ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____ 2025 року № ___

Базовий профіль
безпеки системи, де обробляється службова 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;	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

1	2	3	4	5
		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(13)	1-ий параметр: 30 хвилин

1	2	3	4	5
2.	Забезпечення доступу	Застосовувати затверджені повноваження для логічного доступу до службової інформації та ресурсів у системі.	AC-3	
3.	Управління інформаційними потоками	Застосовувати затверджені дії для управління потоками службової 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); переглянути повноваження, надані користувачам (призначення: періодичність, визначена організацією), щоб підтвердити необхідність таких повноважень; перепризначити або видалити повноваження, за необхідності.	AC-6	
			AC-6(1)	
			AC-6(7)	
			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.			AC-6(9)	

1	2	3	4	5
	Мінімізація повноважень – заборона непривілейованим користувачам виконувати привілейовані функції	Заборонити непривілейованим користувачам виконувати привілейовані функції; ведення журналу виконання привілейованих функцій.	AC-6(10)	
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 службової 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	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

1	2	3	4	5
		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(1)	
11.	Припинення сеансу	Автоматично завершувати сеанс користувача після (призначення: умови або події, що вимагають відключення сеансу, визначені організацією).	AC-12	
12.	Віддалений доступ	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.	AC-17	
			AC-17(3)	
			AC-17(4)	
13.	Бездротовий доступ		AC-18	
			AC-18(1)	користувачі та пристрої

1	2	3	4	5
		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; вимкнути можливості бездротового доступу, якщо вони не призначені для використання, перед їх запуском та розгортанням; захистити бездротовий доступ до системи за допомогою автентифікації та шифрування.	AC-18(3)	
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 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 службової інформації, лише після: перевірки реалізації	AC-20	
			AC-20(1)	
			AC-20(2)	

1	2	3	4	5
		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 службової інформації в загальнодоступних системах; періодично переглядати вміст загальнодоступних систем на предмет наявності службової 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).	AT-2	a.1. щонайменше раз на рік
			AT-2(2)	
			AT-2(3)	
18.	Рольове навчання	1) провести тренінги з безпеки для персоналу організації на основі покладених обов’язків: перед авторизацією доступу до системи або службової інформації, перед виконанням	AT-3	a.1. щонайменше щороку

1	2	3	4	5
		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).		
Аудит та підзвітність				
19.	Події аудиту	Визначити перелік подій, які реєструються в системі: (призначення: типи подій, визначені організацією) 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	
			AU-12	а. всі інформаційні системи та мережеві компоненти

1	2	3	4	5
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.	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	

1	2	3	4	5
26.	Захист інформації аудиту	Захистити інформацію аудиту та інструментів журналювання аудиту від несанкціонованого доступу, зміни та видалення; надавати доступ до управління функціями аудиту тільки підмножині привілейованих користувачів або ролей.	AU-9	
			AU-9(4)	
Управління конфігурацією				
27.	Базова конфігурація	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.	CM-2	b.1. щонайменше щороку
28.	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 будь-які відхилення від встановлених налаштувань конфігурації.	CM-6	c. 1-ий параметр: всі конфігуровані компоненти системи.
29.	Управління змінами конфігурації	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 конфігурації системи;	CM-3	e. 1 рік

1	2	3	4	5
		відстежувати та переглядати дії, пов'язані зі змінами в конфігурації системи, які необхідно контролювати.		
30.	Аналіз впливу на безпеку та приватність	Проаналізувати вплив змін у системі на безпеку перед їх впровадженням; переконайтеся, що дії до безпеки системи продовжують задовольнятися після впровадження змін у системі.	СМ-4	
			СМ-4(2)	
31.	Обмеження доступу до змін	Визначити, задокументувати, затвердити та впровадити фізичні та логічні обмеження доступу, пов'язані зі змінами в системі.	СМ-5	
32.	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.	СМ-7	b. всі функції, порти, протоколи, програмне забезпечення та послуги в системі, які були визначені як непотрібні та/або незахищені
			СМ-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
33.	Мінімально необхідна функціональність – авторизоване програмне забезпечення — білий список	Визначити програмне забезпечення, дозволене для виконання в системі; впровадити політику «заборонити все, дозволити за винятком» для виконання дозволеного програмного забезпечення в системі; переглянути та оновити список дозволеного програмного забезпечення (призначення: частота, визначена організацією).	СМ-7(5)	c. щонайменше раз на рік

1	2	3	4	5
34.	Інвентаризація компонентів системи	Розробити та задокументувати інвентаризацію компонентів системи. Перегляд та оновлення інвентаризації компонентів системи (призначення: частота, визначена організацією); оновлення інвентаризації компонентів системи в рамках встановлення, видалення та оновлення системи.	СМ-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, власник інформаційної системи/компонента, а для мережевого компонента/пристрою - ім'я обладнання b. щонайменше щороку
			СМ-8(1)	
35.	Розташування інформації	Визначити та задокументувати місцезнаходження службової інформації та компонентів системи, в яких обробляється та зберігається інформація; задокументувати зміни в системі або компонентів системи, де обробляється та зберігається службова інформація.	СМ-12	
36.	Базова конфігурація - конфігурація систем та компонентів для сфер з високим ризиком	Надавати системи або системні компоненти з наступними конфігураціями особам, які прямують до зони підвищеного ризику: (призначення: визначені організацією конфігурації системи); застосовувати такі дії безпеки до систем або компонентів, коли особи повертаються з подорожі: (призначення: визначені організацією дії безпеки).	СМ-2(7)	
Ідентифікація та автентифікація				

1	2	3	4	5
37.	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; повторно автентифікувати користувачів, коли (призначення: визначені організацією обставини або ситуації, що вимагають повторної автентифікації).	IA-2	
			IA-11	
38.	Ідентифікація та автентифікація пристроїв	Унікально ідентифікувати та автентифікувати пристрої перед встановленням з'єднання з системою.	IA-3	
39.	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)	
40.	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
41.	Управління ідентифікацією		IA-4	d. щонайменше рік для окремих осіб, груп, ролей

1	2	3	4	5
		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); керувати індивідуальними ідентифікаторами, унікально ідентифікуючи кожну особу як (призначення: визначена організацією характеристика, що ідентифікує статус особи).	IA-4(4)	
42.	Управління автентифікатором – автентифікація на основі пароля	Вести перелік часто використовуваних, очікуваних або скомпрометованих паролів і періодично оновлювати його, а також у разі виникнення підозри, що паролі організації були скомпрометовано; перевіряти, коли користувачі створюють або оновлюють паролі, чи не містяться вони у списку загальновживаних, очікуваних або скомпрометованих паролів; передавати паролі тільки криптографічно захищеними каналами; зберігати паролі в криптографічно захищеному вигляді; встановити новий пароль при першому використанні після відновлення облікового запису; 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

1	2	3	4	5
43.	Зворотний зв'язок автентифікатора	Забезпечити прихований зворотний зв'язок автентифікаційної інформації під час процесу автентифікації.	IA-6	
44.	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				
45.	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	
46.	Моніторинг інциденту	Відстежувати та документувати інциденти, пов'язані з безпекою системи;	IR-5	
			IR-6	a. 2 години

1	2	3	4	5
		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-7	
47.	Перевірка реагувань на інциденти	Перевіряти ефективність спроможності реагування на інциденти (призначення: частота , визначена організацією).	IR-3	1-ий параметр: щонайменше щороку
48.	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
49.	План реагування на інциденти	1) розробити план реагування на інцидент, який: надає організації план дій для реалізації її можливостей реагування на інциденти,	IR-8	b. весь персонал, який має роль або відповідальність за впровадження плану реагування на інциденти

1	2	3	4	5
		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.		d. весь персонал, який має роль або відповідальність за впровадження плану реагування на інциденти
Технічне обслуговування				
50.	Інструменти для обслуговування	Затверджувати, контролювати та відстежувати використання інструментів технічного обслуговування системи;	MA-3	b. щонайменше щороку
			MA-3(1)	
			MA-3(2)	

1	2	3	4	5
		перевіряти інструменти для технічного обслуговування на наявність неналежних або несанкціонованих модифікацій; запобігати вилученню обладнання для обслуговування системи, що містить службову інформацію, шляхом перевірки відсутності службової інформації на обладнанні, санітарної обробки або знищення обладнання, або утримання обладнання в межах об'єкта.	MA-3(3)	
51.	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.	MA-4	
52.	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.	MA-5	
Захист носіїв інформації				

1	2	3	4	5
53.	Зберігання носіїв інформації	Фізично контролювати та безпечно зберігати носії інформації, що містять службову інформацію.	MP-4	
54.	Доступ до носіїв інформації	Обмежити доступ до службової інформації на носіях інформації.	MP-2	1-ий параметр: всі типи цифрових та/або нецифрових носіїв, що містять інформацію, не дозволену для публічного оприлюднення
55.	Знищення інформації на носіях інформації	Очистити носії інформації, що містять службову інформацію, перед утилізацією, випуском з-під контролю організації або повторним використанням.	MP-6	
56.	Маркування носіїв інформації	Маркувати носії інформації, що містять службову інформацію, для позначення обмежень щодо розповсюдження, застережень стосовно поводження з ними та позначок безпеки.	MP-3	
57.	Транспортування носіїв інформації	Захистити і контролювати носії інформації, що містять службову інформацію, під час транспортування за межі контрольованих територій; вести облік носіїв інформації, що містять службову інформацію, під час транспортування за межі контрольованих територій. Документувати дії, пов'язані з транспортуванням системних носіїв, які містять службову інформацію.	MP-5 SC-28	
58.	Використання носіїв інформації	Обмежити або заборонити використання (призначення: типи носіїв інформації, визначені організацією); заборонити використання знімних носіїв інформації без ідентифікованого власника.	MP-7	

1	2	3	4	5
59.	Резервне копіювання	Захистити конфіденційність резервної копії. 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)	
Кадрова безпека				
60.	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	

1	2	3	4	5
61.	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
Фізичний захист і захист робочого середовища				
62.	Авторизація фізичного доступу	Розробити, затвердити та підтримувати список осіб, які мають право доступу до фізичного місця розташування системи;	PE-2	c. щонайменше щороку

1	2	3	4	5
		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.		
63.	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
64.	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	
65.			PE-3	

1	2	3	4	5
	Керування фізичним доступом	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-5	
66.	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				
67.	Оцінювання ризику	Оцінити ризик несанкціонованого розголошення в результаті обробки, зберігання або передачі службової інформації; оновлювати оцінки ризиків (призначення: частота, визначена організацією).	RA-3	d., f. щонайменше щороку
			RA-3(1)	b. щонайменше раз на рік
			SR-6	щонайменше раз на рік або за потребою у зв'язку з певними подіями
68.			RA-5	a. щонайменше кожні 30 днів

1	2	3	4	5
	Сканування вразливостей	Моніторити та сканувати систему на наявність вразливостей (призначення: частота, визначена організацією) та при виявленні нових вразливостей, що впливають на систему. Усунути вразливості системи протягом часу (призначення: час на реагування, визначений організацією). Оновлювати вразливості системи, що підлягають скануванню (призначення: частота, визначена організацією), а також при виявленні нових вразливостей і повідомляти про них.	RA-5(2)	протягом 24 годин до запуску сканування
69.	Реагування на ризики	Реагувати на результати оцінок безпеки, моніторингу та аудитів.	RA-7	
Оцінювання, акредитація та моніторинг безпеки				
70.	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
71.	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	

1	2	3	4	5
72.	Безперервний моніторинг	Розробити та впровадити стратегію безперервного моніторингу на рівні системи, що передбачає постійний моніторинг та оцінку безпеки.	CA-7	
73.	Взаємодія систем	Затвердити та керувати обміном службової 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 та обов'язки для кожної системи як частину договорів про обмін; переглядати та оновлювати (призначення: частота, визначена організацією) договори про обмін.	CA-3	
Захист інформаційної системи та комунікацій				
74.	Захист периметра	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; підключатися до зовнішніх мереж тільки через керовані інтерфейси, що складаються з пристроїв захисту периметра, розташованих відповідно до архітектури безпеки організації.	SC-7	
75.	Інформація в загальних ресурсах системи	Запобігати несанкціонованій і ненавмисній передачі інформації за допомогою загальних ресурсів системи.	SC-4	

1	2	3	4	5
76.	Захист периметра - відмова за замовчуванням - дозвіл за винятком	Заборонити трафік мережевих комунікацій за замовчуванням і дозволити трафік мережевих комунікацій за винятком.	SC-7(5)	
77.	Конфіденційність і цілісність передачі. Захист інформації у стані спокою	Реалізувати механізми криптографічного захисту для запобігання несанкціонованому розкриттю службової 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
78.	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
79.	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	
80.	Криптографічний захист	Впровадити типи криптографічного захисту при використанні системи для захисту конфіденційності службової інформації (призначення: типи криптографії, визначені організацією).	SC-13	
81.	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);	SC-15	а. спеціальні апартаменти ВТЦ, розташовані в затверджених місцях

1	2	3	4	5
		надавати чіткі вказівки щодо використання користувачам, які фізично наявні біля пристроїв.		
82.	Мобільний код	Визначити прийнятний мобільний код і технології мобільного коду; авторизувати, відстежувати та контролювати використання мобільного коду.	SC-18	
83.	Автентифікація сесії	Захистити автентифікацію сеансів зв'язку.	SC-23	
Цілісність системи та інформації				
84.	Виправлення дефектів	Виявляти, повідомляти та виправляти недоліки системи; встановлювати оновлення програмного забезпечення та вбудованих програм, що стосуються безпеки, протягом (призначення: період часу, визначений організацією) після виходу оновлень.	SI-2	с. 30 діб
85.	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;	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

1	2	3	4	5
		блокування шкідливого коду, поміщення шкідливого коду в карантин або інші дії у відповідь на виявлення шкідливого коду.		
86.	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	
87.	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
88.	Управління та збереження інформації	Керувати та зберігати службову інформації в системі та виводити службову інформацію з системи відповідно до чинного законодавства, організаційно-розпорядчих актів, директив, положень, політик, стандартів, інструкцій та операційних дій.	SI-12	
Планування безпеки				
89.	Політика та процедури планування безпеки	Розробити, задокументувати та розповсюдити серед персоналу організації або ролей	AC-1	с.1., с.2. 1-ий параметр: щонайменше щорічно
			AT-1	a. весь персонал

1	2	3	4	5
		політики та процедури, необхідні для виконання дій безпеки; періодично переглядати та оновлювати політики та процедури (призначення: частота, визначена організацією).		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
			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

1	2	3	4	5
				c.1., c.2. 1-ий параметр: щонайменше щороку
90.	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 службової 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
91.	Правила поведінки	1) встановити правила, які описують обов'язки та очікувану поведінку щодо використання системи та захисту службової інформації; 2) ознайомлювати з правилами осіб, яким потрібен доступ до системи; 3) отримувати задокументоване підтвердження від осіб, що вони прочитали, зрозуміли та згодні дотримуватися правил поведінки, перш ніж надавати їм доступ до службової інформації та системи; 4) переглядати та оновити правила поведінки (призначення: частота, визначена організацією).	PL-4	c. щонайменше раз на рік d. щонайменше раз на рік або коли правила переглядаються чи оновлюються
Придбання систем та послуг				

1	2	3	4	5
92.	Принципи інженерії безпеки	Застосовувати наведені нижче принципи інженерії безпеки систем до розробки або модифікації системи та її компонентів: (призначення: принципи інженерії безпеки систем, визначені організацією).	SA-8	
93.	Компоненти системи, що не підтримуються	Замінювати компоненти системи, якщо розробник, постачальник або виробник більше не надає їхню підтримку; надати варіанти зменшення ризиків або альтернативні джерела для продовження підтримки компонентів, що не підтримуються, якщо їх неможливо замінити.	SA-22	
94.	Зовнішні послуги для системи	Вимагати від постачальників зовнішніх послуг для системи, що використовуються для обробки, зберігання або передачі службової інформації, дотримання наступних дій безпеки: (призначення: дії безпеки, визначені організацією); визначити та задокументувати ролі та обов'язки користувачів відносно зовнішніх послуг для системи, включаючи спільні обов'язки із зовнішніми постачальниками; впровадити процеси, методи та техніки для постійного моніторингу дотримання дій безпеки зовнішніми постачальниками послуг.	SA-9	
Управління ризиками ланцюга постачання				
95.	План управління ризиками ланцюга постачання	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;	SR-2	b. щонайменше раз на рік

1	2	3	4	5
		переглядати та оновлювати план управління ризиками ланцюга постачання (призначення: частота, визначена організацією); захищати план управління ризиками ланцюга постачання від несанкціонованого розголошення.		
96.	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	
97.	Контроль ланцюга постачання і процесів	Запровадити процес виявлення та усунення слабких місць або недоліків в елементах та процесах ланцюга постачання; упровадити наведені нижче дії 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: дії безпеки, визначені організацією).	SR-3	

Т.в.о. директора
Департаменту захисту інформації
Адміністрації Держспецзв’язку
полковник Андрій ГОЛОВЕНКО