ЗАТВЕРДЖЕНО
Наказ Держспецзв'язок України
_____ 2026 року №____

Базовий профіль безпеки системи, де обробляється службова інформація, затверджений наказом Адміністрації Держспецзв'язку від 02.07.2025 № 419

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
УПРАВЛІННЯ ДОСТУПОМ (AC)				
1	УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ (AC-2)	a. Визначити та задокументувати типи облікових записів системи, дозволених для використання в ІС для підтримки цілей, завдань, функцій і процесів організації. b. Призначити менеджерів облікових записів для управління системними обліковими записами. c. Створити умови для групового та рольового членства. d. Визначити авторизованих користувачів інформаційної системи, членство в групі та ролі, а також дозволи доступу (наприклад, привілеї) та інші атрибути (за потреби) для кожного облікового запису. e. Вимагати схвалення [Призначення: визначеною організацією відповідальною особою або роллю] запитів на створення облікових записів системи. f. Створювати, активувати, змінювати, деактивувати та видаляти системні облікові записи відповідно до [Призначення: визначених організацією політики, процедур та умов]. g. Впровадити моніторинг використання облікових записів системи. h. Повідомляти адміністраторів облікових записів у межах [Призначення: визначеного організацією часового періоду для кожної ситуації]: 1. коли облікові записи більше не потрібні; 2. коли користувачі звільнені чи переведені; 3. коли використовуються індивідуальні системи або наявні зміни, які потребують нових знань. i. Авторизувати доступ до системи на основі: 1. Дійсної авторизації доступу. 2. Передбачуваного використання системи. 3. Інших атрибутів, що вимагаються організацією. j. Проводити перегляд облікових записів на відповідність вимогам управління обліковими записами з [Призначення: визначеною організацією частотою]. k. Впровадити процес повторного випуску облікових даних спільного/групового облікового запису (якщо він буде розгорнутий), коли особи виходять з групи. l. Узгодити процеси управління обліковими записами з процесами звільнення та переводу (передачі повноважень) персоналу.	AC-2	
		визначено персонал або ролі, необхідні для затвердження запитів на створення облікових записів		Параметр: ac_2_odp_03 Тип: list Значення: admin, security_officer
		визначено персонал або ролі, які мають бути повідомлені		Параметр: ac_2_odp_05 Тип: list Значення: admin, security_officer

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		визначено період часу, протягом якого адміністратори облікових записів повинні бути повідомлені про те, що облікові записи більше не потрібні		Параметр: ac_2_odp_06 Тип: integer Значення: 30
		визначено термін, протягом якого необхідно повідомляти адміністраторів облікових записів про звільнення або переведення користувачів		Параметр: ac_2_odp_07 Тип: integer Значення: 30
		визначено період часу, протягом якого необхідно повідомляти адміністраторів облікових записів про зміни у використанні системи або необхідність знати про зміни для окремої особи		Параметр: ac_2_odp_08 Тип: integer Значення: 30
		визначено періодичність перегляду облікових записів		Параметр: ac_2_odp_10 Тип: integer Значення: 30
		Автоматично деактивувати облікові записи коли: a) їх строк дії минув; b) вони більше не пов'язані з користувачем; c) вони порушують організаційну політику; d) вони були неактивними впродовж [Призначення: визначеного організацією періоду часу].	AC-2(3)	
		Визначено період часу, протягом якого необхідно деактивувати облікові записи		Параметр: ac_2_3_odp_01 Тип: integer Значення: 30
		Визначено період часу неактивності, після закінчення якого облікові записи будуть деактивовані		Параметр: ac_2_3_odp_02 Тип: integer Значення: 30
		Вимагати від користувачів виходити із системи, коли [Призначення: вичерпано визначений організацією періоду часу очікування або опис того, коли необхідно вийти із системи].	AC-2(5)	
		Користувачі повинні виходити з системи, коли період очікуваної бездіяльності або опис часу, коли потрібно вийти з системи		Параметр: ac_2_5_01 Тип: integer Значення: 30
		Визначено часовий період очікуваної бездіяльності або опис, коли потрібно вийти з системи		Параметр: ac_2_5_odp Тип: integer Значення: 30
		Деактивувати облікові записи користувачів, які становлять значний ризик, у межах [Призначення: визначеного організацією періоду часу] після виявлення ризику.	AC-2(13)	
		Облікові записи користувачів деактивуються протягом періоду часу з моменту виявлення значних ризиків		Параметр: ac_2_13_01 Тип: integer Значення: 30
		Визначено період часу, протягом якого необхідно деактивувати облікові записи фізичних осіб, які становлять значний ризик		Параметр: ac_2_13_odp_01 Тип: integer Значення: 30
2	ЗАБЕЗПЕЧЕННЯ ДОСТУПУ (AC-3)	Застосовувати затверджені повноваження для логічного доступу до інформації та ресурсів системи відповідно до чинної політики (правил) управління доступом.	AC-3	
		Затверджені повноваження на логічний доступ до інформації та ресурсів системи виконуються відповідно до чинних політик(правил) управління доступом		Параметр: ac_3_01 Тип: list Значення: default_deny_rule, abac_rule_1
3	УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ (AC-4)	Застосувати затверджені повноваження для управління потоком інформації всередині системи та між пов'язаними системами на основі [Призначення: визначеними організацією політиками управління інформаційним потоком].	AC-4	
		Затверджені повноваження застосовуються для контролю потоку інформації всередині системи та між підключеними системами на основі політики управління інформаційними потоками		Параметр: ac_4_01 Тип: list Значення: default_deny_rule, abac_rule_1

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Визначено політики управління інформаційними потоками всередині системи та між підключеними системами		Параметр: ac_4_odp Тип: list Значення: default_deny_rule, abac_rule_1
4	РОЗМЕЖУВАННЯ ОБОВ'ЯЗКІВ (AC-5)	a. Розмежувати і документувати [Призначення: визначені організацією обов'язки окремих осіб]. b. Установити правила авторизації доступу для підтримки розмежування обов'язків.	AC-5	
5	МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ (AC-6)	Впровадити принцип мінімізації повноважень, який дозволяє користувачам (або процесам, що діють від імені користувачів) здійснювати лише такі авторизовані звернення, які необхідні для виконання визначених завдань відповідно до цілей (призначення, місії) організації та функцій.	AC-6	
		Авторизувати доступ до [Призначення: визначені організацією функції безпеки (розгорнуті в апаратному, програмному та мікропрограмному забезпеченні)] та [Призначення: визначена організацією інформація, що має відношення до безпеки] для [Призначення: визначені організацією особи або ролі].	AC-6(1)	
		a) Переглядати [Призначення: з визначеною організацією частотою] повноваження призначених для [Призначення: визначених організацією посад або класів користувачів] для перевірки необхідності таких повноважень; b) За необхідності перепризначити або зняти повноваження, правильного відображення цілей (місії) організації та потреб організації. для	AC-6(7)	
		Повноваження, призначені ролям і класам, переглядаються з частотою для перевірки необхідності таких повноважень		Параметр: ac_6_7_a Тип: integer Значення: 30
		Визначено частоту перегляду повноважень, призначених ролям або класам користувачів		Параметр: ac_6_7_odp_01 Тип: integer Значення: 30
		Визначено ролі або класи користувачів, яким призначено повноваження		Параметр: ac_6_7_odp_02 Тип: list Значення: admin, security_officer
		Авторизувати доступ до управління функціональністю аудиту тільки для [Призначення: визначеної організацією підмножини привілейованих користувачів].	AU-9(4)	
6	НЕПРИВІЛЕЙОВАНИЙ ДОСТУП ДО НЕЗАХИЩЕНИХ ФУНКЦІЙ (AC-6(2)) (AC-6)	Вимагати від користувачів облікових записів системи або ролей, які мають доступ до [Призначення: визначених організацією функцій безпеки або інформації, що стосується безпеки], використовувати непривілейовані облікові записи чи ролі під час доступу до незахищених функцій.	AC-6(2)	
		Користувачі облікових записів (або ролей) системи з доступом до функцій безпеки або інформації, що стосується безпеки, повинні використовувати непривілейовані облікові записи або ролі під час доступу до незахищених функцій		Параметр: ac_6_2_01 Тип: list Значення: admin, security_officer
		Обмежити привілейовані облікові записи в системі згідно з [Призначення: визначеним організацією персоналом або ролями].	AC-6(5)	
		Привілейовані облікові записи в системі обмежено персонал або ролі		Параметр: ac_6_5_01 Тип: list Значення: admin, security_officer

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Визначено персонал або ролі, яким мають бути обмежені привілейовані облікові записи в системі		Параметр: ac_6_5_odp Тип: list Значення: admin, security_officer
7	АУДИТ ВИКОРИСТАННЯ ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ (AC-6(9)) (AC-6)	Реєструвати виконання привілейованих функцій.	AC-6(9)	
		Вжити заходи для запобігання можливості виконувати привілейовані функції непривілейованими користувачами.	AC-6(10)	
8	НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ (AC-7)	a. Встановити обмеження на [Призначення: визначену організацією кількість] послідовних неуспішних спроб входу користувача в систему впродовж [Призначення: визначеного організацією часового періоду]. b. Автоматично виконати [Вибір (один або декілька): блокування облікового запису/вузла на [Призначення: визначений організацією часовий період]; блокування облікового запису/вузла, доки він не буде розблокований адміністратором; затримання наступної команди входу в систему за [Надання: визначеним організацією алгоритмом затримки]; виконати [Призначення: визначені організацією дії]], коли перевищено максимальну кількість невдалих спроб входу в систему.	AC-7	
		Визначено кількість послідовних неуспішних спроб входу користувача, дозволених протягом певного періоду часу		Параметр: ac_7_odp_01 Тип: integer Значення: 3
		Визначено період часу, яким обмежується кількість послідовних неуспішних спроб входу користувача		Параметр: ac_7_odp_02 Тип: string Значення: 15m
		Період часу, на який буде заблоковано обліковий запис або вузол (якщо вибрано)		Параметр: ac_7_odp_04 Тип: string Значення: 15m

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
9	ПОПЕРЕДЖЕННЯ ПРО ВИКОРИСТАННЯ СИСТЕМИ (AC-8)	a. b. Демонструвати користувачам [Призначення: визначене організацією сповіщення або банер про використання системи] перед тим, як надавати доступ до системи, що забезпечує безпеку та приватність відповідно до чинних законів, нормативних документів, наказів, директив, політик, правил, стандартів і керівних принципів, які зазначають, що: 1. користувачі здійснюють доступ до урядової системи; 2. використання системи може контролюватися, реєструватися та підлягати аудиту; 3. несанкціоноване використання системи забороняється та приводить до кримінальної та цивільної відповідальності; 4. використання системи означає згоду на моніторинг і запис дій користувача. Зберігати сповіщення або банер на екрані, доки користувачі не визнають умови використання та не приймуть явних дій для входу в систему або подальшого доступу до системи. c. Для загальнодоступних систем: 1. демонструвати інформацію про умови використання системи [Призначення: визначені організацією умови], перш ніж надавати подальший доступ до загальнодоступної системи; 2. демонструвати посилання, якщо такі є, на моніторинг, запис або аудит, які узгоджуються з акомодацією приватності для таких систем, які зазвичай забороняють такі дії; 3. мати опис авторизованого використання системи.	AC-8	
10	БЛОКУВАННЯ ПРИСТРОЮ (AC-11)	a. Заборонити подальший доступ до системи шляхом ініціювання блокування пристрою після [Призначення: визначеного організацією періоду] бездіяльності або після отримання запиту від користувача. b. Зберігати блокування пристрою, поки користувач не відновить доступ, використовуючи встановлені процедури ідентифікації та автентифікації.	AC-11	
		Визначено часовий проміжок бездіяльності, після якого ініціюється блокування пристрою		Параметр: ac_11_odp_02 Тип: string Значення: 15m
		Система приховує (через блокування сеансу) інформацію, попередньо видиму на дисплеї, загальнодоступним зображенням.	AC-11(1)	
11	ПРИПИНЕННЯ СЕАНСУ (AC-12)	Сеанс користувача має завершуватися автоматично після [Призначення: визначених організацією умов або тригерних подій, що вимагають припинення сеансу].	AC-12	
		Визначено умови або події, що вимагають припинення сеансу		Параметр: ac_12_odp Тип: list Значення: login, logout, failed_attempt
12	ВІДДАЛЕНИЙ ДОСТУП (AC-17)	a. Встановити та задокументувати обмеження на використання, вимоги до конфігурації/підключення та рекомендації щодо здійснення кожного типу віддаленого доступу. b. Авторизувати віддалений доступ до системи, перш ніж будуть дозволені такі підключення.	AC-17	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Віддалений доступ маршрутизується через авторизовані та керовані точки контролю доступу до мережі.	AC-17(3)	
		Виконання привілейованих команд за допомогою віддаленого доступу дозволено лише для наступних потреб: <AC-17(04)_ ODP[01] потреби >.	AC-17(4)	
13	БЕЗДРОТОВИЙ ДОСТУП (AC-18)	a. Установити обмеження на використання, вимоги до конфігурації/підключення та рекомендації щодо здійснення бездротового доступу. b. Авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення.	AC-18	
		Бездротовий доступ до системи захищено за допомогою автентифікації <AC-18(01)_ ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.	AC-18(1)	
		Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {користувачі; пристрої}		Параметр: ac_18_1_odp Тип: list Значення: користувачі, пристрої
		Бездротовий доступ до системи захищений за допомогою шифрування		Параметр: ac_18_1_02 Тип: string Значення: AES-256-GCM
		Відключено, у разі відсутності необхідності у використанні, вбудовані в компоненти системи можливості бездротових мереж до їх виклику та розгортання.	AC-18(3)	
14	КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ (AC-19)	a. Встановити обмеження на використання, вимоги до конфігурації, вимоги до підключення і рекомендації щодо впровадження мобільних пристроїв, контрольованих організацією. b. Авторизувати підключення мобільних пристроїв до систем, які експлуатуються організацією.	AC-19	
		<AC-19(05)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРІВ> використовується для захисту конфіденційності та цілісності інформації на <AC-19(05)_ODP[02] мобільних пристроях>.	AC-19(5)	
		Вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {повне шифрування пристроїв; шифрування сховищ інформації}		Параметр: ac_19_5_ odp_01 Тип: list Значення: повне шифрування пристроїв, шифрування сховищ інформації
15	ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ (AC-20)	a. [Вибір (один або кілька): Встановіть [Призначення: умови, визначені організацією]; Визначте [Призначення: визначені організацією засоби контролю, які, як стверджується, будуть реалізовані на зовнішніх системах]], узгоджені з довірчими відносинами, встановленими з іншими організаціями, які володіють, експлуатують та/або обслуговують зовнішні системи, дозволяючи уповноваженим особам: 1. доступ до системи із зовнішніх систем; 2. обробляти, зберігати або передавати керовану організацією інформацію за допомогою зовнішніх систем; b. Заборонити використання [Призначення: організаційно-визначені типи зовнішніх систем].	AC-20	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Вибрано одне або більше з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {встановити <AC -20_ODP[02] умови та положення>; визначити <AC-20_ODP[03] заходи захисту>}		Параметр: ac_20_odp_01 Тип: list Значення: умови та положення, заходи захисту
		Визначено умови та положення, що відповідають довірчим відносинам, встановленим з іншими організаціями, які володіють, експлуатують та/або обслуговують зовнішні системи (якщо вибрано)		Параметр: ac_20_odp_02 Тип: list Значення:
		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(1)	
		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)		Параметр: ac_20_1_a Тип: list Значення: admin, security_officer
		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		Параметр: ac_20_1_b Тип: list Значення: admin, security_officer
		Використання портативних пристроїв носіїв інформації уповноваженими особами обмежено у зовнішніх системах за допомогою обмеження.	AC-20(2)	
		Використання портативних пристроїв носіїв інформації уповноваженими особами обмежено у зовнішніх системах за допомогою обмеження		Параметр: ac_20_2_01 Тип: list Значення: admin, security_officer
		Визначено обмеження на використання авторизованими особами портативних носіїв інформації у зовнішніх системах		Параметр: ac_20_2_odp Тип: list Значення: admin, security_officer
16	ПУБЛІЧНО ДОСТУПНИЙ КОНТЕНТ (AC-22)	a. Призначити осіб, що уповноважені на розміщення інформації в загальнодоступній системі. b. Навчати уповноважених осіб тому, щоб загальнодоступна інформація не містила інформацію з обмеженим доступом. c. Переглядати запропонований зміст інформації до публікації в загальнодоступній системі, щоб гарантувати, що там не міститься інформація з обмеженим доступом. d. Переглядати вміст загальнодоступної системи на предмет наявності там інформації з обмеженим доступом з [Призначення: визначеною організацією частотою]; така інформація має бути видалена в разі її виявлення.	AC-22	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
ОБІЗНАНІСТЬ ТА НАВЧАННЯ (AT)				
17	НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ (AT-2)	Впровадити базові тренінги з підвищення обізнаності у сфері безпеки та приватності для користувачів системи (включно з менеджерами, керівниками компаній і підрядниками): a. Забезпечити навчання грамотності з питань безпеки та конфіденційності для користувачів системи (включаючи менеджерів, керівників вищої ланки та підрядників): 1. як частину початкового навчання для нових користувачів і [Призначення: частота, визначена організацією] після цього; 2. якщо цього потребують системні зміни або наступні [Призначення: події, визначені організацією]. b. Використовувати наведені нижче методи, щоб підвищити рівень безпеки та конфіденційності користувачів системи [Завдання: визначені організацією методи поінформованості]; c. Оновлювати навчання грамотності та зміст обізнаності [Завдання: частота, визначена організацією] і наступні [Завдання: події, визначені організацією]; d. Включити уроки, отримані з внутрішніх або зовнішніх інцидентів безпеки або порушень, у навчання грамотності та методи підвищення обізнаності.	AT-2	
		Визначено періодичність проведення навчання грамотності з питань безпеки для користувачів системи (в тому числі менеджерів, вищого керівництва та підрядників) після початкового тренінгу		Параметр: at_2_odp_01 Тип: string Значення: щорічно
		Визначено періодичність проведення навчання грамотності з питань конфіденційності для користувачів системи (в тому числі менеджерів, вищого керівництва та підрядників) після початкового тренінгу		Параметр: at_2_odp_02 Тип: string Значення: щорічно
		Ввести до програми навчання вправи з розпізнавання та виявлення потенційних індикаторів внутрішніх загроз.	AT-2(2)	
		Ввести до програми навчання вправи з підвищення обізнаності щодо розпізнавання та повідомлення про потенційні та фактичні атаки, з використанням методів соціальної інженерії та інтелектуального аналізу соціальних даних.	AT-2(3)	
18	РОЛЬОВЕ НАВЧАННЯ (AT-3)	a. Забезпечити проведення навчання з питань безпеки та приватності на основі ролей для працівників з ролями та обов'язками: [Призначення: визначені організацією ролі та обов'язки]: 1. перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків і [Призначення: частота, визначена організацією] після цього; 2. коли цього потребують системні зміни. b. Оновити навчальний контент на основі ролей [Призначення: частота, визначена організацією] і наступні [Призначення: події, визначені організацією]; c. Включіть у рольове навчання, інформацію, отриману з внутрішніх або зовнішніх інцидентів та порушень безпеки.	AT-3	
		Визначено ролі та обов'язки для тренінгів з безпеки на основі ролей		Параметр: at_3_odp_01 Тип: list Значення: admin, security_officer

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Визначено ролі та обов'язки для тренінгів з конфіденційності на основі ролей		Параметр: at_3_odp_02 Тип: list Значення: admin, security_officer
		Визначено частоту оновлення змісту навчання на основі ролей		Параметр: at_3_odp_04 Тип: integer Значення: 30
АУДИТ ТА ПІДЗВІТНІСТЬ (AU)				
19	ПОДІЇ АУДИТУ (AU-2)	a. Визначити типи подій, які система може реєструвати для підтримки функції аудиту: [Призначення: типи подій, визначені організацією, які система здатна реєструвати]; b. Координувати функції аудиту безпеки з іншими організаційними підрозділами, які вимагають інформації, пов'язаної з аудитом, для посилення взаємної підтримки та допомоги у виборі типів подій, що перевіряються; c. Визначити, які типи подій підлягають аудиту: [Призначення: визначені організацією події, що підлягають аудиту (підмножина подій, що підлягають аудиту, визначених в AU-2 a.), а також частота (або ситуація, що вимагає) проведення аудиту для кожної ідентифікованої події] d. Обґрунтувати, чому типи подій, що перевіряються, вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов'язаних з безпекою та приватністю; e. Перегляньте й оновіть типи подій, вибрані для журналювання [Призначення: частота, визначена організацією].	AU-2	
		Зазначені типи подій реєструються 02_ ODP[03] частота або ситуація>; <AU-		Параметр: au_2_c_02 Тип: string Значення: щорічно
		Переглядаються та оновлюються типи подій, вибрані для реєстрації, частота. у системі		Параметр: au_2_e Тип: string Значення: щорічно
		Визначено частоту або ситуацію, що вимагає проведення аудиту для кожної ідентифікованої події		Параметр: au_2_odp_03 Тип: list Значення: login, logout, failed_attempt
		Частота перегляду та оновлення типів подій, обраних для журналювання		Параметр: au_2_odp_04 Тип: string Значення: щорічно
20	ЗМІСТ ЗАПИСІВ АУДИТУ (AU-3)	Переконатися, що записи аудиту містять інформацію, яка встановлює наступне: a. який тип події стався; b. коли відбулася подія; c. де відбулася подія; d. джерело події; e. наслідки події; f. результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією.	AU-3	
		Записи аудиту містять інформацію, яка встановлює який тип події стався		Параметр: au_3_a Тип: list Значення: login, logout, failed_attempt
		Записи аудиту містять інформацію, яка встановлює джерело події		Параметр: au_3_d Тип: list Значення: login, logout, failed_attempt
		Записи аудиту містять інформацію, яка встановлює наслідки події		Параметр: au_3_e Тип: list Значення: login, logout, failed_attempt
		Записи аудиту містять інформацію, яка встановлює результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією		Параметр: au_3_f Тип: list Значення: login, logout, failed_attempt

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Сформовані записи аудиту містять наступну <AU-03(01)_ODP додаткова інформація>.	AU-3(1)	
21	ЗБЕРЕЖЕННЯ ЗАПИСІВ АУДИТУ (AU-11)	Зберігати записи аудиту впродовж [Призначення: визначеного організацією періоду часу, відповідно політиці зберігання записів], щоб забезпечити підтримку розслідувань (постфактум) інцидентів безпеки та приватності, а також для задоволення вимог нормативних і документів організації щодо збереження даних аудиту.	AU-11	
		a. Забезпечити генерацію даних аудиту для типів подій, що перевіряються в AU-2a в [Призначення: визначених організацією компонентах системи]. b. Дозволити [Призначення: визначеному організацією персоналу або посадам] вибирати, які типи подій, що перевіряються, повинні перевірятися окремими компонентами системи; c. Генерувати записи аудиту для типів подій, визначених в AU-2c. з вмістом згідно з AU-3.	AU-12	
		визначено персонал або ролі, яким дозволено обирати типи подій, що мають реєструватися певними компонентами системи;		Параметр: au_12_odp_2 Тип: list Значення: admin
		<AU-12_ODP[02] персонал або ролі> може/можуть вибирати типи подій, які будуть реєструватися певними компонентами системи;		Параметр: au_12_b Тип: list Значення: admin
22	РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ (AU-5)	a. Сповіщати [Призначення: визначені організацією персонал або посади] у разі збою обробки даних аудиту в [Призначення: визначений організацією період часу]. b. Виконати наступні додаткові дії: [Призначення: визначені організацією дії, які необхідно зробити].	AU-5	
		Персонал або ролі отримують сповіщення у разі збою процесу обробки даних аудиту періоду часу		Параметр: au_5_a Тип: list Значення: admin, security_officer
		Додаткові дії виконуються у разі збою процесу обробки даних аудиту		Параметр: au_5_b Тип: list Значення: login, logout, failed_attempt
		Визначено персонал або ролі, які отримують сповіщення про збої в процесі обробки даних аудиту		Параметр: au_5_odp_01 Тип: list Значення: admin, security_officer
		Визначено період часу, протягом якого персонал або ролі отримують сповіщення про збої в процесі обробки даних аудиту		Параметр: au_5_odp_02 Тип: list Значення: admin, security_officer
		Визначено додаткові дії, яких слід вжити у випадку збою в процесі обробки даних аудиту		Параметр: au_5_odp_03 Тип: list Значення: login, logout, failed_attempt

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
23	ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ (AU-6)	a. Переглядати та аналізувати записи системного аудиту [Призначення: з визначеною організацією частотою] для виявлення [Призначення: визначеної організацією неналежної або незвичайної діяльності]. b. Відправляти звіт про аудит [Призначення: визначеним організацією персоналу або посадам]. c. Налаштувати рівні огляду аудиту, аналізу та звітності в рамках системи, коли змінюється рівень ризику на основі інформації від правоохоронних органів, розвідувальної інформації або від інших достовірних джерел інформації.	AU-6	
		Записи аудиту системи переглядаються та аналізуються частота для виявлення ознак неналежної або незвичної діяльності та потенційного впливу неналежної або незвичної діяльності		Параметр: au_6_a Тип: string Значення: щотижня
		Звіт аудиту відправляється персоналу або ролям		Параметр: au_6_b Тип: list Значення: admin, security_officer
		Визначено частоту, з якою переглядаються та аналізуються записи аудиту системи		Параметр: au_6_odp_01 Тип: integer Значення: 30
		Визначено персонал або ролі які отримують результати оглядів та аналізів системних записів		Параметр: au_6_odp_03 Тип: list Значення: admin, security_officer
		Аналізувати та зіставляти записи аудиту в різних сховищах задля забезпечення ситуативної обізнаності в масштабах організації.	AU-6(3)	
24	СКОРОЧЕННЯ ЗАПИСІВ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ (AU-7)	Забезпечити та реалізувати можливості скорочення записів перевірок аудитом і звітів, до рівня, який: a. підтримує перевірку, аналіз і звітність аудиту на вимогу та розслідування (постфактум) інцидентів безпеки; b. не змінює оригінальний вміст або час упорядкування записів аудиту.	AU-7	
25	ПОЗНАЧКА ЧАСУ (AU-8)	a. Використовувати внутрішньосистемний годинник для створення позначок часу для записів аудиту. b. Застосовувати позначки часу, які відповідають [Призначення: деталізація вимірювання часу, визначена організацією] і використовують всесвітній координований час, мають фіксоване зміщення місцевого часу відносно всесвітнього координованого часу або включають зміщення місцевого часу як частину позначки часу.	AU-8	
26	ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ (AU-9)	a. Захист інформації аудиту та інструментів несанкціонованого доступу, зміни та видалення; журналювання аудиту від b. Сповіщення [Призначення: персонал або ролі, визначені організацією] у разі виявлення несанкціонованого доступу, зміни або видалення інформації аудиту.	AU-9	
		визначено персонал або ролі, які мають бути сповіщені при виявленні несанкціонованого доступу, зміни або видалення інформації аудиту;		Параметр: au_9_odp Тип: list Значення: admin
		<AU-09_ODP персонал або ролі> отримують сповіщення при виявленні несанкціонованого доступу, зміни або видалення інформації аудиту.		Параметр: au_9_b Тип: list Значення: admin
		Авторизувати доступ до управління функціональністю аудиту тільки для [Призначення: визначеної організацією підмножини привілейованих користувачів].	AU-9(4)	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
УПРАВЛІННЯ КОНФІГУРАЦІЄЮ (СМ)				
27	БАЗОВА КОНФІГУРАЦІЯ (СМ-2)	a. Розробити, задокументувати та підтримувати за допомогою заходів конфігурації поточні базові налаштування системи. b. Переглядати та оновлювати базові налаштування системи: 1. з [Призначення: визначеною організацією частотою]; 2. за потреби внаслідок [Призначення: визначених організацією обставин]; 3. коли встановлені нові або оновлені компоненти системи.	СМ-2	
28	НАЛАШТУВАННЯ КОНФІГУРАЦІЇ (СМ-6)	a. Встановити та задокументувати параметри конфігурації компонентів, які застосовуються в системі, які відображають найбільш обмежений режим, що відповідає експлуатаційним вимогам, використовуючи [Призначення: визначені організацією загальні безпечні конфігурації]. b. Реалізувати конфігураційні установки. c. Визначити, задокументувати та затвердити будь-які відхилення від встановлених конфігураційних параметрів конфігурації для [Призначення: визначених організацією компонентів системи] на основі [Призначення: визначених організацією експлуатаційних вимог]. d. Відстежувати та керувати змінами конфігураційних параметрів відповідно до організаційної політики та процедур.	СМ-6	
29	УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ (СМ-3)	a. Визначити типи змін у системі, які контролюються конфігурацією. b. Переглядати запропоновані зміни в конфігурації, контрольовані системою, і схвалити або відхилити ці зміни з явним урахуванням аналізу наслідків безпеки. c. Документувати рішення зі зміни конфігурації системи. d. Впровадити схвалені зміни конфігурації в систему. e. Зберігати записи змін конфігурації системі впродовж [Призначення: певного періоду часу, визначеного організацією]. f. Здійснювати моніторинг і аналіз дій, пов'язаних зі змінами конфігурації системи. g. Координувати та впроваджувати нагляд за діяльністю з управління змінами конфігурації за допомогою [Призначення: елементу управління змінами конфігурації, визначеного організацією], який викликається [Вибір (один або кілька): [Призначення: з визначеною організацією частотою]; [Призначення: визначені організацією умови зміни конфігурації]].	СМ-3	
30	АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ (СМ-4)	Аналізувати зміни в системі, щоб визначити потенційну загрозу безпеці та приватності перед реалізацією змін.	СМ-4	
		Після змін у системі переконайтеся, що відповідні заходи захисту реалізовано правильно і вони функціонують належним чином та дають бажаний результат щодо дотримання вимог безпеки та приватності для системи.	СМ-4(2)	
31	ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ (СМ-5)	Визначити, задокументувати, затвердити та забезпечити застосування фізичних і логічних обмежень доступу, пов'язаних зі змінами в системі.	СМ-5	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
32	МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ (CM-7)	a. Налаштуйте систему для забезпечення лише [Призначення: основні функції, визначені організацією для місії]; b. Заборонити або обмежити використання таких функцій, портів, протоколів, програмного забезпечення та/або служб: [Призначення: визначені організацією заборонені або обмежені функції, системні порти, протоколи, програмне забезпечення та/або служби].	CM-7	
		Система переглядається <CM-07(01)_ ODP[01] частота> для виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг;.	CM-7(1)	
33	АВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ – БІЛИЙ СПИСОК (CM-7(5)) (CM-7)	(a) Визначити [Призначення: визначені організацією програмне забезпечення, яке авторизовано виконується в системі] (b) Впровадити політику «заборони всього, за винятком деяких», щоб дозволити виконання авторизованих програм у системі. (c) Переглядати та оновлювати список авторизованих програм [Призначення: з визначеною організацією частотою].	CM-7(5)	
34	ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ (CM-8)	a. b. Розробити та задокументувати процес інвентаризації компонентів системи, який: 1. точно описує поточну систему; 2. охоплює всі компоненти в межах акредитації системи; 3. не включає повторний облік компонентів або компонентів, будь-якої іншої системи; 4. визначає рівень деталізації, який є необхідним для відстеження та звітування; 5. включає інформацію для досягнення підзвітності компонентів системи: [Призначення: визначена організацією інформація, необхідна для досягнення ефективної підзвітності компонентів системи]. Переглядати та оновлювати опис компонентів системи з [Призначення: визначеною організацією частотою].	CM-8	
		Інвентаризація компонентів системи оновлюється в рамках інсталяцій компонентів системи;.	CM-8(1)	
35	РОЗТАШУВАННЯ ІНФОРМАЦІЇ (CM-12)	Місцезнаходження <CM-12_ODP інформація> визначено та задокументовано;.	CM-12	
36	КОНФІГУРАЦІЯ СИСТЕМ ТА КОМПОНЕНТІВ ДЛЯ СФЕР З ВИСОКИМ РИЗИКОМ (CM-2(7)) (CM-2)	(a) Видавати [Призначення: визначених організацією систем або компонентів систем] з [Призначенням: визначеними організацією конфігураціями] особам, що перебувають у місцях, які організація вважає місцями зі значним ризиком; (b) Застосувати [Призначення: визначені організацією запобіжні заходи безпеки] до компонентів, коли особи повертаються з поїздки.	CM-2(7)	
ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (IA)				
37	ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ (IA-2)	Користувачі унікально ідентифіковані та автентифіковані;.	IA-2	
		Користувачі повинні повторно автентифікуватися, коли <IA-11_ODP обставини або ситуації>.	IA-11	
38	ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ (IA-3)	<IA-03_ODP[01] пристрої та/або типи пристроїв> унікально ідентифіковані та автентифіковано перед встановленням підключення.	IA-3	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
39	БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ (IA-2(1)) (IA-2)	Реалізувати багатофакторну автентифікацію для доступу до привілейованих облікових записів.	IA-2(1)	
		Реалізувати багатофакторну автентифікацію для доступу до непривілейованих облікових записів.	IA-2(2)	
40	ДОСТУП ДО ОБЛІКОВИХ ЗАПИСІВ — СТІЙКІСТЬ ДО ВІДТВОРЕННЯ (IA-2(8)) (IA-2)	Реалізовано стійкі до повторного відтворення механізми автентифікації для доступу до <IA-02(08)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.	IA-2(8)	
41	УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ (IA-4)	Управління ідентифікаторами здійснюється шляхом отримання дозволу від <IA-04_ODP[01] персоналу або ролей> на призначення ідентифікатора особі, групі, ролі або пристрою;.	IA-4	
		Управління індивідуальними ідентифікаторами, однозначно ідентифікуючи кожного індивідуума <IA-04(04)_ODP ознака>, що ідентифікує індивідуальний статус.	IA-4(4)	
42	АВТЕНТИФІКАЦІЯ НА ОСНОВІ ПАРОЛЯ (IA-5(1)) (IA-5)	Для автентифікації на основі паролів підтримується та оновлюється список часто використовуваних, очікуваних або також коли є підозра, що паролі організації були скомпрометовані прямо чи опосередковано;.	IA-5(1)	
43	ПРИХОВУВАННЯ ЗВОРОТНОГО ЗВ'ЯЗКУ АВТЕНТИФІКАТОРА (IA-6)	Забезпечино приховану зворотну передачу інформації автентифікації в про277 цесі автентифікації для забезпечення захисту інформації від можливої експлуатації та використання неавторизованими особами.	IA-6	
44	АВТЕНТИФІКАТОР УПРАВЛІННЯ (IA-5)	Управління системними автентифікаторами здійснюється шляхом перевірки, як частини початкового розподілу автентифікатора, особи, групи, ролі або пристрою, який отримує автентифікатор;.	IA-5	
РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR)				
45	ОБРОБКА ІНЦИДЕНТУ (IR-4)	a. Впровадити можливості обробки інцидентів безпеки та приватності, включно з підготовкою, виявленням і аналізом, локалізацією, ліквідацією та відновленням. b. Координувати діяльність з обробки інцидентів із заходами із забезпечення безперервності функціонування. c. Включити засвоєні уроки від поточних дій з обробки інцидентів до процедур реагування, навчання та перевірки інцидентів і реалізувати відповідні зміни. d. Встановлюйте строгість заходів з обробки інцидентів у порівнянній та передбачуваній формі в межах всієї організації.	IR-4	
		впроваджено можливість обробки інцидентів безпеки включно з підготовкою;		Параметр: ir_4_a_1 Тип: string Значення: Визначено організацією
		впроваджено можливість обробки інцидентів безпеки включно з виявленням;		Параметр: ir_4_a_2 Тип: string Значення: Визначено організацією
		впроваджено можливість обробки інцидентів безпеки включно з аналізом;		Параметр: ir_4_a_3 Тип: string Значення: Визначено організацією

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		впроваджено можливість обробки інцидентів безпеки включно з локалізацією;		Параметр: ir_4_a_4 Тип: string Значення: Визначено організацією
		впроваджено можливість обробки інцидентів безпеки включно з ліквідацією;		Параметр: ir_4_a_5 Тип: string Значення: Визначено організацією
		впроваджено можливість обробки інцидентів безпеки включно з відновленням;		Параметр: ir_4_a_6 Тип: string Значення: Визначено організацією
		діяльність з обробки інцидентів координується із заходами із забезпечення безперервності функціонування;		Параметр: ir_4_b Тип: string Значення: Визначено організацією
		уроки, отримані з поточних дій з обробки інцидентів, включаються в процедури реагування на інциденти, навчання та тестування;		Параметр: ir_4_c_1 Тип: string Значення: Визначено організацією
		зміни, що випливають з отриманих уроків, впроваджуються відповідним чином;		Параметр: ir_4_c_2 Тип: string Значення: Визначено організацією
		строгість заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;		Параметр: ir_4_d_1 Тип: string Значення: Визначено організацією
		інтенсивність заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;		Параметр: ir_4_d_2 Тип: string Значення: Визначено організацією
		обсяг заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;		Параметр: ir_4_d_3 Тип: string Значення: Визначено організацією
		результати діяльності заходів з обробки інцидентів є порівнянною та передбачуваною в межах всієї організації;		Параметр: ir_4_d_4 Тип: string Значення: Визначено організацією
46	МОНІТОРИНГ ІНЦИДЕНТУ (IR-5)	Відстежувати та документувати інциденти безпеки та приватності.	IR-5	
		відстежуються інциденти безпеки та приватності;		Параметр: ir_5_1 Тип: string Значення: Визначено організацією
		документуються інциденти безпеки та приватності.		Параметр: ir_5_2 Тип: string Значення: Визначено організацією
		a. Вимагати від персоналу повідомляти про підозрілі інциденти з безпеки та приватності відповідно до організаційної спроможності реагування на інциденти впродовж [Призначення: визначеного організацією періоду часу]. b. Звітувати про інциденти безпеки, приватності та ланцюжки постачання в [Призначення: визначений організацією уповноважений орган].	IR-6	
		визначено період часу, протягом якого персонал повинен повідомляти про підозрілі інциденти до уповноваженого органу;		Параметр: ir_6_odp_1 Тип: string Значення: Визначено організацією
		визначені органи, до яких слід повідомляти інформацію про інцидент;		Параметр: ir_6_odp_2 Тип: string Значення: Визначено організацією
		персонал зобов'язаний повідомляти про підозрілі інциде нти протягом <IR-06_ ODP[01] періоду часу>;		Параметр: ir_6_a Тип: string Значення: Визначено організацією

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		інформацію про інцидент повідомляється <IR-06_ODP[02] органам>.		Параметр: ir_6_b Тип: string Значення: Визначено організацією
		Надавати ресурси для підтримки реагування на інциденти, що є невіддільною частиною спроможностей організації реагування на інциденти, які являють собою поради та допомогу користувачам інформаційної системи для обробки та формування звітності про інциденти безпеки та приватності.	IR-7	
		IR-07(a) надається ресурс підтримки реагування на інциденти, що є невід'ємною частиною спроможності організації реагувати на інциденти;		Параметр: ir_7_a Тип: string Значення: Визначено організацією
		IR-07(b) ресурс підтримки реагування на інциденти містить поради та допомогу користувачам системи для обробки та формування звітності про інциденти.		Параметр: ir_7_b Тип: string Значення: Визначено організацією
47	ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ (IR-3)	Перевіряти ефективність реагування системи на інциденти [Призначення: з визначеною організацією частотою] за допомогою [Призначення: визначених організацією тестів].	IR-3	
		визначено частоту, з якою необхідно перевіряти ефективність реагування системи на інциденти;		Параметр: ir_3_odp_1 Тип: string Значення: Визначено організацією
		визначено тести, що використовуються для перевірки ефективності реагування на інциденти в системі;		Параметр: ir_3_odp_2 Тип: string Значення: Визначено організацією
		ефективність реагування системи на інциденти перевіряється тестів>.		Параметр: ir_3_01 Тип: string Значення: Визначено організацією
48	НАВЧАННЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR-2)	a. Забезпечити навчання користувачів щодо системи реагування на інциденти, відповідно до призначених ролей та обов'язків: 1. у рамках [Призначення: визначеного організацією періоду часу], впродовж якого авторизована роль або відповідальність за реагування на інциденти; 2. у разі внесення змін у систему; 3. з визначеною [Призначення: визначена організацією частота] у подальшому. b. Переглядайте та оновлюйте навчальний контент із реагування на інциденти [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією].	IR-2	
		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;		Параметр: ir_2_odp_1 Тип: string Значення: Визначено організацією
		визначено частоту, з якою користувачі повинні п роходити навчання з реагування на інциденти;		Параметр: ir_2_odp_2 Тип: string Значення: Визначено організацією
		визначено частоту перегляду та оновлення змісту навчання з реагування на інциденти;		Параметр: ir_2_odp_3 Тип: string Значення: Визначено організацією
		визначено події, які ініціюють перегляд змісту навчання з реагування на інциденти;		Параметр: ir_2_odp_4 Тип: string Значення: Визначено організацією

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		навчання з реагування на інциденти надається користувачам системи відповідно до призначених ролей та обов'язків протягом або обов'язків з реагування на інциденти або отримання доступу до системи;		Параметр: ir_2_a_1 Тип: string Значення: Визначено організацією
		навчання з реагування на інциденти надається користувачам системи відповідно до призначених ролей та обов'язків, коли цього вимагають зміни в системі;		Параметр: ir_2_a_2 Тип: string Значення: Визначено організацією
		користувачам системи надається навчання з реагування на інциденти відповідно до призначених ролей та обов'язків <IR02_ ODP[02] частота>;		Параметр: ir_2_a_3 Тип: string Значення: Визначено організацією
		зміст навчання з реагування на інциденти переглядається та		Параметр: ir_2_b_1 Тип: string Значення: Визначено організацією
		зміст навчання з реагування на інциденти переглядається та		Параметр: ir_2_b_2 Тип: string Значення: Визначено організацією
49	ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR-8)	a. Розробити план реагування на інциденти, який: 1. надає організації дорожню карту для впровадження її можливостей реагування на інциденти; 2. описує структуру та організацію спроможності реагування на інциденти; 3. надає високорівневий підхід до того, як здатність реагування на інциденти вписується в загальну практику організації; 4. відповідає вимогам керівництва організації; 5. визначає інциденти, що вимагають звітування, а також метрики для їх вимірювання в організації; 6. визначає ресурси й керівні принципи управління, необхідні для ефективного функціонування та підтримки спроможності реагування на інциденти. b. Розповсюдити копії плану реагування на інциденти [Призначення: серед визначеного організацією персоналу або ролей]. c. Переглядати план реагування на інциденти [Призначення: з визначеною організацією частотою]. d. Оновлювати план реагування на інциденти для розв'язання проблем із системою й організацією під час перевірок та реагування. e. Повідомляти про зміни у плані реагування на інциденти [Призначення: визначеному організацією персоналу або ролям]. f. Захищати план реагування на інциденти від несанкціонованого розголошення та зміни.	IR-8	
		визначено персонал або ролі, які переглядають та затверджують план реагування на інциденти;		Параметр: ir_8_odp_1 Тип: string Значення: Визначено організацією
		визначено періодичність перегляду та затвердження плану реагування на інциденти;		Параметр: ir_8_odp_2 Тип: string Значення: Визначено організацією
		визначені організації, персонал або ролі, які несуть відповідальність за реагування на інциденти;		Параметр: ir_8_odp_3 Тип: string Значення: Визначено організацією

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		визначено персонал з реагування на інцидент (ідентифікований за іменами та/або за ролями), якому мають бути роздані копії плану реагування на інцидент;		Параметр: ir_8_odp_4 Тип: string Значення: Визначено організацією
		визначено елементи організації, серед яких мають бути розповсюджені копії плану реагування на інцидент;		Параметр: ir_8_odp_5 Тип: string Значення: Визначено організацією
		визначено персонал з реагування на інцидент (ідентифікований за іменами та/або ролями), якому повідомляються зміни до плану реагування на інцидент;		Параметр: ir_8_odp_6 Тип: string Значення: Визначено організацією
		визначено елементи організації, яким повідомляється про зміни в плані реагування на інцидент;		Параметр: ir_8_odp_7 Тип: string Значення: Визначено організацією
		розроблено план реагування на інциденти, який надає організації дорожню карту для впровадження її можливостей реагування на інциденти;		Параметр: ir_8_a_1 Тип: string Значення: Визначено організацією
		розроблено план реагування на інциденти, який описує структуру та організацію спроможності реагування на інциденти;		Параметр: ir_8_a_2 Тип: string Значення: Визначено організацією
		розроблено план реагування на інциденти, який надає високорівневий підхід до того, як здатність реагування на інциденти вписується в загальну практику організації;		Параметр: ir_8_a_3 Тип: string Значення: Визначено організацією
		розроблено план реагування на інциденти, який відповідає унікальним вимогам організації, які пов'язані із завданнями, розміром, структурою і функціями;		Параметр: ir_8_a_4 Тип: string Значення: Визначено організацією
		розроблено план реагування на інциденти, який визначає підзвітні інциденти;		Параметр: ir_8_a_5 Тип: string Значення: Визначено організацією
		розроблено план реагування на інциденти, який надає показники для вимірювання можливостей реагування на інциденти всередині організації;		Параметр: ir_8_a_6 Тип: string Значення: Визначено організацією
		розроблено план реагування на інциденти, який визначає ресурси та управлінську підтримку, необхідну для ефективної підтримки та розвитку можливостей реагування на інциденти;		Параметр: ir_8_a_7 Тип: string Значення: Визначено організацією
		розроблено план реагування на інциденти, який вирішує питання обміну інформацією про інциденти;		Параметр: ir_8_a_8 Тип: string Значення: Визначено організацією
		розроблено план реагування на інцидент, який розглядається та затверджується <IR-08_ODP[01] персоналом або ролями> < IR08_ODP[02] частота>;		Параметр: ir_8_a_9 Тип: string Значення: Визначено організацією
		розроблено план реагування на інциденти, в якому чітко визначено організацій, персоналу або ролей>.		Параметр: ir_8_a_10 Тип: string Значення: Визначено організацією
		копії плану реагування на інцидент розповсюджуються серед <IR309		Параметр: ir_8_b_1 Тип: string Значення: Визначено організацією
		копії плану реагування на інцидент розповсюджуються серед <IR08_ODP[05] елементів організації>;		Параметр: ir_8_b_2 Тип: string Значення: Визначено організацією
		план реагування на інциденти оновлюється з урахуванням змін у системі та організації або проблем, що виникають під час впровадження, виконання або тестування плану;		Параметр: ir_8_c Тип: string Значення: Визначено організацією
		зміни в плані реагування на інцидент повідомляються <IR08_ODP[06] персоналу з реагування на інциденти>;		Параметр: ir_8_d_1 Тип: string Значення: Визначено організацією

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		зміни в плані реагування на інциденти надсилаються до <IR08_ODP[07] елементів організації>;		Параметр: ir_8_d_2 Тип: string Значення: Визначено організацією
		план реагування на інциденти захищений від несанкціонованого розкриття;		Параметр: ir_8_e_1 Тип: string Значення: Визначено організацією
		план реагування на інциденти захищений від несанкціонованої модифікації.		Параметр: ir_8_e_2 Тип: string Значення: Визначено організацією
ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ (MA)				
50	ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ (MA-3)	a. Затвердити, контролювати та відстежувати використання засобів технічного обслуговування. b. Переглядати раніше затверджені інструменти технічного [Призначення: з частотою, визначеною організацією]. обслуговування	MA-3	
		Оглядаються інструменти для технічного обслуговування, які доставлені на об'єкт обслуговуючим персоналом, на предмет неправильних або несанкціонованих модифікацій.	MA-3(1)	
		Перед використанням носіїв у системі перевірити носії, що містять діагностичні та тестові програми на наявність шкідливого коду.	MA-3(2)	
		Запобігти переміщенню обладнання для технічного обслуговування, що містить організаційну інформацію, шляхом: (a) перевірки відсутності організаційної інформації, розміщеної на обладнанні; (b) очищення або знищення обладнання; (c) утримання обладнання на об'єкті; (d) отримання дозволу від [Призначення: визначених організацією персоналу чи ролей], які явно дозволяють переміщення обладнання з об'єкта.	MA-3(3)	
51	ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ (MA-4)	Впроваджено віддалені дії з обслуговування та діагностики;.	MA-4	
52	ТЕХНІЧНИЙ ПЕРСОНАЛ (MA-5)	a. Встановити процедуру авторизації технічного персоналу та вести перелік авторизованих організацій технічного обслуговування або персоналу. b. Перевіряти, що персонал, який не супроводжується та виконує технічне обслуговування в системі, має необхідні дозволи на доступ. c. Визначити персонал організації з необхідними повноваженнями щодо доступу та технічною компетенцією для нагляду за персоналом з технічного обслуговування, який не має необхідних дозволів на доступ.	MA-5	
ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ (MP)				
53	ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ (MP-4)	a. Фізично контролювати та безпечно зберігати [Призначення: визначені організацією типи цифрових та/або нецифрових носіїв інформації] в межах [Призначення: визначених організацією контрольованих зон]. b. Захищати системні носії, які визначені в MP-4 до того часу, як носії знищуються або очищаються, з використанням затвердженого обладнання, методів та процедур.	MP-4	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
54	ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ (MP-2)	Обмежити доступ до [Призначення: визначених організацією типів цифрових та/або нецифрових носіїв інформації] [Призначення: визначеним організацією персоналом або ролями].	MP-2	
55	ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ (MP-6)	a. Очищувати [Призначення: визначені організацією системні носії] перед утилізацією, випуском за межі організаційного контролю, або перед повторним використанням [Призначення: методами та процедурами очищення, визначеними організацією]. b. Використовувати механізми очищення зі стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації.	MP-6	
56	МАРКУВАННЯ НОСІЇВ ІНФОРМАЦІЇ (MP-3)	a. Наносити на носії інформації маркування, що вказують на обмеження поширення, обробки, а також застереження та відповідні мітки безпеки (якщо такі є) інформації. b. Звільнити [Призначення: визначені організацією типи носіїв системи] від маркування, якщо носії залишаються в межах [Призначення: визначених організацією контрольованих зон].	MP-3	
57	ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ (MP-5)	a. Захищати та контролювати [Призначення: визначені організацією типи носіїв системи] під час транспортування за межами контрольованих зон, використовуючи [Призначення: визначені організацією заходи безпеки]. b. Вести облік носіїв системи інформації під час транспортування за межами контрольованих зон. c. Документувати дії, пов'язані з транспортуванням носіїв системи. d. Обмежити діяльність уповноваженого персоналу, пов'язану з транспортуванням носіїв системи.	MP-5	
		Забезпечити [Вибір (один або кілька): конфіденційність; цілісність] [Призначення: визначена організацією інформація] в стані спокою.	SC-28	
58	ВИКОРИСТАННЯ НОСІЇВ ІНФОРМАЦІЇ (MP-7)	a. [Вибір: обмежити; заборонити] використання [Призначення: визначених організацією типів носіїв системи] на [Призначення: визначені організацією системи або компоненти системи], використовуючи [Призначення: визначені організацією заходи безпеки]. b. Заборонити використання портативних пристроїв зберігання даних в системах організації, якщо такі пристрої не мають визначеного власника.	MP-7	
ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ (CP)				
59	РЕЗЕРВНЕ КОПІЮВАННЯ (CP-9)	Резервне копіювання інформації кор истувача, що міститься в.	CP-9	
		Реалізовано криптографічні механізми для запобігання несанкціонованому розкриттю та зміні <CP-09(08)_ODP резервної інформації>.	CP-9(8)	
БЕЗПЕКА ПЕРСОНАЛУ (PS)				
60	ПЕРЕВІРКА ПЕРСОНАЛУ (PS-3)	Проходять особи перевірку перед тим, як надати їм доступ до системи;.	PS-3	
61	ЗВІЛЬНЕННЯ ПЕРСОНАЛУ (PS-4)	При звільненні працівника доступ до системи вимикається протягом <PS-04_ODP[01] часового періоду>;.	PS-4	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Переглядаються та підтверджуються поточні потреби в логічних та фізичних дозволах на доступ до систем та об'єктів при перепризначенні або переведенні осіб на інші посади в організації;.	PS-5	
ФІЗИЧНИЙ ЗАХИСТ ТА ЗАХИСТ НАВКОЛИШНЬОГО СЕРЕДОВИЩА (PE)				
62	PE-2 ДОСТУПУ (PE-2)	Розроблено перелік осіб, які мають право авторизованого доступу до об'єкта, де перебуває система;.	PE-2	
63	МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ (PE-6)	Фізичний доступ до об'єкту, де знаходиться система, моніториться з метою виявлення та реагування на інциденти фізичної безпеки;.	PE-6	
64	АЛЬТЕРНАТИВНЕ РОБОЧЕ МІСЦЕ (PE-17)	Альтернативне робоче місце.	PE-17	
65	ФІЗИЧНИЙ ДОСТУП ДО СИСТЕМИ (PE-3)	Авторизація фізичного доступу забезпечується в <PE-03_ODP[01] пунктах входу і виходу> шляхом перевірки індивідуальних дозволів доступу;.	PE-3	
		Керування фізичним доступом до вихідних даних здійснюється з <PE-05_ODP пристроїв для виведення інформації >, для запобігання несанкціонованого отримання користувачами вихідних даних.	PE-5	
66	PE-4 ЛІНІЙ ЕЛЕКТРОЖИВЛЕННЯ (PE-4)	Фізичний доступ до <PE-04_ODP[01] систем розподілу та постачання живлення> в межах об'єктів організації контролюється.	PE-4	
ОЦІНКА РИЗИКІВ (RA)				
67	ОЦІНЮВАННЯ РИЗИКУ (RA-3)	Частота> або коли відбуваються значні зміни в системі, середовищі її функціонування або інших умовах, які можуть вплинути на стан безпеки або приватності системи.	RA-3	
		Оцінювання ризику ланцюга постачання (ra-3(1)).	RA-3(1)	
		Оцініть і перегляньте ризики ланцюга постачання, пов'язані з постачальниками або підрядниками, системою, системним компонентом або системною послугою, яку вони надають [Призначення: частота, визначена організацією].	SR-6	
68	СКАНУВАННЯ ВРАЗЛИВОСТЕЙ (RA-5)	Здійснюється моніторинг систем та розміщених застосунків на наявність вразливостей <RA-05_ODP[01] частота та/або випадковість відповідно до визначеного організацією процесу>, а також коли виявляються та повідомляються нові вразливості, що потенційно можуть вплинути на систему;.	RA-5	
		Визначено час реагування на усунення законних вразливостей відповідно до організаційної оцінення ризику;.	RA-5(2)	
69	РЕАГУВАННЯ НА РИЗИК (RA-7)	Вживаються заходи реагування на результати оцінок безпеки відповідно до організаційної толерантності до ризиків;.	RA-7	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
ОЦІНЮВАННЯ, АВТОРИЗАЦІЯ ТА МОНІТОРИНГ (CA)				
70	ОЦІНЮВАННЯ (CA-2)	a. Виберіть відповідного оцінювача або команду з оцінки для типу оцінювання, яке буде проводитися; b. Розробіть план контрольної оцінки, який описує обсяг оцінки, в тому числі: 1. заходи захисту та посилені заходи, що підлягають оцінюванню; 2. процедури оцінювання, ефективності заходів; які використовуватимуться для визначення 3. середовище оцінювання, групу оцінювання, ролі й обов'язки з оцінювання. c. Забезпечити розгляд і затвердження плану оцінювання уповноваженою офіційною особою або призначеним для проведення оцінювання представником; d. Оцінити заходи захисту в системі та в її середовищі функціонування з [Призначення: визначеною організацією частотою] для визначення, наскільки коректно реалізовані заходи безпеки і чи працюють вони за призначенням і дають бажаний результат щодо дотримання встановлених вимог безпеки та приватності; e. Підготовити звіт оцінювання безпеки, який документує результати оцінювання; f. Надати результати оцінювання з безпеки [Призначення: особам або ролям, визначеним організацією].	CA-2	
		визначено частоту, з якою слід оцінювати засоби контролю в системі та середовищі її функціонування;		Параметр: ca_2_odp_1 Тип: list Значення: admin
		визначені особи або ролі, яким мають бути надані результати оцінювання з безпеки;		Параметр: ca_2_odp_2 Тип: list Значення: admin
		розроблено план контрольної оцінки, який описує обсяг оцін ки, включаючи заходи захисту та посилені заходи, що підлягають оцінюванню.		Параметр: ca_2_b_1 Тип: list Значення: admin
		розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи процедури оцінювання, які використовуватимуться для визначення ефективності заходів.		Параметр: ca_2_b_2 Тип: list Значення: admin
		розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи групу оцінювання.		Параметр: ca_2_b_3_2 Тип: list Значення: admin
		розроблено план контрольної оцінки, який описує обсяг оцінки, включаючи ролі й обов'язки з оцінювання.		Параметр: ca_2_b_3_3 Тип: list Значення: admin
		результати оцінювання з безпеки надаються <CA-02_ODP[02] особам або ролям>.		Параметр: ca_2_f Тип: list Значення: admin
71	ПЛАН УСУНЕННЯ НЕДОЛІКІВ ТА КОНТРОЛЬНІ ПОКАЗНИКИ (CA-5)	a. Розробити для системи план усунення недоліків та контрольні показники з метою документування запланованих коригувальних дій організації для усунення недоліків і зауважень, які виявлені в ході оцінювання заходів захисту, а також для зменшення або усунення відомих вразливостей у системі. b. Оновлювати чинний план усунення недоліків та контрольні показники з [Призначення: визначеною організацією частотою] на основі результатів оцінювання заходів, незалежних аудитів та постійного моніторингу.	CA-5	
		визначено частоту оновлення чинного плану усунення недоліків та контрольних показників на основі результатів оцінювання заходів захисту, незалежних аудитів та постійного моніторингу;		Параметр: ca_5_odp Тип: list Значення: admin

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		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;		Параметр: ca_5_a Тип: list Значення: admin
72	БЕЗПЕРЕРВНИЙ МОНІТОРИНГ (CA-7)	Розробити стратегію безперервного моніторингу безпеки та приватності й упровадити програму безперервного моніторингу безпеки та приватності, яка охоплює: a. встановлення показників безпеки та приватності, які необхідно відстежувати: [Призначення: визначені організацією метрики]; b. встановлення [Призначення: визначена організацією частота] для моніторингу та [Призначення: визначена організацією частота] для безперервного оцінювання ефективності заходів захисту; c. поточні оцінювання заходів захисту відповідно до стратегії безперервного моніторингу організації; d. постійний моніторинг стану безпеки та приватності відповідно до встановлених організацією метрик і відповідно до стратегії безперервного моніторингу організації; e. зіставлення та аналіз інформації, отриманої в результаті оцінювання та моніторингу безпеки та приватності; f. дії реагування за результатами аналізу інформації, пов'язаної з безпекою та приватністю; g. повідомлення про статус безпеки та приватності системи [Призначення: визначені організацією персонал або ролі] з [Призначення: визначеною організацією частотою].	CA-7	
		визначено частоту, з якою слід моніторити ефективність заходів захисту;		Параметр: ca_7_odp_2 Тип: integer Значення: 30
		визначено частоту, з якою слід оцінювати ефективність заходів захисту;		Параметр: ca_7_odp_3 Тип: integer Значення: 30
		визначено персонал або ролі, яким повідомляється про стан безпеки системи;		Параметр: ca_7_odp_4 Тип: list Значення: admin
		визначено частоту, з якою повідомляється про стан безпеки системи;		Параметр: ca_7_odp_5 Тип: integer Значення: 30
		визначено персонал або ролі, яким повідомляється про стан конфіденційності системи;		Параметр: ca_7_odp_6 Тип: list Значення: admin
		визначено частоту, з якою повідомляється про стан конфіденційності системи;		Параметр: ca_7_odp_7 Тип: integer Значення: 30
		безперервний моніторинг на рівні системи включає поточні контрольні оцінки відповідно до стратегії безперервного моніторингу;		Параметр: ca_7_c Тип: list Значення: admin

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
73	ВЗАЄМОДІЯ СИСТЕМ (CA-3)	a. схвалити та керувати обміном інформацією між системою та іншими системами за допомогою [Вибір (один або кілька): угоди безпеки взаємозв'язку; договори безпеки обміну інформацією; меморандуми про взаєморозуміння; угоди про рівень обслуговування; угоди користувача; угоди про нерозголошення; [Доручення: тип договору, визначений організацією]];. b. документувати, як частину угоди про обмін, характеристики інтерфейсу, вимоги до безпеки та приватності, засоби контролю та відповідальність для кожної системи, а також характер переданої інформації; c. здійснювати перегляд та оновлення угод з [Призначення: визначеною організацією частотою].	CA-3	
		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		Параметр: ca_3_odp_1 Тип: list Значення: admin
		визначено частоту, з якою необхідно переглядати та оновлювати угоди;		Параметр: ca_3_odp_3 Тип: integer Значення: 30
ЗАХИСТ СИСТЕМ ТА КОМУНІКАЦІЙ (SC)				
74	ДОСТУПНІСТЬ РЕСУРСІВ (SC-7)	a. Контролювати та управляти зв'язком на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи. b. Реалізувати підмережі для загальнодоступних компонентів системи, які є [Вибір: фізично; логічно] відділені від внутрішніх мереж організації. c. Підключатися до зовнішніх мереж або систем тільки через керовані інтерфейси, що складаються з пристроїв захисту периметру, і розташованих відповідно до архітектури безпеки та приватності організації.	SC-7	
75	ІНФОРМАЦІЯ В ЗАГАЛЬНИХ СИСТЕМНИХ РЕСУРСАХ (SC-4)	Запобігати несанкціонованій та ненавмисній передачі інформації через спільні системні ресурси.	SC-4	
76	ВІДМОВА ЗА ЗАМОВЧУВАННЯМ - ДОЗВІЛ ЗА ВИНЯТКОМ (SC-7(5)) (SC-7)	Відмова за замовчуванням - дозвіл за винятком (sc-7(5)).	SC-7(5)	
77	КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ (SC-8)	Забезпечити [Вибір (один або кілька): конфіденційність; цілісність] інформації, що передається.	SC-8	
		Забезпечити конфіденційність та цілісність передачі за допомогою криптографічного захисту.	SC-8(1)	
		Забезпечити [Вибір (один або кілька): конфіденційність; цілісність] [Призначення: визначена організацією інформація] в стані спокою.	SC-28	
		Забезпечити криптографічний захист інформації в стані спокою.	SC-28(1)	
		Реалізовані криптографічні механізми для запобігання несанкціонованому розкриттю інформації, що знаходиться в стані спокою на системних компонентах або носіях		Параметр: sc_28_1_01 Тип: string Значення: AES-256-GCM
		Реалізовані криптографічні механізми для запобігання несанкціонованій модифікації інформації, що знаходиться в стані спокою на системних компонентах або носіях		Параметр: sc_28_1_02 Тип: string Значення: AES-256-GCM

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
78	ВІДКЛЮЧЕННЯ МЕРЕЖІ (SC-10)	Завершити з'єднання з мережею, яке пов'язане із сеансом зв'язку в кінці сеансу або після [Призначення: визначений організацією період часу] бездіяльності.	SC-10	
		Визначено період бездіяльності, після якого система розриває мережеве з'єднання, пов'язане з сеансом зв'язку; SC08(05)_ODP[02] мережеве з'єднання, пов'язане з сеансом зв'язку, розірвано в кінці сеансу або після період часу бездіяльності		Параметр: sc_10_odp Тип: integer Значення: 30
79	ВСТАНОВЛЕННЯ КЛЮЧАМИ (SC-12)	Встановити та управляти криптографічними ключами для криптографічних засобів, які використовуються в системі відповідно до [Призначення: визначені організацією вимоги до генерації, поширення, зберігання, доступу та знищення ключів].	SC-12	
		Встановлюються криптографічні ключі, коли в системі використовується криптографія відповідно до < SC-12_ODP вимог >		Параметр: sc_12_01 Тип: string Значення: AES-256-GCM
		Здійснюється управління криптографічними ключами, коли в системі використовується криптографія, відповідно до вимог		Параметр: sc_12_02 Тип: string Значення: AES-256-GCM
80	КРИПТОГРАФІЧНИЙ ЗАХИСТ (SC-13)	a. Визначити [Призначення: використання криптографічних засобів, визначених організацією]; b. Впровадити [Завдання: визначені організацією види криптографії для кожного визначеного криптографічного використання].	SC-13	
		КРИПТОГРАФІЧНИЙ ЗАХИСТ МЕТА ОЦІНКИ: Визначити, чи:		Параметр: sc_13_01 Тип: string Значення: AES-256-GCM
		Визначено використання криптографічних засобів		Параметр: sc_13_odp_01 Тип: string Значення: AES-256-GCM
		Визначено типи криптографії для кожного вказаного криптографічного використання; SC-13a. ідентифіковано використання>; SC-13b. реалізовано типи криптографії для кожного вказаного криптографічного використання (визначеного в SC-13_ODP[01]). криптографічне <SC-13_ODP[01]		Параметр: sc_13_odp_02 Тип: string Значення: AES-256-GCM
81	СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ ТА ЗАСТОСУНКИ (SC-15)	a. Заборонити віддалену активацію спільних обчислювальних пристроїв (хмар) та застосунків з такими виключеннями: [Призначення: визначені організацією виключення, у яких дозволена віддалена активація]. b. Надати явну вказівку щодо використання користувачами фізично присутніми пристроями.	SC-15	
82	МОБІЛЬНИЙ КОД (SC-18)	a. Визначати прийнятні та неприйнятні мобільні коди та технології мобільних кодів. b. Проводити авторизацію, відстежувати та контролювати використання мобільного коду всередині системи.	SC-18	
83	АВТЕНТИФІКАЦІЯ СЕСІЇ (SC-23)	Забезпечити автентифікацію сеансів зв'язку.	SC-23	
ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ (SI)				
84	ВИПРАВЛЕННЯ ДЕФЕКТІВ (SI-2)	Виявлено недоліки системи;.	SI-2	
85	ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ (SI-3)	Захист від шкідливого коду.	SI-3	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Визначено частоту, з якою механізми шкідливого коду виконують сканування		Параметр: si_3_odp_02 Тип: integer Значення: 30
		Визначено дії, яких слід вжити у відповідь на виявлення шкідливого коду (якщо вибрано)		Параметр: si_3_odp_05 Тип: list Значення: login, logout, failed_attempt
86	ПОПЕРЕДЖЕННЯ, РЕКОМЕНДАЦІЇ ТА ДИРЕКТИВИ З БЕЗПЕКИ (SI-5)	Попередження, рекомендації та директиви з безпеки.	SI-5	
		Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {персонал або ролі; елементи; зовнішні організації}		Параметр: si_5_odp_02 Тип: list Значення: admin, security_officer
		Визначено персонал або ролі, до яких мають бути доведені попередження, поради та директиви з безпеки (якщо визначено)		Параметр: si_5_odp_03 Тип: list Значення: admin, security_officer
87	МОНІТОРИНГ СИСТЕМИ (SI-4)	Моніторинг системи.	SI-4	
		Визначені методи та способи, що використовуються для виявлення несанкціонованого використання системи		Параметр: si_4_odp_02 Тип: list Значення: admin, security_officer
		Визначена інформація про моніторинг системи, яка повинна надаватися персоналу або ролям		Параметр: si_4_odp_03 Тип: list Значення: admin, security_officer
		Визначено персонал або ролі, яким має надаватися інформація про моніторинг системи		Параметр: si_4_odp_04 Тип: list Значення: admin, security_officer
		Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {за потребою; частота}		Параметр: si_4_odp_05 Тип: string Значення: щорічно
		Визначені критерії незвичної або несанкціонованої діяльності або умови для вхідного трафіку зв'язку.	SI-4(4)	
		Визначені критерії незвичної або несанкціонованої діяльності або умови для вхідного трафіку зв'язку		Параметр: si_4_4_a_01 Тип: list Значення:
		Визначені критерії незвичайної або несанкціонованої діяльності або умови для вихідного трафіку зв'язку		Параметр: si_4_4_a_02 Тип: list Значення:
		Здійснюється моніторинг вхідного комунікаційного трафіку частота на предмет незвичних або несанкціонованих дій або умов		Параметр: si_4_4_b_01 Тип: string Значення: щорічно
		Контролюється вихідний трафік зв'язку частота на предмет незвичних або несанкціонованих дій або умов. вихідного виявлення		Параметр: si_4_4_b_02 Тип: string Значення: щорічно
88	УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ (SI-12)	Управляти та зберігати інформацію всередині системи та виводити інформацію із системи відповідно до чинного законодавства, виконавчих наказів, директив, правил, політик, стандартів, керівних принципів та експлуатаційних вимог.	SI-12	
		Здійснюється управління інформацією в системі відповідно до чинних законів, наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог		Параметр: si_12_01 Тип: list Значення: default_deny_rule, abac_rule_1
		Зберігається інформація в системі відповідно до чинних законів, указів Президента, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог		Параметр: si_12_02 Тип: list Значення: default_deny_rule, abac_rule_1

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Управління інформацією, що виводиться з системи, здійснюється відповідно до чинних законів, указів Президента, директив, положень, політик, стандартів, інструкцій та операційних вимог		Параметр: si_12_03 Тип: list Значення: default_deny_rule, abac_rule_1
		Зберігається інформація, що виводиться з системи, відповідно до чинних законів, наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог		Параметр: si_12_04 Тип: list Значення: default_deny_rule, abac_rule_1
Політики та процедури з безпеки				
89	Політики та процедури з безпеки	a. Розробити, задокументувати та поширити [Призначення: серед визначеного організацією персоналу або ролей]: 1. 2. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики контролю доступу, яка: (a) містить мету, сферу застосування, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та систему контролю відповідності (compliances); (b) відповідає чинному законодавству, нормативним документам, директивам, нормам, політикам, стандартам і керівним документам. Процедури, що сприяють реалізації політики управління доступом і відповідних заходів управління доступом. b. Призначити на посаду [Призначення: визначену організацією посадову особу] для управління, документування і розповсюдження політики та процедур контролю доступом. c. Переглянути та оновити: 1. поточну політику управління доступом [Призначення: з визначеною організацією частотою] та [Призначення: події, визначені організацією]; 2. поточні процедури управління доступом [Призначення: з визначеною організацією частотою] та [Завдання: події, визначені організацією].	AC-1	
		Визначено персонал або ролі, на які поширюється політика контролю доступу		Параметр: ac_1_odp_01 Тип: list Значення: admin, security_officer
		Визначено персонал або ролі, на які поширюються процедури контролю доступу		Параметр: ac_1_odp_02 Тип: list Значення: admin, security_officer
		Визначено посадову особу, яка керуватиме політикою та процедурами контролю доступу		Параметр: ac_1_odp_04 Тип: list Значення: admin, security_officer
		Визначено частоту, з якою переглядається та оновлюється поточна політика контролю доступу		Параметр: ac_1_odp_05 Тип: list Значення: default_deny_rule, abac_rule_1
		Визначено події, які вимагають перегляду та оновлення поточної політики контролю доступу		Параметр: ac_1_odp_06 Тип: list Значення: default_deny_rule, abac_rule_1
		Визначено частоту, з якою переглядаються та оновлюються поточні процедури контролю доступу		Параметр: ac_1_odp_07 Тип: integer Значення: 30
		Визначено події, які потребують перегляду та оновлення процедур		Параметр: ac_1_odp_08 Тип: integer Значення: 30
		Розроблено та задокументовано політику контролю доступу		Параметр: ac_1_a_01 Тип: integer Значення: 30

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Політика контролю доступу поширюється на <AC-01_ODP[01] персонал або ролі>;		Параметр: ac_1_a_02 Тип: integer Значення: 30
		Розроблені та задокументовані процедури контролю доступу для полегшення впровадження політики контролю доступу та пов'язаних з нею заходів захисту		Параметр: ac_1_a_03 Тип: integer Значення: 30
		Процедури контролю доступу поширюються на <AC-01_ODP[02] персонал або ролі>		Параметр: ac_1_a_04 Тип: integer Значення: 30
		Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить мету		Параметр: ac_1_a_1_a_01 Тип: integer Значення: 30
		Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування		Параметр: ac_1_a_1_a_02 Тип: integer Значення: 30
		Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування		Параметр: ac_1_a_1_a_04 Тип: integer Значення: 30
		Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування		Параметр: ac_1_a_1_a_05 Тип: integer Значення: 30
		Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування		Параметр: ac_1_a_1_a_06 Тип: integer Значення: 30
		Політика контролю доступу <AC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> містить сферу застосування		Параметр: ac_1_a_1_a_07 Тип: integer Значення: 30
		Політика контролю доступу <AC-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> відповідає чинним законам, виконавчим наказам, директивам, положенням, політикам, стандартам та настановам		Параметр: ac_1_a_1_b Тип: integer Значення: 30
		<AC-01_ODP[04] посадова особа> призначається для управління розробкою, документуванням та розповсюдженням політики та процедур контролю доступу		Параметр: ac_1_b Тип: integer Значення: 30
		Переглядається та оновлюється поточна політика контролю доступу <AC-01_ODP[05] частота>		Параметр: ac_1_c_01_1 Тип: integer Значення: 30
		Поточну політику контролю доступу переглянуто та оновлено після <AC-01_ODP[06] подій>		Параметр: ac_1_c_01_2 Тип: integer Значення: 30
		Переглядаються та оновлюються поточні процедури контролю доступу <AC-01_ODP[07] частота>		Параметр: ac_1_c_02_1 Тип: integer Значення: 30
		Поточні процедури контролю доступу переглядаються та оновлюються після <AC-01_ODP[08] подій>		Параметр: ac_1_c_02_2 Тип: integer Значення: 30

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		a. Розробити, задокументувати та поширити [Призначення: серед визначеного організацією персоналу або ролей]: 1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики обізнаності та навчання у сфері забезпечення безпеки та приватності, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам. 2. Процедури, що сприяють реалізації політики підвищення обізнаності та професійної підготовки в галузі безпеки, приватності, а також пов'язаних з ними заходів захисту інформації та персональних даних. b. Призначити [Призначення: визначену організацією посадову особу] для управління політикою та процедурами підвищення обізнаності та навчання у сфері забезпечення безпеки та приватності. c. Переглядати та оновлювати: 1. Поточну політика [Призначення: частота, визначена організацією] і наступне [Призначення: події, визначені організацією]; 2. Процедури [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією].	AT-1	
		Вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи}		Параметр: at_1_odp_03 Тип: list Значення: рівень організації, рівень місії/бізнес-процесу, рівень системи

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		a. Розробити, задокументувати та поширити [Призначення: серед персоналу або ролей, що їх визначила організація]: 1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політика аудиту та підзвітності, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам. 2. Процедури, що сприяють здійсненню політики аудиту та підзвітності, а також пов'язані з ними заходи аудиту та підзвітності. b. Призначити [Призначення: визначену організацією старшу посадову особу] для управління політикою та процедурами аудиту та підзвітності. c. Переглядати та оновлювати поточний аудит та підзвітність: 1. політику [Призначення: частота, визначена організацією] та наступне [Призначення: події, визначені організацією]; 2. процедури аудиту [Призначення: визначеною організацією частотою] та [Завдання: події, визначені організацією].	AU-1	
		Розроблено та задокументовано політику аудиту та підзвітності		Параметр: au_1_a_01 Тип: list Значення: default_deny_rule, abac_rule_1
		Політика аудиту та підзвітності доведена до персонал або ролі		Параметр: au_1_a_02 Тип: list Значення: admin, security_officer
		Розроблені та задокументовані процедури аудиту та підзвітності, що сприяють впровадженню політики аудиту та підзвітності, а також відповідні заходи контролю аудиту та підзвітності		Параметр: au_1_a_03 Тип: list Значення: default_deny_rule, abac_rule_1
		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 частота; AU-01(c)[01][02] переглядається та оновлюється поточна політика аудиту та підзвітності після подій; AU-01(c)[02][01] переглядається та оновлюється поточні процедури аудиту та підзвітності з частота; AU-01(c)[02][02] переглядається та оновлюється поточні процедури аудиту та підзвітності після подій		Параметр: au_1_b Тип: list Значення: admin, security_officer
		Визначено персонал або ролі, до яких має бути доведена політика аудиту та підзвітності		Параметр: au_1_odp_01 Тип: list Значення: admin, security_officer
		Визначено персонал або ролі, на які поширюються процедури аудиту та підзвітності		Параметр: au_1_odp_02 Тип: list Значення: admin, security_officer
		Визначено посадову особу, яка управлятиме політикою та процедурами аудиту та підзвітності		Параметр: au_1_odp_04 Тип: list Значення: admin, security_officer

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Визначено частоту, з якою переглядається та оновлюється поточна політика аудиту та підзвітності		Параметр: au_1_odp_05 Тип: list Значення: default_deny_rule, abac_rule_1
		Визначено події, які потребують перегляду та оновлення поточної політики аудиту та підзвітності		Параметр: au_1_odp_06 Тип: list Значення: default_deny_rule, abac_rule_1
		Визначено частоту, з якою переглядаються та оновлюються поточні процедури аудиту та підзвітності		Параметр: au_1_odp_07 Тип: integer Значення: 30
		Визначено події, які потребують перегляду та оновлення поточної процедури аудиту та підзвітності		Параметр: au_1_odp_08 Тип: list Значення: login, logout, failed_attempt
		a. Розробити, задокументувати та поширити серед [Призначення: визначеного організацією персоналу або посад]: 1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політика оцінювання, авторизації та моніторингу, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинним законам, нормативним документам, наказам, положенням, політиці, стандартам і керівним принципам. 2. Процедури, що сприяють реалізації політики оцінювання, авторизації та моніторингу безпеки та приватності, а також пов'язаних з ними заходів оцінювання, авторизації та моніторингу безпеки та приватності. b. Призначити [Призначення: посадова особа, визначена організацією] для управління розробкою, документуванням і розповсюдженням політики та процедур оцінювання, авторизації та моніторингу; c. Переглядати та оновлювати поточне оцінювання, авторизацію та моніторинг: 1. Політику [Призначення: частота, визначена організацією] та наступне [Призначення: події, визначені організацією]; 2. Процедури [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією].	CA-1	
		визначено персонал або ролі, серед яких має бути поширена політика оцінювання, авторизації та моніторингу;		Параметр: ca_1_odp_1 Тип: list Значення: admin
		визначено персонал або ролі, серед яких мають бути поширені процедури оцінювання, авторизації та моніторингу;		Параметр: ca_1_odp_2 Тип: list Значення: admin
		вибрано одне або декілька з наступних ЗНА ЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес -процесу; рівень системи};		Параметр: ca_1_odp_3 Тип: integer Значення: 30
		визначено частоту, з якою переглядається та оновлюється поточна політика оцінювання, авторизації та моніторингу;		Параметр: ca_1_odp_5 Тип: integer Значення: 30
		визначено частоту, з якою переглядається та оновлюється поточні процедури оцінювання, авторизації та моніторингу;		Параметр: ca_1_odp_7 Тип: integer Значення: 30
		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;		Параметр: ca_1_a_3 Тип: list Значення: admin

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		процедури оцінювання, авторизації та моніторингу поширюються серед <CA-01_ ODP[02] персоналу або ролей>;		Параметр: ca_1_a_4 Тип: list Значення: admin
		політика <CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> оцінювання, авторизації та моніторингу містить ролі;		Параметр: ca_1_a_1_ a_3 Тип: list Значення: admin
		політика <CA-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> оцінювання, авторизації та моніторингу містить систему контролю відповідності;		Параметр: ca_1_a_1_ a_7 Тип: list Значення: admin
		a. Розробити, задокументувати та поширити серед [Призначення: визначених організацією персоналу або ролей]: 1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики управління конфігурацією, яка: 2. (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинним законам, нормативним документам, наказам, положенням, політикам, стандартам і керівним принципам; процедури, що сприяють реалізації політики управління конфігурацією та пов'язаних з нею заходів управління конфігурацією. b. Призначити [Призначення: посадова особа, визначена організацією] для управління розробкою, документуванням і розповсюдженням політики та процедур керування конфігурацією. c. Переглядати та оновлювати поточну політику управління конфігурацією: 1. Політика [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією]; 2. Процедури [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією].	CM-1	
		Розроблено та задокументовано політику ідентифікації та автентифікації;.	IA-1	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		a. Розробити, задокументувати та поширити [Призначення: серед визначеного організацією персоналу або ролей]: 1. 2. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політики реагування на інциденти, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам; процедури, що забезпечують реалізацію політики реагування на інциденти та пов'язані з нею заходи реагування на інциденти. b. Призначити [Призначення: визначену організацією посадову особу вищого керівництва] для управління, документування і розповсюдження політики та процедур реагування на інциденти. c. Переглядати та оновлювати поточні: 1. політику реагування на інциденти [Призначення: з визначеною організацією частотою] і наступні [Призначення: події, визначені організацією]; 2. процедури реагування на інциденти [Призначення: з визначеною організацією частотою] та наступні [Призначення: події, визначені організацією].	IR-1	
		визначено персонал або ролі, до яких має бути доведена політика реагування на інциденти;		Параметр: ir_1_odp_1 Тип: string Значення: Визначено організацією
		визначено персонал або ролі, до яких мають бути доведені процедури реагування на інциденти;		Параметр: ir_1_odp_2 Тип: string Значення: Визначено організацією
		вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес -процесу; рівень системи};		Параметр: ir_1_odp_3 Тип: string Значення: Визначено організацією
		визначено посадову особу, яка керуватиме політикою та процедурами реагування на інциденти;		Параметр: ir_1_odp_4 Тип: string Значення: Визначено організацією
		визначено частоту, з якою переглядається та оновлюється поточна політика реагування на інциденти;		Параметр: ir_1_odp_5 Тип: string Значення: Визначено організацією
		визначаються події, які потребують перегляду та оновлення поточної політики реагування на інциденти;		Параметр: ir_1_odp_6 Тип: string Значення: Визначено організацією
		визначено частоту, з якою переглядаються та оновлюються поточні процедури реагування на інциденти;		Параметр: ir_1_odp_7 Тип: string Значення: Визначено організацією
		визначено події, які пот ребують перегляду та оновлення процедур реагування на інциденти;		Параметр: ir_1_odp_8 Тип: string Значення: Визначено організацією
		розроблено та задокументовано політику реагування на інциденти;		Параметр: ir_1_a_1 Тип: string Значення: Визначено організацією

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		політика реагування на інциденти поширюється серед <IR01_ODP[01] персоналу або ролей>;		Параметр: ir_1_a_2 Тип: string Значення: Визначено організацією
		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;		Параметр: ir_1_a_3 Тип: string Значення: Визначено організацією
		процедури реагування на інциденти поширюються серед <IR01_ODP[02] персоналу або ролей>;		Параметр: ir_1_a_4 Тип: string Значення: Визначено організацією
		політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить мету;		Параметр: ir_1_a_1_a_1 Тип: string Значення: Визначено організацією
		політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить сферу застосування;		Параметр: ir_1_a_1_a_2 Тип: string Значення: Визначено організацією
		політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить ролі;		Параметр: ir_1_a_1_a_3 Тип: string Значення: Визначено організацією
		політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить обов'язки;		Параметр: ir_1_a_1_a_4 Тип: string Значення: Визначено організацією
		політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить відповідальність керівництва;		Параметр: ir_1_a_1_a_5 Тип: string Значення: Визначено організацією
		політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить координацію між підрозділами організації;		Параметр: ir_1_a_1_a_6 Тип: string Значення: Визначено організацією
		політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)> містить систему контролю відповідності;		Параметр: ir_1_a_1_a_7 Тип: string Значення: Визначено організацією
		політика реагування на інциденти <IR-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам;		Параметр: ir_1_a_1_b Тип: string Значення: Визначено організацією
		<IR-01_ODP[04] посадова особа> призначається для управління розробкою, документуванням та розповсюдженням політики та процедур реагування на інциденти;		Параметр: ir_1_b Тип: string Значення: Визначено організацією
		переглядається та оновлюється поточна політика реагування на		Параметр: ir_1_c_1_1 Тип: string Значення: Визначено організацією
		поточна політика реагування на інциденти переглядається та		Параметр: ir_1_c_1_2 Тип: string Значення: Визначено організацією
		переглядаються та оновлюються поточні процедури реагування на		Параметр: ir_1_c_2_1 Тип: string Значення: Визначено організацією
		поточні процедури реагування на інциденти переглядаються та		Параметр: ir_1_c_2_2 Тип: string Значення: Визначено організацією

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		a. Планувати, документувати та переглядати записи з технічного обслуговування, ремонту або заміни компонентів системи відповідно до вимог виробника та постачальників та/або вимог організації. b. Затвердити та здійснювати моніторинг усіх заходів з технічного обслуговування, незалежно від того, виконуються вони на місці або віддалено, а також чи обслуговуються системи або системні компоненти на місці, чи переміщуються в інше місце. c. Вимагати, щоб [Призначення: визначені організацією персонал чи ролі] явно схвалили видалення системи або компоненту системи з організаційного обладнання для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації. d. Очищати обладнання з погляду видалення всієї інформації з носіїв до вилучення обладнання організації для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації. e. Перевірити всі потенційно порушені заходи захисту, щоб переконатися, що вони, як і раніше, працюють належним чином після дій з обслуговування, ремонту або заміни. f. Вносити [Призначення: визначену організацією інформацію, пов'язану з технічним обслуговуванням] до записів з технічного обслуговування.	MA-1	
		a. Розробити, задокументувати та поширити серед [Призначення: визначеного організацією персоналу або посад]: 1. 2. політику захисту носіїв інформації, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам; процедури, які сприяють здійсненню політики та заходів захисту носіїв інформації. b. Призначити [Призначення: визначену організацією посадову особу] для управління розробкою, документування, та розповсюдження політики та процедурами захисту носіїв інформації. c. Переглядати та оновлювати чинну систему захисту носіїв інформації: 1. поточну політику захисту носіїв інформації [Призначення: з визначеною організацією частотою]; 2. поточні процедури захисту носіїв інформації [Призначення: з визначеною організацією частотою].	MP-1	
		Розроблено та задокумен то вано політику фізичного захисту та захисту робочого середовища;.	PE-1	
		Розроблена та задокументована політика планування безпеки.	PL-1	
		Розроблена та задокументована політика безпеки персоналу;.	PS-1	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Поширюється політика оцінки ризиків на <RA-01_ODP[01] персонал або ролі>;.	RA-1	
		Політики та процедури придбання систем та послуг.	SA-1	
		a. Розробити, задокументувати та поширити серед [Призначення: визначеного організацією персоналу або посадових осіб]: 1. 2. Політику захисту системи та комунікацій, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам. Процедури для сприяння впровадженню політики в області захисту систем і комунікацій, а також пов'язаних з ними систем і засобів захисту зв'язку. b. Призначити [Призначення: визначена організацією посадову особу] для управління політикою та процедурами захисту системи та комунікацій. c. Переглядати та оновлювати: 1. поточну політику захисту системи та комунікацій [Призначення: визначена організацією частота]; 2. поточні процедури захисту системи та комунікацій [Призначення: визначена організацією частота].	SC-1	
		Визначено персонал або ролі, до яких має бути доведена політика захисту системи та комунікацій		Параметр: sc_1_odp_01 Тип: list Значення: admin, security_officer
		Визначено персонал або ролі, на які поширюються процедури захисту системи та комунікацій		Параметр: sc_1_odp_02 Тип: list Значення: admin, security_officer
		Визначено посадову особу, яка керуватиме політикою та процедурами захисту системи та комунікацій		Параметр: sc_1_odp_04 Тип: list Значення: admin, security_officer
		Визначена періодичність перегляду та оновлення поточної політики захисту системи та комунікацій		Параметр: sc_1_odp_05 Тип: list Значення: default_deny_rule, abac_rule_1
		Є події, які вимагають перегляду та оновлення поточної політики захисту системи та комунікацій		Параметр: sc_1_odp_06 Тип: list Значення: default_deny_rule, abac_rule_1
		Визначена періодичність перегляду та оновлення поточних процедур захисту системи та засобів зв'язку		Параметр: sc_1_odp_07 Тип: string Значення: щорічно
		Політика і процедури цілісності інформації.	SI-1	
		Визначено персонал або ролі, до яких має бути доведена політика цілісності системи та інформації		Параметр: si_1_odp_01 Тип: list Значення: admin, security_officer
		Визначено персонал або ролі, на які поширюються процедури цілісності системи та інформації		Параметр: si_1_odp_02 Тип: list Значення: admin, security_officer
		Визначено посадову особу, відповідальну за управління системою та політикою і процедурами цілісності інформації		Параметр: si_1_odp_04 Тип: list Значення: admin, security_officer
		Визначено періодичність перегляду та оновлення поточної політики цілісності системи та інформації		Параметр: si_1_odp_05 Тип: list Значення: default_deny_rule, abac_rule_1

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
		Є події, які вимагають перегляду та оновлення поточної політики цілісності системи та інформації		Параметр: si_1_odp_06 Тип: list Значення: default_deny_rule, abac_rule_1
		Визначено частоту, з якою переглядаються та оновлюються поточні цілісності системи та інформації		Параметр: si_1_odp_07 Тип: integer Значення: 30
		a. Розробіть, задокументуйте та поширте [Призначення: персонал або ролі, визначені організацією]: 1. [Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи] політика управління ризиками ланцюга постачання, яка: a) Розглядає мету, сферу діяльності, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та відповідність; b) Відповідає чинним законам, виконавчим наказам, директивам, положенням, політикам, стандартам і вказівкам; 2. Процедури для сприяння впровадженню політики управління ризиками ланцюга постачання та відповідних засобів контролю управління ризиками ланцюга постачання; b. Призначити [Призначення: посадова особа, визначена організацією] для управління розробкою, документуванням і розповсюдженням політики та процедур управління ризиками ланцюга постачання; c. Перегляньте та оновіть поточне управління ризиками ланцюга постачання: 1. Політика [Призначення: частота, визначена організацією] та наступне [Призначення: події, визначені організацією]; 2. Процедури [Призначення: частота, визначена організацією] та наступні [Призначення: події, визначені організацією].	SR-1	
ПЛАНУВАННЯ (PL)				
90	ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ (PL-2)	Розроблено план захисту інформації, який відповідає архітектурі підприємства організації;.	PL-2	
91	ПРАВИЛА ПОВЕДІНКИ (PL-4)	Встановлені правила, які описують обов'язки та очікувану поведінку щодо використання інформації та системи, безпеки та конфіденційності для осіб, яким потрібен доступ до системи;.	PL-4	
ПРИДБАННЯ СИСТЕМ ТА ПОСЛУГ (SA)				
92	БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ (SA-8)	Безпека та приватність принципів інжинірингу.	SA-8	
93	КОМПОНЕНТИ СИСТЕМИ, ЩО НЕ ПІДТРИМУЮТЬСЯ (SA-22)	Компоненти системи, що не підтримуються.	SA-22	
94	ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ (SA-9)	Зовнішні послуги для системи.	SA-9	

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту	Мінімальні необхідні параметри
УПРАВЛІННЯ РИЗИКАМИ В ЛАНЦЮГУ ПОСТАЧАННЯ (SR)				
95	ПЛАН УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ (SR-2)	a. Розробіть план управління ризиками ланцюга постачання, пов'язаними з дослідженнями та розробкою, проектуванням, виробництвом, придбанням, доставкою, інтеграцією, експлуатацією та обслуговуванням, а також утилізацією таких систем, компонентів системи або послуг для системи: [Призначення: системи, визначені організацією, системні компоненти або системні служби]; b. Перегляньте та оновіть план управління ризиками ланцюга постачання [Призначення: частота, визначена організацією] або за потреби для усунення загроз; c. Захистіть план управління ризиками ланцюга постачання від несанкціонованого розголошення та модифікації.	SR-2	
96	СТРАТЕГІЇ ПРИДБАННЯ, ІНСТРУМЕНТИ І МЕТОДИ (SR-5)	Використовуйте наступні стратегії придбання, контрактні інструменти та методи закупівель, щоб захистити від ризиків ланцюга постачання, визначити та пом'якшити їх: [Призначення: визначені організацією стратегії придбання, контрактні інструменти та методи закупівель].	SR-5	
97	КОНТРОЛЬ ЛАНЦЮГА ПОСТАЧАННЯ І ПРОЦЕСІВ (SR-3)	a. Встановлення процесу або процесів для виявлення та усунення слабких місць або недоліків в елементах і процесах ланцюга постачання [Призначення: визначена організацією система або компонент системи] у координації з [Завдання: персонал ланцюга постачання, визначений організацією]; b. Використовуйте такі заходи захисту, щоб захистити систему, компонент системи або системну службу від ризиків ланцюга постачання та обмежити шкоду чи наслідки від подій, пов'язаних із ланцюгом постачання: [Призначення: заходи захисту ланцюга постачання, визначені організацією]; c. Задокументуйте обрані та впроваджені процеси та заходи захисту ланцюгом постачання у [Вибір: плани безпеки та приватності; план управління ризиками ланцюга постачання; [Призначення: документ, визначений організацією]].	SR-3	