ЗАТВЕРДЖЕНО
Наказ Міністерства цифрової трансформації України
_____ 2026 року № ___

Галузевий профіль безпеки систем, що використовується для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або операторам критичної інфраструктури, у яких обробляється відкрита та конфіденційна інформація

№	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. Впровадити моніторинг використання облікових записів системи; 6. Оповістити персонал або ролі організації, коли: (призначення: визначений організацією період часу) коли облікові записи більше не потрібні; (призначення:	AC-2	h.1. 24 години h.2. 24 години h.3. 24 години j. мінімум щоквартально
			AC-2(5)	кінець робочого дня користувача

		визначений організацією період часу) коли користувачі звільняються або переводяться; (призначення: визначений організацією період часу) коли у системі наявні зміни, які потребують нових знань. 7. Вимагати, щоб користувачі виходили з системи після (призначення: визначений організацією період часу) очікуваної бездіяльності або за (призначення: визначені організацією обставин).		
2	Забезпечення доступу	Застосовувати затверджені повноваження для логічного доступу до інформації та ресурсів у системі.	AC-3	
3	Управління інформаційними потоками	Застосовувати затверджені дії для управління потоками відкритої та конфіденційної інформації всередині системи та між підключеними системами.	AC-4	
4	Розмежування обов'язків	Визначити обов'язки осіб, які потребують розмежування;установити правила авторизації доступу для підтримки розмежування обов'язків.	AC-5	
5	Мінімізація повноважень	Надавати користувачам (або процесам, що діють від імені користувачів) лише авторизований доступ до системи, необхідний для виконання поставлених завдань організації; авторизувати доступ до (призначення: функції безпеки, визначені організацією, та важлива для безпеки інформація).	AC-6	
			AC-6(1)	
			AU-9(4)	
6	Мінімізація повноважень – непривілейований доступ до незахищених функцій	Обмежити привілейовані облікові записи в системі для (призначення: персонал або ролі, що визначається організацією); вимагати, щоб користувачі (або ролі) з привілейованими обліковими записами використовували непривілейовані облікові записи для доступу до незахищених функцій або інформації.	AC-6(2)	привілейовані функції
			AC-6(5)	
7	Мінімізація повноважень – заборона	Заборонити непривілейованим користувачам виконувати привілейовані функції.	AC-6(10)	

	непривілейованим користувачам виконувати привілейовані функції			
8	Невдалі спроби входу в систему	Встановити обмеження на кількість (призначення: кількість, яка визначена організацією) невдалих спроб входу в систему протягом певного часу (призначення: проміжок часу, визначений організацією); 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
9	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	
10	Блокування пристрою	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); зберігати блокування пристрою до відновлення користувачем доступу за допомогою встановлених процедур ідентифікації та автентифікації; приховати за допомогою блокування пристрою інформацію, яку раніше було видно на дисплеї, за допомогою публічно доступного зображення.	AC-11	a. ініціювання блокування пристрою через період, що не перевищує 30 хвилин; дія до користувача ініціювати блокування пристрою перед тим, як залишити систему без нагляду
			AC-11(1)	

11	Припинення сеансу	Автоматично завершувати сеанс користувача після (призначення: умови або події, що вимагають відключення сеансу, визначені організацією).	AC-12	
12	Віддалений доступ	1. Встановити обмеження на використання, дії до конфігурації та підключення для кожного типу допустимого віддаленого доступу до системи; авторизувати кожен тип віддаленого доступу до системи перед встановленням таких з'єднань; виконувати маршрутизацію всього віддаленого доступу до системи через авторизовані та керовані точки контролю управління доступом до мережі; авторизувати віддалене виконання привілейованих команд і віддалений доступ до інформації, важливої для безпеки; 2. Забезпечити можливість швидкого відключення або деактивації віддаленого доступу до системи в межах (призначення: визначеного організацією періоду часу).	AC-17	
			AC-17(3)	
			AC-17(9)	
13	Бездротовий доступ	Встановити обмеження на використання, дії до конфігурації та підключення для кожного типу бездротового доступу до системи; авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення.	AC-18	
14	Контроль доступу для мобільних пристроїв	Встановити обмеження на використання, дії до конфігурації та підключення для мобільних пристроїв; авторизувати підключення мобільних пристроїв до системи; 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
15	Використання зовнішніх систем	1. Заборонити використання зовнішніх систем, крім систем дозволених організацією; 2. Установити такі положення, умови та дії щодо безпеки, які повинні бути виконані у зовнішніх системах, перш ніж	AC-20	
			AC-20(1)	
			AC-20(2)	

		дозволити використання або доступ до цих систем авторизованим особам: (призначення: умови, положення та дії визначаються організацією); 3. Дозволити авторизованим особам використовувати зовнішню систему для доступу до системи організації або для обробки, зберігання чи передачі відкритої та конфіденційної інформації, лише після: перевірки реалізації дій 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.		
16	Публічно доступний контент	Навчати авторизованих осіб щодо нерозголошення відкритої та конфіденційної інформації в загальнодоступних системах; 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 та навчання				
17	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); щодо розпізнавання та повідомлення про індикатори внутрішньої загрози, соціальної інженерії, та соціального шпіонажу; 2. Оновлювати зміст тренінгу з безпекової обізнаності (призначення: визначена організацією періодичність) та після (призначення: визначені організацією події); 3. Забезпечити навчання грамотності щодо стійкої постійної загрози;	AT-2	a.1. щонайменше раз на рік
			AT-2(2)	
			AT-2(4)	
			AT-2(5)	
			AT-2(6)	

		4. Забезпечити навчання грамотності щодо середовища кіберзагроз; 5. Відображати поточну інформацію про кіберзагрози в операціях системи (враховувати актуальну інформацію про кіберзагрози під час підготовки та проведення навчання і заходів з підвищення обізнаності персоналу, щоб працівники розуміли сучасні ризики та могли правильно діяти під час експлуатації системи).		
18	Рольове навчання	1. Провести тренінги з безпеки для персоналу організації на основі покладених обов'язків/ролей: перед авторизацією доступу до системи або відкритої та конфіденційної інформації, перед виконанням призначених обов'язків, а також (призначення: частота визначається організацією) після цього; коли цього вимагають зміни в системі або після (призначення: події, визначені організацією); 2. Оновлювати зміст тренінгів (призначення: частота, визначена організацією) на основі покладених обов'язків, а також після (призначення: події, визначені організацією). 3. Надати (призначення: визначеним організацією персоналу чи посадам) з початку роботи та з (призначенням: визначеною організацією частотою) підготовку з питань застосування заходів захисту робочого середовища; 4. 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; 5. 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	a.1. щонайменше щороку
			AT-3(1)	
			AT-3(2)	
			AT-3(5)	
Аудит та підзвітність				

19	Події аудиту	Визначити перелік подій, які реєструються в системі: (призначення: типи подій, визначені організацією); обґрунтувати, чому типи подій, що перевіряються, вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов'язаних з безпекою та приватністю; переглядати та оновлювати (призначення: частота визначається організацією) типи подій, обрані для реєстрації.	AU-2	
20	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)	
21	Збереження записів аудиту	Згенерувати записи аудиту для вибраних типів подій згідно з вмістом записів аудиту, вказаних в п. 19 та в п. 20; зберігати записи аудиту протягом періоду часу, який відповідає політиці зберігання записів аудиту.	AU-11	а. всі інформаційні системи та мережеві компоненти
			AU-12	
22	Реагування на відмови обробки даних аудиту	Сповіщати персонал або ролі організації в межах (призначення: визначений організацією період часу) у разі збою обробки даних аудиту; виконати додаткові дії: (призначення: додаткові дії, визначені організацією).	AU-5	а. 2-ий параметр: майже в реальному часі
23	Огляд, аналіз і звітність аудиту	Переглядати та аналізувати (призначення: частота, визначена організацією) записи аудиту системи на предмет виявлення ознак і потенційного впливу не властивої або незвичної діяльності; повідомляти про результати аудиту співробітникам організації або ролям; аналізувати та зіставляти записи аудиту в різних сховищах задля забезпечення ситуативної обізнаності в масштабах організації.	AU-6	а. 1-ий параметр: щонайменше щотижня (сім днів)
			AU-6(3)	

24	Скорочення записів аудиту та формування звіту	Впровадити функцію скорочення записів аудиту і створення звітів, яка підтримує перегляд записів аудиту, аналіз, дії до звітності та постфактум розслідування інцидентів; зберігати оригінальний зміст і часовий порядок записів аудиту.	AU-7	
25	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)	
26	Позначка часу	Використовувати внутрішній годинник у системі для створення позначок часу для записів аудиту; застосовувати позначки часу, які відповідають (призначення: деталізація вимірювання часу, визначена організацією), і використовують: всесвітній координований час (UTC); фіксоване зміщення місцевого часу відносно UTC або зміщення місцевого часу як частину позначки часу.	AU-8	
27	Захист інформації аудиту	1. Захистити інформацію аудиту та інструментів журналювання аудиту від несанкціонованого доступу, зміни та видалення; 2. Інформація про події інформаційної безпеки (журнали аудиту, реєстри інцидентів) повинна зберігатися на окремих (відчужених) носіях або виділених серверах логування; 3. Надавати доступ до управління функціями аудиту тільки підмножині привілейованих користувачів або ролей.	AU-9	
			AU-9(2)	
			AU-9(4)	
Управління конфігурацією				
			CM-2	b.1. щонайменше щороку

28	Базова конфігурація	1. Розробляти та підтримувати під контролем налаштування поточної базової конфігурації системи; переглядати та оновлювати (призначення: частота, визначена організацією) базову конфігурацію системи, а також при встановленні або модифікації компонентів системи; 2. Підтримувати актуальність, повноту, точність і доступність базової конфігурації системи за допомогою (призначення: автоматизовані механізми, визначені організацією); 3. Підтримувати базову конфігурацію для розробки системи та тестових середовищ, які керуються окремо від робочої базової конфігурації; 4. Видавати (призначення: визначених організацією систем або компонентів систем) з (призначенням: визначеними організацією конфігураціями) особам, що перебувають у місцях, які організація вважає місцями зі значним ризиком; 5. Застосовувати такі дії безпеки до систем або компонентів, коли особи повертаються з подорожі: (призначення: визначені організацією дії безпеки).	СМ-2(2)	
			СМ-2(6)	
			СМ-2(7)	
29	Налаштування конфігурації	Встановити, задокументувати та впровадити параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним діям: (призначення: налаштування конфігурації, визначені організацією); визначити, задокументувати та затвердити будьякі відхилення від встановлених налаштувань конфігурації.	СМ-6	с. 1-ий параметр: всі конфігуровані компоненти системи.
30	Управління змінами конфігурації	1. Визначити типи змін у конфігурації системи, які необхідно контролювати; переглядати запропоновані зміни в конфігурації системи, схвалювати або відхиляти такі зміни, враховуючи вплив на безпеку; упровадити та задокументувати затверджені зміни	СМ-3	е. 1 рік
			СМ-3(4)	
			СМ-3(6)	
			СМ-3(7)	

		конфігурації системи; відстежувати та переглядати дії, пов'язані зі змінами в конфігурації системи, які необхідно контролювати; 2. Вимагати від (призначення: визначеного організацією представника з інформаційної безпеки) бути членом (призначення: визначеного організацією елементу керування зміною конфігурацій).		
31	Аналіз впливу на безпеку та приватність	1. Проаналізувати вплив змін у системі на безпеку перед їх впровадженням; 2. Переконатись, що дії до безпеки системи продовжують задовольнятися після впровадження змін у системі.	CM-4	
			CM-4(2)	
32	Обмеження доступу до змін	1. Визначити, задокументувати, затвердити та впровадити фізичні та логічні обмеження доступу, пов'язані зі змінами в системі; 2. Обмежити повноваження для зміни компонентів системи та інформації, пов'язаної із системою, у виробничому або операційному середовищі; 3. Переглядати та переоцінювати такі повноваження (призначення: визначеною організацією з частотою).	CM-5	
			CM-5(5)	
33	Мінімально необхідна функціональність	Налаштувати систему так, щоб вона надавала лише необхідні для виконання завдань функції; заборонити або обмежити використання таких функцій, портів, протоколів, підключень і служб: (призначення: функції, порти, протоколи, з'єднання та служби, визначені організацією); переглядати (призначення: частота, визначена організацією) систему, щоб виявити непотрібні або небезпечні функції, порти, протоколи, з'єднання та служби; вимкнути або видалити функції, порти, протоколи, з'єднання та служби, які є непотрібними або небезпечними. Визначити програмне забезпечення, дозволене для виконання в системі; впровадити політику «заборонити все,	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, які були

		дозволити за винятком» для виконання дозволеного програмного забезпечення в системі; переглянути та оновити список дозволеного програмного забезпечення (призначення: частота, визначена організацією).		визначені як непотрібні та/або незахищені
			CM-7(5)	c. щонайменше раз на рік
34	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	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, власникінформаційної системи/компонента, а для мережевого компонента/пристрою - ім’я обладнанняb. щонайменше щороку
			CM-8(1)	
35	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.	CM-8(4)	
36	Обмеження використання програмного забезпечення	Використовувати програмне забезпечення та супутні документи відповідно до договірних угод та законів про авторські права.	CM-10	
Придбання систем та послуг				

37	Процес закупівель - використання засобів захисту інформації	1. Використовувати засоби захисту інформації, які пройшли державну експертизу або сертифікацію, створені для технічного та криптографічного захисту інформації; 2. Переконатися, що ці засоби захисту мають позитивний експертний висновок або сертифікат відповідності, а також відповідні дозволи для використання для захисту критичної інформації.	SA-4(6)	
Планування безперервної роботи				
38	План забезпечення безперервної роботи та відновлення функціонування	1. Розробити план забезпечення безперервної роботи та відновлення функціонування системи на випадок надзвичайної ситуації, який визначає основні завдання, функції та пов'язані з ними вимоги щодо безперервної роботи; забезпечує цілі, пріоритети та відповідні показники відновлення функціонування; 2. Здійснити планування ресурсів з метою забезпечення необхідного потенціалу для обробки інформації, телекомунікацій та підтримки навколишнього середовища під час відновлення функціонування системи.	CP-2	
			CP-2(2)	
39	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	щонайменше раз на рік
Ідентифікація та автентифікація				
40	Ідентифікація та автентифікація (користувачів організації)	Унікально ідентифікувати та автентифікувати користувачів організації і пов'язувати цю унікальну ідентифікацію з процесами, що діють від імені цих користувачів.	IA-2	

41	Ідентифікація та автентифікація пристроїв	Унікально ідентифікувати та автентифікувати пристрої перед встановленням з'єднання з системою.	IA-3	
42	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)	
43	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
44	Управління ідентифікацією	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; запобігати повторному використанню ідентифікаторів для (призначення: період часу, визначений організацією).	IA-4	d. щонайменше рік для окремих осіб, груп, ролей
45	Управління автентифікатором – автентифікація на основі пароля	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	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

		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. Провадити правила складу та складності паролів: (призначення: визначені організацією правила складу та складності); 7. Використовуйте (призначення: визначені організацією менеджери паролів) для створення та керування паролями;	IA-5(1) IA-5(18)	50% символів при створенні нових паролів
46	Зворотний зв’язок автентифікатора	Забезпечити прихований зворотний зв’язок автентифікаційної інформації під час процесу автентифікації.	IA-6	
47	Управління автентифікатором	Перевіряти ідентичність особи, групи, ролі, служби або пристрою, які отримують автентифікатор під час початкового розповсюдження автентифікатора; встановити початковий вміст автентифікатора для всіх автентифікаторів, виданих організацією; створити та впровадити адміністративні процедури для початкового розподілу автентифікаторів для втрачених, скомпрометованих або пошкоджених автентифікаторів, а також для відкликання автентифікаторів; змінити автентифікатори за замовчуванням під час першого використання; змінювати або оновлювати автентифікатори періодично або коли відбуваються події: (призначення: події, визначені організацією); захистити вміст автентифікатора від несанкціонованого розкриття та модифікації.	IA-5	f. 1-ий параметр: не більше 180 днів для паролів
Реагування на інциденти				

48	Обробка інциденту	1. Упровадити систему реагування на інциденти, яка відповідає плану реагування на інциденти і передбачає підготовку, виявлення та аналіз, локалізацію, ліквідацію та відновлення інцидентів. 2. Створити та підтримувати інтегровану групу реагування на інциденти, яку можна розгорнути в будь-якому місці, визначеному організацією протягом (призначення: період часу, визначений організацією).	IR-4	
			IR-4(11)	
49	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)	
50	Моніторинг інциденту	Відстежувати та документувати інциденти, пов’язані з безпекою системи; повідомляти про підозрілі інциденти до служби реагування на інциденти в організації протягом часу (призначення: період часу, визначений організацією); повідомити інформацію про інцидент (призначення: органи, визначені організацією); 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 b. повідомити Адміністрацію Держспецзв’язку та урядову команду реагування на комп’ютерні надзвичайні події України CERT-UA, у порядку, затвердженому Адміністрацією Держспецзв’язку, а також публічних користувачів хмарних послуг або користувачів хмарних послуг, що є власниками (держателями, розпорядниками) електронних інформаційних ресурсів, яких ці інциденти стосуються
			IR-7	

51	Перевірка реагувань на інциденти	Перевіряти ефективність спроможності реагування на інциденти (призначення: частота , визначена організацією).	IR-3	1-ий параметр: щонайменше щороку
52	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
53	План реагування на інциденти	1. Розробити план реагування на інцидент, який: надає організації план дій для реалізації її можливостей реагування на інциденти, 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.	IR-8	b. весь персонал, який має роль або відповідальність за впровадження плану реагування на інцидентid. весь персонал, який має роль або відповідальність за впровадження плану реагування на інциденти

		4. Захистити план реагування на інциденти від несанкціонованого розголошення.		
Технічне обслуговування				
54	Інструменти для обслуговування	1. Затверджувати, контролювати та відстежувати використання інструментів технічного обслуговування системи; 2. Переглядати раніше затверджені інструменти технічного обслуговування (призначення: з частотою, визначеною організацією). 3. Перевіряти інструменти для технічного обслуговування на наявність неналежних або несанкціонованих модифікацій. 4. Перед використанням носіїв у системі перевірити носії, що містять діагностичні та тестові програми на наявність шкідливого коду. 5. Перевіряйте засоби захисту, щоб переконатися, що встановлено останні оновлення програмного забезпечення.	MA-3	b. щонайменше щороку
			MA-3(1)	
			MA-3(2)	
			MA-3(6)	

55	Віддалене обслуговування	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; забезпечити завершення сеансу та мережевих з'єднань після завершення віддаленого технічного обслуговування.	МА-4	
56	Технічний персонал	Встановити процес авторизації персоналу з технічного обслуговування; вести список уповноважених організацій або персоналу з технічного обслуговування; переконатися, що персонал без супроводу, який виконує технічне обслуговування системи, має необхідні дозволи на доступ; призначити персонал організації з необхідними повноваженнями доступу та технічною компетентністю для нагляду за діяльністю персоналу з технічного обслуговування, який не має необхідних повноважень доступу.	МА-5	
Захист носіїв інформації				
57	Зберігання носіїв інформації	Фізично контролювати та безпечно зберігати носії інформації, що містять відкриту та конфіденційну інформацію.	МР-4	
58	Доступ до носіїв інформації	Обмежити доступ до конфіденційної інформації на носіях інформації.	МР-2	1-ий параметр: всі типи цифрових та/або нецифрових носіїв, що містять інформацію, не дозволену для публічного оприлюднення
59	Знищення інформації на носіях інформації	Очистити носії інформації, що містять відкриту та конфіденційну інформацію, перед утилізацією, випуском з-під контролю організації або повторним використанням.	МР-6	
60	Маркування носіїв інформації	Маркувати носії інформації, що містять відкриту та конфіденційну інформацію, для позначення обмежень щодо	МР-3	

		розповсюдження, застережень стосовно поводження з ними та позначок безпеки.		
61	Транспортування носіїв інформації	Захистити і контролювати носії інформації, що містять відкриту та конфіденційну інформацію, під час транспортування за межі контрольованих територій; вести облік носіїв інформації, що містять відкриту та конфіденційну інформацію, під час транспортування за межі контрольованих територій. Документувати дії, пов'язані з транспортуванням системних носіїв, які містять відкриту та конфіденційну інформацію.	MP-5 SC-28	
62	Використання носіїв інформації	Обмежити або заборонити використання (призначення: типи носіїв інформації, визначені організацією);заборонити використання знімних носіїв інформації без ідентифікованого власника.	MP-7	
63	Резервне копіювання	1. Проводити резервне копіювання інформації користувачів, що міститься (призначення: системні компоненти, визначені організацією) (призначення: з визначеною організацією частотою, відповідно до часу відновлення та встановлених цілей відновлення). 2. Проводити резервне копіювання системної інформації на системному рівні, що міститься в системі (призначення: з визначеною організацією частотою, відповідно до завдань відновлення і встановлених цілей відновлення). 3. Проводити резервне копіювання системної документації, включно з документацією, пов'язаною із забезпеченням безпеки та приватності (призначення: з визначеною організацією частотою, відповідно до часу відновлення та встановлених цілей відновлення). 4. Забезпечити захист конфіденційності, цілісності та доступності резервних копій інформації в місцях їх зберігання.	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)
Кадрова безпека				

64	Перевірка персоналу	Перевіряти осіб перед тим, як надавати їм доступ до системи; проводити повторні перевірки осіб відповідно до (призначення: умови, що потребують повторної перевірки, визначені організацією).	PS-3	
65	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 відносинb. 1-ий параметр: дії з перепризначення, щоб забезпечити видалення або вимкнення всіх системних доступів, які більше не потрібні
			PS-5	
Фізичний захист і захист робочого середовища				
66	Авторизація фізичного доступу	Розробити, затвердити та підтримувати список осіб, які мають право доступу до фізичного місця розташування системи; надавати повноваження для доступу до об'єкта; періодично перевіряти список фізичного доступу; переглядати список доступу до об'єктів (призначення: частота, визначена організацією). видаляти осіб зі списку фізичного доступу, коли доступ більше не потрібен.	PE-2	c. щонайменше щороку

67	Моніторинг фізичного доступу	Моніторити фізичний доступ до місця розташування системи, щоб виявляти та реагувати на інциденти фізичної безпеки; переглядати журнали фізичного доступу (призначення: частота, визначена організацією) та при виникненні (призначення: події, визначені організацією, або потенційні ознаки подій).	PE-6	b. 1-ий параметр: щонайменше кожні 90 днів
68	Альтернативне робоче місце	Визначити альтернативні робочі місця, дозволені для використання працівниками; застосовувати дії безпеки на альтернативних робочих місцях (призначення: дії безпеки, визначені організацією).	PE-17	
69	Керування фізичним доступом	1. Контролювати фізичний доступ до місця, де знаходиться система: 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); 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. Забезпечити цілодобову безперервну охорону для контролю доступу (призначення: визначені організацією фізичні точки доступу) до об'єкта, де перебуває система; 6. Контролювати фізичний доступ до пристроїв виводу, щоб запобігти доступу сторонніх осіб до конфіденційної інформації.	PE-3	
			PE-3(1)	
			PE-3(3)	
			PE-5	

70	Контроль доступу до джерел і ліній електроживлення. Контроль доступу до пристроїв виведення інформації	Контролювати фізичний доступ до розподільчих ліній системи і ліній електропередач на об’єктах організації.	PE-4	
Оцінювання ризику				
71	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	
72	Оцінювання ризику	Оцінити ризик несанкціонованого розголошення в результаті обробки, зберігання або передачі конфіденційної інформації.	RA-3	d., f. щонайменше щороку
73	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 перелік вразливостей системи, що були просканованої (вибір: один або більше); (призначення: з визначеною організацією частотою; перед новим скануванням; коли виявлені та зареєстровані нові вразливості).	RA-5	a. щонайменше кожні 30 днів
			RA-5(2)	перед новим скануванням
74	Реагування на ризик	Реагувати на результати оцінювання, моніторингу й аудиту безпеки та приватності.	RA-7	

75	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				
76	Оцінювання	1. Оцінювати заходи захисту в системі та в її середовищі функціонування з (призначення: визначеною організацією частотою) для визначення, наскільки коректно реалізовані заходи безпеки і чи працюють вони за призначенням і дають бажаний результат щодо дотримання встановлених вимог безпеки та приватності;	CA-2	d. щонайменше щороку
77	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. Оновити існуючий план дій і показників на основі результатів оцінки безпеки, незалежних аудитів або оглядів, а також безперервного моніторингу.	CA-5	
78	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)	

79	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, дії до безпеки, вимоги до безпеки та приватності, засоби контролю та обов'язки для кожної системи як частину договорів про обмін, а також характер переданої інформації (відповідно до статті 10 Закону України "Про інформацію"); переглядати та оновлювати (призначення: частота, визначена організацією) договори про обмін.	CA-3	
Захист інформаційної системи та комунікацій				
80	Захист периметра	Контролювати та управляти зв'язком на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи;задокументувати заплановані заходи з виправлення слабких місць або недоліків, виявлених під час оцінювання безпеки; зменшити або усунути відомі недоліки системи.	SC-7	
81	Інформація в загальних ресурсах системи	Запобігати несанкціонованій і ненавмисній передачі інформації за допомогою загальних ресурсів системи.	SC-4	
82	Захист периметра - Відмова за замовчуванням - Дозвіл за винятком	Заборонити трафік мережевих комунікацій за замовчуванням і дозволити трафік мережевих комунікацій за винятком.	SC-7(5)	

83	Конфіденційність і цілісність передачі	1. Забезпечити (вибір (один або кілька): конфіденційність; цілісність) інформації, що передається; 2. Реалізувати механізми криптографічного захисту для (вибір (один або більше): запобігання несанкціонованому розкриттю інформації; вияву зміни в інформації) під час передачі.	SC-8	конфіденційність та цілісність
			SC-8(1)	запобігати несанкціонованому розголошенню інформації та виявляти зміни в ній
84	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
85	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
86	Встановлення та управління криптографічними ключами	Встановити криптографічні ключі в системі та керувати ними відповідно до наведених нижче дій (призначення: дії до встановлення та управління ключами, визначені організацією).	SC-12	
87	Криптографічний захист	Впровадити типи криптографічного захисту при використанні системи для захисту конфіденційності відкритої та конфіденційної інформації (призначення: типи криптографії, визначені організацією).	SC-13	
88	Спільні обчислювальні пристрої та застосунки	Заборонити віддалену активацію спільних обчислювальних пристроїв і програмного забезпечення з такими винятками: (призначення: визначені організацією винятки, коли дозволяється віддалена активація); надавати чіткі вказівки щодо використання користувачам, які фізично наявні біля пристроїв.	SC-15	а. спеціальні апартаменти ВТЦ, розташовані в затверджених місцях
89	Мобільний код	Визначити прийнятний мобільний код і технології мобільного коду;	SC-18	

		авторизувати, відстежувати та контролювати використання мобільного коду.		
90	Автентифікація сесії	Захистити автентифікацію сеансів зв'язку.	SC-23	
Цілісність системи та інформації				
91	Виправлення дефектів	Виявляти, виправляти та повідомляти про недоліки системи; перед установкою перевірити програмне забезпечення та оновлення вбудованого програмного забезпечення, що пов'язані з усуненням дефектів, на ефективність та можливі побічні ефекти; встановлювати оновлення програмного забезпечення та вбудованих програм, що стосуються безпеки, протягом (призначення: період часу, визначений організацією) після виходу оновлень; внести виправлення помилок в процес управління конфігурацією організації.	SI-2	с. 30 діб
92	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	с.1 1-ий параметр: щонайменше щотижня с.1 2- ий параметр: кінцеві точки та точки входу/виходу з мережі с.2 1- ий параметр: блокування та карантин шкідливого коду с.2 2- ий параметр: щонайменше відповідальний адміністратор

93	Попередження, рекомендації та директиви з безпеки	Отримувати попередження, рекомендації та директиви щодо безпеки системи від зовнішніх організацій на постійній основі; створювати та розповсюджувати внутрішні попередження системи, рекомендації та директиви щодо безпеки у разі потреби; упроваджувати директиви з безпеки відповідно до встановлених часових рамок.	SI-5	
94	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.	SI-4	
			SI-4(4)	b. безперервно
95	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	
96	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	
97	Запобігання прогнозованим збоям	1. Визначити середній час до збою (MTTF) для (призначення: визначені організацією компоненти системи) в певних середовищах роботи. 2. Надати замінні компоненти системи та засоби для заміни активних компонентів резервними компонентами відповідно до (призначення: визначені організацією критерії заміни).	SI-13	
Планування безпеки				

98	Політика та процедури планування безпеки	Розробити, задокументувати та розповсюдити серед персоналу організації або ролей політики та процедури, необхідні для виконання дій безпеки; періодично переглядати та оновлювати політики та процедури (призначення: частота, визначена організацією).	AC-1	c.1., c.2. 1-ий параметр: щонайменше щорічно
			AT-1	a. весь персонал c.1, c.2. 1-ий параметр: щонайменше раз на рік
			AU-1	a. весь персонал c.1, c.2. 1-ий параметр: щонайменше раз на рік
			CA-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			CM-1	c.1., c.2. 1-ий параметр: щонайменше щороку
			IA-1	c.1., c.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 c.1., c.2. 1-ий параметр: щонайменше щороку
99	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 дій 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 (призначення: частота, визначена організацією); 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
Управління ризиками ланцюга постачання				
100	Контроль ланцюга постачання і процесів	Встановлення процесу або процесів для виявлення та усунення слабких місцьабо недоліків в елементах і процесах ланцюга постачання (призначення: визначена організацією система або компонент системи) у координації з (завдання: персонал ланцюга постачання, визначений організацією).	SR-3	

101	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	

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