	**визначено елементи керування для захисту паролів;**
	IA-05(18)(a)	**<IA-05(18)_ODP[01] менеджери паролів>** використовуються для створення та керування паролями;
	IA-05(18)(b)	паролі захищені за допомогою **<IA-05(18)_ODP[02] елементи керування >**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та аутентифікації; процедури, що стосуються управління ідентифікаторами; план захисту інформації; проєктна документація системи; автоматизовані механізми, що забезпечують динамічну прив'язку ідентифікаторів і автентифікаторіф; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за управління ідентифікацією та автентифікацією; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості управління обліковим записом; автоматизовані механізми, що підтримують та / або реалізують можливості управління ідентифікацією та аутентифікацією для системи].	

IA-06	**ЗВОРОТНИЙ ЗВ'ЯЗОК АВТЕНТИФІКАТОРА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-06	забезпечино приховану зворотну передачу інформації автентифікації в про-

		цесі автентифікації для забезпечення захисту інформації від можливої експлуатації та використання неавторизованими особами.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури звернення до відгуків автентифікатора; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують затемнення зворотного зв'язку інформації про автентифікацію під час автентифікації].	

IA-07	**АВТЕНТИФІКАЦІЯ КРИПТОГРАФІЧНОГО МОДУЛЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-07	впроваджено механізми автентифікації в криптографічний модуль, який відповідає вимогам чинних законів, виконавчих розпоряджень, директив, політик, правил, стандартів та рекомендацій для такої автентифікації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються автентифікації криптографічного модуля; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аутентифікацію криптографічного модуля; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка: :** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують аутентифікацію криптографічного модуля]	

IA-08	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ)**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-08	унікально ідентифікуються та автентифікуються користувачі, що не належать до організації або процеси (що не належать організації), які діють від імені користувачів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту	

	системи; перелік облікових записів системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; персонал організації, відповідальний за управління обліковими записами]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]

IA-08(01)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - ВИЗНАННЯ ПОСВІДЧЕНЬ ІДЕНТИФІКАЦІЙНИХ ДАНИХ ВІД ІНШИХ УСТАНОВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-08(01)[01]	облікові дані (посвідчення ідентифікаційних даних), видані іншими установами для встановлення особи приймаються;
	IA-08(01)[02]	облікові дані (посвідчення ідентифікаційних даних), видані іншими установами для встановлення особи в електронному вигляді перевіряються.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; записи перевірки PIV; докази посвідчення особи PIV; уповноваження PIV; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організації, відповідальний за управління обліковими записами]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, які приймають та перевіряють облікові дані PIV]	

IA-08(02)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - ВИЗНАННЯ ЗОВНІШНІХ ПОСВІДЧЕНЬ ІДЕНТИФІКАЦІЙНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-08(02)(a)	приймаються лише зовнішні облікові дані (посвідчення ідентифікаційних даних), що відповідають вимогам нормативних документів та стандартів;

	IA-08(02)(b)[01]	задокументовано список прийнятих зовнішніх автентифікаторів;
	IA-08(02)(b)[02]	підтримується список прийнятих зовнішніх автентифікаторів;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; план захисту інформації; процедури ідентифікації та автентифікації користувачів; документація щодо скасування підпису в системі; налаштування конфігурації системи та пов'язана з ними документація; записи аудиту системи; перелік сторонніх продуктів, компонентів або послуг з автентифікації, придбаних та впроваджених організацією; записи перевірки автентифікації сторонніх осіб; докази автентифікації сторонніх осіб; дозволи на автентифікацію сторонніх осіб; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організації, який відповідає за управління обліковими записами]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що приймають затверджені зовнішні облікові дані]	

IA-08(03)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - ВИКОРИСТАННЯ ЗАТВЕРДЖЕНИХ ПРОДУКТІВ**
	[Вилучено: Включено до IA-08(02)]

IA-08(04)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - ВИКОРИСТАННЯ ПРОФІЛЕЙ ВИДАНИХ УПОВНОВАЖЕНИМ ОРГАНОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-08(04)_ODP	**визначено профілі керування;**
	IA-08(04)	забезпечена відповідність до **<IA-08(04)_ODP профілів керування>** для управління ідентифікацією.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; політика придбання системи та послуг; процедури, що стосуються ідентифікації та автентифікації користувачів; процедури, що стосуються інтеграції вимог безпеки в процес придбання; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; документація про придбання; договори придбання для закупівель або послуг системи; інші відповідні документи	

	або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; Персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; Персонал організації, який відповідає за управління обліковими записами]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що приймають затверджені зовнішні облікові дані].

IA-08(05)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - ВИЗНАННЯ ПОСВІДЧЕНЬ ОСОБИ (PIV-I)**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-08(05)_ODP	**визначено політику використання ативних облікових даних або облікових даних PKI;**
	IA-08(05)[01]	приймаються облікові дані або дані PKI, які відповідають **<IA-08(05)_ODP політика>**;
	IA-08(05)[02]	підтверджуються облікові дані або дані PKI, які відповідають **<IA-08(05)_ODP політика>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; Записи перевірки PIV-I; докази посвідчення особи PIV-I; Дозвільні документи PIV-I; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організації, відповідальний за управління обліковими даними]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що приймають та перевіряють облікові дані PIV-I].	

IA-08(06)	**ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - РОЗМЕЖУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-08(06)_ODP	**визначено заходи, щоб розмежувати атрибути користувача або зв'язки підтвердження ідентифікатора між окремими особами, постачальниками облікових даних і довіреними**

		сторонами;
	IA-08(06)	впроваджено **<IA-08(06)_ODP заходи>** щоб розмежувати атрибути користувача або зв'язки підтвердження ідентифікатора між окремими особами, постачальниками облікових даних і довіреними сторонами.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; проєктна документація системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; Записи перевірки PIV-I; докази посвідчення особи PIV-I; дозвільні документи PIV-I; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організації, відповідальний за управління обліковими записами]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації; автоматизовані механізми, що приймають та перевіряють облікові дані PIV-I].	

IA-09	**ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-09_ODP	**визначено системні служби та застосунки, які мають бути унікально ідентифіковані та автентифіковані;**
	IA-09	**<IA-09_ODP системні служби та застосунки>** унікально ідентифікуються та автентифікуються перед встановленням зв'язку з пристроями, користувачами або іншими службами чи застосунками.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації послуг; план захисту інформацфї; проєктна документація системи; гарантії безпеки, що використовуються для ідентифікації та автентифікації служб системи; налаштування конфігурації системи та супутня документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організаціїз обов'язками щодо ідентифікації та автентифікації]. **Перевірка:** [ВИБІР: Гарантії безпеки, що реалізують можливість ідентифікації та автентифікації служби]	

IA-09(01)	**ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ - ОБМІН ІНФО-**

	РМАЦІЄЮ
	[Виключено: перенесено до IA-09]

IA-09(02)	ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ - ПЕРЕДАЧА РІШЕНЬ
	[Виключено: перенесено до IA-09]

IA-10	АДАПТИВНА АВТЕНТИФІКАЦІЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-10_ODP[01]	**визначені додаткові методи або механізми автентифікації, які будуть застосовуватися при доступі до системи за певних обставин або ситуацій;**
	IA-10_ODP[01]	**визначені обставини або ситуації, які вимагають від осіб, що отримують доступ до системи, використання додаткових методів або механізмів автентифікації;**
	IA-10	особи, які отримують доступ до системи, повинні використовувати **<IA-10_ODP[01] додаткові методи або механізми автентифікації>** за певних **<IA-10_ODP[02] обставин або ситуацій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються методів або механізмів адаптивної / додаткової ідентифікації та автентифікації; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; додаткові методи та механізми ідентифікації та автентифікації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організаціїз обов'язками щодо ідентифікації та автентифікації]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації].	

IA-11	ПОВТОРНА АВТЕНТИФІКАЦІЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-11_ODP	**визначено обставини або ситуації, що вимагають повторної автен-**

		тифікації;
	IA-11	користувачі повинні повторно автентифікуватися, коли **<IA-11_ODP обставини або ситуації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються повторної автентифікації користувачів та пристроїв; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік обставин або ситуацій, що вимагають повторної автентифікації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організаціїз обов'язками щодо ідентифікації та автентифікації]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]	

IA-12	**ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ)**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-12(a)	користувачі, яким потрібні облікові записи для логічного доступу до систем на основі вимог гарантій відповідного рівня, як це зазначено у відповідних стандартах і рекомендаціях, мають підтверджену ідентичність;
	IA-12(b)	встановлені ідентифікатори користувачів унікальні для особи;
	IA-12(c)[01]	збираються докази ідентичності особи;
	IA-12(c)[02]	затверджуються докази ідентичності особи;
	IA-12(c)[03]	перевіряються докази ідентичності особи;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються повторної автентифікації користувачів та пристроїв; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік обставин або ситуацій, що вимагають повторної автентифікації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організаціїз обов'язками щодо ідентифікації та автентифікації]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]	

IA-12(01)	ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - АВТОРИЗАЦІЯ СУПЕРВАЙЗЕРА	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-12(01)	процес реєстрації для отримання облікового запису для логічного доступу включає авторизацію супервайзера.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються повторної автентифікації користувачів та пристроїв; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік обставин або ситуацій, що вимагають повторної автентифікації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організації з обов'язками щодо ідентифікації та автентифікації]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]	

IA-12(02)	ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПОСВІДЧЕННЯ ОСОБИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-12(02)	документи, що посвідчують особу пред'являються до реєстраційного органу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються повторної автентифікації користувачів та пристроїв; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік обставин або ситуацій, що вимагають повторної автентифікації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організаціїз обов'язками щодо ідентифікації та автентифікації]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]	

IA-12(03)	ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПЕРЕВІРКА ТА ВЕРИФІКАЦІЯ ДОКАЗІВ ІДЕНТИЧНОСТІ

	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-12(03)_ODP	**визначено методи перевірки та верифікації доказів ідентифікації;**
	IA-12(03)	надані докази посвідчення особи підтверджуються та перевіряються за допомогою **<IA-12(03)_ODP методи перевірки та верифікації >**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються повторної автентифікації користувачів та пристроїв; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік обставин або ситуацій, що вимагають повторної автентифікації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організації з обов'язками щодо ідентифікації та автентифікації]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]	

IA-12(04)	**ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ОЧНА ПЕРЕВІРКА ТА ВЕРИФІКАЦІЯ**
	МЕТА ОЦІНКИ: Визначити, чи:
	IA-12(04) — підтвердження та перевірка посвідчення особи проводиться особисто в призначеному органі реєстрації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються перевірки та верифікації; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організаціїз обов'язками щодо ідентифікації та автентифікації]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]

IA-12(05)	**ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПІДТВЕРДЖЕННЯ АДРЕСИ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-12(05)_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {реєстраційний код; повідомлення про перевірку};**
	IA-12(05)	**<IA-12(05)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** доставляється через зовнішні канали для перевірки адреси (фізичної або цифрової) користувача.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються підтвердження адреси; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організаціїз обов'язками щодо ідентифікації та автентифікації]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]	

IA-12(06)	**ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПРИЙНЯТТЯ ІДЕНТИФІКАЦІЙ СХВАЛЕНИХ ТРЕТЬОЮ СТОРОНОЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IA-12(06)_ODP	**визначено рівень гарантії ідентичності для прийняття зовнішньо підтверджених ідентифікаторів;**
	IA-12(06)	приймаються зовнішньо підтверджені ідентифікатори **<IA-12(06)_ODP рівень гарантії ідентичності>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика ідентифікації та автентифікації; процедури, що стосуються прийняття ідентифікацій схвалених третьою стороною; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за функціонування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи; персонал організації з обов'язками щодо ідентифікації та автентифікації]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливості ідентифікації та автентифікації]	

VIII. КЛАС ЗАХОДІВ ЗАХИСТУ IR – РЕАГУВАННЯ НА ІНЦИДЕНТИ

IR-01	ПОЛІТИКА ТА ПРОЦЕДУРИ РЕАГУВАННЯ НА ІНЦИДЕНТИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-01_ODP[01]	**визначено персонал або ролі, до яких має бути доведена політика реагування на інциденти;**
	IR-01_ODP[02]	**визначено персонал або ролі, до яких мають бути доведені процедури реагування на інциденти;**
	IR-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	IR-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами реагування на інциденти;**
	IR-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика реагування на інциденти;**
	IR-01_ODP[06]	**визначаються події, які потребують перегляду та оновлення поточної політики реагування на інциденти;**
	IR-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні процедури реагування на інциденти;**
	IR-01_ODP[08]	**визначено події, які потребують перегляду та оновлення процедур реагування на інциденти;**
	IR-01(a)[01]	розроблено та задокументовано політику реагування на інциденти;
	IR-01(a)[02]	політика реагування на інциденти поширюється серед **<IR-01_ODP[01] персоналу або ролей>**;
	IR-01(a)[03]	розроблені та задокументовані процедури реагування на інциденти, що сприяють впровадженню політики реагування на інциденти та пов'язаних з нею заходів захисту з реагування на інциденти;
	IR-01(a)[04]	процедури реагування на інциденти поширюються серед **<IR-01_ODP[02] персоналу або ролей>**;
	IR-01(a)[01](a)[01]	політика реагування на інциденти **<IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** містить мету;
	IR-01(a)[01](a)[02]	політика реагування на інциденти **<IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** містить сферу застосування;

	IR-01(a)[01](a)[03]	політика реагування на інциденти **<IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** містить ролі;
	IR-01(a)[01](a)[04]	політика реагування на інциденти **<IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** містить обов'язки;
	IR-01(a)[01](a)[05]	політика реагування на інциденти **<IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** містить відповідальність керівництва;
	IR-01(a)[01](a)[06]	політика реагування на інциденти **<IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** містить координацію між підрозділами організації;
	IR-01(a)[01](a)[07]	політика реагування на інциденти **<IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** містить систему контролю відповідності;
	IR-01(a)[01](b)	політика реагування на інциденти **<IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам;
	IR-01(b)	**<IR-01_ODP[04] посадова особа>** призначається для управління розробкою, документуванням та розповсюдженням політики та процедур реагування на інциденти;
	IR-01(c)[01][01]	переглядається та оновлюється поточна політика реагування на інциденти **<IR-01_ODP[05] частота>**;
	IR-01(c)[01][02]	поточна політика реагування на інциденти переглядається та оновлюється після **<IR-01_ODP[06] подій>**;
	IR-01(c)[02][01]	переглядаються та оновлюються поточні процедури реагування на інциденти **<IR-01_ODP[07] частота>**;
	IR-01(c)[02][02]	поточні процедури реагування на інциденти переглядаються та оновлюються після **<IR-01_ODP[08] подій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури реагування на інциденти; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику реагування на інциденти; персонал, відповідальний за інформаційну безпеку].	

IR-02	**НАВЧАННЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ**
	МЕТА ОЦІНКИ: Визначити, чи:

	IR-02_ODP[01]	**визначено період часу, протягом якого має бути проведено навчання з реагування на інциденти для користувачів системи, які беруть на себе роль або відповідальність за реагування на інциденти;**
	IR-02_ODP[02]	**визначено частоту, з якою користувачі повинні проходити навчання з реагування на інциденти;**
	IR-02_ODP[03]	**визначено частоту перегляду та оновлення змісту навчання з реагування на інциденти;**
	IR-02_ODP[04]	**визначено події, які ініціюють перегляд змісту навчання з реагування на інциденти;**
	IR-02(a)[01]	навчання з реагування на інциденти надається користувачам системи відповідно до призначених ролей та обов'язків протягом **<IR-02_ODP[01] періоду часу>** з моменту прийняття на себе ролі або обов'язків з реагування на інциденти або отримання доступу до системи;
	IR-02(a)[02]	навчання з реагування на інциденти надається користувачам системи відповідно до призначених ролей та обов'язків, коли цього вимагають зміни в системі;
	IR-02(a)[03]	користувачам системи надається навчання з реагування на інциденти відповідно до призначених ролей та обов'язків **<IR-02_ODP[02] частота>**;
	IR-02(b)[01]	зміст навчання з реагування на інциденти переглядається та оновлюється **<IR-02_ODP[03] частота>**;
	IR-02(b)[02]	зміст навчання з реагування на інциденти переглядається та оновлюється після **<IR-02_ODP[04] подій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика реагування на інциденти; процедури, що стосуються навчання реагування на інциденти; навчальна програма з реагування на інциденти; навчальні матеріали щодо реагування на інциденти; план захисту інформації; план реагування на інциденти; записи навчання реагування на інциденти; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який пройшов навчання з реагування на інциденти та виконував оперативні обов'язки; персонал організації, який відповідає за інформаційну безпеку].	

IR-02(01)	**НАВЧАННЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ - МОДЕЛЮВАННЯ ПОДІЙ**
	МЕТА ОЦІНКИ: Визначити, чи:

	IR-02(01)	моделювання подій включається в процес навчання з реагування на інциденти для забезпечення ефективного реагування персоналу в кризових ситуаціях.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються навчання реагування на інциденти; навчальна програма з реагування на інциденти; навчальні матеріали щодо реагування на інциденти; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який пройшов навчання з реагування на інциденти та відповідав за оперативні обов'язки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка**: **[**ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують змодельовані події для навчання реагування на інциденти].	

IR-02(02)	**НАВЧАННЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ - АВТОМАТИЗОВАНІ НАВЧАЛЬНІ СЕРЕДОВИЩА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-02(02)_ODP	**визначено автоматизовані механізми, що використовуються в навчальному середовищі реагування на інциденти;**
	IR-02(02)	створено середовище для навчання з реагування на інциденти з використанням **<IR-02(02)_ODP автоматизованих механізмів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються навчання реагування на інциденти; навчальна програма з реагування на інциденти; навчальні матеріали щодо реагування на інциденти; автоматизовані механізми, що підтримують навчання з реагування на інциденти; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який пройшов навчання з реагування на інциденти та відповідає за оперативні обов'язки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка**: [ВИБІР: Автоматизовані механізми, що забезпечують ретельне та реалістичне навчальне середовище реагування на інциденти].	

IR-02(03)	**НАВЧАННЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ - ЗЛАМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-02(03)[01]	проводиться навчання з реагування на інциденти щодо виявлення та реаг

	IR-02(03)[02]	проводиться навчання з реагування на інциденти щодо процесу повідомлення і
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; політика планування на випадок н тестування плану на випадок надзвичайних ситуацій; матеріали тестування реагування на інци на інциденти; план реагування на інциденти; план на випадок надзвичайних ситуацій; план за або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за навчання з реагування на інциде ність].	

IR-03	**ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-03_ODP[01]	**визначено частоту, з якою необхідно перевіряти ефективність реагування системи на інциденти;**
	IR-03_ODP[02]	**визначено тести, що використовуються для перевірки ефективності реагування на інциденти в системі;**
	IR-03	ефективність реагування системи на інциденти перевіряється **<IR-03_ODP[01] частота>** за допомогою **<IR-03_ODP[02] тестів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на аварії; політика планування на випадок непередбачених ситуацій; процедури, що стосуються тестування реагування на аварії; процедури, що стосуються тестування плану дій на випадок непередбачених ситуацій; матеріал для тестування реакції на аварії; результати випробувань реакції на аварії; план випробувань реагування на аварії; план реагування на аварії; резервний план; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за тестування реагування на аварії; персонал організації, який відповідає за інформаційну безпеку].	

IR-03(01)	**ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ - АВТОМАТИЧНЕ ТЕСТУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-03(01)_ODP	**визначено автоматизовані механізми, що використовуються для перевірки здатності реагування на інциденти;**
	IR-03(01)	здатність реагування на інциденти перевіряється за допомогою **<IR-03(01)_ODP автоматизовані механізми>**.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; політика планування на випадок непередбачених ситуацій; процедури, що стосуються тестування реагування на інциденти; процедури, що стосуються тестування плану дій на випадок непередбачених ситуацій; документація на тестування реагування на інциденти; результати випробувань реакції на інциденти; план випробувань реагування на інциденти; план реагування на інциденти; резервний план; план захисту інформації; автоматизовані механізми, що підтримують тести реагування на інциденти; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за тестування реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку] **Перевірка:** [ВИБІР: Автоматизовані механізми, які ретельніше та ефективніше перевіряють можливість реагування на інциденти].

IR-03(02)	**ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ - КООРДИНАЦІЯ З ПОВ'ЯЗАНИМИ ПЛАНАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-03(02)	тестування реагування на інциденти координується з елементами організації, відповідальними за пов'язані плани.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; політика планування на випадок непередбачених ситуацій; процедури, що стосуються тестування реагування на інциденти; документація на тестування реакції на аварії; план реагування на інциденти; плани безперервності роботи; плани на випадок непередбачених ситуацій; плани аварійного відновлення; плани безперервності операцій; кризові плани комунікацій; плани надзвичайних ситуацій для персоналу, який не належить до організації; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за тестування реагування на інциденти; персонал організації, відповідальний за тестування планів пов'язаних з тестуванням реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку].	

IR-03(03)	**ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ - ПОСТІЙНЕ ПОКРАЩЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-03(03)(a)[01]	якісні дані тестування використовуються для визначення ефективності процесів реагування на інциденти;

	IR-03(03)(a)[02]	кількісні дані тестування використовуються для визначення ефективності процесів реагування на інциденти;
	IR-03(03)(b)[01]	якісні дані тестування використовуються для постійного вдосконалення процесів реагування на інциденти;
	IR-03(03)(b)[02]	кількісні дані тестування використовуються для постійного вдосконалення процесів реагування на інциденти;
	IR-03(03)(c)[01]	якісні дані, отримані за результатами тестування , використовуються для забезпечення точних показників та метрик реагування на інциденти;
	IR-03(03)(c)[02]	кількісні дані, отримані за результатами тестування , використовуються для забезпечення точних показників та метрик реагування на інциденти;
	IR-03(03)(c)[03]	якісні дані, отримані за результатами тестування , використовуються для забезпечення послідовності показників та метрик реагування на інциденти;
	IR-03(03)(c)[04]	кількісні дані, отримані за результатами тестування , використовуються для забезпечення послідовності показників та метрик реагування на інциденти;
	IR-03(03)(c)[05]	якісні дані, отримані за результатами тестування , використовуються для забезпечення відтворюваносні показників та метрик реагування на інциденти;
	IR-03(03)(c)[06]	кількусні дані, отримані за результатами тестування , використовуються для забезпечення відтворюваносні показників та метрик реагування на інциденти;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; політика планування на випадок непередбачених ситуацій; процедури, що стосуються тестування реагування на інциденти; документація на тестування реакції на аварії; план реагування на інциденти; плани безперервності роботи; плани на випадок непередбачених ситуацій; плани аварійного відновлення; плани безперервності операцій; кризові плани комунікацій; плани надзвичайних ситуацій для пасажирів; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за тестування реагування на інциденти; персонал організації, відповідальний за тестування реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку].	

IR-04	**ОБРОБКА ІНЦИДЕНТУ**
	МЕТА ОЦІНКИ: Визначити, чи:

	IR-04(a)[01]	впроваджено можливість обробки інцидентів безпеки включно з підготовкою;
	IR-04(a)[02]	впроваджено можливість обробки інцидентів безпеки включно з виявленням;
	IR-04(a)[03]	впроваджено можливість обробки інцидентів безпеки включно з аналізом;
	IR-04(a)[04]	впроваджено можливість обробки інцидентів безпеки включно з локалізацією;
	IR-04(a)[05]	впроваджено можливість обробки інцидентів безпеки включно з ліквідацією;
	IR-04(a)[06]	впроваджено можливість обробки інцидентів безпеки включно з відновленням;
	IR-04(b)	діяльність з обробки інцидентів координується із заходами із забезпечення безперервності функціонування;
	IR-04(c)[01]	уроки, отримані з поточних дій з обробки інцидентів, включаються в процедури реагування на інциденти, навчання та тестування;
	IR-04(c)[02]	зміни, що випливають з отриманих уроків, впроваджуються відповідним чином;
	IR-04(d)[01]	строгість заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;
	IR-04(d)[02]	інтенсивність заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;
	IR-04(d)[03]	обсяг заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;
	IR-04(d)[04]	результати діяльності заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; політика планування на випадок непередбачених ситуацій; процедури, що стосуються врегулювання інцидентів; план реагування на інциденти; резервний план; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, відповідальний за планування на випадок непередбачених ситуацій; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Можливість обробки інцидентів в організації].	

IR-04(01)	**ОБРОБКА ІНЦИДЕНТУ - АВТОМАТИЗОВАНІ ПРОЦЕСИ ОБРОБКИ ІН-**

	ЦИДЕНТІВ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(01)_ODP	**визначено автоматизовані механізми, що використовуються для підтримки процесу обробки інцидентів;**
	IR-04(01)	процес обробки інцидентів підтримується за допомогою **<IR-04(01)_ODP автоматизовані механізми>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; автоматизовані механізми, що підтримують обробку інцидентів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують процес обробки інцидентів].	

IR-04(02)	ОБРОБКА ІНЦИДЕНТУ - ДИНАМІЧНА РЕКОНФІГУРАЦІЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(02)_ODP[01]	**визначено типи динамічної реконфігурації для компонентів системи;**
	IR-04(02)_ODP[02]	**визначено компоненти системи, які потребують динамічної реконфігурації;**
	IR-04(02)	**<IR-04(02)_ODP[01] типи динамічної реконфігурації>** для **<IR-04(02)_ODP[02] компонентів системи>** включені як частина здатності реагування на інциденти.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; автоматизовані механізми, що підтримують обробку інцидентів; перелік компонентів системи, що підлягають динамічному переконфігуруванню як частина можливості реагування на інциденти; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізу-	

	ють динамічну реконфігурацію компонентів як частину реагування на інциденти]

IR-04(03)	**ОБРОБКА ІНЦИДЕНТУ - БЕЗПЕРЕРВНІСТЬ ОПЕРАЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(03)_ODP[01]	**визначено класи інцидентів, що вимагають вживання дій, визначених організацією (визначених в IR-04(03)_ODP[02]);**
	IR-04(03)_ODP[02]	**визначено дії, які необхідно вжити у відповідь на визначені організацією класи інцидентів;**
	IR-04(03)[01]	ідентифіковано **<IR-04(03)_ODP[01] класи інцидентів>**;
	IR-04(03)[02]	**<IR-04(03)_ODP[02] дії>** вживаються у відповідь на ці інциденти (визначені в IR-04(03)_ODP[01]) для забезпечення продовження виконання завдань та функцій організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; план реагування на інциденти; план захисту інформації; перелік класів інцидентів; перелік відповідних дій з реагування на інциденти; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують безперервність операцій].	

IR-04(04)	**ОБРОБКА ІНЦИДЕНТУ - ІНФОРМАЦІЙНА КОРЕЛЯЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(04)	інформація про інциденти та індивідуальне реагування на інциденти зіставляється з метою досягнення загальноорганізаційного бачення на обізнаність про інциденти та реагування на них.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються обробки інцидентів; план реагування на інциденти; план захисту інформації; автоматизовані механізми, що підтримують кореляцію подій та інцидентів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; журнали кореляції управління інцидентами; журнали кореляції управління подіями; інформація про безпеку та журнали управління подіями; звіти про кореляцію управління інцидентами; звіти про кореляцію управління подіями; інформація про безпеку та звіти про управління подіями; записи аудиту; інші від-	

	повідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, який відповідає за інформаційну безпеку; персонал організації, з яким слід співвідносити інформацію про події та реагування на окремі події]. **Перевірка:** [ВИБІР: Процеси організації для співвіднесення інформації про події та індивідуальних реакцій на події; автоматизовані механізми, що підтримують та / або впроваджують співвідношення інформації про реакцію на події з окремими реакціями на події].

IR-04(05)	**ОБРОБКА ІНЦИДЕНТУ - АВТОМАТИЧНЕ ВИМКНЕННЯ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(05)_ODP	**визначено порушення безпеки, які автоматично вимикають систему;**
	IR-04(05)	реалізовано можливість автоматичного відключення системи при виявленні **<IR-04(05)_ODP порушень безпеки>**, що налаштовується.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; автоматизовані механізми, що підтримують обробку інцидентів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, який відповідає за інформаційну безпеку; розробники системи]. **Перевірка:** [ВИБІР: Можливість обробки інцидентів організації; автоматизовані механізми, що підтримують та / або реалізують автоматичне відключення системи]	

IR-04(06)	**ОБРОБКА ІНЦИДЕНТУ - ВНУТРІШНІ ЗАГРОЗИ - ОСОБЛИВІ МОЖЛИВОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(06)	реалізовано можливість обробки інцидентів, пов'язаних з внутрішніми загрозами
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; автоматизовані механізми, що підтримують обробку інцидентів; проєктна документація системи; налаштування конфігурації	

	системи та відповідна документація; план реагування на інциденти; план захисту інформації; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Можливість обробки інцидентів організації]

IR-04(07)	**ОБРОБКА ІНЦИДЕНТУ - ВНУТРІШНІ ЗАГРОЗИ - ВНУТРІШНЬООРГАНІЗАЦІЙНА КООРДИНАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(07)_ODP	**визначено компоненти або елементи організації, які потребують координації для забезпечення здатності обробки інцидентів для внутрішніх загроз;**
	IR-04(07)[01]	**координується обробка інцидентів для внутрішніх загроз;**
	IR-04(07)[02]	координується здатність обробки інцидентів для внутрішніх загроз через **<IR-04(07)_ODP компоненти або елементи>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, який відповідає за інформаційну безпеку; персонал організації / елементи, з якими слід узгоджувати можливості поводження з інцидентами]. **Перевірка:** [ВИБІР: Процеси в організації для координації обробки інцидентів].	

IR-04(08)	**ОБРОБКА ІНЦИДЕНТУ - КООРДИНАЦІЯ З ЗОВНІШНІМИ ОРГАНІЗАЦІЯМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(08)_ODP[01]	**визначено зовнішні організації, з якими необхідно координувати та обмінюватися інформацією про інциденти в організації;**
	IR-04(08)_ODP[02]	**визначено інформацію про інциденти, яку необхідно зіставляти та поширювати із зовнішніми організаціями;**
	IR-04(08)	здійснюється координація з **<IR-04(08)_ODP[01] зовнішніми організаціями>** для кореляції та обміну **<IR-04(08)_ODP[02] інформацією про інциденти>** для досяг-

		нення міжорганізаційного бачення щодо обізнаності про інциденти та більш ефективного реагування на інциденти.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються обробки інцидентів; перелік зовнішніх організацій; записи координації обробки подій із зовнішніми організаціями; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, який відповідає за інформаційну безпеку; персонал із зовнішніх організацій, з якими слід координувати / обмінюватися / співвідносити інформацію щодо реагування на події]. **Перевірка:** [ВИБІР: Процеси для узгодження інформації про обробку інцидентів із зовнішніми організаціями].	

IR-04(09)	**ОБРОБКА ІНЦИДЕНТУ - ЗДАТНІСТЬ ДИНАМІЧНОГО РЕАГУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(09)_ODP	визначено можливості динамічного реагування для ефективного реагування на інциденти безпеки.
	IR-04(09)	використуються **<IR-04(09)_ODP можливості динамічного реагування>** для ефективного реагування на інциденти безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються обробки інцидентів; автоматизовані механізми, що підтримують можливості динамічного реагування; проєктна документація системи; налаштування конфігурації системи та відповідна документація; план реагування на інциденти; план захисту інформації; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси для можливості динамічного реагування; автоматизовані механізми, що підтримують та / або реалізують можливість динамічного реагування для організації]	

IR-04(10)	**ОБРОБКА ІНЦИДЕНТУ - КООРДИНАЦІЯ ЛАНЦЮГА ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(10)	координується діяльність з обробки інцидентів, пов'язана з подіями ланцюжка постачання, з іншими організаціями, що беруть участь у

		ланцюжку постачання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються координації ланцюгів постачання; договори придбання; угоди про рівень обслуговування; план реагування на інциденти; план захисту інформації; плани реагування на інциденти іншої організації, яка бере участь у діяльності ланцюга постачання; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обробку інцидентів; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за ланцюжки постачання].	

IR-04(11)	**ОБРОБКА ІНЦИДЕНТУ - ІНТЕГРОВАНА ГРУПА РЕАГУВАННЯ НА ІНЦЕДЕНТИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(11)_ODP	**визначено період часу, протягом якого може бути розгорнута інтегрована група реагування на інцидент;**
	IR-04(11)[01]	створена та підтримується інтегрована група реагування на інциденти;
	IR-04(11)[02]	інтегрована група реагування на інциденти може бути розгорнута в будь-якому місці, визначеному організацією протягом **<IR-04(11)_ODP часового періоду>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури обробки інцидентів; процедури планування реагування на інциденти; план реагування на інциденти; план захисту інформації; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обробку інцидентів; або персонал організації, відповідальний за інформаційну безпеку та конфіденційність; члени інтегрованої групи реагування на інциденти].	

IR-04(12)	**ОБРОБКА ІНЦИДЕНТУ - ЗЛОВМИСНИЙ КОД ТА КРИМІНАЛІСТИЧНИЙ АНАЛІЗ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(12)[01]	шкідливий код, що залишився в системі, аналізується після інциденту;
	IR-04(12)[02]	інші залишкові артефакти, що залишилися в системі (якщо такі є), аналізуються після інциденту.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури обробки інцидентів; процедури аналізу коду та криміналістичного аналізу; процедури реагування на інциденти; план реагування на інциденти; проектна документація системи; механізми, інструменти та методи захисту від зловмисного коду; результати аналізу зловмисного коду; план захисту інформації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який займається встановленням, налаштуванням та/або обслуговуванням системи; персонал організації, відповідальний за захист від зловмисного коду; персонал організації, відповідальний за реагування на інциденти/управління інцидентами]. **Перевірка:** [ВИБІР: Процес реагування на інциденти; процес проведення аналізу інцидентів; інструменти та методи аналізу характеристик та поведінки шкідливого коду]

IR-04(13)	**ОБРОБКА ІНЦИДЕНТУ - АНАЛІЗ ПОВЕДІНКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(13)_ODP	**визначаються середовища або ресурси, які можуть містити або можуть бути пов'язані з аномальною або підозрілою ворожою поведінкою;**
	IR-04(13)	аналізується аномальна або підозрювана ворожа поведінка в <**IR-04(13)_ODP середовищах або ресурсах**> або пов'язана з ними.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються інструментів і методів моніторингу системи; план реагування на інциденти; журнали або записи моніторингу системи; документація щодо інструментів і методів моніторингу системи; налаштування конфігурації системи та пов'язана з ними документація; інвентаризація компонентів системи; схема мережі; документація щодо системних протоколів; перелік допустимих порогів хибних спрацьовувань і хибних несприятливих результатів; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси організації для виявлення аномальної поведінки]	

IR-04(14)	**ОБРОБКА ІНЦИДЕНТУ - ЦЕНТР БЕЗПЕКИ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	IR-04(14)[01]	створено оперативний центр безпеки;
	IR-04(14)[02]	підтримується оперативний центр безпеки;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; політика планування на випадок надзвичайних ситуацій; процедури, що стосуються обробки інцидентів; процедури, що стосуються роботи оперативного центру безпеки; механізми, що підтримують можливості динамічного реагування; план реагування на інциденти; план на випадок надзвичайних ситуацій; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обробку інцидентів; або персонал організації, відповідальний за планування на випадок надзвичайних ситуацій; персонал оперативного центру безпеки; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Механізми, які підтримують та/або реалізують можливості операційного центру безпеки; механізми, які підтримують та/або реалізують процес обробки інцидентів]	

IR-04(15)	**ОБРОБКА ІНЦИДЕНТУ - ЗВ'ЯЗКИ З ГРОМАДКІСТЮ ТА ВІДНОВЛЕННЯ РЕПУТАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-04(15)[a]	керують зв'язками з громадськістю, пов'язаними з інцидентом;
	IR-04(15)[b]	вживаються заходи для відновлення репутації організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури реагування на інциденти; процедури обробки інцидентів; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обробку інцидентів; або персонал організації, відповідальний за інформаційну безпеку; або персонал організації, відповідальний за комунікації або зв'язки з громадськістю].	

IR-05	**МОНІТОРИНГ ІНЦИДЕНТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-05[01]	відстежуються інциденти безпеки та приватності;
	IR-05[02]	документуються інциденти безпеки та приватності.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються моніторингу інцидентів; записи та документація щодо реагування на інциденти; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за моніторинг інцидентів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Можливість організації моніторингу інцидентів; автоматизовані механізми, що підтримують та / або реалізують відстеження та документування інцидентів системи].

IR-05(01)	**МОНІТОРИНГ ІНЦИДЕНТУ - АВТОМАТИЗОВАНЕ ВІДСТЕЖЕННЯ, ЗБІР ДАНИХ І АНАЛІЗ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-05(01)_ODP[01]	**визначено автоматизовані механізми відстеження інцидентів;**
	IR-05(01)_ODP[02]	**визначено автоматизовані механізми збору інформації про інциденти;**
	IR-05(01)_ODP[03]	**визначено автоматизовані механізми аналізу інформації про інциденти;**
	IR-05(01)[01]	інциденти відстежуються за допомогою **<IR-05(01)_ODP[01] автоматизованих механізмів>**;
	IR-05(01)[02]	інформація про інциденти збирається за допомогою **<IR-05(01)_ODP[02] автоматизованих механізмів>**;
	IR-05(01)[03]	інформація про інциденти аналізується за допомогою **<IR-05(01)_ODP[03] автоматизованих механізмів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються моніторингу інцидентів; автоматизовані механізми, що підтримують моніторинг інцидентів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; план реагування на інциденти; план захисту інформації; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за моніторинг інцидентів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що допомагають відстежувати інциденти безпеки та збирати та аналізувати інформацію про інциденти].	

IR-06	ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-06_ODP[01]	**визначено період часу, протягом якого персонал повинен повідомляти про підозрілі інциденти до уповноваженого органу;**
	IR-06_ODP[02]	**визначені органи, до яких слід повідомляти інформацію про інцидент;**
	IR-06(a)	персонал зобов'язаний повідомляти про підозрілі інциденти протягом **<IR-06_ODP[01] періоду часу>**;
	IR-06(b)	інформацію про інцидент повідомляється **<IR-06_ODP[02] органам>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються повідомлення про інциденти; записи та документація повідомлення про інциденти; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за повідомлення про інциденти; персонал організації, який відповідає за інформаційну безпеку; персонал, який мав / повинен був повідомити про інциденти; персонал (органи влади), якому слід повідомляти інформацію про інциденти]. **Перевірка:** [ВИБІР: Процеси для повідомлення про інциденти; автоматизовані механізми, що підтримують та / або впроваджують повідомлення про інциденти].	

IR-06(01)	ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ - АВТОМАТИЧНЕ ЗВІТУВАННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-06(01)_ODP	визначені автоматичні механізми звітування про інциденти;
	IR-06(01)	використовуються **<IR-06(01)_ODP автоматичні механізми>** звітування про інциденти.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються повідомлення про інциденти; автоматизовані механізми підтримки повідомлення про інциденти; проєктна документація системи; налаштування конфігурації системи та супутня документація; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за повідомлення про інциденти; персонал організації, який відповідає за інформаційну безпеку].	

	Перевірка: [ВИБІР: Процеси для повідомлення про інциденти; автоматизовані механізми, що підтримують та / або впроваджують звітування про інциденти].

IR-06(02)	**ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ - ВРАЗЛИВІСТЬ, ПОВ'ЯЗАНА З ІНЦИДЕНТАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-06(02)_ODP	**визначено персонал або ролі, яким повідомляється про вразливості системи, пов'язані з зареєстрованими інцидентами;**
	IR-06(02)	про вразливості системи, пов'язані із зареєстрованими інцидентами, повідомляється до **<IR-06(02)_ODP персонал або ролі>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються повідомлення про інциденти; план реагування на інциденти; план захисту інформації; звіти про інциденти безпеки та пов'язані з ними вразливості системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за повідомлення про інциденти; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; персонал, якому повідомляється про вразливості, пов'язані з інцидентами безпеки]. **Перевірка:** [ВИБІР: Процеси для повідомлення про інциденти; автоматизовані механізми, що підтримують та / або впроваджують повідомлення про вразливості, пов'язані з інцидентами безпеки].	

IR-06(03)	**ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ - КООРДИНАЦІЯ ЛАНЦЮЖКА ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-06(03)	інформація про інцидент надається постачальнику продукту або послуги та іншим організаціям, які беруть участь у ланцюжку постачання систем або компонентів системи, пов'язаних з інцидентом.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються координації ланцюгів постачання; договори придбання; угоди про рівень обслуговування; план реагування на інциденти; план захисту інформації; плани іншої організації, яка бере участь у діяльності ланцюга постачання; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за повідомлення про інциденти; персонал організації, який відповідає за інформаційну безпеку; персо-	

	нал організації, який відповідає за ланцюжки постачання]. **Перевірка:** [ВИБІР: Процеси для повідомлення про інциденти; автоматизовані механізми, що підтримують та / або впроваджують звіт про інформацію про події, що бере участь у ланцюгу постачання]

IR-07	**ПІДТРИМКА РЕАГУВАННЯ НА ІНЦИДЕНТИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-07[01]	надається ресурс підтримки реагування на інциденти, що є невід'ємною частиною спроможності організації реагувати на інциденти;
	IR-07[01]	ресурс підтримки реагування на інциденти містить поради та допомогу користувачам системи для обробки та формування звітності про інциденти.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються допомоги у реагуванні на інциденти; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за допомогу та підтримку у справах інцидентів; персонал організації, який має доступ до служби підтримки та реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси для надання допомоги у реагуванні на інциденти; автоматизовані механізми підтримки та / або реалізації допомоги у реагуванні на інциденти].	

IR-07(01)	**ПІДТРИМКА РЕАГУВАННЯ НА ІНЦИДЕНТИ - АВТОМАТИЗАЦІЯ ПІДТРИМКИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ІНФОРМАЦІЇ ТА ПІДТРИМКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-07(01)_ODP	**визначено автоматизовані механізми, що використовуються для збільшення доступності інформації та підтримки при реагуванні на інциденти;**
	IR-07(01)	підвищено доступність інформації та підтримки реагування на інциденти з використанням **<IR-07(01)_ODP автоматизованих механізмів>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються допомоги у реагуванні на інциденти; автоматизовані механізми, що підт-	

	римують підтримку та допомогу у реагуванні на інциденти; проєктна документація системи; налаштування конфігурації системи та відповідна документація; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за підтримку та допомогу щодо реагування на інциденти; персонал організації, який має доступ до служби підтримки та реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси для надання допомоги у реагуванні на інциденти; автоматизовані механізми, що підтримують та / або впроваджують збільшення доступності інформації та підтримки реагування на інциденти].

IR-07(02)	**ПІДТРИМКА РЕАГУВАННЯ НА ІНЦИДЕНТИ - КООРДИНАЦІЯ З ЗОВНІШНІМИ ПОСТАЧАЛЬНИКАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-07(02)(a)	встановлено прямі відносини кооперації між здатністю реагування на інциденти та зовнішніми постачальниками можливостей захисту системи.
	IR-07(02)(b)	визначено членів команди реагування на інциденти в організації для зовнішніх постачальників послуг.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються допомоги у реагуванні на інциденти; план реагування на інциденти; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за підтримку та допомогу щодо реагування на інциденти; зовнішні постачальники можливостей захисту системи; персонал організації, який відповідає за інформаційну безпеку]	

IR-08	**ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-08_ODP[01]	**визначено персонал або ролі, які переглядають та затверджують план реагування на інциденти;**
	IR-08_ODP[02]	**визначено періодичність перегляду та затвердження плану реагування на інциденти;**
	IR-08_ODP[03]	**визначені організації, персонал або ролі, які несуть відповідальність за реагування на інциденти;**

	IR-08_ODP[04]	**визначено персонал з реагування на інцидент (ідентифікований за іменами та/або за ролями), якому мають бути роздані копії плану реагування на інцидент;**
	IR-08_ODP[05]	**визначено елементи організації, серед яких мають бути розповсюджені копії плану реагування на інцидент;**
	IR-08_ODP[06]	**визначено персонал з реагування на інцидент (ідентифікований за іменами та/або ролями), якому повідомляються зміни до плану реагування на інцидент;**
	IR-08_ODP[07]	**визначено елементи організації, яким повідомляється про зміни в плані реагування на інцидент;**
	IR-08(a)[01]	розроблено план реагування на інциденти, який надає організації дорожню карту для впровадження її можливостей реагування на інциденти;
	IR-08(a)[02]	розроблено план реагування на інциденти, який описує структуру та організацію спроможності реагування на інциденти;
	IR-08(a)[03]	розроблено план реагування на інциденти, який надає високорівневий підхід до того, як здатність реагування на інциденти вписується в загальну практику організації;
	IR-08(a)[04]	розроблено план реагування на інциденти, який відповідає унікальним вимогам організації, які пов'язані із завданнями, розміром, структурою і функціями;
	IR-08(a)[05]	розроблено план реагування на інциденти, який визначає підзвітні інциденти;
	IR-08(a)[06]	розроблено план реагування на інциденти, який надає показники для вимірювання можливостей реагування на інциденти всередині організації;
	IR-08(a)[07]	розроблено план реагування на інциденти, який визначає ресурси та управлінську підтримку, необхідну для ефективної підтримки та розвитку можливостей реагування на інциденти;
	IR-08(a)[08]	розроблено план реагування на інциденти, який вирішує питання обміну інформацією про інциденти;
	IR-08(a)[09]	розроблено план реагування на інцидент, який розглядається та затверджується **<IR-08_ODP[01] персоналом або ролями> <IR-08_ODP[02] частота>**;
	IR-08(a)[10]	розроблено план реагування на інциденти, в якому чітко визначено відповідальність за реагування на інциденти для **<IR-08_ODP[03] організацій, персоналу або ролей>**.
	IR-08(b)[01]	копії плану реагування на інцидент розповсюджуються серед **<IR-**

		08_ODP[04] персоналу з реагування на інциденти>;
	IR-08(b)[02]	копії плану реагування на інцидент розповсюджуються серед **<IR-08_ODP[05] елементів організації>**;
	IR-08(c)	план реагування на інциденти оновлюється з урахуванням змін у системі та організації або проблем, що виникають під час впровадження, виконання або тестування плану;
	IR-08(d)[01]	зміни в плані реагування на інцидент повідомляються **<IR-08_ODP[06] персоналу з реагування на інциденти>**;
	IR-08(d)[02]	зміни в плані реагування на інциденти надсилаються до **<IR-08_ODP[07] елементів організації>**;
	IR-08(e)[01]	план реагування на інциденти захищений від несанкціонованого розкриття;
	IR-08(e)[02]	план реагування на інциденти захищений від несанкціонованої модифікації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються планування реагування на інциденти; план реагування на інциденти; записи оглядів та затверджень плану реагування на інциденти; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: План реагування на інциденти та пов'язані з ними процеси].	

IR-08(01)	**ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ - ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-08(01)(a)	план реагування на інциденти для інцидентів, пов'язаних з персональними даними, включає процес визначення доцільності повідомлення наглядових організацій і надання такого повідомлення, якщо це доречно;
	IR-08(01)(b)	план реагування на інциденти для інцидентів, пов'язаних з персональними даними, включає процес оцінювання для визначення ступеня шкоди, труднощів, незручностей або несправедливості щодо постраждалих осіб та будь-які механізми пом'якшення такої шкоди;
	IR-08(01)(c)	план реагування на інциденти для інцидентів, пов'язаних з персональними даними, включає ідентифікацію застосовних вимог щодо конфіденційності.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються планування реагування на інциденти; план реагування на інциденти; записи оглядів та затверджень плану реагування на інциденти; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: План реагування на інциденти та пов'язані з ними процеси].

IR-09	**РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-09_ODP[01]	**визначено персонал або ролі, на які покладено відповідальність за реагування на витоки інформації;**
	IR-09_ODP[02]	**визначено персонал або ролі, які мають бути сповіщені про витік інформації за допомогою методу зв'язку, не пов'язаного з витоком;**
	IR-09_ODP[03]	**визначені дії, які необхідно виконати;**
	IR-09(a)	**<IR-09_ODP[01] персонал або ролі>** призначено відповідальним за реагування на витоки інформації;
	IR-09(b)	у відповідь на витік інформації визначається конкретна інформація, пов'язана з джерелом витоку в системі;
	IR-09(c)	**<IR-09_ODP[02] персонал або ролі>** попереджається про витік інформації за допомогою методу зв'язку, не пов'язаного з витоком;
	IR-09(d)	ізоляцюється система або компонент системи де відбувся витік інформації;
	IR-09(e)	інформація видаляється із зараженої системи або компонента у відповідь на витік інформації;
	IR-09(f)	у відповідь на витік інформації визначаються інші системи або компоненти системи, які могли бути згодом джерелом витоку інформації;
	IR-09(g)	**<IR-09_ODP[03] дії>** виконуються у відповідь на витік інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються витоку інформації; план реагування на інциденти; записи попереджень / сповіщень про витік інформації, список персоналу, який повинен отримувати попере-	

	дження про витік інформації; перелік дій, які слід виконати щодо витоку інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси для реагування на витік інформації; автоматизовані механізми, що підтримують та / або реалізують дії щодо реагування на витік інформації та пов'язані з ними комунікації].

IR-09(01)	**РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - ВІДПОВІДАЛЬНИЙ ПЕРСОНАЛ**
	[Вилучено: включено до IR-09]

IR-09(02)	**РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - ТРЕНУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-09(02)_ODP	визначено частоту навчання з реагування на витік інформації;
	IR-09(02)	забезпечено навчання з реагування на витік інформації **<IR-09(02)_ODP частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються тренінгів щодо реагування на витік інформації; навчальна програма з питань реагування на витік інформації; навчальні матеріали щодо реагування на витік інформації; план реагування на інциденти; записи навчальних заходів щодо реагування на витік інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за тренування з питань реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку].	

IR-09(03)	**РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - РОБОТА ПІСЛЯ ВИТОКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-09(03)_ODP	**визначено процедури з метою забезпечення спроможності персоналу організації, на який впливає витік інформації, продовжувати виконувати поставлені завдання, у той час, як постраждалі системи зазнають коригувальних дій.**
	IR-09(03)	реалізувано **<IR-09(03)_ODP процедури>**, з метою забезпечення спроможності для персоналу організації, на який впливає витік інформації, продовжувати виконувати поставлені завдання, у той час, як постраждалі системи зазнають коригу-

		вальних дій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; процедури, що стосуються витоку інформації; план реагування на інциденти; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для операцій після витоку]	

IR-09(04)	**РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - ВИКРИТТЯ НЕАВТОРИЗОВАНОГО ПЕРСОНАЛУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	IR-09(04)_ODP	визначено механізми захисту для персоналу, що має доступ до інформації, яка не відповідає призначеним правам доступу;
	IR-09(04)	застосовуються **<IR-09(04)_ODP механізми захисту>** для персоналу, що має доступ до інформації, яка не відповідає призначеним правам доступу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика реагування на інциденти; процедури, що стосуються врегулювання інцидентів; процедури, що стосуються витоку інформації; план реагування на інциденти; гарантії безпеки щодо витоку інформації / впливу неавторизованого персоналу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси для роботи з інформацією, що потрапляє до несанкціонованого персоналу; автоматизовані механізми, що підтримують та / або впроваджують запобіжні заходи для персоналу, який потрапляє під дію інформації, яка не знаходиться в межах призначених дозволів доступу].	

IR-10	**ІНТЕГРОВАНА КОМАНДА АНАЛІЗУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**
	[Вилучено: перенесено до IR-04(11)]

MA-01	**ПОЛІТИКА ТА ПРОЦЕДУРИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-01_ODP[01]	**визначено персонал або ролі, на які поширюється політика технічного обслуговування;**
	MA-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури технічного обслуговування;**
	MA-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	MA-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами технічного обслуговування;**
	MA-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика технічного обслуговування;**
	MA-01_ODP[06]	**визначено події, які потребують перегляду та оновлення поточної політики технічного обслуговування;**
	MA-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні процедури технічного обслуговування;**
	MA-01_ODP[08]	**визначено події, які потребують перегляду та оновлення процедур технічного обслуговування;**
	MA-01(a)[01]	розроблено та задокументовано політику технічного обслуговування;
	MA-01(a)[02]	політика технічного обслуговування поширюється на **<MA-01_ODP[01] персонал або ролі>**;
	MA-01(a)[03]	розроблені та задокументовані процедури технічного обслуговування, що сприяють впровадженню політики технічного обслуговування та пов'язаних з нею заходів технічного обслуговування;
	MA-01(a)[04]	процедури технічного обслуговування розповсюджуються серед **<MA-01_ODP[02] персоналу або ролей>**;
	MA-01(a)[01](a)[01]	політика технічного обслуговування **<MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить мету**;

	MA-01(a)[01](a)[02]	політика технічного обслуговування **<MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить сферу застосування;
	MA-01(a)[01](a)[03]	політика технічного обслуговування **<MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить ролі;
	MA-01(a)[01](a)[04]	політика технічного обслуговування **<MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить обов'язки;
	MA-01(a)[01](a)[05]	політика технічного обслуговування **<MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить відповідальність керівництва;
	MA-01(a)[01](a)[06]	політика технічного обслуговування **<MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить координацію між підрозділами організації;
	MA-01(a)[01](a)[07]	політика технічного обслуговування **<MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** містить систему контролю відповідності;
	MA-01(a)[01](b)	політика технічного обслуговування **<MA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам;
	MA-01(b)	**<MA-01_ODP[04] посадова особа>** призначається для управління розробкою, документуванням та розповсюдженням політики та процедур технічного обслуговування;
	MA-01(c)[01][01]	переглядається та оновлюється поточна політика обслуговування **<MA-01_ODP[05] частота>**;
	MA-01(c)[01][02]	переглядається та оновлюється поточна політика обслуговування після **<MA-01_ODP[06] подій>**;
	MA-01(c)[02][01]	переглядаються та оновлюються поточні процедури технічного обслуговування **<MA-01_ODP[07] частота>**;
	MA-01(c)[02][02]	переглядаються та оновлюються поточні процедури технічного обслуговування після **<MA-01_ODP[08] подій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури технічного обслуговування; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику технічного обслуговування; персонал, відповідальний за інформаційну безпеку].	

MA-02	**КОНТРОЛЬОВАНЕ ОБСЛУГОВУВАННЯ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-02_ODP[01]	**визначено персонал або ролі, необхідні для явного схвалення видалення системи або компоненту системи з обладнання організації для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації;**
	MA-02_ODP[02]	**визначено інформацію, що підлягає видаленню з пов'язаних носіїв до вилучення обладнання організації для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації;**
	MA-02_ODP[03]	**визначено інформацію, яка має бути внесена до записів з технічного обслуговування;**
	MA-02(a)[01]	технічне обслуговування, ремонт та заміна компонентів системи планується відповідно до вимог виробника або постачальника та/або вимог організації;
	MA-02(a)[02]	технічне обслуговування, ремонт і заміна компонентів системи задокументовані відповідно до вимог виробника або постачальника та/або вимог організації;
	MA-02(a)[03]	записи про технічне обслуговування, ремонт та заміну компонентів системи перевіряються відповідно до вимог виробника або постачальника та/або вимог організації;
	MA-02(b)[01]	затверджені всі заходи з технічного обслуговування, незалежно від того, чи виконуються вони на місці або віддалено, а також незалежно від того, чи обслуговується система або її компоненти на місці, чи переміщуються в інше місце;
	MA-02(b)[02]	здійснюються всі заходи з технічного обслуговування, незалежно від того, чи виконуються вони на місці або віддалено, а також незалежно від того, чи обслуговується система або її компоненти на місці, чи переміщуються в інше місце;
	MA-02(c)	**<MA-02_ODP[01] персонал або ролі>** повинен/повинні явно схвалити видалення системи або компонентів системи з об'єктів організації для обслуговування, ремонту або заміни поза межами експлуатації;
	MA-02(d)	обладнання очищується, щоб видалити **<MA-02_ODP[02] інформацію>** з пов'язаних з ним носіїв перед тим, як вилучити його з об'єктів організації для технічного обслуговування, ремонту або заміни за межами місця експлуатації;
	MA-02(e)	перевіряються всі потенційно порушені заходи захисту, щоб переконатися, що вони, як і раніше, працюють належним чином після дій з обслуговування, ремонту або заміни.

	MA-02(f)	**<MA-02_ODP[03] інформація>** вноситься до записів з технічного обслуговування.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються технічного обслуговування системи; записи технічного обслуговування; технічні характеристики виробника / постачальника; записи технічного обладнання; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за обробку засобів масової інформації; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси в організації для планування, виконання, документування, перегляду, затвердження та моніторингу технічного обслуговування та ремонту системи; процеси в організації для обробки компонентів системи; автоматизовані механізми, що підтримують та / або впроваджують контрольоване обслуговування; автоматизовані механізми, що здійснюють обробку компонентів системи].	

MA-02(01)	**КОНТРОЛЬОВАНЕ ОБСЛУГОВУВАННЯ - ЗМІСТ ЗАПИСУ**
	[Вилучено: Включено до MA-02]

MA-02(02)	**КОНТРОЛЬОВАНЕ ОБСЛУГОВУВАННЯ - АВТОМАТИЗОВАНА ТЕХНІЧНА ДІЯЛЬНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-02(02)_ODP[01]	**визначено автоматизовані механізми, що використовуються для планування дій з технічного обслуговування, ремонту та заміни системи;**
	MA-02(02)_ODP[02]	**визначено автоматизовані механізми, що використовуються для проведення дій з технічного обслуговування, ремонту та заміни системи;**
	MA-02(02)_ODP[03]	**визначено автоматизовані механізми, що використовуються для документування дій з технічного обслуговування, ремонту та заміни системи;**
	MA-02(02)(a)[01]	**<MA-02(02)_ODP[01] автоматизовані механізми>** використовуються для планування дій з технічного обслуговування, ремонту та заміни системи;
	MA-02(02)(a)[02]	**<MA-02(02)_ODP[02] автоматизовані механізми>** використовуються для проведення дій з технічного обслуговування, ремонту та заміни системи;

	MA-02(02)(a)[03]	**<MA-02(02)_ODP[03] автоматизовані механізми>** використовуються для документування дій з технічного обслуговування, ремонту та заміни системи;
	MA-02(02)(b)[01]	надаються актуальні, точні та повні записи про всі замовлені, заплановані, виконувані та завершені дії з технічного обслуговування;
	MA-02(02)(b)[02]	надаються актуальні, точні та повні записи про всі замовлені, заплановані, виконувані та завершені дії ремонту;
	MA-02(02)(b)[03]	надаються актуальні, точні та повні записи про всі замовлені, заплановані, виконувані та завершені дії з заміни;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування системи; автоматизовані механізми, що підтримують діяльність з обслуговування системи; налаштування конфігурації системи та відповідна документація; записи технічного обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують технічне обслуговування; автоматизовані механізми, що підтримують та / або впроваджують виготовлення записів про технічне обслуговування та ремонтні роботи].	

MA-03	**ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-03_ODP	**визначено частоту, з якою слід переглядати раніше затверджені інструменти технічного обслуговування;**
	MA-03(a)[01]	використання засобів технічного обслуговування затверджено;
	MA-03(a)[02]	використання засобів технічного обслуговування контролюється;
	MA-03(a)[03]	використання засобів технічного обслуговування відстажуються;
	MA-03(b)	переглядаються раніше затверджені інструменти технічного обслуговування **<MA-03_ODP частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосу-	

	ються засобів обслуговування системи; засоби технічного обслуговування системи та відповідна документація; записи технічного обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для затвердження, контролю та моніторингу засобів обслуговування; автоматизовані механізми, що підтримують та / або впроваджують затвердження, контроль та / або моніторинг засобів технічного обслуговування].

MA-03(01)	**ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ПЕРЕВІРКА ІНСТРУМЕНТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-03(01)	оглядаються інструменти для технічного обслуговування, які доставлені на об'єкт обслуговуючим персоналом, на предмет неправильних або несанкціонованих модифікацій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються засобів обслуговування системи; засоби технічного обслуговування системи та відповідна документація; записи про перевірку інструменту технічного обслуговування; записи технічного обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для перевірки засобів технічного обслуговування; автоматизовані механізми, що підтримують та / або впроваджують перевірку засобів технічного обслуговування].	

MA-03(02)	**ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ПЕРЕВІРКА НОСІЇВ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-03(02)	перед використанням носіїв у системі перевіряються носії, що містять діагностичні та тестові програми на наявність шкідливого коду.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються засобів обслуговування системи; засоби технічного обслуговування системи та відповідна документація; записи технічного обслуговування; інші відпо-	

	відні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для перевірки носія інформації на наявність шкідливого коду; автоматизовані механізми, що підтримують та / або здійснюють перевірку носіїв, що використовуються для технічного обслуговування].

MA-03(03)	**ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОМУ ПЕРЕМІЩЕННЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-03(03)_ODP	**визначено персонал або ролі, які можуть надавати дозвіл на переміщення обладнання з об'єкту;**
	MA-03(03)(a)	переміщення обладнання для технічного обслуговування, що містить інформацію організації, запобігається шляхом перевірки того, що на обладнанні не міститься ніякої інформації організації; або
	MA-03(03)(b)	переміщення обладнання для технічного обслуговування, що містить інформацію організації, запобігається шляхом очищення або знищення обладнання; або
	MA-03(03)(c)	переміщення обладнання для технічного обслуговування, що містить інформацію організації, запобігається шляхом утримання обладнання на об'єкті; або
	MA-03(03)(d)	переміщення обладнання для технічного обслуговування, що містить інформацію організації, запобігається шляхом отримання дозволу від **<MA-03(03)_ODP персонал або ролі>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються засобів обслуговування системи; засоби технічного обслуговування системи та відповідна документація; записи технічного обслуговування; записи очищення обладнання; записи очищення засобів масової інформації; виключення від вивезення обладнання; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за очищення засобів масової інформації]. **Перевірка:** [ВИБІР: Процес організації запобігання несанкціонованому видаленню інформації; автоматизовані механізми, що підтримують очищення засобів масової інформації або знищення обладнання; автоматизовані механізми, що підтримують перевірку очищення засобів масової інформації].	

MA-03(04)	ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ОБМЕЖЕННЯ ВИКОРИСТАННЯ ІНСТРУМЕНТА
	МЕТА ОЦІНКИ: Визначити, чи: **MA-03(04)** обмежено використання інструментів технічного обслуговування лише авторизованим персоналом. **ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:** **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються засобів обслуговування системи; засоби технічного обслуговування системи та відповідна документація; список персоналу, уповноваженого користуватися інструментами технічного обслуговування; записи використання технічного обслуговування; записи технічного обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процес організації для обмеження використання засобів технічного обслуговування; автоматизовані механізми, що підтримують та / або впроваджують обмежене використання засобів технічного обслуговування].

MA-03(05)	ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ПРИВІЛЕЙОВАНЕ ВИКОНАННЯ
	МЕТА ОЦІНКИ: Визначити, чи: **MA-03(05)** відстежується використання інструментів обслуговування, які виконуються з підвищеними привілеями. **ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:** **Дослідження:** [ВИБІР: Політика технічного обслуговування; процедури, що стосуються інструментів технічного обслуговування системи; інструменти технічного обслуговування системи та пов'язана з ними документація; список осіб, які мають право використовувати інструменти технічного обслуговування; записи про використання інструментів технічного обслуговування; записи про технічне обслуговування; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси обмеження використання засобів технічного обслуговування; процес моніторингу використання засобів технічного обслуговування; механізми моніторингу використання засобів технічного обслуговування].

MA-03(06)	ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ОНОВЛЕННЯ ПРОГРАМ-

	НОГО ЗАБЕЗПЕЧЕННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-03(06)	інструменти технічного обслуговування перевіряються, щоб переконатися, що встановлені найновіші оновлення програмного забезпечення та патчі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика технічного обслуговування; процедури, що стосуються інструментів технічного обслуговування системи; інструменти технічного обслуговування системи та пов'язана з ними документація; список осіб, які мають право використовувати інструменти технічного обслуговування; записи про використання інструментів технічного обслуговування; записи про технічне обслуговування; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації перевірки засобів технічного обслуговування; процеси організації оновлення засобів технічного обслуговування; механізми підтримки та/або впровадження перевірки засобів технічного обслуговування; механізми підтримки та/або впровадження оновлення засобів технічного обслуговування].	

MA-04	**ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-04(a)[01]	впроваджено віддалені дії з обслуговування та діагностики;
	MA-04(a)[02]	відстежуються віддалені дії з обслуговування та діагностики;
	MA-04(b)[01]	використання віддалених засобів технічного обслуговування та діагностики дозволено лише відповідно до політики організації;
	MA-04(b)[02]	використання віддалених засобів технічного обслуговування та діагностики задокументовано в плані захисту інформації;
	MA-04(c)	надійна автентифікація використовується при встановленні віддалених технічних та діагностичних сеансів;
	MA-04(d)	ведеться облік віддалених дій з обслуговування та діагностики;
	MA-04(e)[01]	сесія припиняється, коли завершено віддалене обслуговування
	MA-04(e)[02]	мережеве з'єднання припиняється, коли завершено віддалене

		обслуговування
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування віддаленої системи; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи технічного обслуговування; діагностичні записи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування інформаційної системи; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для управління віддаленим обслуговуванням; автоматизовані механізми реалізації, підтримки та / або управління віддаленим технічним обслуговуванням; автоматизовані механізми для надійної автентифікації віддалених діагностичних сеансів обслуговування; автоматизовані механізми припинення віддалених сеансів технічного обслуговування та мережевих з'єднань].	

MA-04(01)	**ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - АУДИТ ТА ОГЛЯД**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-04(01)_ODP[01]	**визначено події аудиту, які слід журналювати для віддалених сеансів обслуговування;**
	MA-04(01)_ODP[02]	**визначено події аудиту, які слід журналювати для віддалених сеансів діагностики;**
	MA-04(01)(a)[01]	**<MA-04(01)_ODP[01] події аудиту>** журналюються для віддалених сеансів обслуговування;
	MA-04(01)(a)[02]	**<MA-04(01)_ODP[02] події аудиту>** журналюються для віддалених сеансів діагностики;
	MA-04(01)(b)[01]	здійснюється огляд записів про сеанси віддаленого обслуговування;
	MA-04(01)(b)[02]	здійснюється огляд записів про сеанси віддаленої діагностики.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування відділеної системи; перелік подій аудиту; налаштування конфігурації системи та відповідна документація; записи технічного обслуговування; діагностичні записи; записи аудиту; огляди записів сеансів обслуговування та діагностики; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за аудит та перевірку; адміністратори системи /	

	мережі]. **Перевірка:** [ВИБІР: Процеси організації для аудиту та перегляду віддаленого обслуговування; автоматизовані механізми, що підтримують та / або впроваджують аудит та огляд віддаленого обслуговування].

MA-04(02)	**ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - ДОКУМЕНТУВАННЯ ВІДДАЛЕНОГО ОБСЛУГОВУВАННЯ**
	[Вилучено: включено до MA-01 та MA-04]

MA-04(03)	**ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - ПОРІВНЯЛЬНА БЕЗПЕКА І ОЧИЩЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-04(03)(a)[01]	віддалені послуги з технічного обслуговування повинні виконуватися з системи, яка реалізує заходи захисту, співставні з заходами захисту, реалізованими в системі, що обслуговується;
	MA-04(03)(a)[02]	віддалені послуги з діагностики повинні виконуватися з системи, яка реалізує заходи захисту, співставні з заходами захисту, реалізованими в системі, що обслуговується;
	MA-04(03)(b)[01]	компонент, що підлягає обслуговуванню, видаляється з системи перед проведенням віддаленого технічного обслуговування або діагностики;
	MA-04(03)(b)[02]	компонент, що підлягає обслуговуванню, пройшов процедуру очищення (від інф ормації організації);
	MA-04(03)(b)[03]	компонент перевіряється та очищується (на наявність потенційно шкідливого програмного забезпечення) після виконання послуги та перед повторним підключенням компонента до системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування віддаленої системи; контракти про надання послуг та / або угоди про рівень послуг; записи технічного обслуговування; протоколи перевірок; записи аудиту; записи очищення обладнання; записи очищення засобів масової інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи; постачальник технічного обслуговування системи; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за очищення засобів масової інформації; адміністратори системи / мережі]. **Перевірка**: [ВИБІР: Процеси організації для безпеки та очищення компонентів	

	для віддаленого обслуговування; процеси організації з видалення, очищення та перевірки компонентів, що обслуговуються через віддалене технічне обслуговування; автоматизовані механізми підтримки та / або впровадження очищення та інспекції компонентів].

MA-04(04)	**ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - АВТЕНТИФІКАЦІЯ ТА РОЗПОДІЛ СЕСІЇ ОБСЛУГОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-04(04)_ODP	**визначено автентифікатори, стійкі до повторного відтворення;**
	MA-04(04)(a)	віддалені сеанси обслуговування захищені використанням **<MA-04(04)_ODP автентифікаторів, стійких до повторного відтворення>**;
	MA-04(04)(b)(01)	віддалені сеанси технічного обслуговування захищені шляхом відокремлення сеансів технічного обслуговування від інших мережевих сеансів роботи з системою за допомогою фізично відокремлених шляхів зв'язку; або
	MA-04(04)(b)(02)	відокремлення сеансів технічного обслуговування від інших мережевих сеансів роботи з системою за допомогою логічно відокремлених шляхів зв'язку;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування віддаленої системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи технічного обслуговування; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи; мережеві інженери; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для захисту віддалених сеансів технічного обслуговування; автоматизовані механізми, що реалізують стійкі до відтворення автентифікатори; автоматизовані механізми, що реалізують логічно розділені / зашифровані шляхи зв'язку].	

MA-04(05)	**ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - СХВАЛЕННЯ ТА ПОВІДОМЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-04(05)_ODP[01]	**визначено персонал або ролі, необхідні для затвердження кожного віддаленого сеансу технічного обслуговування;**

	MA-04(05)_ODP[02]	**визначено персонал та ролі, які мають бути повідомлені про дату та час запланованого віддаленого технічного обслуговування;**
	MA-04(05)(a)	схвалення кожного віддаленого сеансу обслуговування від **<MA-04(05)_ODP[01] персонал або ролі>**;
	MA-04(05)(b)	**<MA-04(05)_ODP[02] персонал і ролі>** повідомлено про дату і час запланованого віддаленого технічного обслуговування.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування віддаленої системи; план захисту інформації; повідомлення, що підтримують віддалені сеанси технічного обслуговування; записи технічного обслуговування; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи; персонал організації, який відповідає за повідомлення; персонал організації, що відповідає за затвердження; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для затвердження та повідомлення персоналу щодо віддаленого технічного обслуговування; автоматизовані механізми, що підтримують повідомлення та затвердження віддалення технічного обслуговування].	

MA-04(06)	**ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - КРИПТОГРАФІЧНИЙ ЗАХИСТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-04(06)_ODP	**визначено криптографічні механізми, які необхідно впровадити для захисту цілісності та конфіденційності віддалених сеансів технічного обслуговування та діагностики;**
	MA-04(06)[01]	**<MA-04(06)_ODP криптографічні механізми>** реалізовано для захисту цілісності віддалених сеансів технічного обслуговування та діагностики;
	MA-04(06)[02]	**<MA-04(06)_ODP криптографічні механізми>** реалізовано для захисту конфіденційності віддалених сеансів технічного обслуговування та діагностики;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування віддаленої системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; криптографічні механізми, що захищають віддалену діяльність з технічного обслуговування; записи технічного обслуговування; діагностичні записи; записи аудиту; інші відпо-	

	відні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи; мережеві інженери; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Криптографічні механізми захисту комунікацій віддаленого технічного обслуговування та діагностики].

MA-04(07)	**ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - ПЕРЕВІРКА ВІДДАЛЕНОГО РОЗ'ЄДНАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-04(07)[01]	реалізувано перевірку роз'єднання у разі припинення віддалених сеансів обслуговування
	MA-04(07)[02]	реалізувано перевірку роз'єднання у разі припинення віддалених сеансів діагностики
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування віддаленої системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; криптографічні механізми, що захищають віддалену діяльність з технічного обслуговування; записи технічного обслуговування; діагностичні записи; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи; мережеві інженери; Персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Механізми, що реалізують перевірку відключення кінцевих віддалених сеансів технічного обслуговування та діагностики].	

MA-05	**ТЕХНІЧНИЙ ПЕРСОНАЛ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-05(a)[01]	запроваджено процес авторизації технічного персоналу;
	MA-05(a)[02]	ведеться перелік авторизованих організацій або персоналу з технічного обслуговування;
	MA-05(b)	персонал без супроводу, який виконує технічне обслуговування системи, має необхідні дозволи на доступ;
	MA-05(c)	персонал організації з необхідними повноваженнями доступу та технічною компетентністю призначений/призначені для нагляду за

		діяльністю з технічного обслуговування персоналу, який не має необхідних дозволів на доступ.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговуючого персоналу; договори про надання послуг; угоди про рівень обслуговування; список уповноваженого персоналу; записи технічного обслуговування; записи контролю доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для уповноваження та управління обслуговуючим персоналом; автоматизовані механізми, що підтримують та / або впроваджують дозвіл обслуговуючого персоналу].	

MA-05(01)	**ТЕХНІЧНИЙ ПЕРСОНАЛ - ОСОБИ БЕЗ НАЛЕЖНОГО ДОСТУПУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-05(01)_ODP	**визначені альтернативні заходи захисту, які мають бути розроблені та впроваджені на випадок, якщо компонент системи не може бути очищений, вилучений або відключений від системи;**
	MA-05(01)(a)[01]	впроваджені процедури залучення персоналу з технічного обслуговування, який не має відповідних дозволів (допуску) або не є громадянами України, містять вимогу: обслуговуючий персонал, що не має необхідних прав доступу, рівня допуску, або офіційного затвердженого доступу,повинен супроводжуватися та бути під наглядом уповноваженого організацією персоналу, з необхідним рівнем допуску, а також мати відповідну технічну кваліфікацію для виконання технічного обслуговування та діагностичних заходів у системі;
	MA-05(01)(a)[02]	впроваджені процедури залучення персоналу з технічного обслуговування, який не має відповідних дозволів (допуску) або не є громадянами України, містять вимогу: перед тим, як розпочати технічне обслуговування або діагностику персоналом, який не має необхідних прав допуску, рівня допуску або офіційного затвердженого доступу,упевнитися, що всі компоненти енергонезалежного зберігання інформації в системі очищуються, а всі енергонезалежні носії видаляються або фізично відключаються від системи та надійно захищаються;
	MA-05(01)(b)	**<MA-05(01)_ODP альтернативні заходи захисту>** розробляються і впроваджуються у випадку, якщо систему неможливо очистити, вилучити або відключити від систе-

		ми.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговуючого персоналу; політика захисту носіїв інформації системи; політика щодо фізичного захисту та захисту середовища роботи; план захисту інформації; перелік обслуговуючого персоналу, що вимагає супроводу / нагляду; записи технічного обслуговування; записи контролю доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи; персонал організації, який відповідає за забезпечення персоналу; персонал організації, який відповідає за фізичний контроль доступу; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за очищення носіїв інформації; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для управління обслуговуючим персоналом без відповідного доступу; автоматизовані механізми, що підтримують та / або впроваджують альтернативні гарантії безпеки; автоматизовані механізми підтримки та / або впровадження очищення носіїв інформації].	

MA-05(02)	**ТЕХНІЧНИЙ ПЕРСОНАЛ - ОФОРМЛЕННЯ ДОПУСКУ ДЛЯ СИСТЕМ, ЩО ОБРОБЛЯЮТЬ ІНФОРМАЦІЮ З ОБМЕЖЕНИМ ДОСТУПОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-05(02)[01]	персонал, який виконує роботи з технічного обслуговування та діагностики в системі, що обробляє, зберігає або передає інформацію з обмеженим доступом, має відповідний рівень допуску;
	MA-05(02)[02]	персонал, який виконує роботи з технічного обслуговування та діагностики в системі, що обробляє, зберігає або передає інформацію з обмеженим доступом, має офіційне схвалення на допуск;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговуючого персоналу; кадровий облік; записи технічного обслуговування; записи контролю доступу; облікові дані доступу; дозволи на доступ; інші відповідні документи або записи]. **Співбесіда: [**ВИБІР: Персонал організації, який відповідає за обслуговування системи; персонал організації, який відповідає за забезпечення персоналу; персонал організації, який відповідає за фізичний контроль доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для управління дозволами безпеки для обслуговуючого персоналу].	

MA-05(03)	ТЕХНІЧНИЙ ПЕРСОНАЛ - ВИМОГИ ДО ГРОМАДЯНСТВА	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-05(03)	працівники, які виконують технічне обслуговування та діагностичні заходи з обробки, зберігання або передачі інформації з обмеженим доступом, є громадянами України.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговуючого персоналу; кадровий облік; записи технічного обслуговування; записи контролю доступу; облікові дані доступу; дозволи на доступ; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи; персонал організації, який відповідає за забезпечення персоналу; персонал організації, який відповідає за інформаційну безпеку].	

MA-05(04)	ТЕХНІЧНИЙ ПЕРСОНАЛ - ІНОЗЕМНІ ГРОМАДЯНИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-05(04)(a)	іноземні громадяни з відповідним рівнем допуску залучаються для проведення технічного обслуговування та діагностичних робіт у системах, що обробляють інформацію з обмеженим доступом тільки тоді, коли ці системи спільно належать і експлуатуються урядами України та закордонних союзників, або належать та експлуатуються виключно іноземними союзними урядами;
	MA-05(04)(b)[01]	схвалення, що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування та діагностики систем, що обробляють інформацію з обмеженим доступом, повністю задокументовані в Меморандумі про угоду.
	MA-05(04)(b)[02]	згоди, що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування та діагностики систем, що обробляють інформацію з обмеженим доступом, повністю задокументовані в Меморандумі про угоду.
	MA-05(04)(b)[03]	додаткові умови експлуатації, що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування та діагностики систем, що обробляють інформацію з обмеженим доступом, повністю задокументовані в Меморандумі про угоду.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговуючого персоналу; політика захисту носіїв інформації системи; політика та процедури контролю доступу; політика та процедури фізичного захисту та захисту робочого середовища; меморандум про угоду; записи технічного обслуговування; записи контролю доступу; облікові дані доступу; дозволи на доступ; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обслуговування системи, персонал організації, який відповідає за безпеку персоналу; персонал організації, який керує меморандумами про угоди; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для управління іноземним обслуговуючим персоналом].

MA-05(05)	**ТЕХНІЧНИЙ ПЕРСОНАЛ - НЕСИСТЕМНЕ ОБСЛУГОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-05(05)	персонал, який не супроводжується, що здійснює ремонтні роботи, не пов'язаний безпосередньо з системою, але знаходиться фізично близько від системи, має необхідні дозволи на доступ.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговуючого персоналу; політика захисту носіїв інформації системи; політика та процедури контролю доступу; політика та процедури фізичного захисту та захисту робочого середовища; записи технічного обслуговування; записи контролю доступу; дозволи на доступ; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, який відповідає за забезпечення персоналу; персонал організації, який відповідає за фізичний контроль доступу; персонал організації, який відповідає за інформаційну безпеку].	

MA-06	**СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-06_ODP[01]	**визначено компоненти системи, для яких отримується технічна підтримка та/або запасні частини;**
	MA-06_ODP[02]	**визначено період часу, протягом якого можна отримати технічну підтримку та/або запасні частини у разі відмови;**
	MA-06	технічна підтримка та/або запасні частини отримуються для **<MA-06_ODP[01] компонентів системи>** протягом **<MA-06_ODP[02] періоду часу>** після відмови.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування системи; договори про надання послуг; угоди про рівень обслуговування; інвентаризація та наявність запасних частин; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, який відповідає за придбання; персонал організації, відповідальний за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для забезпечення своєчасного обслуговування].

MA-06(01)	**СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ - ПРОФІЛАКТИЧНЕ ОБСЛУГОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-06(01)_ODP[01]	**визначено компоненти системи яким необхідно здійснювати профілактичне обслуговування;**
	MA-06(01)_ODP[02]	**визначено часові інтервали з якими необхідно здійснювати профілактичне обслуговування визначеним компонентам системи;**
	MA-06(01)	здійснюється профілактичне обслуговування **<MA-06(01)_ODP[01] компонентів системи>** у **<MA-06(01)_ODP[02] часові інтервали>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування системи; договори про надання послуг; угоди про рівень обслуговування; план захисту інформації; записи технічного обслуговування; перелік компонентів системи, що вимагають профілактичного обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, відповідальний за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для профілактичного обслуговування; автоматизовані механізми підтримки та / або впровадження профілактичного обслуговування].	

MA-06(02)	**СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ - ПЛАНОВЕ ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ**
	МЕТА ОЦІНКИ: Визначити, чи:

	MA-06(02)_ODP[01]	**визначено компоненти системи яким необхідно здійснювати планове технічне обслуговування;**
	MA-06(02)_ODP[02]	**визначено часові інтервали з якими необхідно здійснювати планове технічне обслуговування;**
	MA-06(02)	здійснюється планове технічне обслуговування **<MA-06(02)_ODP[01] компонентів системи>** у **<MA-06(02)_ODP[02] часові інтервали>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування системи; договори про надання послуг; угоди про рівень обслуговування; план захисту інформації; записи технічного обслуговування; перелік компонентів системи, що вимагають технічного обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, відповідальний за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для технічного обслуговування; автоматизовані механізми, що підтримують та / або впроваджують технічного обслуговування].	

MA-06(03)	**СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ - АВТОМАТИЗОВАНА ПІДТРИМКА ПЛАНОВОГО ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-06(03)_ODP	**визначено автоматизовані механізми для передачі даних планового технічного обслуговування до комп'ютеризованої системи управління обслуговуванням;**
	MA-06(03)	використовуються **<MA-06(03)_ODP автоматизовані механізми>** для передачі даних планового технічного обслуговування до комп'ютеризованої системи управління обслуговуванням.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика обслуговування системи; процедури, що стосуються обслуговування системи; договори про надання послуг; угоди про рівень обслуговування; план захисту інформації; записи технічного обслуговування; перелік компонентів системи, що вимагають технічного обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; персонал організації, відповідальний за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують передачу даних	

	технічного обслуговування в комп’ютеризовану систему управління технічним обслуговуванням; операції системи управління комп'ютерним обслуговуванням].

MA-07	**ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ В ПОЛЬОВИХ УМОВАХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MA-07_ODP[01]	**визначені системи або компоненти системи, на яких технічне обслуговування в польових умовах обмежене або заборонене**
	MA-07_ODP[02]	**визначено довірені засоби технічного обслуговуваннятехнічного обслуговування**
	MA-07	технічне обслуговування в польових умовах <**MA-07_ODP[01] систем або компонентів системи**> обмежене або заборонене для <**MA-07_ODP[02] довірених засобів технічного обслуговування**>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика технічного обслуговування; процедури, що стосуються технічного обслуговування в польових умовах; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи про технічне обслуговування; діагностичні записи; план захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обслуговування системи; або персонал організації, відповідальний за інформаційну безпеку; системні/мережеві адміністратори]. **Перевірка:** [ВИБІР: Процеси управління технічним обслуговуванням на місцях; механізми впровадження, підтримки та/або управління технічним обслуговуванням на місцях; механізми надійної автентифікації діагностичних сеансів технічного обслуговування на місцях; механізми завершення сеансів технічного обслуговування на місцях та мережевих з'єднань**.**].	

X. КЛАС ЗАХОДІВ ЗАХИСТУ МР – ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ

MP-01	**ПОЛІТИКА ТА ПРОЦЕДУРИ ЩОДО ЗАХИСТУ НОСІЇВ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-01_ODP[01]	**визначено персонал або ролі, серед яких має бути поширена політика захисту носіїв інформації;**
	MP-01_ODP[02]	**визначено персонал або ролі, серед яких мають бути поширені процедури захисту носіїв інформації;**
	MP-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	MP-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами захисту носіїв інформації;**
	MP-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика захисту носіїв інформації;**
	MP-01_ODP[06]	**визначено події, які потребують перегляду та оновлення чинної політики захисту носіїв інформації;**
	MP-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються чинні процедури захисту носіїв інформації;**
	MP-01_ODP[08]	**визначено події, які потребують перегляду та оновлення процедур захисту носіїв інформації;**
	MP-01(a)[01]	розроблено та задокументовано політику захисту носіїв інформації;
	MP-01(a)[02]	політика захисту носіїв інформації поширюється на **<MP-01_ODP[01] персонал або ролі>**;
	MP-01(a)[03]	розроблено та задокументовано процедури захисту носіїв інформації, що сприятимуть реалізації політики захисту носіїв інформації та заходів захисту носіїв інформації;
	MP-01(a)[04]	процедури захисту носіїв інформації поширюються на **<MP-01_ODP[02] персонал або ролі>**;
	MP-01(a)[01](a)[01]	**<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика захисту носіїв інформації містить мету;

	MP-01(a)[01](a)[02]	**<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика захисту носіїв інформації містить сферу застосування;
	MP-01(a)[01](a)[03]	**<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика захисту носіїв інформації містить ролі;
	MP-01(a)[01](a)[04]	**<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика захисту носіїв інформації містить обов'язки;
	MP-01(a)[01](a)[05]	**<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика захисту носіїв інформації містить відповідальність керівництва;
	MP-01(a)[01](a)[06]	**<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика захисту носіїв інформації містить координацію між підрозділами організації;
	MP-01(a)[01](a)[07]	**<MP-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика захисту носіїв інформації містить систему контролю відповідності;
	MP-01(a)[01](b)	політика захисту носіїв інформації відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам;
	MP-01(b)	**<MP-01_ODP[04] посадова особа>** призначається для управління розробкою, документуванням та розповсюдженням політики та процедур захисту носіїв інформації.
	MP-01(c)[01][01]	переглядається та оновлюється поточна політика захисту носіїв інформації **<MP-01_ODP[05] частота>**;
	MP-01(c)[01][02]	переглядається та оновлюється поточна політика захисту носіїв інформації після **<MP-01_ODP[06] подій>**;
	MP-01(c)[02][01]	переглядаються та оновлюються поточні процедури захисту носіїв інформації **<MP-01_ODP[07] частота>**;
	MP-01(c)[02][02]	переглядаються та оновлюються поточні процедури захисту носіїв інформації після **<MP-01_ODP[08] подій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури захисту носіїв інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику захисту носіїв інформації; персонал, відповідальний за інформаційну безпеку].	

MP-02	**ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-02_ODP[01]	**визначено типи цифрових носіїв інформації, доступ до яких обмежено;**
	MP-02_ODP[02]	**визначено персонал або ролі, уповноважені на доступ до цифрових носіїв інформації;**
	MP-02_ODP[03]	**визначено типи нецифрових носіїв інформації, доступ до яких обмежено;**
	MP-02_ODP[04]	**визначено персонал або ролі, уповноважені на доступ до нецифрових носіїв інформації;**
	MP-02[01]	доступ до **<MP-02_ODP[01] типів цифрових носіїв інформації>** обмежено для **<MP-02_ODP[02] персоналу або ролей>**;
	MP-02[02]	доступ до **<MP-02_ODP[03] типів нецифрових носіїв інформації>** обмежено для **<MP-02_ODP[04] персоналу або ролей>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються обмежень доступу до носіїв інформації; політика та процедури контролю доступу; політика та процедури фізичного та екологічного захисту; засоби зберігання носіїв інформації; записи контролю доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за захист носіїв інформації в системі; персонал організації, відповідальний за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для обмеження носіїв інформації; автоматизовані механізми, що підтримують та / або запроваджують обмеження доступу до носіїв інформації].	

MP-02(01)	**ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ - АВТОМАТИЗОВАНИЙ ОБМЕЖЕННИЙ ДОСТУП**
	[Вилучено: Включено до MP-04(02)]

MP-02(02)	**ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ**
	[Вилучено: Включено до SC-28(01)]

MP-03	**МАРКУВАННЯ НОСІЇВ ІНФОРМАЦІЇ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-03_ODP[01]	**визначено типи носіїв інформації, які звільняються від маркування під час перебування на контрольованих зонах;**
	MP-03_ODP[02]	**визначено контрольовані зони, де носії інформації звільняються від маркування;**
	MP-03(a)	носії інформації маркуються, щоб вказати на обмеження поширення, обробки, а також застереження та відповідні мітки безпеки (якщо такі є) інформації;
	MP-03(b)	**<MP-03_ODP[01] типи носіїв інформації>** залишаються в межах **<MP-03_ODP[02] контрольованих зон>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються маркування носіїв інформації; політика та процедури фізичного та екологічного захисту; план захисту інформації; перелік носіїв інформації системи, що позначають атрибути безпеки; визначені контрольовані зони; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за захист та маркування носіїв інформації системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для маркування носіїв інформації; автоматизовані механізми, що підтримують та / або впроваджують маркування носіїв інформації].	

MP-04	**ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-04_ODP[01]	**визначено типи цифрових носіїв інформації, які підлягають фізичному контролю (якщо вибрано);**
	MP-04_ODP[02]	**визначено типи нецифрових носіїв інформації, які підлягають фізичному контролю (якщо вибрано);**
	MP-04_ODP[03]	**визначено типи цифрових носіїв інформації для безпечного зберігання (якщо вибрано);**
	MP-04_ODP[04]	**визначено типи нецифрових носіїв інформації для безпечного зберігання (якщо вибрано);**
	MP-04_ODP[05]	**визначено контрольовані зони, в яких можна безпечно зберігати цифрові носії інформації;**

	MP-04_ODP[06]	**визначено контрольовані зони, в яких можна безпечно зберігати нецифрові носії інформації;**
	MP-04(a)[01]	**<MP-04_ODP[01] типи цифрових носіїв>** контролюються фізично;
	MP-04(a)[02]	**<<MP-04_ODP[02] типи нецифрових носіїв>** контролюються фізично;
	MP-04(a)[03]	**<MP-04_ODP[03] типи цифрових носіїв>** безпечно зберігаються в **<MP-04_ODP[05] контрольованих зонах>**;
	MP-04(a)[04]	**<MP-04_ODP[04]** типи нецифрових носіїв> безпечно зберігаються в **<MP-04_ODP[06] контрольованих зонах>**;
	MP-04(b)	типи носіїв інформації (визначені в MP-04_ODP[01], MP-04_ODP[02], MP-04_ODP[03], MP-04_ODP[04]) захищені доти, доки носії інформації не будуть знищені або очищені за допомогою визначеного обладнання, методик та процедур.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються зберігання носіїв інформації; політика та процедури фізичного захисту та захисту робочого середовища; політика та процедури контролю доступу; план захисту інформації ;носії інформаційної системи; визначені контрольовані зони; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за захист та зберігання носіїв інформації; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для зберігання носіїв інформації; автоматизовані механізми, що підтримують та / або впроваджують безпечне зберігання носіїв інформації / захист носіїв інформації].	

MP-04(01)	**ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ**
	[Вилучено: Включено до SC-28(01)].

MP-04(02)	**ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ - АВТОМАТИЗОВАНИЙ ОБМЕЖЕНИЙ ДОСТУП**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-04(02)_ODP[01]	**визначено автоматизовані механізми обмеження доступу до зон зберігання носіїв інформації;**
	MP-04(02)_ODP[02]	**визначено автоматизовані механізми реєстрації спроб доступу до зон зберігання носіїв інформації;**

	MP-04(02)_ODP[03]	**визначено автоматизовані механізми реєстрації доступу, наданого до зон зберігання носіїв інформації;**
	MP-04(02)[01]	доступ до зон зберігання носіїв інформації обмежено за допомогою **<MP-04(02)_ODP[01] автоматизованих механізмів>**;
	MP-04(02)[02]	спроби доступу до зон зберігання носіїв інформації реєструються за допомогою **<MP-04(02)_ODP[02] автоматизованих механізмів>**;
	MP-04(02)[03]	доступ, наданий до зон зберігання носіїв, реєструється за допомогою **<MP-04(02)_ODP[03] автоматизованих механізмів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються зберігання носіїв інформації; політика та процедури контролю доступу; політика та процедури фізичного захисту та захисту робочого середовища; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби зберігання носіїв інформації; пристрої контролю доступу; записи контролю доступу; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за захист та зберігання носіїв інформації; персонал організації, відповідальний за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що обмежують доступ до зон зберігання носіїв інформації; автоматизовані механізми, що перевіряють спроби доступу та доступ, наданий до зон зберігання носіїв інформації].	

MP-05	**ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-05_ODP[01]	**визначено типи носіїв інформації системи для захисту та контролю під час транспортування за межі контрольованих зон;**
	MP-05_ODP[02]	**визначено заходи безпеки, що використовуються для захисту носіїв інформації системи поза контрольованими зонами;**
	MP-05_ODP[03]	**визначено заходи безпеки, що використовуються для контролю носіїв інформації системи за межами контрольованих зон;**
	MP-05(a)[01]	**<MP-05_ODP[01] типи носіїв інформації системи>** захищаються під час транспортування за межі контрольованих зон за допомогою **<MP-05_ODP[02] заходів безпеки>**;
	MP-05(a)[02]	**<MP-05_ODP[01] типи носіїв інформації системи>**

		контролюються під час транспортування за межі контрольованих зон за допомогою **<MP-05_ODP[03] заходів безпеки>**;
	MP-05(b)	під час транспортування за межі контрольованих зон ведеться облік носіїв інформації системи;
	MP-05(c)	діяльність, пов'язана з транспортуванням носіїв інформації системи, задокументована;
	MP-05(d)[01]	визначено персонал, уповноважений здійснювати діяльність з транспортування носіїв інформації;
	MP-05(d)[02]	діяльність, пов'язана з транспортуванням носіїв інформації системи, обмежується визначеним уповноваженим персоналом.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються зберігання носіїв інформації; політика та процедури фізичного захисту та захисту робочого середовища; політика та процедури контролю доступу; план захисту інформації; носії інформаційної системи; визначені контрольовані зони; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за захист та зберігання носіїв інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для зберігання носіїв інформації; автоматизовані механізми, що підтримують та / або впроваджують носій інформації / захист носія інформації].	

MP-05(01)	**ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗАХИСТ ПОЗА КОНТРОЛЬОВАНИМИ ЗОНАМИ**
	[Вилучено: Включено до MP-05].

MP-05(02)	**ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - ДОКУМЕНТУВАННЯ ДІЙ**
	[Вилучено: Включено до MP-05].

MP-05(03)	**ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗБЕРІГАЧІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-05(03)[01]	визначено зберігачів інформації під час транспортування носіїв інформації системи за межі контрольованих зон.
	MP-05(03)[02]	залучено визначених зберігачів інформації під час транспорту-

		вання носіїв інформації системи за межі контрольованих зон.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються транспортування носіїв інформації; політика та процедури фізичного захисту та захисту робочого середовища; записи транспортування носіїв інформаційні системи; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за транспортутвання носіїв інформації системи; персонал організації, який відповідає за інформаційну безпеку].	

MP-05(04)	**ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ**
	[Вилучено: Включено до SC-28(01)].

MP-06	**ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-06_ODP[01]	**визначено носії інформації системи, які підлягають очищенню перед утилізацією;**
	MP-06_ODP[02]	**визначено носії інформації системи, які підлягають очищенню перед випуском за межі контрольованої зони;**
	MP-06_ODP[03]	**визначені носії інформації системи, що підлягають очищенню перед повторним використанням;**
	MP-06_ODP[04]	**визначено методи та процедури очищення, які слід використовувати для очищення перед утилізацією;**
	MP-06_ODP[05]	**визначено методи та процедури очищення, які слід використовувати для очищення перед випуском за межі контрольованої зони;**
	MP-06_ODP[06]	**визначено методи та процедури очищення, які слід використовувати для очищення перед повторним використанням;**
	MP-06(a)[01]	**<MP-06_ODP[01] носії інформації системи>** перед утилізацією піддаються очищенню за допомогою **<MP-06_ODP[04] методів та процедур очищення>**;
	MP-06(a)[02]	**<MP-06_ODP[02] носії інформації системи>** очищаються за допомогою **<MP-06_ODP[05] методів та процедур очищення>** перед випуском за межі контрольованої зони;
	MP-06(a)[03]	**<MP-06_ODP[03] носії інформації системи>** очищуються за

		допомогою **<MP-06_ODP[06] методів і процедур очищення>** перед повторним використанням;
	MP-06(b)	застосовуються механізми очищення, надійність і цілісність яких відповідає категорії безпеки або рівню секретності інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються очищення та утилізації носіїв інформації; державні стандарти та політики, що стосуються очищення носіїв інформації; записи очищення носіїв інформації; записи аудиту; проєктна документація системи; налаштування конфігурації системи та відповідна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за очищення носіїв інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для очищення носіїв інформації; автоматизовані механізми підтримки та / або впровадження очищення носіїв інформації].	

MP-06(01)	**ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ПЕРЕГЛЯДАТИ, ЗАТВЕРДЖЕННЯ, ВІДСТЕЖЕННЯ, ДОКУМЕНТУВАННЯ ТА ПЕРЕВІРКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-06(01)[01]	переглядаються заходи з очищення та утилізації носіїв інформації;
	MP-06(01)[02]	затверджуються заходи з очищення та утилізації носіїв інформації;
	MP-06(01)[03]	відстежуються заходи з очищення та утилізації носіїв інформації;
	MP-06(01)[04]	документуються заходи з очищення та утилізації носіїв інформації;
	MP-06(01)[05]	перевіряються заходи з очищення та утилізації носіїв інформації;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються очищення та утилізації носіїв інформації; записи про очищення та утилізацію носіїв інформації; записи заходів щодо очищення та утилізації носіїв інформації; погодження заходів щодо очищення та утилізації носіїв інформації; відстеження записів; записи перевірки; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за очищення та утилізацію носіїв інформації; персонал організації, який відповідає за інформаційну	

	безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для очищення носіїв інформації; автоматизовані механізми підтримки та / або впровадження очищення носіїв інформації].

MP-06(02)	**ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ПЕРЕВІРКА ОБЛАДНАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-06(02)_ODP[01]	**визначена частота, з якою проводиться перевірка обладнання для очищення;**
	MP-06(02)_ODP[02]	**визначено частоту, з якою потрібно перевіряти процедури очищення;**
	MP-06(02)[01]	обладнання для очищення тестується **<MP-06(02)_ODP[01] частота>**, щоб переконатися в досягненні запланованого очищення;
	MP-06(02)[02]	процедури санітарної обробки тестуються **<MP-06(02)_ODP[02] частота>**, щоб переконатися в досягненні запланованого очищення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються очищення та утилізації носіїв інформації; процедури, що стосуються випробувань засобів очищення носіїв інформації; результати тестування обладнання та процедур очищення носіїв інформації; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за очищення носіїв інформації; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для очищення носіїв інформації; автоматизовані механізми підтримки та / або впровадження очищення носіїв інформації].	

MP-06(03)	**ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - НЕРУЙНІВНІ МЕТОДИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-06(03)_ODP	визначено умови, які вимагають очищення зовнішніх носіїв інформації;
	MP-06(03)	застосовуються методи неруйнівного очищення до зовнішніх носіїв інформації перед підключенням таких пристроїв до

		системи при **<MP-06(03)_ODP умовах>**, що вимагають очищення зовнішніх носіїв інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються очищення та утилізації носіїв інформації; перелік умов, що вимагають очищення зовнішніх носіїв інформації; записи очищення носіїв інформації; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за очищення носіїв інформації; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для очищення зовнішніх носіїв інформації; автоматизовані механізми підтримки та / або впровадження очищення носіїв інформації].	

MP-06(04)	**ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - КЕРОВАНА НЕСЕКРЕТНА ІНФОРМАЦІЯ**
	[Вилучено: Включено до MP-06].

MP-06(05)	**ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - СЕКРЕТНА ІНФОРМАЦІЯ**
	[Вилучено: Включено до MP-06].

MP-06(06)	**ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ЗНИЩЕННЯ НОСІЇВ ІНФОРМАЦІЇ**
	[Вилучено: Включено до MP-06].

MP-06(07)	**ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ПОДВІЙНА АВТОРИЗАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-06(07)_ODP	**визначено носії інформації для яких необхідно здійснювати подвійну авторизацію для очищення;**
	MP-06(07)	здійснюється подвійна авторизація для очищення **<MP-06(07)_ODP носії інформації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються очищення та утилізації носіїв інформації; перелік носіїв інфор-	

	мації системи, що потребують подвійної авторизації на очищення; записи авторизації; записи очищення носіїв інформації; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за очищення носіїв інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації, що вимагають по подвійної авторизації на очищення носіїв інформації; автоматизовані механізми підтримки та / або впровадження очищення носіїв інформації; автоматизовані механізми, що підтримують та / або реалізують подвійну авторизацію].

MP-06(08)	**ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ВІДДАЛЕНЕ ОЧИЩЕННЯ АБО СТИРАННЯ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-06(08)_ODP[01]	**визначено системи або компоненти системи для очищення або стирання інформації віддалено або за певних умов;**
	MP-06(08)_ODP[02]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {віддалено; за умов <MP-06(08)_ODP[03]>};**
	MP-06(08)_ODP[03]	**визначаються умови, за яких інформація підлягає очищенню або стиранню (якщо вибрано);**
	MP-06(08)	передбачено можливість очищення або стирання інформації з **<MP-06(08) _ODP[01] систем або компонентів системи> <MP-06(08) _ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються очищення та утилізації носіїв інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи очищення носіїв інформації; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за очищення носіїв інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації з очищення / стирання носіїв інформації; автоматизовані механізми, що підтримують та / або реалізують можливості очищення / стирання].	

MP-07	**ВИКОРИСТАННЯ НОСІЇВ ІНФОРМАЦІЇ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-07_ODP[01]	**визначено типи носіїв інформації, які мають бути обмежені або заборонені до використання в системі або компонентах системи;**
	MP-07_ODP[02]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {обмежити; заборонити};**
	MP-07_ODP[03]	**системи або компоненти системи, для яких визначено використання певних типів носіїв інформації, що підлягають обмеженню або забороні;**
	MP-07_ODP[04]	**визначено заходи безпеки для обмеження або заборони використання певних типів носіїв інформації в системах або компонентах системи;**
	MP-07(a)	використання **<MP-07_ODP[01] типів носіїв інформації системи>** є <**MP-07_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРІВ>** на **<MP-07_ODP[03] системах або компонентах системи>** з використанням **<MP-07_ODP[04] заходи безпеки>**;
	MP-07(b)	використання зовнішніх носіїв інформації в системах організації заборонено, якщо такі пристрої не мають власника, якого можна ідентифікувати.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; політика використання системи; процедури, що стосуються обмежень використання носіїв інформації; план захисту інформації; правила поведінки; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за використання носіїв інформації в системі; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для використання носіїв інформації; автоматизовані механізми, що обмежують або забороняють використання носіїв інформації на системах або компонентах системи].	

MP-07(01)	**ВИКОРИСТАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗАБОРОНА ВИКОРИСТАННЯ БЕЗ ВИЗНАЧЕНОГО ВЛАСНИКА**
	[Вилучено: Включено до MP-07]

MP-07(02)	**ВИКОРИСТАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗАБОРОНА ВИКОРИСТАННЯ**

	СТІЙКИХ ДО ОЧИЩЕННЯ НОСІЇВ ІНФОРМАЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-07(02)[01]	ідентифіковано стійкі до очищення носії інформації;
	MP-07(02)[02]	використання стійких до очищення носіїв інформації в системах організації заборонено.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи, політика використання системи; процедури, що стосуються обмежень використання носіїв інформації; правила поведінки; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за використання носіїв інформації в системі; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для використання носіїв інформації; автоматизовані механізми, що забороняють використання носіїв інформації в системах або компонентах системи].	

MP-08	**ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-08_ODP[01]	**визначено процес зниження категорії безпеки носіїв інформації;**
	MP-08_ODP[02]	**визначено носії інформації системи, що вимагають зниження категорії безпеки;**
	MP-08(a)[01]	встановлено **<MP-08_ODP[01] процес зниження категорії безпеки носіїв інформаці>**;
	MP-08(a)[02]	**<MP-08_ODP[01] процес зниження категорії безпеки носіїв інформаці>** охоплює використання механізмів зниження грифа секретності носіїв інформації за стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації;
	MP-08(b)[01]	здійснюється перевірка того, що процес зниження категорії безпеки носіїв інформації відповідає категорії безпеки та/або рівню секретності інформації, що підлягає видаленню;
	MP-08(b)[02]	здійснюється перевірка того, що процес зниження категорії безпеки носіїв інформації співмірний з правами доступу потенційних одержувачів пониженої інформації;

	MP-08(c)	визначено **<MP-08_ODP[02] носії інформації системи, що потребують пониження статусу>**;
	MP-08(d)	визначений носій інформації понижено у категорії безпеки за допомогою **<MP-08_ODP[01] процес зниження категорії безпеки носіїв інформації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються процесу зниження категорії безпеки носіїв інформації; список носіїв інформації, що вимагають зниження категорії безпеки; записи про зниження категорії безпеки носіїв інформації; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за зниження категорії безпеки носіїв інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі]. **Перевірка:** [ВИБІР: Процеси організації для зниження категорії безпеки носіїв інформації; автоматизовані механізми підтримки та / або зниження категорії безпеки носіїв інформації].	

MP-08(01)	**ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - ДОКУМЕНТУВАННЯ ПРОЦЕСУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-08(01)	документуються дії зі зниження категорії безпеки носіїв інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються зниження категорії безпеки носіїв інформації; список носіїв інформації, що вимагають зниження категорії безпеки; записи про зниження категорії безпеки носіїв інформації; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за зниження категорії безпеки носіїв інформації; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для зниження категорії безпеки носіїв інформації; автоматизовані механізми підтримки та / або впровадження зниження категорії безпеки носіїв інформації].	

MP-08(02)	**ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - ПЕРЕВІРКА ОБЛАДНАННЯ**
	МЕТА ОЦІНКИ: Визначити, чи:

	MP-08(02)_ODP[01]	**визначено частоту, з якою потрібно перевіряти обладнання для заниження категорії безпеки ;**
	MP-08(02)_ODP[02]	**визначено частоту, з якою потрібно перевіряти процедури для заниження категорії безпеки ;**
	MP-08(02)[01]	обладнання для заниження категорії безпеки перевіряється **<MP-08(02)_ODP[01] частота>**, щоб переконатися в досягненні запланованих заходів щодо зниження;
	MP-08(02)[02]	процедури для заниження категорії безпеки перевіряється **<MP-08(02)_ODP[02] частота>**, щоб переконатися в досягненні запланованих заходів щодо зниження;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; процедури, що стосуються зниження категорії безпеки носіїв інформації; процедури, що стосуються випробувань обладнання, що знижує категорії безпеки носіїв інформації; результати тестування обладнання та процедур, що знижують категорії безпеки носіїв інформації; записи аудиту: інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за зниження категорії безпеки носіїв інформації; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для зниження категорії безпеки носіїв інформації; автоматизовані механізми підтримки та / або впровадження зниження категорії безпеки носіїв інформації; автоматизовані механізми, що підтримують та / або впроваджують випробування для зниження категорії безпеки носіїв інформації].	

MP-08(03)	**ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - КРИТИЧНА ІНФОРМАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-08(03)[01]	визначено критичну інформацію за наявності якої на носії інформації, знижують категорію безпеки до рівня публічного доступу.
	MP-08(03)[02]	знижується категорія безпеки носіїв інформації, що містять визначену критичну інформацію до рівня публічного доступу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; політика авторизації доступу; процедури, що стосуються зниження категорії безпеки носіїв інформації, що містять критичну інформацію; зниження категорії безпеки носіїв інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за зниження категорії	

	безпеки носіїв інформації; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для зниження категорії безпеки носіїв інформації; автоматизовані механізми підтримки та / або впровадження зниження категорії безпеки носіїв інформації].

MP-08(04)	**ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - ТАЄМНА ІНФОРМАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	MP-08(04)[01]	ідентифіковано носії інформації, що містять інформацію з обмеженим доступом;
	MP-08(04)[02]	носії інформації, що містять інформацію з обмеженим доступом, знижуються в класі перед передачею особам, які не мають необхідних дозволів на доступ.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту носіїв інформації системи; політика авторизації доступу; процедури зниження категорії безпеки носіїв інформації, що містять інформацію з обмеженим доступом; процедури, що стосуються обробки інформації з обмеженим доступом; стандарти та політика щодо захисту інформації з обмеженим доступом; зниження категорії безпеки носіїв інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за зниження категорії безпеки носіїв інформації; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для зниження категорії безпеки носіїв інформації; автоматизовані механізми підтримки та / або впровадження зниження категорії безпеки носіїв інформації].	

XI. КЛАС ЗАХОДІВ ЗАХИСТУ PE - ФІЗИЧНИЙ ЗАХИСТ ТА ЗАХИСТ РОБОЧОГО СЕРЕДОВИЩА

PE-01	**ПОЛІТИКА ТА ПРОЦЕДУРИ ФІЗИЧНОГО ЗАХИСТУ ТА ЗАХИСТУ РОБОЧОГО СЕРЕДОВИЩА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-01_ODP[01]	**визначено персонал або ролі, до яких має бути доведена політика фізичного захисту та захисту робочого середовища;**
	PE-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури фізичного захисту та захисту робочого середовища;**
	PE-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	PE-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами фізичного захисту та захисту робочого середовища;**
	PE-01_ODP[05]	**визначено частоту, з якою переглядається та оновлюється поточна політика фізичного захисту та захисту робочого середовища;**
	PE-01_ODP[06]	**визначено події, які потребують перегляду та оновлення поточної політики фізичного захисту та захисту робочого середовища;**
	PE-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні процедури фізичного захисту та захисту робочого середовища;**
	PE-01_ODP[08]	**визначено події, які потребують перегляду та оновлення процедур фізичного захисту та захисту робочого середовища;**
	PE-01(a)[01]	розроблено та задокументовано політику фізичного захисту та захисту робочого середовища;
	PE-01(a)[02]	політика фізичного захисту та захисту робочого середовища розповсюджується серед **<PE-01_ODP[01] персоналу або ролей>**;
	PE-01(a)[03]	розроблені та задокументовані процедури фізичного захисту та захисту робочого середовища, що сприяють впровадженню політики фізичного захисту та захисту робочого середовища, а також пов'язані з ними заходи захисту;

	PE-01(a)[04]	процедури фізичного захисту та захисту робочого середовища поширюються на **<PE-01_ODP[02] персонал або ролі>**;
	PE-01(a)[01](a)[01]	**<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика фізичного захисту та захисту робочого середовища містить мету;
	PE-01(a)[01](a)[02]	**<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика фізичного захисту та захисту робочого середовища містить сферу застосування;
	PE-01(a)[01](a)[03]	**<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика фізичного захисту та захисту робочого середовища містить ролі;
	PE-01(a)[01](a)[04]	**<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика фізичного захисту та захисту робочого середовища містить обов'язки;
	PE-01(a)[01](a)[05]	**<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика фізичного захисту та захисту робочого середовища містить відповідальність керівництва;
	PE-01(a)[01](a)[06]	**<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика фізичного захисту та захисту робочого середовища містить координацію між підрозділами організації;
	PE-01(a)[01](a)[07]	**<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика фізичного захисту та захисту робочого середовища містить систему контролю відповідності;
	PE-01(a)[01](b)	**<PE-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика фізичного захисту та захисту робочого середовища відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам;
	PE-01(b)	**<PE-01_ODP[04] посадова особа>** призначається для управління розробкою, документуванням та розповсюдженням політики та процедур фізичного захисту та захисту робочого середовища;
	PE-01(c)[01][01]	переглядається та оновлюється поточна політика фізичного захисту та захисту робочого середовища **<PE-01_ODP[05] частота>**;
	PE-01(c)[01][02]	поточна політика фізичного захисту та захисту робочого середовища переглядається та оновлюється після **<PE-01_ODP[06] подій>**;
	PE-01(c)[02][01]	переглядаються та оновлюються поточні процедури фізичного захисту та захисту робочого середовища **<PE-01_ODP[07] частота>**;

	PE-01(c)[02][02]	поточні процедури фізичного та екологічного захисту переглядаються та оновлюються після **<PE-01_ODP[08] подій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури фізичного захисту та захисту робочого середовища; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику фізичного захисту та захисту робочого середовища; персонал, відповідальний за інформаційну безпеку].	

PE-02	**АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-02_ODP	**визначено періодичність перегляду списку доступу, у якому закріплений перелік персоналу або ролей, яким дозволений санкціонований доступ до об'єкта;**
	PE-02(a)[01]	розроблено перелік осіб, які мають право авторизованого доступу до об'єкта, де перебуває система;
	PE-02(a)[02]	затверджено перелік осіб, які мають право авторизованого доступу до об'єкта, де перебуває система;
	PE-02(a)[03]	ведеться перелік осіб, які мають право авторизованого доступу до об'єкта, де перебуває система;
	PE-02(b)	для доступу до об'єкта надаються повноваження;
	PE-02(c)	переглядається список доступу, , у якому закріплений перелік персоналу або ролей, яким дозволений санкціонований доступ до об'єкта **<PE-02_ODP частота>**;
	PE-02(d)	особи видаляються зі списку доступу до об'єкта, коли доступ більше не потрібен.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються дозволів фізичного доступу; план захисту інформації; список доступу уповноваженого персоналу; огляди списків фізичного доступу; записи про припинення фізичного доступу та відповідна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за дозвіл на фізичний доступ; персонал організаціїз фізичним доступом до об'єкта системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для дозволів фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують дозволи фізичного доступу].	

PE-02(01)	АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ - ДОСТУП НА ОСНОВІ ПОСАДИ АБО РОЛІ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-02(01)	фізичний доступ до об'єкта, де перебуває система, авторизується на основі посади або ролі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються дозволів фізичного доступу; журнали або записи фізичного контролю доступу; перелік посад / ролей та відповідних дозволів фізичного доступу; точки входу та виходу системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за дозвіл фізичного доступу; персонал організації з фізичним доступом до системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для дозволів фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують дозволи фізичного доступу].	

PE-02(02)	АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ - ДВІ ФОРМИ ІДЕНТИФІКАЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-02(02)_ODP	визначено список прийнятних форм ідентифікації
	PE-02(02)	вимагається дві форми ідентифікації від **<PE-02(02)_ODP списку прийнятних форм ідентифікації>** для доступу відвідувачів до об'єкта, де знаходиться система.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються дозволів фізичного доступу; перелік прийнятних форм ідентифікації для доступу відвідувачів до об'єкту, де знаходиться система; доступ до форм авторизації; журнали або записи фізичного контролю доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за дозвіл на фізичний доступ; персонал організації з фізичним доступом до об'єкта системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для дозволів фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують дозволи фізичного доступу].	

PE-02(03)	АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ - ОБМЕЖЕННЯ ДОСТУПУ БЕЗ СУПРОВОДУ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-02(03)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень допуску для всієї інформації, що міститься в системі; авторизація офіційного доступу до всієї інформації, що міститься в системі; необхідність доступу до всієї інформації, що міститься в системі; <PE-02(03)_ODP[02] повноваження фізичного доступу>};**
	PE-02(03)_ODP[02]	**визначено повноваження фізичного доступу для доступу без супроводу до об'єкта, де знаходиться система (якщо вибрано);**
	PE-02(03)	доступ без супроводу до приміщення, де знаходиться система, обмежено для персоналу з **<PE-02(03)_ODP[01] ВИБРАНИМ ЗНАЧЕННЯМ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються дозволів фізичного доступу; список доступу уповноваженого персоналу; дозволи на доступ; авторизації доступу; журнали або записи контролю фізичного доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за дозвіл на фізичний доступ; персонал організації з фізичним доступом до об'єкта системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для дозволів фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують дозволи фізичного доступу].	

PE-03	КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-03_ODP[01]	**визначено точки входу та виходу в об'єкт, в якому знаходиться система;**
	PE-03_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<PE-03_ODP[03] системи або пристрої>; охоронці};**
	PE-03_ODP[03]	**визначено фізичні системи або пристрої контролю доступу, що використовуються для контролю входу та виходу на об'єкт (якщо вибрано);**

	PE-03_ODP[04]	**визначено точки входу або виходу, для яких ведуться журнали контролю фізичного доступу;**
	PE-03_ODP[05]	**визначено заходи захисту для контролю доступу в зони всередині об'єкту, позначені як загальнодоступні;**
	PE-03_ODP[06]	**визначено умови, що вимагають супроводу відвідувачів та моніторингу активності відвідувачів;**
	PE-03_ODP[07]	**визначені пристрої фізичного доступу, що підлягають інвентаризації;**
	PE-03_ODP[08]	**визначено частоту проведення інвентаризації пристроїв фізичного доступу;**
	PE-03_ODP[09]	**визначено частоту, з якою потрібно змінювати коди доступу;**
	PE-03_ODP[10]	**визначено частоту, з якою потрібно змінювати ключі;**
	PE-03(a)[01]	авторизація фізичного доступу забезпечується в **<PE-03_ODP[01] пунктах входу і виходу>** шляхом перевірки індивідуальних дозволів доступу;
	PE-03(a)[02]	авторизація фізичного доступу здійснюється у **<PE-03_ODP[01] точках входу та виходу>** шляхом управління входом та виходом на об'єкт за допомогою **<PE-03_ODP[02] ВИБРАНОГО ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**;
	PE-03(b)	журнали контролю фізичного доступу ведуться для **<PE-03_ODP[04] точок входу або виходу>**;
	PE-03(c)	доступ в зони всередині об'єкту, визначені як загальнодоступні, підтримується шляхом впровадження **<PE-03_ODP[05] заходів захисту>**;
	PE-03(d)[01]	відвідувачів супроводжують;
	PE-03(d)[02]	активність відвідувачів контролюється **<PE-03_ODP[06] умови>**;
	PE-03(e)[01]	ключі захищені;
	PE-03(e)[02]	коди доступу захищені;
	PE-03(e)[03]	інші пристрої фізичного доступу захищені;
	PE-03(f)	**<PE-03_ODP[07] пристрої фізичного доступу>** інвентаризуються **<PE-03_ODP[08] частота>**;
	PE-03(g)[01]	коди доступу змінюється **<PE-03_ODP[09] частота>**, коли код скомпрометовано, або коли особи, які володіють кодом, переводяться або звільняються;

	PE-03(g)[02]	ключі змінюються **<PE-03_ODP[10] частота>**, коли ключі втрачено, або коли особи, що володіють ключами, переводяться або звільняються.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; журнали або записи контролю фізичного доступу; пристрої фізичного контролю доступу; дозволи на доступ; авторизації доступу; точки входу та виходу системи; перелік зон в організації, що містять системи або компоненти системи, що потребують додаткового фізичного захисту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за фізичний дозвіл на доступ; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для контролю фізичного доступу до системи / компонентів; автоматизовані механізми, що підтримують та / або впроваджують фізичний контроль доступу до об'єктів, що містять компоненти системи].	

PE-03(01)	**КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ДОСТУП ДО СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-03(01)_ODP	**визначено фізичні приміщення, що містять один або декілька компонентів системи;**
	PE-03(01)[01]	фізичні авторизації доступу до системи є обов'язковими;
	PE-03(01)[02]	для об'єкта застосовуються засоби контролю фізичного доступу в **<PE-03(01)_ODP фізичні приміщення>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; журнали або записи контролю фізичного доступу; пристрої контролю фізичного доступу; дозволи на доступ; авторизації доступу; точки входу та виходу до системи; перелік приміщень в організації, що містять системи або компоненти системи, що потребують додаткового фізичного захисту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за фізичний дозвіл на доступ; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для контролю фізичного доступу до системи / компонентів; автоматизовані механізми, що підтримують та / або впроваджують контроль фізичного доступу до об'єктів, що містять компоненти системи].	

PE-03(02)	**КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - МЕЖІ ОБ'ЄКТУ ТА СИСТЕМИ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-03(02)_ODP	**не визначено частоту проведення перевірок безпеки на фізичній межі об'єкта або системи на предмет витоку інформації або вилучення компонентів системи;**
	PE-03(02)	перевірки безпеки проводяться **<PE-03(02)_ODP частота>** на фізичному периметрі об'єкта або системи на предмет витоку інформації або вилучення компонентів системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; журнали або записи контролю фізичного доступу; записи перевірок безпеки; звіти про аудит безпеки; звіти про перевірку безпеки; документація з планування об'єкта; точки входу та виходу системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за фізичний контроль доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для контролю фізичного доступу до об'єкта та / або системи; автоматизовані механізми, що підтримують та / або впроваджують контроль фізичного доступу до об'єкта або системи; автоматизовані механізми, що підтримують та / або впроваджують перевірки безпеки на предмет несанкціонованого розповсюдження інформації].	

PE-03(03)	**КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - БЕЗПЕРЕРВНА ОХОРОНА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-03(03)_ODP	**визначено фізичні точки доступу до яких необхідно забезпечити цілодобову безперервну охорону для контролю доступу до об'єкта, де знаходиться система;**
	PE-03(03)	забезпечено цілодобову безперервну охорону для контролю доступу **<PE-03(03)_ODP фізичні точки доступу>** до об'єкта, де знаходиться система
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; журнали або записи контролю фізичного доступу; пристрої контролю фізичного доступу; записи спостереження за об'єктами; документація з планування об'єкта; точки входу та виходу системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за контроль фізичного доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для контролю фізичного доступу до	

	об'єкта, де знаходиться система; автоматизовані механізми, що підтримують та / або впроваджують контроль фізичного доступу до об'єкта, де знаходиться система].

PE-03(04)	**КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ШАФИ З БЛОКУВАННЯМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-03(04)_ODP	**визначено компоненти системи для яких необхідно використовувати фізичні шафи посиленого захисту**
	PE-03(04)	використовуються фізичні шафи посиленого захисту для захисту **<PE-03(04)_ODP компонентів системи>** від несанкціонованого фізичного доступу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; план захисту інформації; перелік компонентів системи, що потребують захисту через шафи посиленого захисту; фізичні шафи посиленого захисту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за контроль фізичного доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Шафи посиленого захисту].	

PE-03(05)	**КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ЗАХИСТ ВІД ЗЛОМУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-03(05)_ODP[01]	**визначено заходи захисту від фізичної підробки або підміни;**
	PE-03(05)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {виявлення; запобігання};**
	PE-03(05)_ODP[03]	**визначено апаратні компоненти, які мають бути захищені від фізичної підробки або підміни;**
	PE-03(05)	**<PE-03(05)_ODP[01] заходи захисту >** застосовуються для **<PE-03(05)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** фізичної підробки або підміни **<PE-03(05)_ODP[03] апаратних компонентів>** всередині системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середо-	

	вища; процедури, що стосуються контролю фізичного доступу; перелік гарантій безпеки для виявлення / запобігання фізичним фальсифікаціям чи змінам апаратних компонентів системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за фізичний контроль доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для виявлення / запобігання фізичному втручанню чи зміні апаратних компонентів системи; автоматизовані механізми / гарантії безпеки, що підтримують та / або реалізують виявлення / запобігання фізичному втручанню / чергуванню апаратних компонентів системи].

PE-03(06)	**КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ТЕСТУВАННЯ НА МОЖЛИВІСТЬ ПРОНИКНЕННЯ**
	[Вилучено: включено до CA-08].

PE-03(07)	**КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ФІЗИЧНІ ПЕРЕШКОДИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-03(07)	обмежено доступ за допомогою фізичних перешкод.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; перелік фізичних перешкод для обмеження доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за фізичний контроль доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для виявлення / запобігання фізичному втручанню; автоматизовані механізми / гарантії безпеки, що підтримують та / або реалізують виявлення / запобігання фізичному втручанню до компонентів системи].	

PE-03(08)	**КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - КОНТРОЛЬ ДОСТУПУ У ВЕСТИБЮЛІ (ХОЛІ)**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-03(08)_ODP	**визначено місця на об'єкті, де необхідний контроль доступу;**
	PE-03(08)	контроль доступу використовуються в <**PE-03(08)_ODP місцях**>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; перелік фізичних перешкод для обмеження доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за фізичний контроль доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для виявлення / запобігання фізичному втручанню; автоматизовані механізми / гарантії безпеки, що підтримують та / або реалізують виявлення / запобігання фізичному втручанню до компонентів системи].

PE-04	**КОНТРОЛЬ ДОСТУПУ ДО ДЖЕРЕЛ ТА ЛІНІЙ ЕЛЕКТРОЖИВЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-04_ODP[01]	**визначені системи розподілу та постачання живлення, які потребують фізичного контролю доступу;**
	PE-04_ODP[02]	**визначено заходи захисту, які необхідно впровадити для контролю фізичного доступу до систем розподілу та постачання живлення в межах об'єкту організації;**
	PE-04	фізичний доступ до **<PE-04_ODP[01] систем розподілу та постачання живлення>** в межах об'єктів організації контролюється за допомогою **<PE-04_ODP[02] заходів захисту>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю доступу до середовища передачі; проєктна документація системи; комунікаційні та електричні схеми об'єкта; перелік засобів фізичної безпеки, що застосовуються до ліній розподілу та передачі системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за контроль фізичного доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для контролю доступу до ліній розподілу та передачі; автоматизовані механізми / гарантії безпеки, що підтримують та / або впроваджують контроль доступу до ліній розподілу та передачі].	

PE-05	**КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-05_ODP	**визначено пристрої для виведення інформації над якими необхідний контроль над фізичним доступом до вихідних даних;**

	PE-05	керування фізичним доступом до вихідних даних здійснюється з **<PE-05_ODP пристроїв для виведення інформації>**, для запобігання несанкціонованого отримання користувачами вихідних даних.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю доступу до системи виведення; фактичні показники від компонентів системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за контроль фізичного доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для контролю доступу до пристроїв виведення; автоматизовані механізми, що підтримують та / або впроваджують контроль доступу до вихідних пристроїв].	

PE-05(01)	**КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ - ДОСТУП ДО ВИХІДНИХ ДАНИХ УПОВНОВАЖЕНИМИ ОСОБАМИ**
	[Вилучено: включено до PE-05].

PE-05(02)	**КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ - ДОСТУП ДО ВИХІДНИХ ДАНИХ ФІЗИЧНИМИ ОСОБАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-05(02)	пов'язуються дані про цифрову ідентичність з підтвердженням отримання даних від вихідних пристроїв
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю фізичного доступу; проєктна документація системи; налаштування конфігурації системи та супутня документація; перелік пристроїв виведення та супутніх виходів, що вимагають контролю фізичного доступу; журнали або записи контролю фізичного доступу для зон, що містять пристрої виведення та відповідні виходи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за контроль фізичного доступу; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи / мережі; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для контролю доступу до вихідних пристроїв; автоматизовані механізми, що підтримують та / або впроваджують контроль доступу до вихідних пристроїв].	

PE-05(03)	**КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ - МАРКУВАННЯ ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ**

	[Вилучено: включено до PE-22].

PE-06	**МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-06_ODP[01]	**визначено частоту перегляду журналів фізичного доступу;**
	PE-06_ODP[02]	**визначено події або потенційні ознаки подій, що вимагають перегляду журналів фізичного доступу;**
	PE-06(a)	фізичний доступ до об'єкту, де знаходиться система, моніториться з метою виявлення та реагування на інциденти фізичної безпеки;
	PE-06(b)[01]	переглядаються журнали фізичного доступу **<PE-06_ODP[01] частота>;**
	PE-06(b)[02]	журнали фізичного доступу переглядаються при виникненні **<PE-06_ODP[02] подій>;**
	PE-06(c)[01]	результати переглядів узгоджуються з можливостями організації щодо реагування на інциденти;
	PE-06(c)[02]	результати розслідувань узгоджуються з можливостями організації щодо реагування на інциденти;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу фізичного доступу; план захисту інформації; журнали або записи фізичного доступу; записи моніторингу фізичного доступу; огляди журналу фізичного доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за контроль фізичного доступу; персонал організації, відповідальний за реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації для моніторингу фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують моніторинг фізичного доступу; автоматизовані механізми, що підтримують та / або здійснюють перегляд журналів фізичного доступу].	

PE-06(01)	**МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - ОХОРОННА СИГНАЛІЗАЦІЯ ТА ОБЛАДНАННЯ ДЛЯ СПОСТЕРЕЖЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-06(01)[01]	фізичний доступ до об'єкта, де розміщена система, моніториться за допомогою сигналізації;

	PE-06(01)[02]	фізичний доступ до об'єкта, де розміщена система, моніториться за допомогою обладнання для спостереження;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу фізичного доступу; план захисту інформації; журнали або записи фізичного доступу; записи моніторингу фізичного доступу; огляди журналу фізичного доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за контроль фізичного доступу; персонал організації, відповідальний за реагування на інциденти; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу фізичних сигналізацій про вторгнення та обладнання спостереження; автоматизовані механізми, що підтримують та / або впроваджують фізичний моніторинг доступу; автоматизовані механізми, що підтримують та / або впроваджують сигналізацію про фізичне вторгнення та обладнання спостереження].	

PE-06(02)	**МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - АВТОМАТИЧНЕ РОЗПІЗНАВАННЯ ВТОРГНЕНЬ ТА ВІДПОВІДНА РЕАКЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-06(02)_ODP[01]	**визначено класи або типи вторгнень, які мають розпізнаватися автоматизованими механізмами;**
	PE-06(02)_ODP[02]	**визначено реакції, які мають ініціюватися автоматизованими механізмами при розпізнаванні визначених організацією класів або типів вторгнень;**
	PE-06(02)_ODP[03]	**визначено автоматизовані механізми, що використовуються для розпізнавання класів або типів вторгнень та ініціювання дій реагування (визначені в PE-06(02)_ODP);**
	PE-06(02)[01]	розпізнаються **<PE-06(02)_ODP[01] класи або типи вторгнень>**;
	PE-06(02)[02]	**<PE-06(02)_ODP[02] реакції>** ініціюються за допомогою **<PE-06(02)_ODP[03] автоматизованих механізмів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу фізичного доступу; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; список дій відповіді, які слід розпочати, коли розпізнаються конкретні класи / типи вторгнень; інші відповідні документи або за-	

	писи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за контроль фізичного доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують моніторинг фізичного доступу; автоматизовані механізми, що підтримують та / або реалізують розпізнавання класів / типів вторгнень та ініціювання відповіді].

PE-06(03)	**МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - ВІДЕОСПОСТЕРЕЖЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-06(03)_ODP[01]	**визначено зони, де буде застосовуватися відеоспостереження;**
	PE-06(03)_ODP[02]	**визначено частоту перегляду відеозаписів;**
	PE-06(03)_ODP[03]	**визначено період часу, протягом якого необхідно зберігати відеозаписи;**
	PE-06(03)(a)	ведеться відеоспостереження за **<PE-06(03)_ODP[01] зонами>**;
	PE-06(03)(b)	відеозаписи переглядаються **<PE-06(03)_ODP[02] частота>**;
	PE-06(03)(c)	відеозаписи зберігаються протягом **<PE-06(03)_ODP[03] періоду часу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу фізичного доступу; обладнання відеоспостереження, що використовується для спостереження за робочими зонами; відеозаписи зон, де застосовується відеоспостереження; журнали або записи обладнання відеоспостереження; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за контроль фізичного доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу фізичного доступу; автоматизовані механізми, що підтримують та / або впроваджують моніторинг фізичного доступу; автоматизовані механізми підтримки та / або впровадження відеоспостереження].	

PE-06(04)	**МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ ДО СИСТЕМИ**
	МЕТА ОЦІНКИ: Визначити, чи:

	PE-06(04)_ODP	**визначено фізичні приміщення, що містять один або більше компонентів системи;**
	PE-06(04)	моніторинг фізичного доступу до системи здійснюється на додаток до моніторингу фізичного доступу до об'єкта в **<PE-06(04)_ODP фізичні приміщення>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу фізичного доступу; журнали або записи фізичного контролю доступу; пристрої фізичного контролю доступу; дозволи на доступ; авторизації доступу; перелік приміщень на об'єкті, що містять системи або компоненти системи, що вимагають додаткового моніторингу фізичного доступу; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за контроль фізичного доступу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу фізичного доступу до системи; автоматизовані механізми, що підтримують та / або впроваджують моніторинг фізичного доступу до областей, що містять компоненти системи].	

PE-07	**КОНТРОЛЬ ВІДВІДУВАЧІВ**
	[Вилучено: Включено до PE-02 і PE-03].

PE-08	**РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-08_ODP[01]	**визначено період часу, протягом якого зберігатимуться записи про доступ відвідувачів до об'єкта, на якому перебуває система;**
	PE-08_ODP[02]	**визначено частоту перегляду записів про доступ відвідувачів;**
	PE-08_ODP[03]	**визначено персонал, якому повідомляється про порушення записів про доступ відвідувачів;**
	PE-08(a)	записи про доступ відвідувачів для об'єкта, на якому знаходиться система, зберігаються протягом **<PE-08_ODP[01] період часу>**;
	PE-08(b)	переглядаються записи про доступ відвідувачів **<PE-08_ODP[02] частота>**;
	PE-08(c)	про порушення записів про доступ відвідувачів повідомляється **<PE-08_ODP[03] персоналу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються записів про доступ відвідувачів; план захисту інформації; журнали або записи контролю доступу відвідувачів; огляд доступу відвідувачів або огляди журналів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за записи відвідувачів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для ведення та перегляду записів про доступ відвідувачів; автоматизовані механізми, що підтримують та / або впроваджують обслуговування та перегляд записів доступу відвідувачів].

PE-08(01)	**РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ - АВТОМАТИЗОВАНЕ ВЕДЕННЯ ТА ПЕРЕГЛЯД РЕЄСТРУ ВІДВІДУВАЧІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-08(01)_ODP[01]	**визначено автоматизовані механізми, що використовуються для ведення реєстру доступу відвідувачів;**
	PE-08(01)_ODP[02]	**визначено автоматизовані механізми перегляду реєстру доступу відвідувачів;**
	PE-08(01)[01]	реєстр доступу відвідувачів ведеться за допомогою **<PE-08(01)_ODP[01] автоматизованих механізмів>**;
	PE-08(01)[02]	реєстр доступу відвідувачів переглядається за допомогою **<PE-08(01)_ODP[02] автоматизованих механізмів>**;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються записів про доступ відвідувачів; автоматизовані механізми, що підтримують управління записами доступу відвідувачів; журнали або записи контролю доступу відвідувачів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за ведення запису відвідувачів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації для ведення та перегляду записів про доступ відвідувачів; автоматизовані механізми, що підтримують та / або впроваджують обслуговування та перегляд записів доступу відвідувачів].	

PE-08(02)	**РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ - РЕЄСТР ФІЗИЧНОГО ДОСТУПУ**
	[Вилучено: включено до PE-02].

PE-08(03)	**РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ - ОБМЕЖЕННЯ ІНФОРМАЦІЇ, ЩО ІДЕНТИФІКУЮТЬ ОСОБУ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-08(03)_ODP	**в оцінці ризиків для конфіденційності визначено елементи, що обмежуються в реєстрі відвідувачів**
	PE-08(03)	інформація, що ідентифікує особу, яка міститься в реєстрах доступу відвідувачів, обмежується <**PE-08(03)_ODP елементи**>, визначеними в оцінці ризиків для конфіденційності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються записів про доступ відвідувачів; автоматизовані механізми, що підтримують управління записами доступу відвідувачів; журнали або записи контролю доступу відвідувачів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за ведення запису відвідувачів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації для ведення та перегляду записів про доступ відвідувачів; автоматизовані механізми, що підтримують та / або впроваджують обслуговування та перегляд записів доступу відвідувачів].	

PE-09	**ЕНЕРГЕТИЧНЕ ОБЛАДНАННЯ ТА КАБЕЛІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-09[01]	енергетичне обладнання системи захищене від пошкоджень і руйнувань;
	PE-09[02]	силові кабелі системи захищене від пошкоджень і руйнувань;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються захисту енергетичного обладнання / кабелів; об'єкти, в яких розміщується енергетичне обладнання / кабелі; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захист енергетичного обладнання / кабелів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують захист енергетичного обладнання / кабелів].	

PE-09(01)	**ЕНЕРГЕТИЧНЕ ОБЛАДНАННЯ ТА КАБЕЛІ - РЕЗЕРВНІ КАБЕЛІ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-09(01)_ODP	визначено відстань, на яку повинні бути відокремлені резервні силові кабельні системи;
	PE-09(01)	використовувати резервні силові кабельні системи, які фізично відокремлені на **<PE-09(01)_ODP відстань>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження: [**ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються захисту енергетичного обладнання / кабелів; об'єкти, в яких розміщується енергетичне обладнання / кабелі; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захист енергетичного обладнання / кабелів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують захист енергетичного обладнання / кабелів].	

PE-09(02)	**ЕНЕРГЕТИЧНЕ ОБЛАДНАННЯ ТА КАБЕЛІ - АВТОМАТИЧНЕ КЕРУВАННЯ НАПРУГОЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-09(02)_ODP	визначено критичні компоненти системи для яких необхідно впровадити механізми автоматичного керування напругою;
	PE-09(02)	впроваджено механізми автоматичного керування напругою для **<PE-09(02)_ODP критичних компонентів системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю напруги; план безпеки; перелік важливих компонентів інформаційної системи, що вимагають автоматичного регулювання напруги; автоматичні механізми регулювання напруги та відповідні конфігурації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захисту робочого середовища компонентів системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують автоматичне регулювання напруги].	

PE-10	**АВАРІЙНЕ ВІДКЛЮЧЕННЯ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-10_ODP[01]	**визначено систему або окремі компоненти системи, які потребують можливості вимкнення живлення в надзвичайних ситуаціях;**
	PE-10_ODP[02]	**визначено розташування перемикачів або пристроїв аварійного вимкнення в системі або компоненті системи;**
	PE-10(a)	передбачена можливість відключення живлення **<PE-10_ODP[01] системи або окремих компонентів системи>** в надзвичайних ситуаціях;
	PE-10(b)	аварійні перемикачі або пристрої вимкнення розміщені в <PE-10_ODP[02] розташування>, щоб забезпечити доступ для персоналу;
	PE-10(c)	можливість аварійного вимкнення живлення захищена від несанкціонованої активації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються аварійного відключення джерела живлення; план захисту інформації; аварійне відключення вимикачів та пристроїв; місця розміщення аварійних вимикачів та пристроїв; запобіжні заходи, що захищають можливість аварійного відключення живлення від несанкціонованої активації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аварійне відключення живлення (як впровадження, так і можливості використання); персонал організації, який відповідає за інформаційну безпеку]. **Перевірка: [**ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують аварійне відключення живлення].	

PE-10(01)	**АВАРІЙНЕ ВІДКЛЮЧЕННЯ - ВИПАДКОВА І НЕСАНКЦІОНОВАНА АКТИВАЦІЯ**
	[Виключено: включено до PE-10].

PE-11	**АВАРІЙНЕ ЕНЕРГОЗАБЕЗПЕЧЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-11_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {впорядковане виключення системи; перехід системи на довгострокову альтернативну систему живлення};):**

	PE-11	передбачено джерело безперебійного живлення для полегшення **<PE-11_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** у випадку втрати основного джерела живлення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури вирішення надзвичайних ситуацій; джерело безперебійного живлення; документація на джерело безперебійного живлення; записи випробувань джерела безперебійного живлення; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аварійне живлення; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують джерело безперебійного живлення; джерело безперебійного живлення].	

PE-11(01)	**АВАРІЙНЕ ЕНЕРГОЗАБЕЗПЕЧЕННЯ - ДОВГОСТРОКОВЕ АЛЬТЕРНАТИВНЕ ДЖЕРЕЛО ЖИВЛЕННЯ - МІНІМАЛЬНІ ЕКСПЛУАТАЦІЙНІ МОЖЛИВОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-11(01)_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {вручну; автоматично};**
	PE-11(01)[01]	активується альтернативне джерело живлення, передбачене для системи **<PE-11(01)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**;
	PE-11(01)[02]	альтернативне джерело живлення, передбачене для системи, може підтримувати мінімально необхідну працездатність у разі тривалої втрати основного джерела живлення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури вирішення надзвичайних ситуацій; аварійне джерело живлення; документація про альтернативне джерело живлення; записи про випробування джерел живлення; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аварійне живлення; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують альтернативне джерело живлення; альтернативне джерело живлення].	

PE-11(02)	**АВАРІЙНЕ ЕНЕРГОЗАБЕЗПЕЧЕННЯ - ДОВГОСТРОКОВЕ АЛЬТЕРНАТИВНЕ ДЖЕРЕЛО ЖИВЛЕННЯ – АВТОНОМНЕ ЖИВЛЕННЯ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	PE-11(02)_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {вручну; автоматично};**
	PE-11(02)_ODP[02]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {мінімально необхідні операційні можливості; повна експлуатаційна здатність};**
	PE-11(02)	активується альтернативне джерело живлення, передбачене для системи **<PE-11(02)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**;
	PE-11(a)	альтернативне джерело живлення, передбачене для системи, є автономним;
	PE-11(b)	альтернативне джерело живлення, передбачене для системи, не залежить від зовнішнього постачання енергії;
	PE-11(c)	альтернативне джерело живлення, передбачене для системи, здатне підтримувати **<PE-11(02)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** у разі тривалої втрати основного джерела живлення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури вирішення надзвичайних ситуацій; змінне джерело живлення; документація про альтернативне джерело живлення; записи про випробування джерел живлення; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аварійне живлення; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують альтернативне джерело живлення; альтернативне джерело живлення].	

PE-12	**АВАРІЙНЕ ОСВІТЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-12[01]	автоматичне аварійне освітлення, яке вмикається в разі відключення або збою в електропостачанні;
	PE-12[02]	підтримується автоматичне аварійне освітлення, яке вмикається в разі відключення або збою в електропостачанні;
	PE-12[03]	автоматичне аварійне освітлення системи освітлює евакуаційні виходи в межах об'єкта;
	PE-12[04]	автоматичне аварійне освітлення системи освітлює шляхи евакуації в

		межах об'єкта;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються аварійного освітлення; документація на аварійне освітлення; протоколи випробувань аварійного освітлення; аварійні виходи та шляхи евакуації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аварійне освітлення; gерсонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість аварійного освітлення].	

PE-12(01)	**АВАРІЙНЕ ОСВІТЛЕННЯ - ОСНОВНІ ЗАВДАННЯ ТА ФУНКЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-12(01)	аварійне освітлення передбачено для всіх зон , що підтримують виконання основних завдань і функцій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються аварійного освітлення; документація на аварійне освітлення; протоколи випробувань аварійного освітлення; аварійні виходи та шляхи евакуації; зони в межах організації, що підтримують основні завдання і функції;інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за аварійне освітлення; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість аварійного освітлення].	

PE-13	**ПРОТИПОЖЕЖНИЙ ЗАХИСТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-13[01]	застосовуються системи пожежної сигналізації;
	PE-13[02]	системи пожежної сигналізації підтримуються незалежним джерелом енергії;
	PE-13[03]	підтримуються в робочому стані системи пожежної сигналізації;
	PE-13[04]	застосовуються системи пожежогасіння;
	PE-13[05]	системи пожежогасіння підтримуються незалежним джерелом енергії;

	PE-13[06]	підтримуються в робочому стані системи пожежогасіння.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються протипожежного захисту; прилади / системи пожежогасіння та виявлення пожежі; пристрої / системи гасіння та виявлення пожежі; протоколи випробувань приладів / систем гасіння та виявлення пожежі; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за прилади / системи виявлення та гасіння пожежі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують пристрої / системи пожежогасіння / виявлення].	

PE-13(01)	**ПРОТИПОЖЕЖНИЙ ЗАХИСТ - ПРИСТРОЇ ТА СИСТЕМИ ВИЯВЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-13(01)_ODP[01]	**визначено персонал або ролі, які мають бути повідомлені у випадку пожежі;**
	PE-13(01)_ODP[02]	**визначено аварійні команди, які мають бути сповіщені у випадку пожежі;**
	PE-13(01)[01]	використовуються системи пожежної сигналізації, які автоматично спрацьовують у разі пожежі;
	PE-13(01)[02]	використовуються системи виявлення пожежі, які автоматично сповіщають **<PE-13(01)_ODP[01] персонал або ролі>** у разі виникнення пожежі;
	PE-13(01)[03]	використовуються системи виявлення пожежі, які автоматично сповіщають **<PE-13(01)_ODP[02] аварійні команди>** у разі виникнення пожежі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються протипожежного захисту; угоди про рівень сигналізації; протоколи випробувань приладів / систем гасіння та виявлення пожежі; пристрої / системи документації щодо придушення та виявлення пожежі; оповіщення / повідомлення про пожежні події; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за прилади / системи виявлення та гасіння пожежі; персонал організації, відповідальний за повідомлення відповідного персоналу, ролей та аварійну команду; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують пристрої / системи виявлення пожежі; активація пристроїв / систем вияв-	

	лення пожежі (змодельовані); автоматизовані повідомлення].

PE-13(02)	**ПРОТИПОЖЕЖНИЙ ЗАХИСТ - ПРИСТРОЇ ТА СИСТЕМИ АВТОМАТИЧНОГО ПОЖЕЖОГАСІННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-13(02)_ODP[01]	**визначено персонал або ролі, які мають бути сповіщені у випадку пожежі;**
	PE-13(02)_ODP[02]	**визначені аварійні команди, які повинні бути сповіщені в разі пожежі;**
	PE-13(02)(a)[01]	застосовуються системи пожежогасіння, які активуються автоматично;
	PE-13(02)(a)[02]	використовуються системи пожежогасіння, які автоматично сповіщають **<PE-13(02)_ODP[01] персонал або ролі>**;
	PE-13(02)(a)[03]	використовуються системи пожежогасіння, які автоматично сповіщають **<PE-13(02)_ODP[02] аварійні команди>**;
	PE-13(02)(b)	використовується автоматична система пожежогасіння, коли об’єкт не укомплектований відповідним персоналом на постійній основі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються протипожежного захисту; пристрої / системи документації щодо придушення та виявлення пожежі; угоди про рівень сигналізації; протоколи випробувань приладів / систем гасіння та виявлення пожежі; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за прилади / системи виявлення та гасіння пожежі; персонал організації, відповідальний за автоматичне сповіщення про будь-яке спрацьовування приладів / систем протипожежного захисту для відповідного персоналу, ролей та аварійних служб; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка**: [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують пристрої / системи пожежогасіння; активація приладів / систем пожежогасіння (змодельовані); автоматизовані повідомлення].	

PE-13(03)	**ПРОТИПОЖЕЖНИЙ ЗАХИСТ - АВТОМАТИЧНЕ ПОЖЕЖОГАСІННЯ**
	[Виключено: включено до PE-13(02)].

PE-13(04)	ПРОТИПОЖЕЖНИЙ ЗАХИСТ - ПЕРЕВІРКИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-13(04)_ODP[01]	**визначено частоту проведення перевірок пожежної безпеки на об'єкті;**
	PE-13(04)_ODP[02]	**визначено термін для усунення недоліків, виявлених перевірками пожежного нагляду;**
	PE-13(04)[01]	об'єкт проходить перевірки пожежної безпеки **<PE-13(04)_ODP[01] частота>** уповноваженими та кваліфікованими інспекторами;
	PE-13(04)[02]	виявлені недоліки за результатами перевірок пожежної безпеки усуваються у **<PE-13(04)_ODP[02] термін>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються протипожежної безпеки; план захисту інформації; плани інспекції; результати перевірки; протоколи випробувань приладів / систем гасіння та виявлення пожежі; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування, затвердження та виконання пожежних інспекцій; персонал організації, який відповідає за інформаційну безпеку].	

PE-14	КОНТРОЛЬ ТЕМПЕРАТУРИ ТА ВОЛОГОСТІ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-14_ODP[01]	**визначено прийнятні рівні для температури та вологості;**
	PE-14_ODP[02]	**визначено частоту моніторингу рівнів температури та вологості;**
	PE-14(a)	температура та вологість підтримуються на **<PE-14_ODP[01] рівні>** у приміщенні, де знаходиться система;
	PE-14(b)	контролюються рівні температури та вологості **<PE-14_ODP[02] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю температури та вологості; план захисту інформації; регулювання температури та вологості; приміщення, в якому розміщена система; документація щодо контролю температури та вологості; записи температури та вологості; інші відповідні документи або записи].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за захист робочого середовища; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують технічне обслуговування та моніторинг рівня температури та вологості].

PE-14(01)	**КОНТРОЛЬ ТЕМПЕРАТУРИ ТА ВОЛОГОСТІ - АВТОМАТИЧНИЙ КОНТРОЛЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-14(01)_ODP	**визначено механізми автоматичного регулювання температури та вологості;**
	PE-14(01)	впроваджено **<PE-14(01)_ODP механізми>** на об’єкті для запобігання потенційно шкідливим для системи коливанням.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються контролю температури та вологості; приміщення, в якому розміщена система; автоматизовані механізми для температури та вологості; регулювання температури та вологості; документація щодо температури та вологості; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за контроль за робочим середовищем системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують рівні температури та вологості].	

PE-14(02)	**КОНТРОЛЬ ТЕМПЕРАТУРИ ТА ВОЛОГОСТІ - МОНІТОРИНГ ЗА ДОПОМОГОЮ СИГНАЛІЗАЦІЙ ТА СПОВІЩЕНЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-14(02)_ODP	**визначено персонал або ролі, які необхідно повідомляти в рамках моніторингу температури та вологості , коли зміни температури та вологості є потенційно шкідливими для персоналу або обладнання;**
	PE-14(02)[01]	застосовується моніторинг температури та вологості;
	PE-14(02)[02]	функція моніторингу температури та вологості надає сигнал тривоги або повідомлення **<PE-14(02)_ODP персоналу або ролям>**, коли зміни є потенційно шкідливими для персоналу або обладнання.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу температури та вологості; приміщення, в якому розміщена система; журнали або записи контролю за температурою та вологістю; записи змін температури та рівня вологості, які генерують сигнали тривоги або сповіщення; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за контроль робочого середовища системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або впроваджують моніторинг температури та вологості].

PE-15	**ЗАХИСТ ВІД ПОШКОДЖЕННЯ ВОДОЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-15[01]	система захищена від пошкоджень внаслідок витоку води за допомогою запобіжних клапанів;
	PE-15[02]	головні запобіжні клапани є доступним;
	PE-15[03]	головні запобіжні клапани працюють належним чином;
	PE-15[04]	головні запобіжні клапан відомі персоналу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються захисту від водної шкоди; приміщення, в якому розміщена система; головні запобіжні клапани; список ключового персоналу, що знає місце розташування та процедури активації головних запобіжних клапанів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за контроль робочого середовища системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Основні водозапірні клапани; процес активації води].	

PE-15(01)	**ЗАХИСТ ВІД ПОШКОДЖЕННЯ ВОДОЮ - АВТОМАТИЧНА ПІДТРИМКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-15(01)_ODP[01]	**визначено персонал або ролі, які слід сповіщати, коли біля системи виявлено присутність води;**
	PE-	**визначено автоматизовані механізми, що використовують-**

	15(01)_ODP[02]	**ся для виявлення присутності води поблизу системи;**
	PE-15(01)[01]	наявність води поблизу системи можна виявити автоматично;
	PE-15(01)[02]	**<PE-15(01)_ODP[01] персонал або ролі>** оповіщаються за допомогою **<PE-15(01)_ODP[02] автоматизованих механізмів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються захисту від водної шкоди; приміщення, в якому розміщена система; автоматизовані механізми для запобіжних клапанів; автоматизовані механізми, що визначають наявність води поблизу системи; попередження / повідомлення про виявлення води в приміщенні системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за контроль робочого середовища системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують можливість виявлення води та попередження для системи].	

PE-16	**ДОСТАВКА ТА ВИДАЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-16_ODP[01]	**визначено типи компонентів системи, які підлягають авторизації та контролю при вході на об'єкт;**
	PE-16_ODP[02]	**визначено типи компонентів системи, які підлягають авторизації та контролю при виході з об'єкта;**
	PE-16(a)[01]	**<PE-16_ODP[01] типи компонентів системи>** авторизуються при вході на об'єкт;
	PE-16(a)[02]	**<PE-16_ODP[01] типи компонентів системи>** контролюються при вході на об'єкт;
	PE-16(a)[03]	**<PE-16_ODP[02] типи компонентів системи>** авторизуються при виході з об'єкта;
	PE-16(a)[04]	**<PE-16_ODP[02] типи компонентів системи>** контролюються при виході з об'єкта;
	PE-16(b)	ведеться облік компонентів системи, зазначених вище
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються доставки та вивезення компонентів системи з об'єкта;	

	план захисту інформації; приміщення, в якому розміщена система; записи компонентів, що входять і виходять з об'єкта; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за контроль за компонентами системи, що входять і виходять з об'єкту; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процес авторизації, моніторингу та контролю елементів, пов'язаних з системою, що входять і виходять із об'єкта; автоматизовані механізми, що підтримують та / або впроваджують авторизацію, моніторинг та контроль елементів, пов'язаних з системою, що входять і виходять з об'єкта].

PE-17	**АЛЬТЕРНАТИВНЕ РОБОЧЕ МІСЦЕ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-17_ODP[01]	**визначені альтернативні робочі місця, дозволені для використання працівниками;**
	PE-17_ODP[02]	**визначаються заходи захисту, які будуть застосовуватися на альтернативних робочих місцях;**
	PE-17(a)	**<PE-17_ODP[01] альтернативні робочі місця>** визначені та задокументовані;
	PE-17(b)	**<PE-17_ODP[02] заходи захисту>** впроваджені на альтернативних робочих місцях;
	PE-17(c)	оцінюється ефективність заходів захисту на альтернативних робочих місцях;
	PE-17(d)	працівникам надаються засоби комунікації з персоналом служби інформаційної безпеки на випадок інцидентів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються альтернативних місць роботи персоналу організації; план захисту інформації; перелік заходів захисту, необхідних для альтернативних робочих місць; оцінки заходів захисту на альтернативних робочих місцях; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, що схвалює використання альтернативних робочих місць; персонал організації, що використовує альтернативні робочі місця; персонал організації, що оцінює заходи захисту на альтернативних робочих місцях; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси для безпеки на альтернативних робочих місцях; автоматизовані механізми, що підтримують альтернативні робочі місця; заходи захисту, що застосовуються на альтернативних робочих місцях; засоби зв'язку між персоналом на місцях альтернативних робіт та персоналом охорони].	

PE-18	РОЗТАШУВАННЯ КОМПОНЕНТІВ СИСТЕМИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-18_ODP	**визначено фізичні та екологічні небезпеки, які можуть призвести до потенційного пошкодження компонентів системи на об'єкті;**
	PE-18	компоненти системи розміщені в межах об'єкта так, щоб мінімізувати потенційну шкоду від **<PE-18_ODP фізичні та екологічні небезпеки>** і звести до мінімуму можливість несанкціонованого доступу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються позиціювання компонентів системи; документація, що встановлює розташування компонентів системи всередині об'єкта; розташування компонентів системи в межах об'єкта; перелік фізичних та екологічних небезпек, що можуть призвести до пошкодження компонентів системи всередині об'єкта; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за розміщення компонентів системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси для позиціювання компонентів системи].	

PE-18(01)	РОЗТАШУВАННЯ КОМПОНЕНТІВ СИСТЕМИ - МІСЦЕ РОЗМІЩЕННЯ ОБ'ЄКТА
	[Виключено: включено до PE-23].

PE-19	ВИТІК ІНФОРМАЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-19	забезпечено захист від витоку інформації шляхом випромінювання електромагнітних сигналів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються витоку інформації внаслідок випромінювання електромагнітних сигналів; механізми захисту системи від електронного випромінювання сигналів; приміщення, в якому розміщена система; записи тестів на випромінювання електромагнітних сигналів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захист робочого середовища системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та / або реалізують захист від витоку інформації внаслідок випромінювання електромагнітних сигналів].	

PE-19(01)	ВИТІК ІНФОРМАЦІЇ - НАЦІОНАЛЬНІ ПОЛІТИКИ ТА ПРОЦЕДУРИ ЩОДО ПЕМВ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-19(01)[01]	компоненти системи захищені відповідно до національних політик і процедур захисту від ПЕМВ на основі категорії безпеки або класифікації інформації;
	PE-19(01)[02]	передача даних захищається відповідно до національних політик і процедур захисту від ПЕМВ на основі категорії безпеки або класифікації інформації;
	PE-19(01)[03]	мережі захищені відповідно до національних політик і процедур захисту від ПЕМВ на основі категорії безпеки або класифікації інформації;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються витоку інформації, що відповідає національним політикам і процедурам захисту від побічного електромагнітного випромінювання; проєктна документація на компоненти системи; налаштування конфігурації системи та супутня документація, інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захист робочого середовища системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Компоненти системи, що відповідають національним політикам і процедурам захисту від побічного електромагнітного випромінювання].	

PE-20	МОНІТОРИНГ ТА ВІДСТЕЖЕННЯ АКТИВІВ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-20_ODP[01]	**визначено технології, які будуть використовуватися для відстеження та моніторингу місцезнаходження та переміщення активів;**
	PE-20_ODP[02]	**визначено активи, місцезнаходження та переміщення яких необхідно відстежувати та моніторити;**
	PE-20_ODP[03]	**визначено контрольовані зони, в межах яких місцезнаходження та переміщення активів підлягають відстеженню та моніторингу;**
	PE-20	**<PE-20_ODP[01] технології>** використовуються для відстеження та моніторингу місцезнаходження і переміщення **<PE-**

		20_ODP[02] активів> в межах **<PE-20_ODP[03] контрольованої зони>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються моніторингу та відстеження активів; технології розміщення активів та пов'язана з ними конфігураційна документація; перелік активів, що вимагають відстеження та моніторингу; записи про моніторинг та відстеження активів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за моніторинг та відстеження активів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси для відстеження та моніторингу активів; автоматизовані механізми підтримки та / або реалізації відстеження та моніторингу активів].	

PE-21	**ЗАХИСТ ВІД ЕЛЕКТРОМАГНІТНОГО ІМПУЛЬСУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-21_ODP[01]	**визначено заходи захисту від пошкодження електромагнітними імпульсами;**
	PE-21_ODP[02]	**визначено систему та компоненти системи, що потребують захисту від пошкодження електромагнітними імпульсами;**
	PE-21	**<PE-21_ODP[01] заходи захисту>** застосовуються проти пошкодження електромагнітними імпульсами для **<PE-21_ODP[02] системи та компонентів системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються захисту від пошкодження електромагнітним імпульсом; заходи захисту проти пошкодження електромагнітним імпульсом та пов'язана з ними конфігураційна документація; перелік систем, яким необхідний захист від пошкодження електромагнітним імпульсом; записи про проведені заходи захисту проти пошкодження електромагнітним імпульсом; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за захист від пошкодження електромагнітним імпульсом; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси для захисту від пошкодження електромагнітним імпульсом; автоматизовані механізми підтримки та / або реалізації захисту від пошкодження електромагнітним імпульсом].	

PE-22	**МАРКУВАННЯ КОМПОНЕНТІВ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	PE-22_ODP	**визначено апаратні компоненти системи, які підлягають маркуванню із зазначенням рівня впливу або класифікації інформації, яку дозволено обробляти, зберігати або передавати за допомогою апаратного компонента;**
	PE-22	**<PE-22_ODP апаратні компоненти системи>** позначаються із зазначенням рівня впливу або класифікації інформації, яку дозволено обробляти, зберігати або передавати за допомогою апаратного компонента.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР Політики фізичного захисту та захисту робочого середовища; процедури, що стосуються з маркування компонентів; перелік апаратних компонентів, які підлягають маркуванню; записи про проведене маркування компонентів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за маркування компонентів; Персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси для маркування компонентів; автоматизовані механізми підтримки та / або реалізації маркування компонентів].	

PE-23	**РОЗТАШУВАННЯ ОБ'ЄКТА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PE-23(a)	місце розташування або ділянка об'єкта, де знаходиться система, планується з урахуванням фізичних та екологічних небезпек;
	PE-23(b)	для існуючих об'єктів фізичні та екологічні небезпеки враховуються в стратегії управління ризиками організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика фізичного захисту та захисту навколишнього середовища; документи з планування об'єкта; оцінка ризиків організацією; план дій у надзвичайних ситуаціях; документація зі стратегії зменшення ризиків; план захисту інформації; інші відповідні документи або записи.]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за вибір місця для розміщення системи; персонал організації, відповідальний за зменшення ризиків; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для планування об'єкту].	