ЗАТВЕРДЖЕНО
Наказ Міністерства цифрової
трансформації України
_____ 2025 року №____

Галузевий профіль безпеки систем, що використовуються для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або критично важливим об'єктам інфраструктури

№ з/п	Назва дії з безпеки інформації	Зміст дії	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24	Мінімальні необхідні параметри налаштування заходів захисту відповідно до НД ТЗІ 3.6-006-24
1	2	3	4	5
Управління доступом				
1	Управління обліковими записами	1. Визначити дозволені та заборонені типи облікових записів у системі. 2. Створювати, активувати, змінювати, деактивувати та видаляти облікові записи із системи відповідно до політики, процедур, передумов і критеріїв організації. 3. Визначити авторизованих користувачів системи, належність до груп і ролей, а також повноваження доступу (тобто привілеї). 4. Авторизувати доступ до системи на основі чинного дозволу на доступ та цілей використання системи. 5. Контролювати використання облікових записів у системі. 6. Вимкнути системні облікові записи, коли: термін дії облікових записів закінчився, облікові записи були неактивні протягом [призначення: визначений організацією час період], облікові записи більше не пов'язані з користувачем або особою, облікові записи порушують політику організації, або виявлено значні ризики, пов'язані з фізичними особами. 7. Оповістити персонал або ролі організації, коли: [призначення: визначений організацією період часу] коли облікові записи більше не потрібні; [призначення: визначений організацією період часу] коли користувачі звільняються або переводяться; [призначення: визначений організацією період часу] коли у системі наявні зміни, які потребують нових знань. 8. Вимагати, щоб користувачі виходили з системи після [призначення: визначений організацією період часу] очікуваної бездіяльності або за [призначення: визначені організацією обставин].	AC-2	h.1. 24 години h.2. 24 години h.3. 24 години j. мінімум щоквартально
			AC-2(3)	1-ий параметр: не більше 72 годин d. 90 днів
			AC-2(5)	кінець робочого дня користувача
			AC-2(13)	1-ий параметр: 30 хв.
2	Управління обліковими записами - автоматизоване управління системними обліковимии записами	Використовувати автоматизовані механізми для підтримки управління системними обліковими записами.	AC-2(1)	
3	Управління обліковими записами - видалення тимчасових та екстренних облікових записів	Автоматично [вибір: видаляти, деактивувати] тимчасові та екстрені облікові записи після [призначення: визначеного організацією часового періоду для кожного типу облікових записів].	AC-2(2)	
4	Управління обліковими записами - дії при авоматизованому аудіти	Проводити автоматизований аудит створення, модифікації, активації, деактивації та видалення облікових записів і сповіщення про дії.	AC-2(4)	
5	Управління обліковими записами - схеми, засновані на ролях	1. Створювати й адмініструвати привілейовані облікові записи користувачів відповідно до схеми доступу на основі ролей (role-based), яка реалізує дозволений доступ до системи та призначення привілеїв для ролей. 2. Проводити моніторинг призначення привілейованих ролей. 3. Відстежувати зміни ролей або атрибутів. 4. Скасовувати доступ, коли призначені привілейовані ролі більше не потрібні.	AC-2(7)	

6	Управління обліковими записами - обмеження на використання спільних та групових облікових записів	Використовувати лише ті спільні та групові облікові записи, які відповідають [призначення: визначеним організацією умовам для створення спільних та групових облікових записів].	AC-2(9)	
7	Управління обліковими записами - умови використання	Забезпечити дотримання [призначення: обставин та/або умов використання, визначених організацією] для [призначення: визначених організацією облікових записів системи].	AC-2(11)	
8	Управління обліковими записами - моніторинг нетипового використання облікових записів	1. Проводити моніторинг облікових записів системи на [призначення: визначене організацією нетипове використання]. 2. Повідомляти про нетипове використання облікових записів системи [призначення: визначеного організацією персоналу або ролей].	AC-2(12)	
9	Забезпечення доступу	Застосовувати затверджені повноваження для логічного доступу до конфіденційної інформації та ресурсів у системі.	AC-3	
10	Забезпечення доступу - інформація щодо безпеки	Запобігати доступу до інформації щодо безпеки, за винятком випадків, коли наявні безпечні неробочі стани системи.	AC-3(5)	
11	Забезпечення доступу - управління доступом на основі ролей	Застосовувати політику управління доступом на основі ролей щодо визначених суб'єктів і об'єктів та управління доступом на основі та користувачів, уповноважених приймати такі ролі.	AC-3(7)	
12	Управління інформаційними потоками	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	
13	Управління інформаційними потоками - управління потоком зашиврованої інформації	Запобігати обходу [призначення: механізмів управління потоками, визначених організацією] зашифрованої інформації шляхом [вибір (один або декілька): дешифрування інформації; блокування потоку зашифрованої інформації; завершення сеансів зв'язку, що намагаються передавати зашифровану інформацію; [призначення: визначеними організацією процедурою або методом]].	AC-4(4)	
14	Управління інформаційними потоками - фізичне та логічне вивільнення інформаційних потоків	Відокремлювати потоки інформації логічно або фізично, використовуючи [призначення: визначені організацією механізми та/або методи] для досягнення [призначення: визначеного організацією необхідного поділу за типами інформації].	AC-4(21)	
15	Розмежування обов'язків	1. Визначити обов'язки осіб, які потребують розмежування. 2. Установити правила авторизації доступу для підтримки розмежування обов'язків.	AC-5	
16	Мінімізація повноважень	1. Надавати користувачам (або процесам, що діють від імені користувачів) лише авторизований доступ до системи, необхідний для виконання поставлених завдань організації; 2. Авторизувати доступ до [призначення: функції безпеки, визначені організацією, та важлива для безпеки інформація]. 3. Періодично перевірятипривілеї, призначені ролям або класам користувачів, щоб підтвердити необхідность таких привілеївь. 4. За необхідності перепризначити або видалити привілеї.	AC-6 AC-6(1) AC-6(7) AU-9(4)	
17	Мінімізація повноважень - непривілейований доступ до незахищених функцій	1. Обмежити привілейовані облікові записи в системі для [призначення: персонал або ролі, що визначається організацією]. 2. Вимагати, щоб користувачі (або ролі) з привілейованими обліковими записами використовували непривілейовані облікові записи для доступу до незахищених функцій або інформації.	AC-6(2) AC-6(5)	привілейовані функції

18	Мінімізація повноважень - мережевий доступ до привілейованих команд	Авторизувати мережевий доступ до [призначення: визначених організацією привілейованих команд] тільки для [призначення: визначених організацією невідкладних операційних потреб] та задокументувати обґрунтування необхідності такого доступу в плані безпеки системи.	AC-6(3)	
19	Мінімізація повноважень – рівні привілеїв для виконання коду	Запобігати виконанню програмного забезпечення на рівні привілеїв вищому, ніж доступний користувачеві, який використовує програмне забезпечення [призначення: визначене організацією програмне забезпечення].	AC-6(8)	
20	Мінімізація повноважень – непривілейованим користувачам виконувати привілейовані функції	1. Реєструвати виконання привілейованих функцій. 2. Заборонити непривілейованим користувачам виконувати привілейовані функції.	AC-6(9) AC-6(10)	
21	Невдалі спроби входу в систему	1. Встановити обмеження на кількість [призначення: кількість, яка визначена організацією] невдалих спроб входу в систему протягом певного часу [призначення: проміжок часу, визначений організацією]. 2. Автоматично [вибір (один або декілька): заблокувати обліковий запис або вузол на [призначення: період часу, визначений організацією]; заблокувати обліковий запис або вузол до зняття адміністратором; відкласти наступний запит на вхід; повідомити системного адміністратора; вжити інших заходів], коли перевищено максимальну кількість невдалих спроб входу в систему.	AC-7	b. повідомити відповідального адміністратора
22	Невдалі спроби входу в систему - використання альтернативного фактора	1. Дозволити використання факторів автентифікації, які відрізняються від основних факторів автентифікації після перевищення визначеної організацією кількості послідовних невдалих спроб входу в систему. 2. Обмежити кількість послідовних невдалих спроб входу за допомогою використання альтернативних факторів користувачем протягом визначеного періоду часу.	AC-7(4)	
23	Попередження про використання системи	Відображати повідомлення в системі з попередженнями про конфіденційність і безпеку відповідно до застосовних правил керівних документів для відкритої та конфіденційної інформації перед тим, як надати доступ до системи.	AC-8	
24	Сповіщення про попередній вхід (доступ)	Сповіщати користувача після успішного входу (доступу) до системи про дату та час останнього входу (доступу).	AC-9	
25	Управління паралельною сесією	Обмежити кількість одночасних сеансів для кожного [призначення: визначеного організацією облікового запису та/або типу облікового запису] до [призначення: визначеної організацією кількості].	AC-10	
26	Блокування пристрою	1. Заборонити доступ до системи за допомогою дій [вибір (один або декілька): ініціювання блокування пристрою після [призначення: період часу, визначений організацією] бездіяльності; вимагати від користувача ініціювати блокування пристрою перед тим, як залишити систему без нагляду]. 2. Зберігати блокування пристрою до відновлення користувачем доступу за допомогою встановлених процедур ідентифікації та автентифікації. 3. Приховати за допомогою блокування пристрою інформацію, яку раніше було видно на дисплеї, за допомогою публічно доступного зображення.	AC-11 AC-11(1)	a. Ініціювання блокування пристрою через період, що не перевищує 30 хвилин; дія до користувача ініціювати блокування пристрою перед тим, як залишити систему без нагляду
27	Припинення сеансу	Автоматично завершувати сеанс користувача після [призначення: умови або події, що вимагають відключення сеансу, визначені організацією].	AC-12	
28	Дозводеня дії без ідентифікації або автентифікації	1. Визначити [призначення: дозволені організацією дії користувачів], які можуть виконуватися в системі без ідентифікації або автентифікації відповідно до завдань та функцій організації. 2. Документувати та визначити відповідне обгрунтування в плані безпеки системи дій користувача, які не потребують ідентифікації або автентифікації.	AC-14	

29	Віддалений доступ	1. Встановити обмеження на використання, вимоги до конфігурації та підключення для кожного типу допустимого віддаленого доступу до системи. 2. авторизувати кожен тип віддаленого доступу до системи перед встановленням таких з'єднань. 3. виконувати маршрутизацію всього віддаленого доступу до системи через авторизовані та керовані точки контролю управління доступом до мережі. 4. авторизувати віддалене виконання привілейованих команд і віддалений доступ до інформації, важливої для безпеки;	AC-17 AC-17(3) AC-17(4)	
30	Віддалений доступ - автоматизований моніторинг та управління	Проводити моніторинг та управління методами віддаленого доступу.	AC-17(1)	
31	Віддалений доступ - захист конфіденційності і цілісності за допомогою шифрування	Запровадити криптографічні механізми для захисту конфіденційності та цілісності сесій віддаленого доступу.	AC-17(2)	
32	Віддалений доступ - захист інформації	Забезпечити захист інформації щодо механізмів віддаленого доступу від неавторизованого використання та розкриття.	AC-17(6)	
33	Віддалений доступ - відключення або деактивація доступу	Забезпечити можливість швидкого відключення або деактивації віддаленого доступу до системи в межах [призначення: визначеного організацією періоду часу].	AC-17(9)	
34	Бездротовий доступ	1. Встановити обмеження на використання, вимоги до конфігурації та підключення та рекомендації щодо здійснення бездротового доступу до системи. 2. Авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення. 3. Вимкнути перед розгортанням та запуском бездротові мережі, якщо вони не призначені для використання.	AC-18 AC-18(3)	
35	Бездротовий доступ - автентифікація та шифрування	Забезпечити захист бездротового доступу до системи за допомогою автентифікації [вибір (один або кілька): користувачів; пристроїв] та шифрування.	AC-18(1)	користувачі та пристрої
36	Бездротовий доступ - обмеження налаштування користувачами	Встановити та явно авторизувати користувачів, яким дозволено самостійно налаштовувати можливості бездротових мереж.	AC-18(4)	
37	Бездротовий доступ - антени та рівень потужності передачі	Вибрати радіоантени та калібрувати рівень потужності передачі, щоб зменшити ймовірність того, що сигнали від бездротових точок доступу можуть бути отримані за межами контрольованих організацією меж.	AC-18(5)	
38	Контроль доступу для мобільних пристроїв	1. Встановити обмеження на використання, вимоги до конфігурації та підключення для мобільних пристроїв. 2. Авторизувати підключення мобільних пристроїв до системи. 3. Застосувати повне шифрування носія інформації пристрою або шифрування на основі шифрування сховищ інформації (контейнерів).	AC-19 AC-19(5)	 2-ий параметр: всі мобільні комп'ютери/ пристрої, які обробляють дані організації
39	Використання зовнішніх систем	1. Заборонити використання зовнішніх систем, крім систем дозволених організацією. 2. Установити такі положення, умови та вимоги щодо безпеки, які повинні бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованим особам: [призначення: умови, положення та вимоги визначаються організацією]. 3. Дозволити авторизованим особам використовувати зовнішню систему для доступу до системи організації або для обробки, зберігання чи передачі інформації, лише після: перевірки реалізації вимог безпеки на зовнішній системі, як зазначено в планах безпеки організації; збереження затверджених угод про підключення або обробку даних з організацією, що розміщує зовнішню систему, з якою укладено відповідну угоду. 4. Обмежити використання портативних пристроїв зберігання даних авторизованими особами на зовнішніх системах.	AC-20 AC-20(1) AC-20(2)	

40	Розповсюдження інформації	1. Спростити обмін інформацією, надаючи авторизованим користувачам змогу визначати, чи відповідають повноваження на доступ, що призначені партнерам для обміну, обмеженням доступу та повноваженням з приватності щодо інформації для [призначення: визначених організацією обставин обміну інформацією, коли це необхідно користувачу]. 2. Використовувати [призначення: визначені організацією автоматизовані механізми або ручні процеси], щоб допомогти користувачам в ухваленні рішень щодо обміну інформацією та співпраці.	AC-21	
41	Публічно доступний контент	1. Навчати авторизованих осіб щодо нерозголошення відкритої та конфіденційної інформації в загальнодоступних системах. 2. Періодично переглядати вміст загальнодоступних систем на предмет наявності відкритої та конфіденційної інформації та видаляти таку інформацію, якщо її виявлено.	AC-22	d. щоквартально або в міру надходження нової інформації
Обізнаність і навчання				
42	Навчання з підвищення обізнаності	1. Забезпечити навчання користувачів системи з питань безпеки: як частину початкового навчання для нових користувачів і періодично після цього; якщо цього потребують зміни в системі або наступні [призначення: події, визначені організацією]; про розпізнавання та повідомлення про ознаки внутрішньої загрози, соціальної інженерії та соціфльного майнінгу. 2. Періодично оновлювати зміст тренінгу з безпекової обізнаності [призначення: визначені організацією події].	AT-2 AT-2(2) AT-2(3)	a.1. щонайменше раз на рік
43	Навчання з підвищення обізнаності -	1. Забезпечити навчання грамотності щодо стійкої постійної загрози. 2. Забезпечити навчання грамотності щодо середовища кіберзагроз. 3. Відображати поточну інформацію про кіберзагрози в операціях системи.	AT-2(4) AT-2(5) AT-2(6)	
44	Рольове навчання	1. Провести навчання з безпеки для персоналу організації на основі покладених обов'язків: перед авторизацією доступу до системи або інформації, перед виконанням призначених обов'язків, а також періодично після цього; коли цього вимагають зміни в системі або після [призначення: події, визначені організацією]. 2. Періодично оновлювати зміст навчання на основі покладених обов'язків, а також після [призначення: події, визначені організацією].	AT-3	a.1. щонайменше щороку
45	Рольове навчання	1. Надати [призначення: визначеним організацією персоналу чи посадам] з початку роботи та з [призначенням: визначеною організацією частотою] підготовку з питань застосування заходів захисту робочого середовища. 2. Надати [призначення: визначеним організацією персоналу чи ролям] з початку роботи та з [призначення: визначеною організацією частотою] підготовку з питань застосування та експлуатації заходів фізичної безпеки. 3. Забезпечити [призначення: персонал або посади, визначені організацією] початкове та [призначення: частота, визначену організацією] навчання з використання та управління обробкою персональних даних та контролю прозорості.	AT-3(1) AT-3(2) AT-3(5)	
46	Навчальні записи	1) Документувати та відстежувати індивідуальні навчальні заходи із забезпечення безпеки та приватності, включно з базовою підготовкою з питань безпеки та приватності, а також спеціальною підготовкою з питань безпеки та приватності визначених посадових осіб. 2) Зберігати індивідуальні записи про навчання впродовж [призначення: визначеного організацією періоду часу].	AT-4	
Аудит і підзвітність				
47	Події аудиту	1. Визначити перелік подій, які реєструються в системі: [призначення: типи подій, визначені організацією]. 2. Періодично переглядати та оновлювати типи подій, обрані для реєстрації (журналювання).	AU-2	
48	Зміст записів аудиту	1. Записи аудиту повинні містити таку інформацію: який тип події стався; коли відбулася подія; де відбулася подія; джерело події; наслідки події; результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією. 2. За потреби надавати додаткову інформацію для записів аудиту.	AU-3 AU-3(1)	
49	Місткість сховища запису аудитів	Розподіляти місткість сховища записів аудиту у відповідності до [призначення: визначених організацією вимог до зберігання записів аудиту].	AU-4	

50	Реагування на відмови обробки даних аудиту	1. Сповіщати персонал або ролі організації в межах [призначення: визначений організацією період часу] у разі збою обробки даних аудиту. 2. Виконати додаткові дії: [призначення: додаткові дії, визначені організацією].	AU-5	а. 2-ий параметр: майже в реальному часі
51	Реагування на відмови обробки даних аудиту - місткість сховища даних аудиту	Забезпечити попередження [призначення: визначених організацією персоналу, ролей та/або місць] у межах [призначення: визначеного організацією періоду часу], коли обсяг записів аудиту, що зберігаються, досягає максимуму місткості сховища.	AU-5(1)	
52	Реагування на відмови обробки даних аудиту - тривожне сповіщення в реальному часі	Забезпечити сповіщення в [призначення: визначений організацією період реального часу] [призначення: визначених організацією персоналу, ролей та/або місць], коли відбуваються такі події збою аудиту: [призначення: визначені організацією події, пов'язані зі збоями та помилками аудиту, які вимагають тривоги в реальному часі].	AU-5(2)	
53	Реагування на відмови обробки даних аудиту - можливість альтернативного журнулювання аудиту	Надання альтернативної можливості журналювання аудиту в разі збою основної можливості журналювання аудиту, яка реалізується [призначення: визначена організацією функція альтернативного журналювання аудиту]	AU-5(5)	
54	Огляд, аналіз і звітність аудиту	1. Переглядати та аналізувати [призначення: частота, визначена організацією] записи аудиту системи на предмет виявлення ознак і потенційного впливу не властивої або незвичної діяльності. 2. Повідомляти про результати аудиту співробітникам організації або ролям. 3. Аналізувати та зіставляти записи аудиту в різних сховищах задля забезпечення ситуативної обізнаності в масштабах організації.	AU-6 AU-6(3)	а. 1-ий параметр: щонайменше щотижня (сім днів)
55	Огляд, аналіз і звітність аудиту - автоматизована інтеграція процесів	Інтегрувати процеси перегляду, аналізу та звітності записів аудиту за допомогою [призначення: автоматизовані механізми, визначені організацією].	AU-6(1)	
56	Огляд, аналіз і звітність аудиту - централізований перегляд та аналіз	Забезпечити та впровадити можливість централізованого перегляду та аналізу записів аудиту з декількох компонентів у системі.	AU-6(4)	
57	Огляд, аналіз і звітність аудиту - інтегрований аналіз записів аудиту	Інтегрувати аналіз записів аудиту з аналізом [вибір (один або більше): інформації про сканування уразливостей; даних про продуктивність; інформації про моніторинг системи; [призначення: визначених організацією даних/інформації, зібраних з інших джерел]] для подальшого підвищення здатності виявляти неприйнятну або незвичайну діяльність.	AU-6(5)	
58	Огляд, аналіз і звітність аудиту - кореляція з фізичним моніторингом	Зіставляти інформацію із записів аудиту з інформацією, отриманою від моніторингу фізичного доступу, для подальшого підвищення здатності ідентифікувати підозрілу, неприйнятну, незвичайну або зловмисну діяльність.	AU-6(6)	
59	Огляд, аналіз і звітність аудиту - дозволені дії	Визначити дозволені дії для кожного [Вибір (один або кілька): системного процесу; ролі; користувача], пов'язаного з переглядом, аналізом та поданням інформації про аудит.	AU-6(7)	
60	Скорочення записів аудиту та формування звіту	1. Упровадити функцію скорочення записів аудиту і створення звітів, яка підтримує перегляд записів аудиту, аналіз, вимоги до звітності та постфактум розслідування інцидентів. 2. Створити та зберігати журнали та записи аудиту системи в обсязі, необхідному для моніторингу, аналізу, розслідування та звітування про незаконну або несанкціоновану діяльність у системі. 3. Зберігати оригінальний зміст і часовий порядок записів аудиту.	AU-7	
61	Скорочення записів аудиту та формування звіту - автоматична обробка	Забезпечити та реалізувати можливість обробки записів аудиту для подій, що становлять інтерес, на основі [призначення: визначених організацією полів у записах аудиту].	AU-7(1)	

62	Позначка часу	1. Використовувати внутрішній годинник у системі для створення позначок часу для записів аудиту. 2. Застосовувати позначки часу, які відповідають [призначення: деталізація вимірювання часу, визначена організацією], і використовують: всесвітній координований час (UTC). 3. Фіксоване зміщення місцевого часу відносно UTC або зміщення місцевого часу як частину позначки часу.	AU-8	
63	Захист інформації аудиту	1. Захистити інформацію аудиту та інструментів журналювання аудиту від несанкціонованого доступу, зміни та видалення. 2. Надавати доступ до управління функціями аудиту тільки підмножині привілейованих користувачів або ролей.	AU-9 AU-9(4)	
64	Неспростовність	Надавайте неспростовні докази того, що особа (або процес, який діє від імені особи) виконала [призначення: дії, визначені організацією, на які поширюється принцип неспростовності].	AU-10	
65	Збереження записів аудиту	1. Згенерувати записи аудиту для вибраних типів подій згідно з вмістом записів аудиту, вказаних в п. 47 та п. 48. 2. Зберігати записи аудиту протягом періоду часу, який відповідає політиці зберігання записів аудиту.	AU-11	
			AU-12	a. всі інформаційні системи та мережеві компоненти
66	Генерація даних аудиту - загальносистемний та синхронізований за часом журнал аудиту	Скомпонувати записи аудиту з [призначення: визначеними організацією системними компонентами] в загальносистемний (логічний або фізичний) журнал аудиту, який синхронізований за часом у межах [призначення: визначеного організацією допустимого рівня для взаємозв'язку між мітками часу окремих записів у журналах аудиту].	AU-12(1)	
67	Генерація даних аудиту - зміни, що вносять авторизовані особи	Забезпечити та реалізувати можливість для [призначення: визначених організацією окремих осіб або ролей] змінити аудит, який виконуватиметься на [призначення: визначених організацією компонентах системи] на основі [призначення: визначених організацією критеріїв вибору подій] у межах [призначення: визначених організацією часових порогів].	AU-12(3)	
Управління конфігурацією				
68	Базова конфігурація	1. Розробляти та підтримувати під контролем налаштування поточної базової конфігурації системи. 2. Переглядати та оновлювати [призначення: частота, визначена організацією] базову конфігурацію системи, а також при встановленні або модифікації компонентів системи.	CM-2	b.1. щонайменше щороку
69	Базова конфігурація - автоматизація підтримки задля точності та актуальності	Підтримувати актуальність, повноту, точність і доступність базової конфігурації. системи за допомогою [призначення: автоматизовані механізми, визначені організацією].	CM-2(2)	
70	Базова конфігурація - зберігання попередніх версій конфігурації	Зберігати [призначення: кількість, визначена організацією] попередніх версій базових конфігурацій системи для підтримки відкату.	CM-2(3)	
71	Базова конфігурація - розробка та середовище тестування	Підтримувати базову конфігурацію для розробки системи та тестових середовищ, які керуються окремо від робочої базової конфігурації.	CM-2(6)	
72	Базова конфігурація - конфігурація систем та компонентів для сфер з високим ризиком	1. Надавати системи або системні компоненти з наступними конфігураціями особам, які прямують до зони підвищеного ризику: [призначення: визначені організацією конфігурації системи]. 2. Застосовувати такі дії безпеки до систем або компонентів, коли особи повертаються з подорожі: [призначення: визначені організацією дії безпеки].	CM-2(7)	
73	Управління змінами конфігурації	1. Визначити типи змін у конфігурації системи, які необхідно контролювати. 2. Переглядати запропоновані зміни в конфігурації системи, схвалювати або відхиляти такі зміни, враховуючи вплив на безпеку. 3. Упровадити та задокументувати затверджені зміни конфігурації системи. 4. Відстежувати та переглядати дії, пов'язані зі змінами в конфігурації системи, які необхідно контролювати. 5. Зберігати записи змін конфігурації системі впродовж [призначення: певного періоду часу, визначеного організацією].	CM-3	e. 1 рік

74	Управління змінами конфігурації - автоматизоване документування, повідомлення та заборона внесення змін	Впровадити автоматизовані механізми для: документування запропонованих змін у системі; повідомлення [призначення: визначених організацією органів влади, що проводять авторизацію] про запропоновані зміни в системі та схвалення запитів змін; виділення запропонованих змін у системі, які не були схвалені або відхилені за [призначенням: визначений організацією період часу]; заборони внесення змін до системи, до отримання відповідного погодження; документування всіх змін у системі; повідомлення [призначення: визначеному організацією персоналу], коли завершено погоджені зміни в системі.	СМ-3(1)	
75	Управління змінами конфігурації - тестування, валідація та документування змін	Тестувати, перевіряти та документувати зміни в системі до повної їх реалізації.	СМ-3(2)	
76	Управління змінами конфігурації - представник безпеки	Вимагати від [призначення: визначеного організацією представника з інформаційної безпеки] бути членом [призначення: визначеного організацією елементу керування зміною конфігурацій].	СМ-3(4) СМ-3(6) СМ-3(7)	
77	Управління змінами конфігурації - управління засобами криптографічного захисту	Забезпечити, щоб криптографічні механізми, які використовуються для забезпечення відповідних заходів захисту перебували під управлінням конфігурацією [призначення: визначених організацією заходів безпеки].	СМ-3(6)	
78	Управління змінами конфігурації - перегляд змін у системі	Перегляньте зміни в системі [призначення: частота, визначена організацією] або коли [призначення: обставини, визначені організацією], щоб визначити, чи відбулися неавторизовані зміни.	СМ-3(7)	
79	Аналіз впливу на безпеку та приватність	1. Проаналізувати вплив змін у системі на безпеку перед їх впровадженням. 2. Аналізувати зміни в системі в окремому тестовому середовищі до впровадження змін в операційному середовищі, шукаючи вплив на безпеку та приватність через недоліки, слабкості, несумісність або навмисне спричинення шкоди. 3. 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 СМ-4(1) СМ-4(2)	
80	Обмеження доступу до змін	1. Визначити, задокументувати, затвердити та впровадити фізичні та логічні обмеження доступу, пов'язані зі змінами в системі. 2. Застосовувати обмеження доступу за допомогою [призначення: автоматизовані механізми, визначені організацією]; автоматично генерувати записи аудиту для виконаних дій. 3. Обмежити повноваження для зміни компонентів системи та інформації, пов’язаної із системою, у виробничому або операційному середовищі. 4. Переглядати та переоцінювати такі повноваження [призначення: визначеною організацією з частотою].	СМ-5 СМ-5(1) СМ-5(5)	
81	Налаштування конфігурації	1. Встановити, задокументувати та впровадити параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам: [призначення: налаштування конфігурації, визначені організацією]. 2. Визначити, задокументувати та затвердити будь- які відхилення від встановлених налаштувань конфігурації.	СМ-6	с. 1-ий параметр: всі конфігуровані компоненти системи.
82	Налаштування конфігурації - автоматизоване управління, застосування та верифікація	Керувати, застосовувати та перевіряти налаштування конфігурації для [призначення: системні компоненти, визначені організацією] за допомогою [призначення: визначені організацією автоматизовані механізми].	СМ-6(1)	

83	Налаштування конфігурації - реагування на несанкціоновані зміни	Виконайте такі дії у відповідь на неавторизовані зміни в [призначення: параметри конфігурації, визначені організацією]: [призначення: дії, визначені організацією].	CM-6(2)	
84	Мінімально необхідна функціональність	1. Налаштувати систему так, щоб вона надавала лише необхідні для виконання завдань функції. 2. Заборонити або обмежити використання таких функцій, портів, протоколів, підключень і служб: [призначення: функції, порти, протоколи, з'єднання та служби, визначені організацією]. 3. Переглядати [призначення: частота, визначена організацією] систему, щоб виявити непотрібні або небезпечні функції, порти, протоколи, з'єднання та служби. 4. Вимкнути або видалити функції, порти, протоколи, з'єднання та служби, які є непотрібними або небезпечними.	CM-7	b. всі функції, порти, протоколи, програмне забезпечення та послуги в системі, які були визначені як непотрібні та/або незахищені
			CM-7(1)	a. щонайменше раз на рік або в міру внесення змін до системи чи виникнення інцидентів b. всі функції, порти, протоколи, програмне забезпечення та послуги в системі, визначені як непотрібні та/або незахищені
85	Мінімально необхідна функціональність - заборона виконання програми	Заборонити виконання програми відповідно до [вибір (один або кілька): [призначення: визначеної організацією політики, правил поведінки та/або угод про доступ щодо використання програмного забезпечення та обмежень]; правил, що встановлюють терміни та умови використання програмного забезпечення].	CM-7(2)	
86	Мінімально необхідна функціональність - авторизоване програмне забезпечення - білий список	1) Визначити [призначення: визначені організацією програмне забезпечення, яке авторизовано виконується в системі]. 2) Впровадити політику «заборони всього, за винятком деяких», щоб дозволити виконання авторизованих програм у системі. 3) Переглядати та оновлювати список авторизованих програм [призначення: з визначеною організацією частотою].	CM-7(5)	c. щонайменше раз на рік
87	Мінімально необхідна функціональність - заборона використання неавторизованого обладнання	1. Визначити [призначення: апаратні компоненти, визначені організацією, авторизовані для використання в системі]. 2. Заборонити використання або підключення неавторизованих апаратних компонентів. 3. Перегляд та оновлення списку авторизованих апаратних компонентів [призначення: частота, визначена організацією].	CM-7(9)	
88	Інвентаризація компонентів системи	1. Розробити та задокументувати процес інвентаризації компонентів системи, який: точно описує поточну систему; охоплює всі компоненти в межах акредитації системи; не включає повторний облік компонентів або компонентів, будь-якої іншої системи; визначає рівень деталізації, який є необхідним для відстеження та звітування; включає інформацію для досягнення підзвітності компонентів системи: [призначення: визначена організацією інформація, необхідна для досягнення ефективної підзвітності компонентів системи]. 2. Переглядати та оновлювати опис компонентів системи з [призначення: визначеною організацією частотою]. 3. Оновлення інвентаризації компонентів системи в рамках встановлення, видалення та оновлення системи.	CM-8 CM-8(1)	a.5. як мінімум, але не обмежуючись: технічні характеристики обладнання (виробник, тип, модель, серійний номер, фізичне місцезнаходження), програмне забезпечення та інформація про ліцензію на програмне забезпечення, власник інформаційної системи/компонента, а для мережевого компонента/пристрою - ім'я обладнання b. щонайменше щороку
89	Інвентаризація компонентів системи - авторизована підтримка	Підтримувати актуальність, повноту, точність і доступність інвентаризації компонентів системи за допомогою [Завдання: автоматизовані механізми, визначені організацією].	CM-8(2)	
90	Інвентаризація компонентів системи - авторизоване виявлення неавторизованих компонентів	1. Виявляти наявність несанкціонованого обладнання, програмного забезпечення та мікропрограмних компонентів у системі за допомогою [призначення: автоматизовані механізми, визначені організацією][призначення: частота, визначена організацією]. 2. При виявленні неавторизованих компонентів виконувати такі дії: [вибір (один або кілька): відключення доступу до мережі такими компонентами; ізолювати компоненти; повідомити [призначення: визначені організацією персонал або посади]].	CM-8(3)	

91	Інвентаризація компонентів системи - інформація про підзвітність	Увести в інвентаризаційну інформацію компоненту системи засіб для ідентифікації за [вибір (один або більше): ім'ям; позицією; роллю] осіб, відповідальних і підзвітних за управління цими компонентами.	СМ-8(4)	
92	План управління конфігурацією	Розробити, задокументувати та реалізувати план управління конфігурацією системи, який: описує ролі, відповідальність, процеси та процедури управління конфігурацією; встановлює процес ідентифікації елементів конфігурації протягом всього життєвого циклу розробки системи та для управління конфігурацією елементів; визначає елементи конфігурації для системи та розміщує елементи конфігурації під управлінням конфігурації; розглядає та затверджує [призначення: визначеним організацією персоналом або ролями]; захищає план управління конфігурацією від несанкціонованого розкриття та модифікації.	СМ-9	
93	Обмеження використання програмного забезпечення	1. Використовувати програмне забезпечення та супутні документи відповідно до договірних угод та законів про авторські права. 2. Відстежувати використання програмного забезпечення та пов'язаної документації, захищеної ліцензіями, для контролю копіювання та розповсюдження. 3. Контролювати та документувати використання технології одноранговогo обміну файлами, щоб гарантувати, що ця можливість не використовується для несанкціонованого розповсюдження, відображення, виконання або відтворення програмного забезпечення, захищеного авторським правом.	СМ-10	
94	Встановлене користувачем програмне забезпечення	1. Встановити [призначення: визначені організацією правила (політики)], що регулюють встановлення програмного забезпечення користувачами. 2. Застосувати правила (політики) встановлення програмного забезпечення за допомогою таких методів: [призначення: визначені організацією методи]. 3. Відстежувати відповідність правилам (політики) з [призначення: визначеною організацією частотою].	СМ-11	
95	Розташування інформації	1. Визначити та задокументувати місцезнаходження службової інформації та компонентів системи, в яких обробляється та зберігається інформація. 2. Радокументувати зміни в системі або компонентів системи, де обробляється та зберігається службова інформація.	СМ-12	
96	Розташування інформації - автоматизовані інфструменти підтримки розташування інформації	Використовувати автоматизовані інструменти для ідентифікації [призначення: визначеної організацією інформації за типом інформації] на [призначення: визначених організацією компонентах системи] для впровадження належних заходів захисту щодо інформації про організацію і персональних даних.	СМ-12(1)	
97	Підписані компоненти	Запобігати інсталяції [призначення: програмне забезпечення та мікропрограмні компоненти, визначені організацією] без перевірки того, що компонент має цифровий підпис за допомогою сертифіката, визнаного та схваленого організацією.	СМ-14	
Планування безперервної роботи				

98	План забезпечення безперервної роботи та відновлення функціонування	1. Розробити план забезпечення безперервної роботи та відновлення функціонування системи на випадок надзвичайної ситуації. 2. Поширити копії плану забезпечення безперервної роботи та відновлення функціонування серед [призначення: визначеного організацією ключового персоналу з непередбачених обставин (ідентифікується за ім'ям та/або за ролями) та елементів організації]. 3. Координувати діяльність з планування безперервної роботи із заходами по усуненню інцидентів. 4. Переглядати план забезпечення безперервної роботи та відновлення функціонування системи з [призначення: визначеною організацією частотою]. 5. Оновлювати план забезпечення безперервної роботи та відновлення функціонування з урахуванням змін в організації, системі або середовищі експлуатації, а також проблем, що виникають при реалізації, виконанні або тестуванні плану забезпечення безперервної роботи та відновлення функціонування. 6. Повідомляти про зміни в плані забезпечення безперервної роботи та відновлення функціонування [призначення: визначений організацією ключовий персонал з відновлення функціонування (ідентифікується за ім'ям та/або за ролями) та елементів організації]. 7. Включати уроки, отримані під час тестування плану забезпечення безперервної роботи та відновлення функціонування у навчання та тестування для випадків надзвичайних ситуацій. 8. Забезпечити захист плану забезпечення безперервної роботи та відновлення функціонування від несанкціонованого доступу або змін.	CP-2	
99	План забезпечення безперервної роботи та відновлення функціонування-координація з пов'язаними планами	Координувати розробку плану забезпечення безперервної роботи та відновлення функціонування зі структурними підрозділами, які відповідають за розробку та реалізацію пов'язаних планів.	CP-2(1)	
100	План забезпечення безперервної роботи та відновлення функціонування - планування ресурсів	Здійснити планування ресурсів з метою забезпечення необхідного потенціалу для обробки інформації, телекомунікацій та підтримки навколишнього середовища під час відновлення функціонування системи.	CP-2(2)	
101	План забезпечення безперервної роботи та відновлення функціонування - відновлення критичних функції	План відновлення [вибір: усі; істотні] місія та бізнес-функції протягом [призначення: визначений організацією період часу] активації плану на випадок надзвичайних ситуацій.	CP-2(3)	
102	План забезпечення безперервної роботи та відновлення функціонування - безперервність виконання критичних функцій	Планувати безперервність виконання критичних функцій [вибір: усі; основні] з мінімальною втратою або без втрати безперервності роботи та підтримувати безперервну роботу до повного відновлення системи в місцях первинної обробки та/або зберігання.	CP-2(5)	

103	План забезпечення безперервної роботи та відновлення функціонування - визначення критичних активів	Визначити критичні активи системи, що підтримують критичні функції [вибір: усі; основні].	CP-2(8)	
104	Навчання із забезпечення безперервної роботи	1. Проводити навчання користувачів системи на випадок надзвичайних ситуацій відповідно до призначених ролей і обов'язків. 2. Переглядати та оновлювати зміст тренінгів на випадок надзвичайних ситуацій.	CP-3	
105	Навчання із забезпечення безперервної роботи - зімітовані події	Впровадити моделювання подій у навчанні, щоб забезпечити ефективне реагування персоналу на надзвичайні ситуації.	CP-3(1)	
106	Тестування плану забезпечення безперервної роботи та відновлення функціонування	1. Протестувати план забезпечення безперервної роботи та відновлення функціонування системи, використовуючи тести, з метою визначення ефективності плану та організаційної готовності виконати план. 2. Переглядати результати тестування плану. 3. За необхідності ініціювати коригувальні дії.	CP-4	
107	Тестування плану забезпечення безперервної роботи та відновлення функціонування - координація з пов'язаними планами	Координувати тестування плану забезпечення безперервної роботи та відновлення функціонування з організаційними підрозділами, що відповідають за реалізацію пов'язаних планів.	CP-4(1)	
108	Тестування плану забезпечення безперервної роботи та відновлення функціонування - альтернативна платформа тестування	Організація тестує план забезпечення безперервної роботи та відновлення функціонування на альтернативній платформі тестування: ознайомлює персонал з об'єктом та наявними ресурсами; оцінює можливості альтернативної платформи тестування для підтримки безперервної роботи.	CP-4(2)	
109	Альтернативне місце зберігання	1. Створити альтернативне місце зберігання, включно з необхідними угодами, що дозволяють зберігати та видавати інформацію резервного копіювання системи. 2. Переконатися, що в альтернативному місці зберігання впроваджені заходи захисту, аналогічні заходам захисту основної локації.	CP-6	
110	Альтернативне місце зберігання - відділення від первинного сховища	Визначити альтернативне місце зберігання, яке відокремлене від основного місця зберігання, щоб зменшити сприйнятливість до тих самих загроз.	CP-6(1)	
111	Альтернативне місце зберігання - час відновлення та встановлення цілей відновлення	Налаштувати альтернативне місце зберігання для полегшення операцій відновлення відповідно до часу відновлення та встановлених цілей відновлення.	CP-6(2)	
112	Альтернативне місце зберігання - доступність	Визначити потенційні проблеми доступності для альтернативного місця зберігання в разі збоїв або стихійних лих по всьому регіоні та в загальних рисах окреслити дії щодо пом'якшення наслідків.	CP-6(3)	

113	Альтернативний майданчик роботи	1. Створити альтернативний майданчик для роботи, включно з необхідними угодами, які дозволяють передачу та відновлення [призначення: визначених організацією операцій системи] для основних завдань і функцій у рамках [призначення: визначеного організацією періоду часу, відповідно термінам відновлення та встановленим цілям відновлення], коли можливості основного майданчика недоступні. 2. Забезпечити на альтернативному майданчику доступними для роботи інформацію, обладнання та прилади, необхідні для передачі та відновлення роботи або укласти контракти протягом встановленого організацією періоду часу для передачі та відновлення роботи. 3. Впровадити на альтернативному майданчику роботи заходи захисту, еквівалентні тим, що впровадженні на основному майданчику.	СР-7	
114	Альтернативний майданчик роботи - відділення від основного майданчика	Визначити альтернативний майданчик для роботи, який відокремлений від основного майданчика, з метою зменшення вразливості до тих самих загроз.	СР-7(1)	
115	Альтернативний майданчик роботи--доступність	Визначити потенційні проблеми доступності для альтернативного майданчика для роботи в разі збоїв або катастрофи по всьому регіону та окреслити чіткі заходи щодо пом’якшення наслідків.	СР-7(2)	
116	Альтернативний майданчик роботи - приоритет обслуговування	Розробити угоди про альтернативний майданчик для роботи, які містять положення щодо пріоритету обслуговування відповідно до вимог стосовно організаційної доступності (включно з вимогами щодо часу відновлення).	СР-7(3)	
117	Альтернативний майданчик роботи - підготовка до використання	Підготувати альтернативний майданчик для роботи таким чином, щоб майданчик був готовий до використання як оперативний майданчик, що підтримує виконання основних завдань і функцій.	СР-7(4)	
118	Електронні комунікаційні послуги	Впровадити альтернативні електорнні комунікаційні послуги, включно з необхідними угодами, що дозволять відновити [призначення: визначені організацією системні операції] для основних завдань і функцій у [призначення: визначений організацією період часу], коли основні можливості зв’язку недоступні на основному місці локації або розташовані на альтернативному майданчику для роботи чи зберігання.	СР-8	
119	Електронні комунікаційні послуги - пріоритет постачання послуг	1. Розробити основні та альтернативні угоди про надання електорнних комунікаційних послуг, які містять пріоритетні положення про надання послуг відповідно до вимог організаційної доступності (включно з вимогами щодо часу відновлення). 2. Надсилати запит про пріоритети електорнних комунікаційних послуг для всіх електорнних комунікаційних послуг, що використовуються для забезпечення безперервності роботи, якщо основні та/або альтернативні електорнні комунікаційні послуги надаються загальним оператором.	СР-8(1)	
120	Електронні комунікаційні послуги - єдині точки відпови	Отримати альтернативні електронні комунікаційні послуги з метою зменшення ймовірності спільного використання єдиної точки відмови з основними електронними комунікаційними послугами.	СР-8(2)	
121	Електронні комунікаційні послуги - відділення основних та альтернативних провайдерів	Отримувати альтернативні електронні комунікаційні послуги від постачальників, які відокремлені від основних постачальників послуг, щоб зменшити сприйнятливості до тихь самих загроз.	СР-8(3)	

122	Електронні комунікаційні послуги - план забезпечення безперервної роботи постачальника електронних комунікаційних послуг	1. Вимагати, щоб постачальники основних та альтернативних електронних комунікаційних послуг мали плани забезпечення безперервної роботи. 2. Переглядати плани забезпечення безперервної роботи постачальників електронних комунікаційних послуг для забезпечення відповідності планам забезпечення безперервної роботи організації. 3. Отримати свідчення про тестування планів забезпечення безперервної роботи та навчання постачальників електронних комунікаційних послуг [призначення: з визначеною організацією частотою].	CP-8(4)	
123	Резервне копіювання	1. Захистити конфіденційність резервної копії. 2. Впровадити криптографічні механізми для запобігання несанкціонованому розкриттю службової інформації в місцях зберігання резервних копій.	CP-9	a. 2- ий параметр: щонайменше щотижня або як визначено в плані дій у надзвичайних ситуаціях (за наявності) b. щонайменше щотижня або як визначено в плані дій у надзвичайних ситуаціях (за наявності) c. при створенні, отриманні, оновленні або як визначено в плані дій у надзвичайних ситуаціях (за наявності)
			CP-9(8)	
124	Резервне копіювання - випробування на надійність та цілісність	Тестувати носії резервних копій інформації [призначення: з визначеною організацією частотою] для перевірки надійності носіїв та цілісності інформації.	CP-9(1)	
125	Резервне копіювання - тестування відновлення з використанням зразків	Використовувати зразок резервної копії інформації при відновленні вибраних функцій системи як частину тестування плану забезпечення безперервної роботи та відновлення функціонування.	CP-9(2)	
126	Резервне копіювання - відокремлене сховище критичної інформації	Зберігати резервні копії [призначення: визначеного організацією критичного системного програмного забезпечення та іншої інформації, пов’язаної з безпекою] в окремому сховищі або у вогнестійкому контейнері, які не пов’язані із системою.	CP-9(3)	
127	Резервне копіювання - передача на альтернативне сховище зберігання	Перенести резервні копії інформації системи на альтернативне сховище [призначення: у визначений організацією період часу та швидкість передачі, відповідні часу відновлення та встановленим цілям відновлення].	CP-9(5)	
128	Відновлення та відтворення системи	Забезпечити відновлення та відтворення системи до відомого стану після збою, компрометації або помилок у межах [призначення: визначеного організацією періоду часу, відповідного часу відновлення та встановлених цілей відновлення].	CP-10	
129	Відновлення та відтворення системи - відновлення транзакцій	Реалізувати відновлення транзакцій для систем, що базуються на транзакціях.	CP-10(2)	
130	Відновлення та відтворення системи - відновлення в межах часового періоду	Забезпечити можливість відновлення компонентів системи в межах [призначення: визначеного організацією періоду відновлення] з інформації управління конфігурацією та захищеною цілісністю, яка описує відомий робочий стан компонентів.	CP-10(4)	
Ідентифікація та автентифікація				

131	Ідентифікація та автентифікація (користувачів організації)	1. Унікально ідентифікувати та автентифікувати користувачів організації і пов'язувати цю унікальну ідентифікацію з процесами, що діють від імені цих користувачів. 2. Повторно автентифікувати користувачів, коли [призначення: обставини або ситуації, що вимагають повторної автентифікації, визначені організацією].	IA-2, IA-11	
132	Ідентифікація та автентифікація (користувачів організації) – багатофакторна автентифікація привілейованих облікових записів	Упровадити багатофакторну автентифікацію для доступу до облікових записів системи.	IA-2(1), IA-2(2)	
133	Ідентифікація та автентифікація (користувачів організації) – індивідуальна автентифікація з груповою автентифікацією	Якщо використовуються спільні облікові записи або автентифікатори, вимагайте від користувачів індивідуальної автентифікації перед наданням доступу до спільних облікових записів або ресурсів.	IA-2(5)	
134	Ідентифікація та автентифікація (користувачів організації) – мережевий доступ до привілейованих облікових записів - окремий пристрій	Реалізація багатофакторної автентифікації для [вибір (один або кілька): локальний; мережевий; віддалений] доступ до [вибір (один або кілька): привілейовані облікові записи; непривілейовані облікові записи] такі, що: один із факторів забезпечується пристроєм, окремим від системи, який отримує доступ; пристрій відповідає [призначення: визначені організацією вимоги до міцності механізму].	IA-2(6)	
135	Ідентифікація та автентифікація (користувачів організації) – доступ до облікових записів – стійкість до відтворення	Упровадити механізми автентифікації, стійкі до повторного відтворення, для доступу до облікових записів у системі.	IA-2(8)	як мінімум привілейовані облікові записи
136	Ідентифікація та автентифікація (користувачів організації) – прийняття повноважень для верифікації сособистої інформації	Прийняти та електронним шляхом підтвердити повноваження облікових даних особистої ідентифікації.	IA-2(12)	
137	Ідентифікація та автентифікація пристроїв	Унікально ідентифікувати та автентифікувати пристрої перед встановленням з'єднання з системою.	IA-3	
138	Управління ідентифікацією	1. Отримати дозвіл від персоналу або ролей організації на призначення ідентифікатора особи, групи, ролі, служби або пристрою; вибрати та призначити ідентифікатор, який ідентифікує особу, групу, роль, службу або пристрій. 2. Запобігати повторному використанню ідентифікаторів для [призначення: період часу, визначений організацією]. 3. Унікально ідентифікувати статус кожної особи за допомогою ідентифікаційної характнристики.	IA-4 IA-4(4)	d. щонайменше рік для окремих осіб, груп, ролей

139	Управління автентифікатором	1. Перевіряти ідентичність особи, групи, ролі, служби або пристрою, які отримують автентифікатор під час початкового розповсюдження автентифікатора. 2. Встановити початковий вміст автентифікатора для всіх автентифікаторів, виданих організацією. 3. Створити та впровадити адміністративні процедури для початкового розподілу автентифікаторів для втрачених, скомпрометованих або пошкоджених автентифікаторів, а також для відкликання автентифікаторів. 4. Змінити автентифікатори за замовчуванням під час першого використання. 5. Змінювати або оновлювати автентифікатори періодично або коли відбуваються події: [призначення: події, визначені організацією]. 6. Захистити вміст автентифікатора від несанкціонованого розкриття та модифікації.	IA-5	f. 1-ий параметр: не більше 180 днів для паролів
140	Управління автентифікатором - Автентифікація на основі паролю	1. Вести перелік часто використовуваних, очікуваних або скомпрометованих паролів і періодично оновлювати його, а також у разі виникнення підозри, що паролі організації були скомпрометовано. 2. Перевіряти, коли користувачі створюють або оновлюють паролі, чи не містяться вони у списку загальновживаних, очікуваних або скомпрометованих паролів. 3. Передавати паролі тільки криптографічно захищеними каналами. 4. Зберігати паролі в криптографічно захищеному вигляді. 5. Встановити новий пароль при першому використанні після відновлення облікового запису. 6. Упровадити правила складу та складності паролів: [призначення: визначені організацією правила складу та складності].	IA-5(1)	a. щонайменше щоквартально h. 12-символьний набір з великих, малих літер, цифр та спеціальних символів, що включає принаймні по одному символу кожного регістру; змінювати принаймні 50% символів при створенні нових паролів
141	Управління автентифікатором - Автентифікація на основі відкритого ключа	1. Для автентифікації на основі відкритого ключа: забезпечити авторизований доступ до відповідного закритого ключа; зіставити автентифіковану особу з обліковим записом особи чи групи. 2. При використанні інфраструктури відкритого ключа (PKI): перевіряти сертифікати шляхом створення та перевірки шляху сертифікації до прийнятої довіреної прив'язки, включно з перевіркою інформації про статус сертифіката; впровадити локальний кеш даних для підтримки виявлення та перевірки шляху.	IA-5(2)	
142	Управління автентифікатором - захист автентифікаторів	Захищати автентифікатори відповідно з категорією безпеки інформації, до якої надає доступ використання автентифікатора.	IA-5(6)	
143	Управління автентифікатором - відсутність вбудованих незашифрованих статичних автентифікаторів	Переконатися, що незашифровані статичні автентифікатори не вбудовані в застосунки або сценарії доступу та не збережені на функціональній клавіші.	IA-5(7)	
144	Управління автентифікатором - багатосистемні облікові записи	Реалізувати [призначення: визначені організацією заходи безпеки] для управління ризиком компрометації через те, що користувачі мають облікові записи в декількох системах.	IA-5(8)	
145	Управління автентифікатором - закінчення терміну кешування автентифікаторів	Заборонити використання кешованих автентифікаторів після [призначення: визначеного організацією періоду часу].	IA-5(13)	
146	Управління автентифікатором - Менеджер паролів	1. Використовуйте [призначення: визначені організацією менеджери паролів] для створення та керування паролями; 2. Захистіть паролі за допомогою [призначення: елементи керування, визначені організацією].	IA-5(18)	
147	Послуги ідентифікації та автентифікації	Ідентифікувати та автентифікувати визначені надавачем системні служби та застосунки, перш ніж встановлювати зв'язок з пристроями, користувачами або іншими послугами чи застосунками.	IA-9	

148	Адаптивна автентифікація	Вимагати, щоб особи, які отримують доступ до системи, використовували [призначення: визначені організацією додаткові методи або механізми автентифікації] відповідно до конкретних [призначення: визначених організацієюобставин або ситуацій].	IA-10	
149	Зворотний зв'язок автентифікатора	Забезпечити прихований зворотний зв'язок автентифікаційної інформації під час процесу автентифікації.	IA-6	
150	Автентифікація криптографічного модуля	Впровадити механізми автентифікації в криптографічний модуль, який відповідає вимогам чинних законів, виконавчих розпоряджень, директив, політик, правил, стандартів та рекомендацій для такої автентифікації.	IA-7	
151	Ідентифікація та автентифікація (користувачі, що не належать до організації)	Унікально ідентифікувати та автентифікувати користувачів, що не належать до організації або процеси (що не належать організації), які діють від імені користувачів.	IA-8	
152	Повторна ідентифікація	Вимагати від користувачів повторної автентифікації, при [призначення: визначених організацією обставинах або ситуаціях, що вимагають повторної автентифікації].	IA11	
153	Перевірка справжності (ідентичності)	1) Засвідчити особи користувачів, яким потрібні облікові записи для логічного доступу до систем на основі вимог гарантій відповідного рівня, як це зазначено у відповідних стандартах і рекомендаціях. 2) Встановити ідентифікатори користувачів унікальні для особи. 3) Збирати, затверджувати та перевіряти докази (свідчення) ідентичності особи.	IA-12	
154	Перевірка справжності (ідентичності) - посвідчення особи	Вимагати пред'явлення до реєстраційного органу документів, що посвідчують особу.	IA-12(2)	
155	Перевірка справжності (ідентичності) - перевірка та верифікація доказів ідентичності	Вимагати, щоб надані докази ідентифікації були підтверджені та перевірені за допомогою [призначення: визначені організацією методи перевірки та верифікації].	IA-12(3)	
156	Перевірка справжності (ідентичності) - очна перевірка та ідентифікація	Вимагати, щоб підтвердження та перевірка посвідчень особи проводилися особисто в призначеному органі реєстрації.	IA-12(4)	
157	Перевірка справжності (ідентичності) - підтвердження адреси	Вимагати, щоб [вибір: реєстраційний код; повідомлення про перевірку] доставлялися через зовнішній канал для перевірки адреси (фізичної або цифрової) реєстрації користувачів.	IA-12(5)	
Реагування на інциденти				
158	Обробка інциденту	Упровадити систему реагування на інциденти, яка відповідає плану реагування на інциденти і передбачає підготовку, виявлення та аналіз, локалізацію, ліквідацію та відновлення інцидентів.	IR-4	
159	Обробка інциденту - автоматизовані процеси обробки інцидентів	Використовувати авто матизовані механізми для підтримки процесу обробкиінцидентів.	IR-4(1)	
160	Обробка інциденту - динамічна реконфігурація	Внести динамічну реконфігурацію [призначення: у визначені організацією системні компоненти] як частину здатності реагування на інциденти [призначення: типи динамічної реконфігурації, визначені організацією].	IR-4(2)	
161	Обробка інциденту - безперервність операції	Ідентифікувати [призначення: визначені організацією класи інцидентів] та [призначення: визначені організацією дії, які необхідно вжити у відповідь згідно з класом інциденту] для забезпечення безперервності виконання завдань та функцій організації.	IR-4(3)	

162	Обробка інциденту - інформаційна кореляція	Зіставляти інформацію про інцидент та про індивідуальне реагування на інцидент з метою досягнення загальноорганізаційного бачення на обізнаність про інциденти та реагування на них.	IR-4(4)	
163	Обробка інциденту - внутрішні загрози - особливі можливості	Реалізувати можливість обробки інцидентів, пов’язаних з внутрішніми загрозами.	IR-4(6)	
164	Інтегроана група на реагування на інцидент	Утворити та підтримувати інтегровану групу працівників організації з реагування на інциденти, яку можна розгорнути в будь-якому місці та за певний період часу, визначенеми	IR-4(11)	
165	Моніторинг інциденту	1. Відстежувати та документувати інциденти, пов'язані з безпекою системи. 2. Повідомляти про підозрілі інциденти до служби реагування на інциденти в організації протягом часу [призначення: період часу, визначений організацією]. 3. Повідомити інформацію про інцидент [призначення: органи, визначені організацією]. 4. Забезпечити ресурс підтримки реагування на інциденти, який пропонує поради та допомогу користувачам системи щодо обробки та звітування про інциденти.	IR-5	
			IR-6	a. 2 години
			IR-7	
166	Моніторинг інциденту- автоматизоване відстеження, збір даних і аналіз	Відстежувати інциденти, збирати й аналізувати інформацію про інциденти за допомогою [призначення: автоматизовані механізми, визначені організацією].	IR-5(1)	
167	Звітність про інциденти - автоматичне звітування	Повідомляйте про інциденти за допомогою [призначення: автоматизовані механізми, визначені організацією].	IR-6(1)	
168	Звітність про інциденти - координація ланцюжка постачання	Надати інформацію про інциденти безпеки та приватності постачальнику продукту або послуги та іншим організаціям, які беруть участь у ланцюжку постачання систем або компонентів системи, пов’язаних з інцидентом.	IR-6(3)	
169	Підтримка реагування на інцифенти - атоматизація підтримки для забезпечення доступності інформації та підтримки	Впровадити автоматизовані механізми [призначення: автоматизовані механізми, визначені організацією] для збільшення доступності пов’язаної з реагуванням на інциденти інформації та підтримки.	IR-7(1)	
170	Перевірка реагувань на інциденти	Періодично перевіряти ефективність системи реагування на інциденти.	IR-3	
171	Перевірка реагувань на інциденти - координація з пов’язаними планами	Координувати тестування реагування на інциденти з елементами організаці, що відповідають за пов’язані плани.	IR-3(2)	
172	Навчання з реагування на інциденти	1. Проводити навчання з реагування на інциденти для користувачів системи відповідно до призначених ролей та обов'язків: протягом [призначення: період часу, визначений організацією] з моменту прийняття на себе ролі чи відповідальності за реагування на інцидент або отримання доступу до системи; коли цього вимагають зміни в системі [призначення: частота, визначена організацією] надалі. 2. Переглядати та оновлювати зміст навчання з реагування на інциденти [призначення: періодичність, визначена організацією] та наступні [призначення: події, визначені організацією].	IR-2	a.1: 30 робочих днів a.3: щонайменше щороку b. 1-ий параметр: щонайменше щороку
173	Навчання з реагування на інциденти - моделювання подій	Впровадити в процес навчання моделювання події реагування на інциденти для забезпечення ефективного реагування персоналу в кризових ситуаціях.	IR-2(1)	

174	Навчання з реагування на інциденти - автоматизовані навчальні середовища	Забезпечте навчальне середовище реагування на інциденти, використовуючи [призначення: автоматизовані механізми, визначені організацією].	IR-2(2)	
175	План реагування на інциденти	1. Розробити план реагування на інцидент, який: надає організації план дій для реалізації її описує структуру та організацію системи реагування на інциденти, забезпечує високорівневий підхід до того, як спроможність реагування на інциденти вписується в загальну структуру організації, визначає інциденти, про які необхідно повідомляти, вирішує питання обміну інформацією про інциденти, і розподіляє обов'язки між структурними підрозділами, персоналом або ролями. 2. Розповсюдити копії плану реагування на інцидент серед призначеного персоналу, відповідального за реагування на інцидент (ідентифікованого за іменами та/або за ролями), та організаційних елементів. 3. Оновлювати план реагування на інциденти з урахуванням змін в системі та організації або проблем, що виникли під час впровадження, виконання або тестування плану. 4. Захистити план реагування на інциденти від несанкціонованого розголошення.	IR-8	b. весь персонал, який має роль або відповідальність за впровадження плану реагування на інциденти; d. весь персонал, який має роль або відповідальність за впровадження плану реагування на інциденти
176	Реагування на витік інформації	Реагувати на витік інформації шляхом: призначення [призначення: персонал або ролі, визначені організацією] відповідального за реагування на витік інформації; визначення конкретної інформації, пов'язаної з джерелом витоку в системі; попередження [призначення: визначеного організацією персоналу або ролей] про витік інформації за допомогою методу зв'язку, не пов'язаного з витоком; ізолювання системи або системної компоненти, де відбувся витік інформації; видалення інформації із системи або компонента; визначення іншої системи або компонента системи, які згодом могли б бути джерелом витоку інформації; виконання таких додаткових дій: [призначення: визначених організацією дій].	IR-9	
177	Реагування на витік інформації - тренування	Забезпечити навчання з реагування на витік інформації [призначення: з визначеною організацією частотою].	IR-9(2)	
178	Реагування на витік інформації - робота після витоку	Реалізувати [призначення: визначені організацією процедури] з метою забезпечення, щоб персонал організації, на який впливає витік інформації, був спроможний продовжувати виконувати поставлені завдання, тоді як постраждалі системи зазнають коригувальних дій.	IR-9(3)	
179	Реагування на витік інформації - викриття неавторизованого персоналу	Застосовуйте [призначення: визначені організацією механізми захисту] для персоналу, що має доступ до інформації, яка не відповідає призначеним правам доступу.	IR-9(4)	
Технічне обслуговування				
180	Контрольоване обслуговування	1. Планувати, документувати та переглядати записи з технічного обслуговування, ремонту або заміни компонентів системи відповідно до вимог виробника та постачальників та/або вимог організації. 2. 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. 3. 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. 4. Очищати обладнання з погляду видалення всієї інформації з носіїв до вилучення обладнання організації для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації. 5. Перевірити всі потенційно порушені заходи захисту, щоб переконатися, що вони, як і раніше, працюють належним чином після дій з обслуговування, ремонту або заміни. 6. Вносити [призначення: визначену організацією інформацію, пов'язану з технічним обслуговуванням] до записів з технічного обслуговування.	MA-2	

181	Контрольоване обслуговування - автоматизована технічна діяльність	1. Використовувати автоматизовані механізми для планування, проведення та документування дій з обслуговування, ремонту та заміни системи або її компонентів. 2. Надавати оновлені, точні та повні записи про всі дії з технічного обслуговування, ремонту та заміни; замовлених, запланованих, виконуваних та завершених дій.	MA-2(2)	
182	Інструменти для обслуговування	1. Затверджувати, контролювати та відстежувати використання інструментів технічного обслуговування системи. 2. Перевіряти інструменти для технічного обслуговування на наявність неналежних або несанкціонованих модифікацій. 3. Запобігати вилученню обладнання для обслуговування системи, що містить службову інформацію, що надається організаціям, у яких вони виконують функції управління щодо інформації, шляхом перевірки відсутності службової інформації наобладнанні, санітарної обробки або знищення обладнання, або утримання обладнання в межах об'єкта.	MA-3 MA-3(1) MA-3(2) MA-3(3)	b. щонайменше щороку
183	Віддалене обслуговування	1. Затверджувати та контролювати віддалені сеанси з технічного обслуговування та діагностики;упровадити багатофакторну автентифікацію та стійкість до повторного відтворення при створенні віддалених сеансів технічного обслуговування та діагностики. 2. Забезпечити завершення сеансу та мережевих з'єднань після завершення віддаленого технічного обслуговування.	MA-4	
184	Віддалене обслуговування - порівняльна безпека та очищення	1. Вимагати, щоб віддалені послуги з обслуговування та діагностики виконувалися із системи, яка реалізує заходи безпеки і які можна порівняти із заходами, реалізованими в системі, що обслуговується. 2. Видалити компонент, який підлягає обслуговуванню, із системи до віддаленого обслуговування або діагностичних послуг; очистити компонент (від інформації, що належить організації) після того, як обслуговування виконано, перевірити та очистити компонент (від потенційно шкідливого програмного забезпечення) перед тим, повторним підключенням компонентів до системи.	MA-4(3)	
185	Технічний персонал	1. Встановити процес авторизації персоналу з технічного обслуговування. 2. Вести список уповноважених організацій або персоналу з технічного обслуговування; переконатися, що персонал без супроводу, який виконує технічне обслуговування системи, має необхідні дозволи на доступ. 3. Призначити персонал організації з необхідними повноваженнями доступу та технічною компетентністю для нагляду за діяльністю персоналу з технічного обслуговування, який не має необхідних повноважень доступу.	MA-5	
186	Технічний персонал - особи без належного доступу	1. Реалізувати процедури залучення персоналу з технічного обслуговування, який не має відповідних дозволів (допуску) або не є громадянами України, які (процедури) містять такі вимоги: обслуговуючий персонал, що не має необхідних прав доступу, рівня допуску, або офіційного затвердженого доступу, повинен супроводжуватися та бути під наглядом уповноваженого організацією персоналу, з необхідним рівнем допуску, а також мати відповідну технічну кваліфікацію для виконання технічного обслуговування та діагностичних заходів у системі; перед тим, як розпочати технічне обслуговування або діагностику персоналом, який не має необхідних прав допуску, рівня допуску або офіційного затвердженого доступу, упевнитися, що всі компоненти енергонезалежного зберігання інформації в системі очищуються, а всі енергонезалежні носії видаляються або фізично відключаються від системи та надійно захищаються. 2. Розробити та впровадити альтернативні заходи безпеки, якщо компонент системи не може бути очищено, вилучено або відключено від системи.	MA-5(1)	
187	Своєчасне обслуговування	Отримати технічну підтримку та/або запасні частини для [призначення: визначених організацією компонентів системи] в межах [призначення: визначеного організацією періоду часу] у разі відмови.	MA-6	
Захист носіїв інформації				

188	Доступ до носіїв інформації	Обмежити доступ до [призначення: визначених організацією типів цифрових та/або нецифрових носіїв інформації] [призначення: визначеним організацією персоналом або ролями].	MP-2	1-ий параметр: всі типи цифрових та/або нецифрових носіїв, що містять інформацію, не дозволену для публічного оприлюднення
189	Маркування носіїв інформації	Наносити маркування на носії інформації, що: вказує на обмеження щодо поширення, обробки та доступу до інформації, яка зберігається або передається на цих носіях; містить застереження та мітки безпеки, якщо інформація підлягає спеціальному захисту згідно із законодавством, політиками організації або вимогами класифікації.	MP-3	носії інформації на яких зберігаються, обробляються дані публічних користувачів та/або об'єтів критичної інфраструктури
190	Зберігання носіїв інформації	Фізично контролювати та безпечно зберігати [призначення: визначені організацією типи цифрових та/або нецифрових носіїв інформації] в межах [призначення: визначених організацією контрольованих зон]. Захищати такі системні носії, які визначені організацією до того часу, як носії знищуються або очищаються, з використанням затвердженого обладнання, методів та процедур.	MP-4	носії інформації на яких зберігаються, обробляються дані публічних користувачів та/або об'єтів критичної інфраструктури
191	Транспортування носіїв інформації	1. Захистити і контролювати носії інформації під час транспортування за межі контрольованих територій. 2. Вести облік носіїв інформації під час транспортування за межі контрольованих територій. 3. Документувати дії, пов'язані з транспортуванням системних носіїв.	MP-5, SC-28	носії інформації на яких зберігаються, обробляються дані публічних користувачів та/або об'єтів критичної інфраструктури
192	Знищення інформації на носіях інформації	1. Очищувати [призначення: визначені організацією системні носії] перед утилізацією, випуском за межі організаційного контролю, або перед повторним використанням [призначення: методами та процедурами очищення, визначеними організацією]. 2. Використовувати механізми очищення зі стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації.	MP-6	
193	Знищення інформації на носіях інформації	1. Переглядати, затверджувати, відстежувати, документувати та перевіряти очищення носіїв інформації та дії з їх утилізації. 2. Перевіряти обладнання та процедури для очищення [призначення: з визначеною організацією частотою], щоб переконатися в досягненні запланованого очищення. 3. Застосовувати методи неруйнівного очищення до портативних запам'ятовувальних пристроїв перед підключенням таких пристроїв до системи за наступних обставин: [призначення: визначених організацією умов, що вимагають очищення портативних запам'ятовувальних пристроїв].	MP-6(1) MP-6(2) MP-6(3)	
194	Використання носіїв інформації	1. Обмежити або заборонити використання [призначення: типи носіїв інформації, визначені організацією]. 2. Заборонити використання знімних носіїв інформації без ідентифікованого власника.	MP-7	
Кадрова безпека				
195	Звільнення персоналу. Переведення персоналу	1. Коли припиняється індивідуальна трудова діяльність: заборонити доступ до системи протягом [призначення: період часу, визначений організацією]; припинити дію або відкликати автентифікатори та облікові записи, пов'язані з особою; відновити властивості системи, пов'язані з безпекою. 2. Коли працівників призначають або переводять на інші посади в організації: переглянути та підтвердити поточну оперативну потребу в поточних логічних і фізичних дозволах доступу до системи та об'єкта; ініціювати [призначення: дії з переведення або призначення, визначені організацією] протягом [призначення: період часу після дії з переведення або призначення, визначений організацією]; змінювати авторизацію доступу відповідно до будь-яких змін в оперативних потребах.	PS-4	a. у разі добровільного звільнення - якомога швидше, але не більше ніж за 5 робочих днів; у разі примусового звільнення - у той самий день, що й припинення трудових відносин
			PS-5	b. 1-ий параметр: дії з перепризначення, щоб забезпечити видалення або вимкнення всіх системних доступів, які більше не потрібні
196	Звільнення персоналу - автоматизоване сповіщення	Впровадити автоматизовані механізми для повідомлення [призначення: визначеного організацією персоналу або ролей] після звільнення особи.	PS-4(2)	
197	Визначення посадового ризику	1. Визначити ризики для всіх посад організації. 2. Встановити критерії відбору осіб, які заміщують ці посади. 3. Переглядати та оновлювати посадові ризики.	PS-2	

198	Перевірка персоналу	1. Перевіряти окремих осіб перед дозволом на доступ до інформаційної системи. 2. Переглядати окремих осіб відповідно до визначених умов, що вимагають перегляду, та якщо це визначено необхідною частотою повторного перегляду.	PS-3	
199	Перевірка персоналу - інформація, що потребує додаткових заходів захисту	Переконатися, що особи, які звертаються до ІС та які зберігають, обробляють або передають інформацію, що потребує додаткових заходів захисту: мають чинний дозвіл на доступ, який відповідає законам, наказам, настановам, директивам тощо; задовольняють [призначення: визначені організацією додаткові критерії відбору персоналу].	PS-3(3)	
200	Переведення персоналу	1. Переглядати та підтверджувати поточну оперативну потребу в поточних дозволах логічного та фізичного доступу до систем і об'єктів, коли особи перепризначаються або переводяться на інші посади в організації. 2. Змінювати повноваження доступу, якщо це необхідно, щоб відповідати будь-яким змінам операційної потреби через перепризначення або переведення. 3. Повідомляти про переведення персоналу в рамках визначеного періоду часу.	PS-5	
201	Угоди про доступ	1. Розробити та оформити угоди про доступ до інформаційних систем організації. 2. Переглядати та оновлювати угоди про доступ [призначення: з визначеною організацією частотою]. 3. Переконатися, що особи, які потребують доступу до організаційної інформації та систем: підписали відповідні угоди про доступ перед тим, як отримати доступ; повторно підписали угоди про доступ для підтримки доступу до інформаційних систем організації, коли угоди про доступ були оновлені або [призначення: з визначеною організацією частотою].	PS-6	
202	Безпека зовнішнього персоналу	1. Встановити вимоги щодо безпеки персоналу, включно з ролями й обов'язками щодо безпеки для зовнішніх постачальників послуг. 2. Вимагати від зовнішніх постачальників дотримання правил і процедур кадрової безпеки, встановлених організацією. 3. Вимагати від зовнішніх постачальників повідомляти щодо будь-яких переведень або звільнення зовнішнього персоналу, який володіє організаційними повноваженнями або має системні привілеї в межах визначеного строку. 4. Контролювати відповідності постачальника визначеним вимогам щодо безпеки інформації.	PS-7	
203	Кадрові санкції	1. Використовувати формальний процес санкцій для осіб, які не дотримуються встановлених правил і процедур інформаційної безпеки. 2. Повідомляти [призначення: визначений організацією персонал або ролі] в межах [призначення: визначеного організацією періоду часу], коли починається офіційний процес накладання санкцій працівникам, визначаючи особу та причину санкції.	PS-8	
204	Опис позицій	Включіть ролі й обов'язки з безпеки та приватності в опис посади в організації.	PS-9	
Фізичний захист і захист робочого середовища				
205	Авторизація фізичного доступу	1. Розробити, затвердити та підтримувати список осіб, які мають право доступу до фізичного місця розташування системи. 2. Надавати повноваження для доступу до об'єкта; періодично перевіряти список фізичного доступу. 3. Переглядати список доступу до об'єктів [призначення: частота, визначена організацією]. 4. Видаляти осіб зі списку фізичного доступу,коли доступ більше не потрібен.	PE-2	c. щонайменше щороку
206	Моніторинг фізичного доступу	1. Моніторити фізичний доступ до місця розташування системи, щоб виявляти та реагувати на інциденти фізичної безпеки. 2. Періодично переглядати журнали фізичного доступу.	PE-6	b. 1-ий параметр: щонайменше кожні 90 днів
207	Моніторинг фізичного доступу	1. Здійснювати моніторинг фізичного доступу до об'єкта, де розміщується система, використовуючи засоби сигналізації та обладнання для спостереження. 2. На додаток до моніторингу фізичного доступу до об'єкта здійснювати моніторинг фізичного доступу до системи в [призначення: визначені організацією фізичні приміщення, що містять один або більше компонентів системи].	PE-6(1) PE-6(4)	
208	Керування фізичним доступом	1. Контролювати фізичний доступ до розподільчих ліній системи і ліній електропередач на об'єктах організації.	PE-4	

209	Керування фізичним доступом - межі об'кту та системи	1. Застосовувати авторизацію фізичного доступу до системи на додаток до керування фізичного доступу до об'єкта в [призначення: визначені організацією фізичні приміщення, що містять один або більше компонентів системи]. 2. Забезпечити цілодобову безперервну охорону для контролю доступу [призначення: визначені організацією фізичні точки доступу] до об'єкта, де перебуває система.	PE-3(1) PE-3(3)	
210	Контроль доступу до джерел і ліній електроживлення. Контроль доступу до пристроїв виведення інформації	1. Контролювати фізичний доступ до місця, де знаходиться система: перевіряти індивідуальні фізичні дозволи на доступ перед наданням доступу; контролювати вхід і вихід за допомогою систем/пристроїв фізичного контролю доступу або охоронців. 2. Вести журнали контролю фізичного доступу для точок входу та виходу. 3. Супроводжувати відвідувачів і контролювати їхню діяльність. 4. Забезпечити захист ключів, кодів доступу та інших пристроїв фізичного доступу. 5. Контролювати фізичний доступ до пристроїв виводу, щоб запобігти доступу сторонніх осіб до службової інформації.	PE-3 PE-5	
211	Реєстр доступу відвідувачів	1. Вести реєстр доступу відвідувачів до об'єкта, де перебуває система. 2. Переглядати реєстр доступу відвідувачів з визначеною частотою. 3. Повідомляти про порушення в реєстрі відвідувачів. 4. Впровадити автоматизовані механізми для ведення та перегляду (аналізу) реєстру відвідувачів.	PE-8, PE-8(1)	
212	Енергетичне обладнання та кабелі	Захищати енергетичне обладнання і силові кабелі системи від пошкоджень і руйнувань	PE-9	
213	Аварійне відключення	1. Забезпечити можливість відключення системи або окремих компонентів системи від живлення в надзвичайних ситуаціях. 2. Встановити перемикачі або пристрої аварійного відключення в [призначення: визначені організацією місця розташування в системі або в компоненті системи] для забезпечення безпечного та легкого доступу персоналу. 3. Захищати механізми (систему) аварійного відключення живлення від несанкціонованої активації.	PE-10	
214	Аварійне енергозабезпечення	1. Впровадити тимчасове джерело безперебійного живлення для забезпечення живлення в разі втрати первинного джерела живлення. 2. Забезпечити для системи наявність довгострокового альтернативного джерела живлення, яке може підтримувати мінімально необхідну експлуатаційну спроможність у разі тривалої втрати первинного джерела живлення.	PE-11 PE-11(1)	
215	Аварійне освітлення	Використовувати та підтримувати системи автоматичного аварійного освітлення, які активуються в разі відключення електроживлення або збою та які охоплюють аварійні виходи та маршрути евакуації всередині об'єкта.	PE-12	
216	Протипожежний захист	Використовувати та підтримувати в працездатньому стані пристрої та системи пожежогасіння й виявлення пожежі. Забезпечити роботу систем протипожежного захисту незалежним джерелом живлення.	PE-13	
217	Протипожежний захист - пристрої та системи виявлення	Використовувати такі пристрої/системи для виявлення пожежі в системі, які активуються автоматично та повідомляють [призначення: визначені організацією персонал або посадові особи] та [призначення: визначену організацією аварійну команду] у разі пожежі.	PE-13(1)	
218	Протипожежний захист - пристрої та системи автоматичного пожежогасіння	1. Використовувати такі пристрої/системи пожежогасіння для системи, які забезпечують автоматичне сповіщення про будь-яку активацію [призначення: визначені організацією персонал або ролі] і [призначення: визначену організацією аварійну команду]. 2. Впровадити системи та засоби автоматичного гасіння пожежі, коли об'єкт не укомплектований відповідним персоналом на постійній основі.	PE-13(2)	
219	Контроль температури та вологості	1. Підтримувати температуру та вологість у приміщенні, де розташована система в рамках визначеного організацією рівня. 2. Контролювати рівні температури та вологості з визначеною частотою.	PE-14	

220	Захист від пошкодження водою	1. Забезпечити захист інформаційної системи від пошкоджень, що виникають у разі витоку води, використовуючи відповідні ізоляційні або запірні клапани. 2. Впровадити автоматизовані механізми виявлення води поблизу інформаційної системи та оповіщення [призначення: визначеного організацією персоналу або ролей].	PE-15 PE-15(1)	
221	Доставка та видалення	1. Проводити авторизацію, моніторинг і контроль [призначення: визначені організацією типи компонентів інформаційної системи], що входять і виходять з об'єкта. 2. Вести облік цих елементів.	PE-16	
222	Альтернативне робоче місце	1. Визначити альтернативні робочі місця, дозволені для використання працівниками. 2. Застосовувати дії безпеки на альтернативних робочих місцях [призначення: дії безпеки, визначені організацією].	PE-17	
223	Розташування компонентів системи	Встановити компоненти інформаційної системи на об'єкті, з метою мінімізації потенційної шкоди від [призначення: визначеної організацією фізичної та екологічної небезпеки], та мінімізації можливості несанкціонованого доступу.	PE-18	
224	Маркування компонентів	Позначати апаратні компоненти, що вказують рівень впливу або класифікацію інформації, яка дозволена для обробки, зберігання або передачі з використанням апаратних компонентів.	PE-22	
Оцінка ризику				
225	Категоріювання безпеки	1. Здійснити категоріювання інформаційної системи й інформації, яку вона обробляє, зберігає та передає. 2. Задокументувати результати категоріювання безпеки, включно з обґрунтуванням, у плані захисту інформаційної системи. 3. Підтвердити, що посадова особа або уповноважений офіційний представник переглядає та затверджує рішення про категоріювання безпеки.	RA-2	
226	Оцінювання ризику	1. Оцінити ризик несанкціонованого розголошення в результаті обробки, зберігання або передачі інформації, яку вона обробляє, зберігає та передає; а також будь-якої пов'язаної інформації. 2. Оновлювати оцінки ризиків [призначення: з визначеною організацією частотою].	RA-3 RA-3(1) SR-6	d., f. щонайменше щороку b. щонайменше раз на рік щонайменше раз на рік або за потребою у зв'язку з певними подіями
227	Сканування вразливостей	1. Моніторити та сканувати систему на наявність вразливостей [призначення: частота, визначена організацією] та при виявленні нових вразливостей, що впливають на систему. 2. Усунути вразливості системи протягом часу [призначення: час на реагування, визначений організацією]. 3. Оновлювати вразливості системи, що підлягають скануванню [призначення: частота, визначена організацією], а також при виявленні нових вразливостей і повідомляти про них.	RA-5 RA-5(2)	a. щонайменше кожні 30 днів протягом 24 годин до запуску сканування
228	Сканування вразливостей - широта та глибина покриття	Запровадити процедури сканування вразливостей, які дозволять визначити широту й глибину покриття.	RA-5(3)	
229	Сканування вразливостей - привілейований доступ	Реалізувати авторизацію привілейованого доступу до [призначення: визначених організацією компонентів системи] для [призначення: визначеної організацією діяльності з виявлення вразливостей].	RA-5(5)	
230	Сканування вразливостей - оглядсжурналів аудиту за минулі періоди	Переглядати журнали аудиту за минулі періоди, щоб визначити, чи була вразливість, яка виявлена в [призначення: системі, визначеній організацією], була використана до її виявлення протягом [призначення: визначеного організацією періоду часу].	RA-5(8)	
231	Сканування вразливостей - програма публічного оприлюднення	Встановіть публічний канал для отримання повідомлень про вразливості в системах організації і компонентах системи.	RA-5(11)	
232	Реагування на ризик	Реагувати на результати оцінювання, моніторингу й аудиту безпеки та приватності.	RA-7	
233	Аналіз критичності	Визначити критичні компоненти інформаційної системи та функції, виконавши аналіз критичності для [призначення: визначених організацією систем, компонентів системи або послуг для системи] в [призначення: визначенні організацією точки ухвалення рішень у життєвому циклі розробки системи].	RA-9	
Оцінювання, акредитація та моніторинг безпеки				

234	Оцінювання	1. Оцінювати дії [призначення: частота, визначена організацією] до безпеки системи та середовища її функціонування, щоб визначити, чи були ці дії виконанні. 2. Залучати незалежних експертів або групи з оцінювання для проведення оцінювання безпеки та приватності.	CA-2 CA-2(1)	d. щонайменше щороку
235	Оцінювання - зовнішні організації	Використовуйте результати контрольного оцінювання, які виконує [призначення: зовнішня організація, визначена організацією] на [призначення: система, визначена організацією], коли оцінювання відповідає [завдання: вимоги, визначені організацією].	CA-2(3)	
236	План усунення недоліків та контрольні показники	1. Розробити план дій і контрольні показники для системи: задокументувати заплановані заходи з виправлення слабких місць або недоліків, виявлених під час оцінювання безпеки; зменшити або усунути відомі недоліки системи. 2. Періодично оновлювати існуючий план дій і показників на основі результатів оцінки безпеки, незалежних аудитів або оглядів, а також безперервного моніторингу.	CA-5	
237	Акредитація	1. Призначити старшого керівника, який відповідає за систему. 2. Призначити старшого керівника, відповідального за систему, та будь-які загальні заходи захисту, успадковані системою. 3. Переконатися перед початком функціонування системи, що посадова особа: акредитує загальні заходи захисту, що успадковані системою; акредитує систему на функціонування за призначенням. 4. Переконайтеся, що посадова особа, яка акредитує засоби захисту, дозволяє використання цих засобів захисту для успадкування організаційними системами. 5. Оновлювати акредитацію [призначення: з визначеною організацією частотою].	CA-6	
238	Безперервний моніторинг	1. Розробити та впровадити стратегію безперервного моніторингу на рівні системи, що передбачає постійний моніторинг та оцінку безпеки. 2. Залучити незалежних експертів або групи з оцінювання, щоб постійно спостерігати за заходами захисту в системі. 3. Забезпечити моніторинг ризиків, що є невід'ємною частиною стратегії постійного моніторингу та включає: моніторинг ефективності; моніторинг відповідності; моніторинг змін. 4. Забезпечити точність, актуальність і доступність результатів моніторингу для системи за допомогою автоматизованих механізмів.	CA-7 CA-7(1) CA-7(4) CA-7(6)	
239	Взаємодія систем	Затвердити та керувати обміном конфіденційної інформації між системою та іншими системами, використовуючи [вибір (один або декілька): угоди про безпеку з'єднання; угоди про безпеку обміну інформацією; меморандуми або угоди про взаєморозуміння; угоди про рівень обслуговування; угоди з користувачами; угоди про нерозголошення інформації]; документувати характеристики інтерфейсу, вимоги до безпеки та обов'язки для кожної системи як частину договорів про обмін; періодично переглядати та оновлювати договори про обмін.	CA-3	
240	Взаємодія систем - передача дозволів	Переконатися, що особи або системи, які передають дані між взаємопов'язаними системами, мають необхідні повноваження (тобто дозволи на запис або привілеї), до прийняття таких даних.	CA-3(6)	
241	Внутрішні з'єднання ситсеми	1. Авторизувати внутрішні підключення [призначення: системні компоненти або класи компонентів, що організація визначила] до системи. 2. Задокументувати, для кожного внутрішнього з'єднання, характеристики інтерфейсу, вимоги безпеки та приватності, а також характер переданої інформації. 3. Розірвати внутрішні системні підключення після [призначення: умови, визначені організацією]. 4. Переглядати [призначення: частота, визначена організацією] постійну потребу в кожному внутрішньому з'єднанні.	CA-9	
242	Тестування на проникнення	Проводити тестування на проникнення з [призначення: визначеною організацією частотою] у [призначення: визначеній організацією інформаційній системі чи системному компоненті].	CA-8	
Захист інформаційної системи та комунікацій				
243	Розділення функцій	Розділяти функціональність користувача, включно зі службами, що призначені для користувача інтерфейсу, від функціональності системного управління.	SC-2	

244	Ізоляція функції безпеки	Надавач повинен ізолювати функції безпеки від інших функцій.	SC-3	
245	Інформація в загальних ресурсах системи	Запобігати несанкціонованій і ненавмисній передачі інформації за допомогою загальних ресурсів системи.	SC-4	
246	Захист від атак «відмова в обслуговуванні»	1. Обмежити наслідки наступних типів подій відмови в обслуговуванні (DoS). 2. Застосувати наступні заходи захисту для досягнення мети відмови обслуговування.	SC-5	
247	Захист периметра	1. Контролювати та управляти зв'язком на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи; реалізувати підмережі для загальнодоступних компонентів системи, які фізично або логічно відділені від внутрішніх мереж. 2. Підключатися до зовнішніх мереж тільки через керовані інтерфейси, що складаються з пристроїв захисту периметра, розташованих відповідно до архітектури безпеки організації.	SC-7	
248	Захист периметра - точки доступу	Обмежити кількість зовнішніх мережевих підключень до системи.	SC-7(3)	
249	Захист периметра - зовнішні комунікаційні служби	1. Запровадити керований інтерфейс для кожної зовнішньої комунікаційної служби. 2. Створити політику управління трафіком для кожного керованого інтерфейсу. 3. Забезпечити конфіденційність та цілісність інформації, що передається через кожний інтерфейс. 4. Документувати кожне виключення з політики управління трафіком за допомогою підтримки завдань / потреби та тривалості цієї потреби. 5. Переглянути виключення з політики управління трафіком [призначення: визначення організацією частота] та видалити виключання, які більше не явно підтримуються цілями. 6. Запобігти несанкціонованому обміну трафіком управління із зовнішніми мережами. 7. Публікувати інформацію, щоб дозволити віддаленим мережам виявляти несанкціонований трафік керування з внутрішніх мереж. 8. Фільтрувати несанкціонований трафік керування із зовнішніх мереж.	SC-7(4)	
250	Захист периметра - Відмова за замовчуванням - Дозвіл за винятком	Заборонити трафік мережевих комунікацій за замовчуванням і дозволити трафік мережевих комунікацій за винятком.	SC-7(5)	
251	Захист периметра - запобігання поділу тунелювання для віддалених пристроїв	Запобігати розділеному тунелюванню для віддалених пристроїв, які підключаються до систем організації, якщо розділений тунель не убезпечений за допомогою [призначення: визначені організацією заходи безпеки].	SC-7(7)	
252	Захист периметра - маршрутизація з автефікованих проксі-серверів	Здійснювати маршрутизацію [призначення: визначений організацією внутрішній трафік комунікацій] до [призначення: визначені організацією зовнішні мережі] через автентифіковані проксі-сервери на керованих інтерфейсах.	SC-7(8)	
253	Захист периметра - запобігання ексфільтрації	1. Запобігати ексфільтрації інформації. 2. Проводити тести на ексфільтрацію [призначення: визначена організацією частота].	SC-7(10)	
254	Захист периметра - захист на основі хосту	Реалізувати [призначення: визначені організацією механізми захисту периметру на основі хосту] в [призначення: визначені організацією компоненти системи].	SC-7(12)	
255	Захист периметра - збій у безпеці	Запобігати входу систем у незахищені стани в разі аварійного завершення роботи пристрою захисту периметра.	SC-7(18)	
256	Захист периметра - динамічна ізоляція та відокремлення	Надавати можливість динамічно ізолювати або відокремлювати [призначення: визначені організацією системні компоненти] від інших компонентів системи.	SC-7(20)	
257	Захист периметра - ізоляція компонентів системи	Впровадити механізми захисту периметра, щоб відокремити [призначення: визначений організацією компонент системи], що підтримує [призначення: визначені організацією цілі та/або функції].	SC-7(21)	

258	Конфіденційність і цілісність передачі	1. Реалізувати механізми криптографічного захисту для [Вибір (один або більше): запобігання несанкціонованому розкриттю інформації; вияву зміни в інформації] під час передачі. 2. Забезпечити [вибір (один або кілька): конфіденційність; цілісність] інформації, що передається.	SC-8	
			SC-8(1)	запобігати несанкціонованому розголошенню інформації та виявляти зміни в ній
259	Захист інформації у стані спокою	1. Забезпечити [вибір (один або кілька): конфіденційність; цілісність] [призначення: визначена організацією інформація] в стані спокою. 2. Впровадити криптографічні механізми для запобігання несанкціонованому розкриттю та модифікації [призначення: визначена організацією інформація] у стані спокою на [призначення: визначені організацією компоненти системи].	SC-28	1-ий параметр: конфіденційність та цілісність 2-ий параметр: вся інформація
			SC-28(1)	1-ий параметр: вся інформація 2-ий параметр: всі компоненти системи та носії інформації
260	Відключення мережі	Завершити з'єднання з мережею, яке пов'язане із сеансом зв'язку в кінці сеансу або після періоду бездіяльності.	SC-10	не більше 15 хвилин
261	Встановлення та управління криптографічними ключами, доступність	1. Встановити криптографічні ключі в системі та керувати ними відповідно до наведених нижче вимог [призначення: вимоги до встановлення та управління ключами, визначені організацією]. 2. Підтримувати доступність інформації в разі втрати користувачами криптографічних ключів.	SC-12 SC-12(1)	
262	Криптографічний захист	Впровадити типи криптографічного захисту при використанні системи для захисту конфіденційності відкритої та конфіденційної інформації [призначення: типи криптографії, визначені організацією].	SC-13	
263	Спільні обчислювальні пристрої та застосунки	Заборонити віддалену активацію спільних обчислювальних пристроїв і програмного забезпечення з такими вийнятками: [призначення: визначені організацією винятки, коли дозволяється віддалена активація]	SC-15	а. спеціальні апартаменти ВТЦ, розташовані в затверджених місцях
264	Мобільний код	1. Визначити прийнятний мобільний код і технології мобільного коду. 2. Авторизувати, відстежувати та контролювати використання мобільного коду.	SC-18	
265	Безпечна служба імен/адрес (уповноважена особа)	1. Надати додаткові дані автентифікації та перевірки цілісності джерела даних разом з офіційними даними розпізнавання імен, які система повертає у відповідь на запити дозволу імен/адрес. 2. Надати засоби для вказання статусу безпеки дочірніх зон і (якщо дочірня зона підтримує служби безпечного дозволу) забезпечити перевірку ланцюга довіри між батьківськими та дочірніми доменами при роботі в складі розподіленого ієрархічного простору імен.	SC-20	
266	Безпечна служба імен/адрес (рекурсивний або кешувальний перетворювач)	Зробити запит та виконати перевірку автентичності джерела даних і перевіркуь цілісності даних у відповідях на дозвіл імен/адрес, які система отримує від уповноважених джерел.	SC-21	
267	Архітектура та забезпечення служби імен/адрес	Переконатися, що системи, які спільно надають послуги розпізнавання імен/адрес для організації, є відмовостійкими та забезпечують поділ внутрішніх і зовнішніх ролей.	SC-22	
268	Автентифікація сесії	Захистити автентифікацію сеансів зв'язку.	SC-23	
269	Увведення у відомий стан	Увести систему в [призначення: визначений організацією відомий стан системи] у разі [призначення: визначені організацією типи збоїв системи] зі збереженням [призначення: визначена організацією інформація про стан системи] при збої.	SC-24	
270	Ізоляція процесу	Підтримувати окремий домен виконання для кожного процесу, що виконується в системі.	SC-39	
271	Синхронізація системи з часом	1. Синхронізація системного годинника в системі та компонентах системи і між ними. 2. Порівняйте внутрішні системні годинники [призначення: частота, визначена організацією] з [призначення: визначене організацією авторитетне джерело часу]. 3. Синхронізувати внутрішні системні годинники з офіційним джерелом часу, коли різниця в часі перевищує [призначення: період часу, визначений організацією].	SC-45 SC-45(1)	
Цілісність системи та інформації				

272	Виправлення дефектів	1. Виявляти, повідомляти та виправляти недоліки системи. 2. Встановлювати оновлення програмного забезпечення та вбудованих програм, що стосуються безпеки, протягом [призначення: період часу, визначений організацією] після виходу оновлень. 3. Встановлювати [призначення: визначене організацією відповідне оновлення програмного забезпечення та вбудованого програмного забезпечення] автоматично на [призначення: визначені організацією компоненти системи].	SI-2 SI-2(5)	c. 30 діб
273	Виправлення дефектів	1. Впровадити автоматизовані механізми [призначення: визначена організацією частота] для визначення стану компонентів системи стосовно усунення дефектів. 2. Вимірювати час між виявленням та виправленням дефектів. 3. Встановити [призначення: визначені організацією орієнтири] для вжиття коригувальних дій.	SI-2(2) SI-2(3)	
274	Захист від шкідливого коду	1. Упровадити механізми захисту від шкідливого коду у визначених місцях системи для виявлення та знищення шкідливого коду. 2. Оновлювати механізми захисту від шкідливого коду в міру виходу нових версій відповідно до політики та процедур управління конфігурацією. 3. Налаштувати механізми захисту від шкідливого коду на: виконання сканування системи [призначення: частота, визначена організацією] та сканування файлів із зовнішніх джерел у реальному часі на кінцевих точках або точках входу та виходу з мережі під час завантаження, відкриття або виконання файлів; блокування шкідливого коду, поміщення шкідливого коду в карантин або інші дії у відповідь на виявлення шкідливого коду.	SI-3	c.1 1-ий параметр: щонайменше щотижня c.1 2- ий параметр: кінцеві точки та точки входу/виходу з мережі c.2 1- ий параметр: блокування та карантин шкідливого коду c.2 2- ий параметр: щонайменше відповідальний адміністратор
275	Попередження, рекомендації та директиви з безпеки	1. Отримувати попередження, рекомендації та директиви щодо безпеки системи від зовнішніх організацій на постійній основі. 2. Створювати та розповсюджувати внутрішні попередження системи, рекомендації та директиви щодо безпеки у разі потреби. 3. Упроваджувати директиви з безпеки відповідно до встановлених часових рамок.	SI-5	
276	Попередження, рекомендації та директиви з безпеки - атоматичні попереджання та рекомендації	Впровадити автоматизовані механізми, щоб зробити попередження та рекомендації з безпеки доступними для всієї організації.	SI-5(1)	
277	Моніторинг системи	1. Проводити моніторинг системи для виявлення: атак та індикаторів потенційних атак; неавторизованих підключень. 2. Виявляти неавторизоване використання системи. 3. Проводити моніторинг вхідного та вихідного комунікаційного трафіка для виявлення незвичних або несанкціонованих дій чи умов. 4. Впровадити автоматизовані засоби та механізми для підтримки аналізу подій у режимі, близькому до реального часу. 5. Підключати та налаштовувати окремі засоби виявлення вторгнень у загальну систему виявлення вторгнень. 6. Попереджати [призначення: визначені організацією персонал або посадові особи], коли виникають наступні системні ознаки компрометації або потенційної компрометації: [призначення: визначені організацією показники компрометації].	SI-4 SI-4(1) SI-4(2) SI-4(5)	
			SI-4(4)	b. безперервно
278	Моніторинг системи - видимість зашифрованих комунікацій	Вживати заходи, щоб [призначення: визначений організацією зашифрований трафік зв'язку] було видно на [призначення: визначені організацією засоби та механізми моніторингу системи].	SI-4(10)	
279	Моніторинг системи - аналіз аномалій трафіку комунікацій	Проводити аналіз трафіку вихідних комунікацій на зовнішній межі системи та в окремих [призначення: визначених організацією внутрішніх точках всередині системи] для виявлення аномалій.	SI-4(11)	
280	Моніторинг системи - створенні організацією атоматизовані сповіщення	Впровадити автоматизовані механізми для оповіщення [призначення: визначені організацією персонал або посадові особи], коли виникають такі ознаки невідповідної або незвичайної діяльності з наслідками для безпеки чи приватності: [призначення: визначені організацією заходи, які спричиняють сповіщення].	SI-4(12)	

281	Моніторинг системи - виявлення бездротового вторгнення	Впровадити бездротову систему виявлення вторгнень, щоб визначати зловмисні бездротові пристрої та виявляти спроби атаки й потенційні компрометації або порушення системи.	SI-4(14)	
282	Моніторинг системи - зіставлення інформації моніторингу	Зіставляти інформацію з інструментів і механізмів моніторингу, що використовуються в системі.	SI-4(16)	
283	Моніторинг системи - аналіх трафіку та прихованої ексфільтрації	Аналізувати трафік вихідних комунікацій на зовнішній межі або периметрі системи та на [призначення: визначені організацією внутрішні точки всередині системи] для виявлення прихованої ексфільтрації інформації.	SI-4(18)	
284	Моніторинг системи - особи, які становлять більший ризик	Здійснювати [призначення: визначений організацією додатковий моніторинг] осіб, які були визначені [призначенням: визначеними організацією джерелами], як такі, що становлять підвищений рівень ризику.	SI-4(19)	
285	Моніторинг системи - привілейовані особи	Реалізувати [призначення: визначений організацією додатковий моніторинг привілейованих користувачів.	SI-4(20)	
286	Моніторинг системи - несанкціоновані посуги мережі	Виявляти послуги мережі, які не були дозволені або схвалені [призначення: визначені організацією процеси авторизації або затвердження] та здійснити [вибір (один або більше): перевірка; попередження [призначення: визначених організацією персоналу чи посадових осіб]].	SI-4(22)	
287	Моніторинг системи - пристрої на основі хоста	Реалізувати [призначення: визначені організацією механізми моніторингу на основі хоста] на [призначення: визначені організацією компоненти системи].	SI-4(23)	
288	Перевірка функцій безпеки таприватності	1. Перевіряти правильність роботи [призначення: визначені організацією функції безпеки та приватності]. 2. Виконувати перевірку [вибір (один або кілька): [призначення: визначені організацією системні перехідні стани]; за командою користувача з відповідними повноваженнями; [призначення: визначена організацією частота]]. 3. Повідомляти [призначення: визначені організацією персонал або посадові особи] про невдалі перевірки безпеки та приватності. 4. [вибір (один або кілька): Вимкнути систему; Перезапустити систему; [призначення: визначені організацією альтернативні дії]], коли виявляються аномалії.	SI-6	
289	Цілісність прграмного забезпечення, вбудованого програмного забезпечення та інформації	Впровадити інструменти перевірки цілісності для виявлення несанкціонованих змін [призначення: визначеного організацією програмного забезпечення, вбудованого програмного забезпечення та інформації].	SI-7	
290	Цілісність прграмного забезпечення, вбудованого програмного забезпечення та інформації	1. Виконати перевірку цілісності [призначення: визначені організацією програмне забезпечення, вбудоване програмне забезпечення та інформація] [вибір (один або більше): під час запуску; під час [призначення: визначені організацією перехідні стани або події, що стосуються безпеки]; [призначення: визначена організацією частота]]. 2. Впровадити автоматизовані інструменти, які надсилають повідомлення до [призначення: визначені організацією персонал або посадові особи] після виявлення розбіжностей під час перевірки цілісності. 3. Автоматично [вибір (один або більше): вимкнути систему; перезапустити систему; реалізувати [призначення: визначені організацією захисні заходи]], коли виявляються порушення цілісності.	SI-7(1) SI-7(2) SI-7(5)	

291	Цілісність прграмного забезпечення, вбудованого програмного забезпечення та інформації - інтеграція виявлення і інтегрування	Внести виявлення наступних несанкціонованих змін у можливості організації реагувати на інциденти: [призначення: визначені організацією відповідні зміни в системі].	SI-7(7)	
292	Цілісність прграмного забезпечення, вбудованого програмного забезпечення та інформації - автентифікація коду	Запровадити криптографічні механізми для автентифікації [призначення: визначене організацією програмне забезпечення або компоненти вбудованого програмного забезпечення] перед його встановленням.	SI-7(15)	
293	Захист від спаму	1. Впровадити механізми захисту від спаму в точках входу та виходу системи, щоб виявляти та протидіяти небажаним повідомленням. 2. Оновлювати механізми захисту від спаму, коли доступні нові механізми відповідно до організаційної політики та процедур управління конфігурацією. 3. Автоматично оновлювати механізми захисту від спаму [призначення: з визначеною організацією частотою].	SI-8, SI-8(2)	
294	Захист пам'яті	Виконати [призначення: визначені організацією заходи безпеки] для захисту системної пам'яті від несанкціонованого коду, що виконується.	SI-16	
295	Управління та збереження інформації	Керувати 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	
296	Перевірка вводу інформації	Перевіряти дійсність [призначення: визначена організацією введена інформація].	SI-10	
297	Фільтарція вихіднх данх	Перевіряти інформацію, що виходить з [призначення: визначені організацією програмні продукти та/або застосунки], щоб переконатися, що інформація відповідає очікуваному змісту.	SI-15	
298	Відмовостійкі процедури	Виконати [призначення: визначені організацією відмовостійкі процедури], коли настають [призначення: визначені організацією умови виявлення несправностей].	SI-17	
299	Операції забезпечення якості даних	1. Перевіряти точність, актуальність, своєчасність і повноту персональної інформації протягом її життєвого циклу [Завдання: частота, визначена організацією]. 2. Виправляти або видаляти неточну або застарілу персональну інформацію.	SI-18	
300	Обробка помилок	1. Створити повідомлення про помилки, які надають інформацію, необхідну для реалізації виправних дій, без виявлення інформації, що може бути використана. 2. Показувати повідомлення про помилки лише [призначення: визначений організацією персонал або посадові особи].	SI-11	
Планування безпеки				
301	Політика та процедури планування безпеки	1. Розробити, задокументувати та розповсюдити серед персоналу організації або ролей політики та процедури, необхідні для виконання вимог безпеки. 2. Періодично переглядати та оновлювати політики та процедури.	AC-1	с.1., с.2. 1-ий параметр: щонайменше щорічно
			AT-1	а. весь персонал с.1, с.2. 1-ий параметр: щонайменше раз на рік
			AU-1	а. весь персонал с.1, с.2. 1-ий параметр: щонайменше раз на рік
			CA-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			CM-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			CP-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			IA-1	с.1., с.2. 1-ий параметр: щонайменше щороку

			IR-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			MA-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			MP-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			PE-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			PL-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			PS-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			RA-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			SA-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			SC-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			SI-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			SR-1	a. як мінімум, ключовий персонал з питань кібербезпеки або уповноважену особу
302	Плани захисту інформації та персональних даних	1. Розробити план захисту інформації, який: визначає складові компоненти системи; описує робоче середовище системи; описує конкретні загрози для системи, які викликають занепокоєння в організації; надає огляд вимог до безпеки системи; визначає з'єднання з іншими системами; визначає осіб, які виконують ролі та обов'язки в системі; містить іншу інформацію, необхідну для захисту відкритої та конфіденційної інформації. 2. Періодично переглядати та оновлювати план захисту інформації. 3. Захистити план захисту інформації від неавторизованого розголошення.	PL-2	a.14. щонайменше, призначена особа або персонал з кібербезпеки b. щонайменше, призначена особа або персонал з кібербезпеки c. щонайменше щороку
303	Правила поведінки	1. Створити та надати особам, що потребують доступу до інформаційної системи, правила, які описують їхні обов'язки й очікувану поведінку щодо інформації та використання інформаційної системи, безпеки та приватності. 2. Отримати документальне підтвердження від таких осіб про те, що вони прочитали, зрозуміли та погодилися дотримуватися правил поведінки, перш ніж дозволяти доступ до інформації та інформаційної системи. 3. Переглядати й оновлювати правила поведінки [призначення: з визначеною організацією частотою]. 4. Вимагати від осіб, які підписали попередню версію правил поведінки, перечитати та повторно підписати правила [Вибір (один або декілька): [призначення: з визначеною організацією частотою]; коли правила переглядаються чи оновлюються].	PL-4	c. щонайменше раз на рік d. щонайменше раз на рік або коли правила переглядаються чи оновлюються
304	Правила поведінки - обмеження на соціальні медіа та мережу	1. Внести до правил поведінки обмеження щодо: використання соціальних медіапорталів, вебсайтів, а також зовнішніх/сторонніх сайтів/додатків; розміщення інформації, що належить організації, на загальнодоступних вебсайтах; використання наданих організацією ідентифікаторів (наприклад, електронна пошта) та секретів автентифікації (наприклад, паролі) для створення акаунтів на зовнішніх/сторонніх вебсайтах/додатках.	PL-4(1)	

305	Архітектура безпеки та прватності	1. Розробити архітектуру безпеки та приватності для інформаційної системи, яка: характеризує методологію, вимоги та підходи, які слід вживати для забезпечення конфіденційності, цілісності та доступності інформації, що циркулює в системі; характеризує методологію, вимоги та підхід до обробки персональних даних для мінімізації ризику їх втрати; характеризує, як архітектури безпеки та приватності інтегруються в архітектуру підприємства; характеризує будь-які припущення, що пов'язані з безпекою та приватністю, щодо зовнішніх служб і залежності від них. 2. Переглядати й оновлювати архітектуру безпеки та приватності [призначення:з визначеною організацією частотою], щоб відображати оновлення в архітектурі підприємства. 3. Відображати заплановані зміни архітектури плану безпеки та приватності, концепції експлуатації інформаційної системи, аналізу критичності, організаційних заходах, постачань та закупівель.	PL-8	
Управління ризиками ланцюга постачання				
306	План управління ризиками ланцюга постачання	1. Розробити план управління ризиками ланцюга постачання, пов'язаними з дослідженнями, розробкою, проектуванням, виробництвом, придбанням, постачанням, інтеграцією, експлуатацією, обслуговуванням та утилізацією системи, компонентів системи або послуг для системи. 2. Періодично переглядати та оновлювати план управління ризиками ланцюга постачання; захистити план управління ризиками ланцюга постачання від несанкціонованого розголошення.	SR-2	b. щонайменше раз на рік
307	Створення команди управління ризиками ланцюга постачання	Створіть команду з управління ризиками ланцюга постачання, що складається з [призначення: визначений організацією персонал, ролі та обов'язки] для керівництва та підтримки наступних заходів SCRM: [призначення: діяльність з управління ризиками ланцюга постачання, визначена організацією].	SR-2(1)	
308	Стратегії придбання, інструменти і методи	Розробляти та впроваджувати стратегії придбання, контрактні інструменти та методи придбання для виявлення, захисту та зменшення ризиків у ланцюгу постачання.	SR-5	
309	Контроль ланцюга постачання і процесів	Запровадити процес виявлення та усунення слабких місць або недоліків в елементах та процесах ланцюга постачання; упровадити наведені нижче вимоги безпеки для захисту від ризиків ланцюга постачання для системи, компонентів системи або послуг для системи, а також для обмеження шкоди або наслідків від подій, пов'язаних з ланцюгом постачання: [призначення: вимоги безпеки, визначені організацією].	SR-3	
310	Оцінка постачальників	Оцініть і перегляньте ризики ланцюга постачання, пов'язані з постачальниками або підрядниками, системою, системним компонентом або системною послугою, яку вони надають.	SR-6	
311	Повідомлення про порушення ланцюга постачання	Затвердити угоди та процедури з суб'єктами, залученими до ланцюга постачання для системи, системного компонента або системної послуги для [Вибір (одного або кількох): повідомлення про порушення ланцюга постачання; результати оцінювання або аудитів; [призначення: інформація, визначена організацією]].	SR-8	
312	Перевірка системи і компонентів системи	Перевірте наступні системи або системні компоненти [Вибір (один або більше): випадковим чином обраних; на [призначення: частота, визначена організацією], після [призначення: визначені організацією ознаки необхідності перевірки]] для виявлення втручання: [призначення: визначені організацією системи або компоненти системи].	SR-10	

313	Автентичність компоненту	1. Розробити та впровадити політику та процедури боротьби з підробками, які включають засоби для виявлення та запобігання потраплянню підроблених компонентів у систему. 2. Повідомляти про підроблені системні компоненти [Вибір (один або кілька): джерело підробленого компонента; [призначення: зовнішні звітні організації,визначені організацією]; [призначення: персонал або ролі, визначені організацією]]. 3. Навчити [призначення: персонал або ролі, визначені організацією] виявленню підроблених компонентів системи (включаючи апаратне, програмне та мікропрограмне забезпечення). 4. Зберігайте контроль конфігурації для компонентів системи, які очікують обслуговування або ремонту, і компонентів, які очікують повернення в експлуатацію після обслуговування або ремонту: [призначення: системні компоненти, визначені організацією].	SR-11, SR-11(1) SR-11(2)	
314	Утилізація компоненту	Утилізуйте [призначення: визначені організацією дані, документація, інструменти або системні компоненти] за допомогою таких прийомів і методів: [призначення: визначені організацією прийоми та методи].	SR-12	
Придбання системи та послуг				
315	Життєвий цикл розробки системи	1. Придбати, розробити та керувати системою, використовуючи життєвий цикл розробки, який охоплює питання захисту інформації та приватності. 2. Визначити та задокументувати роль і обов'язки із забезпечення безпеки та приватності інформації протягом усього життєвого циклу розробки системи. 3. Визначити осіб, які мають повноваження та обов'язки в області інформаційної безпеки та приватності. 4. Інтегрувати процес управління інформаційною безпекою та приватністю в процеси життєвого циклу розробки системи.	SA-2	
316	Життєвий цикл розробки системи	1. Придбати, розробити та керувати системою, використовуючи [призначення: визначений організацією життєвий цикл розробки], який охоплює питання захисту інформації та приватності. 2. Визначити та задокументувати роль і обов'язки із забезпечення безпеки та приватності інформації протягом усього життєвого циклу розробки системи. 3. Визначити осіб, які мають повноваження та обов'язки в області інформаційної безпеки та приватності. 4. Інтегрувати процес управління інформаційною безпекою та приватністю в процеси життєвого циклу розробки системи.	SA-3	
317	Процес закупівель	Включітити такі вимоги, описи та критерії, явно або за допомогою посилання, використовуючи [Вибір (один або більше): стандартні пункти договору; [призначення: пункти договору, визначені організацією]] в договорі про придбання системи, системного компонента або системної послуги: функціональні вимоги безпеки та приватності; вимоги до стійкості механізму; вимоги до забезпечення безпеки та приватності; заходи захисту для забезпечення вимог безпеки та приватності; вимоги до захисту документації з безпеки та приватності; опис середовища розробки системи та середовища, у якому система призначена для роботи; розподіл відповідальності або визначення сторін, відповідальних за управління інформаційною безпекою, приватністю та управлінням ланцюгами постачання; критерії прийнятності.	SA-4	

318	Процес закупівель	1. Вимагати від розробника системи, компонента системи або системної служби надати опис функціональних властивостей заходів захисту, які повинні бути реалізовані. 2. Вимагати від розробника системи, компонента системи або системної служби надати інформацію про розробку та реалізацію для вибраних заходів, яка містить: [вибір (один або більше): пов'язані з безпекою зовнішні системні інтерфейси; архітектуру (проєкт) високого рівня; архітектури (проєкт) низького рівня; вихідний код або апаратні схеми; [призначення: визначена організацією інформація щодо розробки та впровадження]] на [призначення: визначений організацією рівень деталізації]. 3. Вимагати від розробника системи, компонента системи або системної служби: встановити систему, компонент або системну службу за допомогою [призначення: визначених організацією конфігурацій безпеки]; використовувати ці конфігураційні налаштування за замовчуванням для будь-якої наступної переінсталяції або оновлення системи, компонента чи послуги. 4. Вимагати від розробника системи, компонента системи або системної служби визначити функції, порти, протоколи та послуги, призначені для використання організацією.	SA-4(1) SA-4(2) SA-4(5) SA-4(9)	
319	Системна документація	1. Отримати або розробити документацію адміністратора для системи, системного компонента або системної служби, яка описує: безпечне налаштування, установку та роботу системи, компонента або служби; ефективне використання, підтримку функцій та механізмів безпеки та приватності; відомі вразливості щодо конфігурації та використання адміністративних або привілейованих функцій. 2. Отримати або розробити документацію користувача для системи, системного компонента або системної служби, яка описує: функції та механізми безпеки та приватності та способи ефективного використання цих функцій і механізмів; методи взаємодії з користувачем, що дозволяють окремим особам використовувати систему, компонент або службу безпечнішим чином та захищати індивідуальну приватність; обов'язки користувача щодо забезпечення безпеки системи, компонента або служби та приватності окремих осіб. 3. Документувати спроби отримати доступ до документації системи, системного компонента чи системної служби, коли така документація недоступна або ж відсутня, і вжити [призначення: визначені організацією заходи] у відповідь. 4. Поширити документацію серед [призначення: визначеного організацією персоналу або посадових осіб].	SA-5	
320	Безпека та приватність принципів інжинірингу	Застосовувати [призначення: визначені організацією принципи інжинірингу безпеки та конфіденційності системи] в специфікації, проєктуванні, розробці, впровадженні та зміні системи й компонентів системи.	SA-8	
321	Зовнішні послуги для системи	1. Вимагати, щоб постачальники зовнішніх послуг для системи відповідали вимогам безпеки та приватності в організації та застосовували такі заходи захисту [призначення: встановлені організацією заходи безпеки та приватності]. 2. Визначити та задокументувати нагляд організаціїповноваження та обов'язки користувачів щодо зовнішніх послуг для системи. 3. Використовувати наступні процеси, методи та техніки для постійного моніторингу дотримання контролю зовнішніми постачальниками послуг: призначення: визначені організацією процеси, методи та техніки].	SA-9	
322	Зовнішні послуги для системи - оцінювання ризиків та організаційні погодження	1. Проводити організаційне оцінювання ризиків перед придбанням або переданням послуг інформаційної безпеки служб інформаційної безпеки. 2. Переконатися, що придбання або передача спеціалізованих служб інформаційної безпеки погоджені [призначення: визначеним організацією персоналом або посадовими особами].	SA-9(1)	

323	Процеси, стандарти та інструменти розробки	1. Вимагати від розробника системи, системного компонента або системної служби слідувати документованому процесу розробки, який: явно відповідає вимогам безпеки та приватності; визначає стандарти й інструменти, які використовуються в процесі розробки; документує конкретні параметри та конфігурації інструментарію, що використовуються в процесі розробки; документує, управляє та забезпечує цілісність змін у процесі та/або інструментах, які використовуються в процесі розробки. 2. Ознайомитися з процесом розробки, стандартами, інструментами, параметрами інструментарію і конфігураціями інструментів [призначення: визначена організацією частота], щоб визначити, чи можуть вибрані й використовувані процеси, стандарти, інструменти, параметри та конфігурації інструментів задовольнити [призначення: визначені організацією вимоги до безпеки та приватності].	SA-10	
324	Тестування та оцінювання розробника	1. Вимагати від розробника системи, системного компонента або системної служби на всіх етапах проєктування та життєвого циклу розробки системи: створити та впровадити план з оцінювання безпеки та приватності; виконати [вибір (один або кілька): одиниця; інтеграція; система; регресія] тестування/оцінювання [призначення: з визначеною організацією частотою] з [призначення: визначена організацією глибиною та охопленням]; надати докази (свідчення) виконання плану оцінювання та результати тестування й оцінювань; впровадити перевірку процесу виправлення недоліків; виправити дефекти, виявлені під час тестування та оцінювання. 2. Вимагати від розробника системи, системного компонента або системної служби використовувати інструменти аналізу статичних кодів для виявлення поширених недоліків і документувати результати аналізу. 3. Вимагати від розробника системи, системного компонента або системної служби виконувати моделювання загроз та аналіз вразливостей під час розробки та під час подальшого тестування й оцінювання системи, компонента або служби, що: використовує [призначення: визначену організацією інформацію щодо критичності, середовища функціювання, відомих або передбачуваних загроз і прийнятних рівнів ризику]; використовує такі інструменти та методи: [завдання: інструменти та методи, визначені організацією]; впровадив [призначення: визначені організацією інструменти та методи]; проводить моделювання та аналізи на такому рівні ретельності: завдання: визначена організацією широта та глибина моделювання та аналізу]; надає докази (свідчення), які відповідають таким критеріям прийнятності [призначення: визначеним організацією критеріям прийняття].	SA-11 SA-11(1) SA-11(2)	
325	Процеси, стандарти та інструменти розробки	1. Вимагати від розробника системи, системного компонента або системної служби слідувати документованому процесу розробки, який: явно відповідає вимогам безпеки та приватності; визначає стандарти й інструменти, які використовуються в процесі розробки; документує конкретні параметри та конфігурації інструментарію, що використовуються в процесі розробки; документує, управляє та забезпечує цілісність змін у процесі та/або інструментах, які використовуються в процесі розробки. 2. Ознайомитися з процесом розробки, стандартами, інструментами, параметрами інструментарію і конфігураціями інструментів [призначення: визначена організацією частота], щоб визначити, чи можуть вибрані й використовувані процеси, стандарти, інструменти, параметри та конфігурації інструментів задовольнити [призначення: визначені організацією вимоги до безпеки та приватності].	SA-15	
326	Навчання, що надається розробником	Вимагати від розробника системи, системного компонента або системної служби забезпечити наступне навчання щодо правильного використання та функціонування реалізованих функцій, заходів і механізмів безпеки та приватності [призначення: визначене організацією навчання].	SA-16	
327	Перевірка розробника	Вимагати, щоб розробник [призначення: визначених організацією системи, компонент системи або послуги]: мав відповідні дозволи доступу, як визначено призначеним [призначення: визначеним організацією уповноваженим органом]; відповідає таким додатковим критеріям перевірки персоналу: [призначення: визначені організацією додаткові критерії перевірки персоналу].	SA-21	

328	Компоненти системи, що не підтримуються	1. Замінювати компоненти системи, якщо підтримка компонентів більше не доступна розробнику, постачальнику або виробнику. 2. Надавати такі варіанти альтернативних джерел для подальшої підтримки непідтримуваних компонентів [вибір (один або більше): внутрішня підтримка; [призначення: підтримка, визначена організацією від зовнішніх постачальників]].	SA-22	

Директор директорату
з кіберзахисту та хмарних послуг
Міністерства цифрової трансформації України **Вадим КОНОВАЛ**