ЗАТВЕРДЖЕНО
Наказ Міністерства цифрової трансформації України
_____ 2026 року № ___

Галузевий профіль безпеки систем у сфері електронних довірчих послуг, в яких обробляється відкрита або конфіденційна інформація

№	Назва дії з безпеки інформації	Зміст дії	Заходи захисту 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. 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;	AC-2	h.1. 24 години h.2. 24 години h.3. 24 години j. мінімум щоквартально
			AC-2(5)	кінець робочого дня користувача

		(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 конфіденційної 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	1. Визначити обов'язки осіб, які потребують розмежування. 2. Установити правила авторизації доступу для підтримки розмежування обов'язків.	AC-5	
5	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).	AC-6 AC-6(1) AU-9(4)	
6	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
7	Мінімізація повноважень – заборона	Заборонити непривілейованим користувачам виконувати привілейовані функції.	AC-6(10)	

	непривілейованим користувачам виконувати привілейовані функції			
8	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
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	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).	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)	

		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.		
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. 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)	
13	Бездротовий доступ	1. Встановити обмеження на використання, дії до конфігурації та підключення для кожного типу бездротового доступу до системи. 2. Авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення.	AC-18	
14	Контроль доступу для мобільних пристроїв	1. Встановити обмеження на використання, дії 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
			AC-20	

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 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.	AC-20(1) AC-20(2)	
16	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 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;	AT-2 AT-2(2)	a.1. щонайменше раз на рік

		– 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).		
18	Рольове навчання	1. Провести тренінги з безпеки для персоналу організації на основі покладених обов'язків: – 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).	AT-3	a.1. щонайменше щороку
Аудит та підзвітність				
19	Події аудиту	1. Визначити перелік подій, які реєструються в системі: (призначення: типи подій, визначені організацією). 2. 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;	AU-3 AU-3(1)	

		– 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.		
21	Збереження записів аудиту	1. Згенерувати записи аудиту для вибраних типів подій згідно з вмістом записів аудиту, вказаних в п. 19 та в п. 20. 2. Зберігати записи аудиту протягом періоду часу, який відповідає політиці зберігання записів аудиту.	AU-11	
			AU-12	а. всі інформаційні системи та мережеві компоненти
22	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
23	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	а. 1-ий параметр: щонайменше щотижня (сім днів)
			AU-6(3)	
24	Скорочення записів аудиту та формування звіту	1. Впровадити функцію скорочення записів аудиту і створення звітів, яка підтримує перегляд записів аудиту, аналіз, дії до звітності та постфактум розслідування інцидентів. 2. Зберігати оригінальний зміст і часовий порядок записів аудиту.	AU-7	
25	Позначка часу	1. Використовувати внутрішній годинник у системі для створення позначок часу для записів аудиту.	AU-8	

		2. 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.		
26	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)	
27	Неспростовність	Надайте неспростовні докази того, що особа (або процес, який діє від імені особи) виконала (призначення: дії, визначені організацією, на які поширюється принцип неспростовності).	AU-10	
Управління конфігурацією				
28	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
29	Налаштування конфігурації	1. Встановити, задокументувати та впровадити параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним діям: (призначення: налаштування конфігурації, визначені організацією). 2. Визначити, задокументувати та затвердити будь які відхилення від встановлених налаштувань конфігурації.	CM-6	c. 1-ий параметр: всі конфігуровані компоненти системи.

30	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.	CM-3	e. 1 рік
31	Аналіз впливу на безпеку та приватність	Проаналізувати вплив змін у системі на безпеку перед їх впровадженням.	CM-4	
32	Обмеження доступу до змін	Визначити, задокументувати, затвердити та впровадити фізичні та логічні обмеження доступу, пов'язані зі змінами в системі.	CM-5	
33	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
Ідентифікація та автентифікація				
34	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	

35	Ідентифікація та автентифікація пристроїв	Унікально ідентифікувати та автентифікувати пристрої перед встановленням з'єднання з системою.	IA-3	
36	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)	
37	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
38	Управління ідентифікацією	1. Отримати дозвіл від персоналу або ролей організації на призначення ідентифікатора особи, групи, ролі, служби або пристрою. 2. Вибрати та призначити ідентифікатор, який ідентифікує особу, групу, роль, службу або пристрій. 3. Запобігати повторному використанню ідентифікаторів для (призначення: період часу, визначений організацією).	IA-4	d. щонайменше рік для окремих осіб, груп, ролей
39	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 паролі, чи не містяться вони у списку загальновживаних, очікуваних або скомпрометованих паролів. 3. Передавати паролі тільки криптографічно захищеними каналами.	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

		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).		
40	Зворотний зв'язок автентифікатора	Забезпечити прихований зворотний зв'язок автентифікаційної інформації під час процесу автентифікації.	IA-6	
41	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
Реагування на інциденти				
42	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	
	Моніторинг інциденту		IR-5	

43		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-6 IR-7	a. 2 години
44	Перевірка реагувань на інциденти	Перевіряти ефективність спроможності реагування на інциденти (призначення: частота , визначена організацією).	IR-3	1-ий параметр: щонайменше щороку
45	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; – надалі із (призначення: частота, визначена організацією). 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
46	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;	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

		– 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; – 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.		впровадження плану реагування на інциденти
Технічне обслуговування				
47	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.	MA-3 MA-3(1) MA-3(2)	b. щонайменше щороку
48	Віддалене обслуговування	1. Затверджувати та контролювати віддалені сеанси з технічного обслуговування та діагностики. 2. Упровадити багатофакторну автентифікацію та стійкість до повторного відтворення при створенні віддалених сеансів технічного обслуговування та діагностики. 3. Забезпечити завершення сеансу та мережевих з'єднань після завершення віддаленого технічного обслуговування.	MA-4	

49	Технічний персонал	1. Встановити процес авторизації персоналу з технічного обслуговування. 2. Вести список уповноважених організацій або персоналу з технічного обслуговування. 3. Переконатися, що персонал без супроводу, який виконує технічне обслуговування системи, має необхідні дозволи на доступ; 4. 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	
Захист носіїв інформації				
50	Зберігання носіїв інформації	Фізично контролювати та безпечно зберігати носії інформації, що містять відкриту та конфіденційну інформацію.	MP-4	
51	Доступ до носіїв інформації	Обмежити доступ до конфіденційної інформації на носіях інформації.	MP-2	1-ий параметр: всі типи цифрових та/або нецифрових носіїв, що містять інформацію, не дозволену для публічного оприлюднення
52	Знищення інформації на носіях інформації	Очистити носії інформації, що містять відкриту та конфіденційну інформацію, перед утилізацією, випуском з-під контролю організації або повторним використанням.	MP-6	
53	Маркування носіїв інформації	Маркувати носії інформації, що містять відкриту та конфіденційну інформацію, для позначення обмежень щодо розповсюдження, застережень стосовно поводження з ними та позначок безпеки.	MP-3	
54	Транспортування носіїв інформації	1. Захистити і контролювати носії інформації, що містять відкриту та конфіденційну інформацію, під час транспортування за межі контрольованих територій.	MP-5 SC-28	

		2. Вести облік носіїв інформації, що містять відкриту та конфіденційну інформацію, під час транспортування за межі контрольованих територій. 3. Документувати дії, пов'язані з транспортуванням системних носіїв, які містять відкриту та конфіденційну інформацію.		
55	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	
56	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; – визначає ролі, обов'язки та відповідальних осіб з контактною інформацією; – спрямований на підтримку основних завдань і функції, попри системні збої, компрометації або помилки; – спрямований на повне відновлення функціонування системи без погіршення запланованих і реалізованих заходів захисту інформації та персональних даних; – вирішує питання обміну інформацією про надзвичайні ситуації; – переглядається та затверджується (призначення: персонал або ролі, визначені організацією). 2. Поширити копії плану забезпечення безперервної роботи та відновлення функціонування серед (призначення: визначеного організацією ключового персоналу з непередбачених обставин	CP-2	

		(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.		
57	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).	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

		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.		надзвичайних ситуаціях (за наявності) c. при створенні, отриманні, оновленні або як визначено в плані дій у надзвичайних ситуаціях (за наявності)
Кадрова безпека				
58	Перевірка персоналу	1. Перевіряти осіб перед тим, як надавати їм доступ до системи. 2. Проводити повторні перевірки осіб відповідно до (призначення: умови, що потребують повторної перевірки, визначені організацією).	PS-3	
59	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;	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
		– 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;	PS-5	b. 1-ий параметр: дії з перепризначення, щоб забезпечити видалення або вимкнення всіх системних доступів, які більше не потрібні

		– 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.		
Фізичний захист і захист робочого середовища				
60	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. 3. Періодично перевіряти список фізичного доступу. 4. Переглядати список доступу до об'єктів (призначення: частота, визначена організацією). 5. Видаляти осіб зі списку фізичного доступу, коли доступ більше не потрібен.	PE-2	c. щонайменше щороку
61	Моніторинг фізичного доступу	1. Моніторити фізичний доступ до місця розташування системи, щоб виявляти та реагувати на інциденти фізичної безпеки. 2. 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
62	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	
63	Керування фізичним доступом	1. Контролювати фізичний доступ до місця, де знаходиться система: – перевіряти індивідуальні фізичні дозволи на доступ перед наданням доступу;	PE-3 PE-5	

		– 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 конфіденційної інформації.		
64	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	
Повноваження на обробку персональних даних				
65	Політика та процедури обробки персональних даних	1. Розробіть, задокументуйте та поширте (призначення: персонал або ролі, визначені організацією) (вибір (один або декілька): Рівень організації; Рівень місії/бізнеспроцесу; рівень системи), обробки персональних даних та політики прозорості, який: – розглядає мету, сферу діяльності, ролі, відповідальність, зобов’язання керівництва, координацію між організаційними підрозділами та відповідність; – відповідає чинним законам, розпорядженням, директивам, положенням, політикам, стандартам і рекомендаціям. 2. Призначте (призначення: посадову особу, визначену організацією) для керування розробкою, документуванням і розповсюдженням політики й	PT-1	

		процедур щодо обробки персональних даних та прозорості. 3. Перегляньте та оновіть поточні процедури обробки та прозорість персональних даних: – політика (призначення: частота, визначена організацією) і наступні (призначення: події, визначені організацією); – процедури (призначення: частота, визначена організацією) та наступні (призначення: подія, визначена організацією).		
66	Повноваження на обробку персональних даних	1. Визначити та задокументувати (призначення: повноваження, визначені організацією з урахуванням підстав для обробки персональних даних, передбачених Законом України «Про захист персональних даних»), які дозволяють (призначення: обробку, визначену організацією) персональних даних. 2. Обмежити (призначення: обробку, визначену організацією) персональних даних лише таким чином, яким дозволено (тільки до того, що дозволено).	PT-2	
67	Цілі обробки персональних даних	1. Визначити та задокументувати (призначення: мету, визначену організацією) обробки персональних даних. 2. Описати мету у публічних повідомленнях про обробку персональних даних і політиках організації. 3. Обмежити (призначення: обробку, визначену організацією) персональних даних лише тією, яка сумісна з визначеною метою. 4. Відстежувати зміни в обробці персональних даних та впроваджувати (завдання: визначені організацією механізми), щоб гарантувати, що будь-які зміни вносяться відповідно до (завдання: визначені організацією вимоги) та Закону України «Про захист персональних даних».	PT-3	

68	Повідомлення про конфіденційність	1. Впровадити повідомлення про обробку персональних даних суб'єктам персональних даних, які: – виражені простою мовою; – визначають підстави для обробки персональних даних; – визначають мету обробки персональних даних; – містять інформацію про володільця персональних даних; – містять інформацію про склад та зміст зібраних персональних даних; – містять інформацію про права суб'єкта персональних даних, визначені Законом України «Про захист персональних даних», та осіб, яким передаються персональні дані. 2. Повідомляти суб'єктів персональних даних про обробку персональних даних у випадках, визначених Законом України «Про захист персональних даних».	PT-5 PT-5(1)	
Оцінювання ризику				
69	Оцінювання ризику	Оцінити ризик несанкціонованого розголошення в результаті обробки, зберігання або передачі конфіденційної інформації.	RA-3	d., f. щонайменше щороку
70	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).	RA-5	a. щонайменше кожні 30 днів
Оцінювання, акредитація та моніторинг безпеки				
71	Оцінювання	Оцінювати дії (призначення: частота, визначена організацією) до безпеки системи та середовища її функціонування, щоб визначити, чи були ці дії виконані.	CA-2	d. щонайменше щороку

72	План усунення недоліків та контрольні показники	1. Розробити план дій і контрольні показники для системи: – задокументувати заплановані заходи виправлення слабких місць або недоліків, з 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	
73	Безперервний моніторинг	Розробити та впровадити стратегію безперервного моніторингу на рівні системи, що передбачає постійний моніторинг та оцінку безпеки.	CA-7	
74	Взаємодія систем	1. 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). 2. Документувати характеристики інтерфейсу, дії до безпеки та обов'язки для кожної системи як частину договорів про обмін. 3. Переглядати та оновлювати (призначення: частота, визначена організацією) договори про обмін.	CA-3	
Захист інформаційної системи та комунікацій				
75	Захист периметра	1. Контролювати та управляти зв'язком на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи. 2. Реалізувати підмережі для загальнодоступних компонентів системи, які фізично або логічно відділені від внутрішніх мереж. 3. Підключатися до зовнішніх мереж тільки через керовані інтерфейси, що складаються з пристроїв	SC-7	

		захисту периметра, розташованих відповідно до архітектури безпеки організації.		
76	Інформація в загальних ресурсах системи	Запобігати несанкціонованій і ненавмисній передачі інформації за допомогою загальних ресурсів системи.	SC-4	
77	Захист від атак «Відмова в обслуговуванні»	1. Захистити та/або обмежити від наслідків наступних типів подій відмови в обслуговуванні: (призначення: визначені організацією типи подій відмови в обслуговуванні). 2. Застосувати наступні заходи захисту для досягнення мети відмови обслуговування (призначення: заходи захисту визначені організацією, за типом події відмови в обслуговуванні).	SC-5	
78	Захист периметра – Відмова за замовчуванням – Дозвіл за винятком	Заборонити трафік мережевих комунікацій за замовчуванням і дозволити трафік мережевих комунікацій за винятком.	SC-7(5)	
79	Конфіденційність і цілісність передачі. Захист інформації у стані спокою	Реалізувати механізми криптографічного захисту для запобігання несанкціонованому розкриттю конфіденційної інформації під час передачі та зберігання.	SC-8	
			SC-8(1)	запобігати несанкціонованому розголошенню інформації та виявляти зміни в ній
			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
80	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
81	Встановлення та управління	Встановити криптографічні ключі в системі та керувати ними відповідно до наведених нижче дій	SC-12	

	криптографічними ключами	(призначення: дії до встановлення та управління ключами, визначені організацією).		
82	Криптографічний захист	Впровадити типи криптографічного захисту при використанні системи для захисту конфіденційності відкритої та конфіденційної інформації (призначення: типи криптографії, визначені організацією).	SC-13	
83	Спільні обчислювальні пристрої та застосунки	1. Заборонити віддалену активацію спільних обчислювальних пристроїв і програмного забезпечення з такими винятками: (призначення: визначені організацією винятки, коли дозволяється віддалена активація). 2. Надавати чіткі вказівки щодо використання користувачам, які фізично наявні біля пристроїв.	SC-15	а. спеціальні апартаменти ВТЦ, розташовані в затверджених місцях
84	Мобільний код	1. Визначити прийнятний мобільний код і технології мобільного коду. 2. Авторизувати, відстежувати та контролювати використання мобільного коду.	SC-18	
85	Автентифікація сесії	Захистити автентифікацію сеансів зв’язку.	SC-23	
Цілісність системи та інформації				
86	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.	SI-2	с. 30 діб
87	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:	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

		– 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.		с.2 2-ий параметр: щонайменше відповідальний адміністратор
88	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	
89	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
Планування безпеки				
90	Політика та процедури планування безпеки	1. Розробити, задокументувати та розповсюдити серед персоналу організації або ролей політики та процедури, необхідні для виконання дій безпеки. 2. Періодично переглядати та оновлювати політики та процедури (призначення: частота, визначена організацією).	AC-1	с.1., с.2. 1-ий параметр: щонайменше щорічно
			AT-1	a. весь персонал с.1, с.2. 1-ий параметр: щонайменше раз на рік
			AU-1	a. 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
			IA-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			IR-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			MA-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			MP-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			PE-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			PL-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			PS-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			RA-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			SA-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			SC-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			SI-1	с.1., с.2. 1-ий параметр: щонайменше щороку
			SR-1	а. як мінімум, ключовий персонал з питань кібербезпеки або уповноважену особу с.1., с.2. 1-ий параметр: щонайменше щороку

91	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
Менеджмент інформаційної безпеки				
92	Стратегія управління ризиками	Розробити комплексну стратегію управління: – ризиками безпеки для операцій та активів організації, фізичних осіб, інших організацій і держави, пов'язаних з експлуатацією та використанням систем організації; – ризиками приватності для фізичних осіб, які можуть виникати внаслідок обробки персональних даних. 2. Реалізувати стратегію управління ризиками в масштабах організації. 3. Переглядати й оновлювати стратегію управління ризиками (призначення: з визначеною організацією частотою) або, якщо потрібно, у разі змін в організації.	PM-9	

Директор директорату
з кіберзахисту та хмарних послуг **Вадим КОНОВАЛ**