Додаток
до наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____ 2024 року № ___

Базовий профіль безпеки інформації

Розділ І. Для інформаційно-комунікаційної системи, де обробляється відкрита інформація.

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
1.	**Управління доступом**		**АС**
1.1.	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: облікові записи більше не потрібні; користувачі звільняються або переводяться; у системі наявні зміни, які потребують нових знань.	АС-2
1.2.	Забезпечення доступу	Застосовувати затверджені повноваження для логічного доступу до конфіденційної інформації та ресурсів у системі.	АС-3
1.3.	Управління інформаційними потоками	Застосовувати затверджені вимоги для управління потоками відкритої та конфіденційної інформації всередині системи та між підключеними системами.	АС-4
1.4.	Розмежування обов'язків	Визначити обов'язки осіб, які потребують розмежування; установити правила авторизації доступу для підтримки розмежування обов'язків.	АС-5
1.5.	Мінімізація повноважень	Надавати користувачам (або процесам, що діють від імені користувачів) лише авторизований	АС-6, АС-6(1), AU-9(4)

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
		доступ до системи, необхідний для виконання поставлених завдань організації; авторизувати доступ до [*призначення: функції безпеки, визначені організацією, та важлива для безпеки інформація*].	
1.6.	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), AC-6(5)
1.7.	Мінімізація повноважень – заборона непривілейованим користувачам виконувати привілейовані функції	Заборонити непривілейованим користувачам виконувати привілейовані функції.	AC-6(10)
1.8.	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*].	AC-7
1.9.	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
1.10.	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, AC-11(1)
1.11.	Припинення сеансу	Автоматично завершувати сеанс користувача після [*призначення: умови або події, що*	AC-12

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
		вимагають відключення сеансу, визначені організацією].	
1.12.	Віддалений доступ	Встановити обмеження на використання, вимоги 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)
1.13.	Бездротовий доступ	Встановити обмеження на використання, вимоги до конфігурації та підключення для кожного типу бездротового доступу до системи; авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення.	AC-18
1.14.	Контроль доступу для мобільних пристроїв	Встановити обмеження на використання, вимоги 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)
1.15.	Використання зовнішніх систем	1) Заборонити використання зовнішніх систем, крім систем дозволених організацією; 2) установити такі положення, умови та вимоги щодо безпеки, які повинні бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованим особам: [*призначення: умови, положення та вимоги визначаються організацією*]; 3) дозволити авторизованим особам використовувати зовнішню систему для доступу до системи організації або для обробки, зберігання чи передачі відкритої та конфіденційної інформації, лише після: перевірки реалізації вимог безпеки на зовнішній системі, як зазначено в планах безпеки організації; збереження затверджених угод про підключення або обробку даних з організацією, що розміщує зовнішню систему, з якою укладено відповідну угоду;	AC-20, AC-20(1), AC-20(2)

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
		4) обмежити використання портативних пристроїв зберігання даних авторизованими особами на зовнішніх системах.	
1.16.	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
2.	**Обізнаність і навчання**		**AT**
2.1.	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*]; 2) періодично оновлювати зміст тренінгу з безпекової обізнаності [*призначення*: *визначені організацією події*].	AT-2, AT-2(2)
2.2.	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 періодично після цього; коли цього вимагають зміни в системі або після [*призначення: події, визначені організацією*]; 2) періодично оновлювати зміст тренінгів на основі покладених обов'язків, а також після [*призначення: події, визначені організацією*].	AT-3
3.	**Аудит і підзвітність**		**AU**
3.1.	Події аудиту	Визначити перелік подій, які реєструються в системі: [*призначення: типи подій, визначені організацією*]; періодично переглядати та оновлювати типи подій, обрані для реєстрації.	AU-2
3.2.	Зміст записів аудиту	1) Записи аудиту повинні містити таку інформацію: який тип події стався; коли відбулася подія; де відбулася подія; джерело події; наслідки події;	AU-3, AU-3(1)

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
		результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією; 2) за потреби надавати додаткову інформацію для записів аудиту.	
3.3.	Збереження записів аудиту	Згенерувати записи аудиту для вибраних типів подій згідно з вмістом записів аудиту, вказаних в 3.1 та в 3.2; зберігати записи аудиту протягом періоду часу, який відповідає політиці зберігання записів аудиту.	AU-11, AU-12
3.4.	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
3.5.	Огляд, аналіз і звітність аудиту	Переглядати та аналізувати 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, AU-6(3)
3.6.	Скорочення записів аудиту та формування звіту	Упровадити функцію скорочення записів аудиту і створення звітів, яка підтримує перегляд записів аудиту, аналіз, вимоги до звітності та постфактум розслідування інцидентів. Створити та зберігати журнали та записи аудиту системи в обсязі, необхідному для моніторингу, аналізу, розслідування та звітування про незаконну або несанкціоновану діяльність у системі; зберігати оригінальний зміст і часовий порядок записів аудиту.	AU-7
3.7.	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

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
3.8.	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)
4.	**Управління конфігурацією**		**CM**
4.1.	Базова конфігурація	Розробляти та підтримувати під контролем налаштування поточної базової конфігурації системи; періодично переглядати та оновлювати базову конфігурацію системи, а також при встановленні або модифікації компонентів системи.	CM-2
4.2.	Налаштування конфігурації	Встановити, задокументувати та впровадити параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам: [*призначення: налаштування конфігурації, визначені організацією*]; визначити, задокументувати та затвердити будь-які відхилення від встановлених налаштувань конфігурації.	CM-6
4.3.	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; відстежувати та переглядати дії, пов'язані зі змінами в конфігурації системи, які необхідно контролювати.	CM-3
4.4.	Аналіз впливу на безпеку та приватність	Проаналізувати вплив змін у системі на безпеку перед їх впровадженням.	CM-4
4.5.	Обмеження доступу до змін	Визначити, задокументувати, затвердити та впровадити фізичні та логічні обмеження доступу, пов'язані зі змінами в системі.	CM-5
4.6.	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*];	CM-7, CM-7(1)

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
		періодично переглядати 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.	
5.	**Ідентифікація та автентифікація**		**ІА**
5.1.	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.	ІА-2
5.2.	Ідентифікація та автентифікація пристроїв	Унікально ідентифікувати та автентифікувати пристрої перед встановленням з'єднання з системою.	ІА-3
5.3.	Ідентифікація та автентифікація (користувачів організації) – Багатофакторна автентифікація привілейованих облікових записів	Упровадити багатофакторну автентифікацію для доступу до облікових записів системи.	ІА-2(1), ІА-2(2)
5.4.	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.	ІА-2(8)
5.5.	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*].	ІА-4
5.6.	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	ІА-5(1)

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
		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*].	
5.7.	Зворотний зв'язок автентифікатора	Забезпечити прихований зворотний зв'язок автентифікаційної інформації під час процесу автентифікації.	IA-6
5.8.	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
6.	**Реагування на інциденти**		**IR**
6.1.	Обробка інциденту	Розробити план реагування на інциденти, який забезпечить організацію стратегії для реалізації її можливостей реагування на інциденти; упровадити систему реагування на інциденти, яка відповідає плану реагування на інциденти і передбачає підготовку, виявлення та аналіз, локалізацію, ліквідацію та відновлення інцидентів; оновити план реагування на інциденти, щоб врахувати зміни в системі та зміни в організації	IR-4, IR-8

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
		або проблеми, що виникли під час впровадження, виконання або тестування плану.	
6.2.	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, IR-7
6.3.	Перевірка реагувань на інциденти	Періодично перевіряти ефективність системи реагування на інциденти.	IR-3
6.4.	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; періодично після змін у системі; 2) періодично переглядати та оновлювати зміст навчання з реагування на інциденти [*призначення: події, визначені організацією*].	IR-2
7.	**Технічне обслуговування**		**MA**
7.1.	Інструменти для обслуговування	Затверджувати, контролювати та відстежувати використання інструментів технічного обслуговування системи; перевіряти інструменти для технічного обслуговування на наявність неналежних або несанкціонованих модифікацій; перевіряти носії, що містять діагностичні та тестові програми, на наявність шкідливого коду, перш ніж використовувати їх у системі.	MA-3, MA-3(1), MA-3(2)
7.2.	Віддалене обслуговування	Затверджувати та контролювати віддалені сеанси з технічного обслуговування та діагностики;	MA-4

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
		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.	
7.3.	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
8.	**Захист носіїв інформації**		**MP**
8.1.	Зберігання носіїв інформації	Фізично контролювати та безпечно зберігати носії інформації, що містять відкриту та конфіденційну інформацію, до моменту їх знищення або очищення за допомогою затвердженого обладнання, методів і процедур.	MP-4
8.2.	Доступ до носіїв інформації	Обмежити доступ до конфіденційної інформації на носіях інформації.	MP-2
8.3.	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
8.4.	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
8.5.	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.	MP-5, SC-28, SC-28(1)

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
8.6.	Використання носіїв інформації	Обмежити або заборонити використання [*призначення: типи носіїв інформації, визначені організацією*]; заборонити використання знімних носіїв інформації без ідентифікованого власника.	MP-7
9.	**Кадрова безпека**		**PS**
9.1.	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
9.2.	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, PS-5
10.	**Фізичний захист і захист робочого середовища**		**PE**
10.1.	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; видаляти осіб зі списку фізичного доступу, коли доступ більше не потрібен.	PE-2
10.2.	Моніторинг фізичного доступу	Моніторити фізичний доступ до місця розташування системи, щоб виявляти та реагувати на інциденти фізичної безпеки; періодично переглядати журнали фізичного доступу.	PE-6

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
10.3.	Альтернативне робоче місце	Визначити альтернативні робочі місця, дозволені для використання працівниками; застосовувати вимоги безпеки на альтернативних робочих місцях [*призначення: вимоги безпеки, визначені організацією*].	PE-17
10.4.	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 [призначення: обставини, що вимагають супроводу відвідувачів та контролю за їхньою діяльністю, визначені організацією]; 4) забезпечити захист ключів, кодів доступу та інших пристроїв фізичного доступу.	PE-3
10.5.	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; контролювати фізичний доступ до пристроїв виводу, щоб запобігти доступу сторонніх осіб до конфіденційної інформації.	PE-4, PE-5
11.	**Оцінка ризику**		**RA**
11.1.	Оцінювання ризику	Оцінити ризик несанкціонованого розголошення в результаті обробки, зберігання або передачі конфіденційної інформації; періодично оновлювати оцінки ризиків.	RA-3
11.2.	Сканування вразливостей	Періодично проводити перевірку, відстеження та сканування системи на наявність вразливостей, а також при виявленні нових вразливостей, що впливають на систему; усунути вразливості системи протягом часу [*призначення: час на реагування, визначений організацією*].	RA-5
12.	**Оцінювання, акредитація та моніторинг безпеки**		**CA**
12.1.	Оцінювання	Періодично оцінювати вимоги до безпеки системи та середовища її функціонування, щоб визначити, чи були ці вимоги виконані.	CA-2

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
12.2.	План усунення недоліків та контрольні показники	1) Розробити план дій і контрольні показники для системи: задокументувати заплановані заходи з виправлення слабких місць або недоліків, виявлених під час оцінювання безпеки; зменшити або усунути відомі недоліки системи; 2) періодично оновлювати існуючий план дій і показників на основі результатів оцінки безпеки, незалежних аудитів або оглядів, а також безперервного моніторингу.	CA-5
12.3.	Безперервний моніторинг	Розробити та впровадити стратегію безперервного моніторингу на рівні системи, що передбачає постійний моніторинг та оцінку безпеки.	CA-7
12.4.	Взаємодія систем	Затвердити та керувати обміном конфіденційної інформації між системою та іншими системами, використовуючи [*вибір (один або декілька): угоди про безпеку з'єднання; угоди про безпеку обміну інформацією; меморандуми або угоди про взаєморозуміння; угоди про рівень обслуговування; угоди з користувачами; угоди про нерозголошення інформації*]; документувати характеристики інтерфейсу, вимоги до безпеки та обов'язки для кожної системи як частину договорів про обмін; періодично переглядати та оновлювати договори про обмін.	CA-3
13.	**Захист інформаційної системи та комунікацій**		**SC**
13.1.	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
13.2.	Інформація в загальних ресурсах системи	Запобігати несанкціонованій і ненавмисній передачі інформації за допомогою загальних ресурсів системи.	SC-4

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
13.3.	Захист периметра - Відмова за замовчуванням - Дозвіл за винятком	Заборонити трафік мережевих комунікацій за замовчуванням і дозволити трафік мережевих комунікацій за винятком.	SC-7(5)
13.4.	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), SC-28, SC-28(1)
13.5.	Відключення мережі	Завершити з'єднання з мережею, яке пов'язане із сеансом зв'язку в кінці сеансу або після періоду бездіяльності.	SC-10
13.6.	Встановлення та управління криптографічними ключами	Встановити криптографічні ключі в системі та керувати ними відповідно до наведених нижче вимог [*призначення: вимоги до встановлення та управління ключами, визначені організацією*].	SC-12
13.7.	Криптографічний захист	Впровадити типи криптографічного захисту при використанні системи для захисту конфіденційності відкритої та конфіденційної інформації [*призначення: типи криптографії, визначені організацією*].	SC-13
13.8.	Спільні обчислювальні пристрої та застосунки	Заборонити віддалену активацію спільних обчислювальних пристроїв і програмного забезпечення; надавати чіткі вказівки щодо використання користувачам, які фізично наявні біля пристроїв.	SC-15
13.9.	Мобільний код	Визначити прийнятний мобільний код і технології мобільного коду; авторизувати, відстежувати та контролювати використання мобільного коду.	SC-18
13.10.	Автентифікація сесії	Захистити автентифікацію сеансів зв'язку.	SC-23
14.	**Цілісність системи та інформації**		**SI**
14.1.	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
14.2.	Захист від шкідливого коду	1) Упровадити механізми захисту від шкідливого коду у визначених місцях системи для виявлення та знищення шкідливого коду;	SI-3

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
		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.	
14.3.	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
14.4.	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)
15.	**Планування безпеки**		**PL**
15.1.	Політика та процедури планування безпеки	Розробити, задокументувати та розповсюдити серед персоналу організації або ролей політики та процедури, необхідні для виконання вимог безпеки; періодично переглядати та оновлювати політики та процедури.	AC-1, AT-1, AU-1, CA-1, CM-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1, SR-1
15.2.	Плани захисту інформації та персональних даних	1) Розробити план захисту інформації, який: визначає складові компоненти системи; описує робоче середовище системи;	PL-2

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
		описує конкретні загрози для системи, які викликають занепокоєння в організації; надає огляд вимог до безпеки системи; визначає з'єднання з іншими системами; визначає осіб, які виконують ролі та обов'язки в системі; містить іншу інформацію, необхідну для захисту відкритої та конфіденційної інформації; 2) періодично переглядати та оновлювати план захисту інформації; 3) захистити план захисту інформації від неавторизованого розголошення.	

Розділ ІІ. Для інформаційно-комунікаційної системи, де обробляється службова інформація.

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
1.	**Управління доступом**		**АС**
1.1.	Управління обліковими записами	2) 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) деактивувати облікові записи в системі, коли: термін дії облікових записів закінчився; облікові записи були неактивні протягом [*призначення: період часу, визначений організацією*]; облікові записи більше не пов'язані з користувачем або фізичною особою; облікові записи порушують політику організації; виявлено значні ризики, пов'язані з фізичними особами.	АС-2, АС-2(3), АС-2(13)

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
		7) оповістити персонал або ролі організації, коли: облікові записи більше не потрібні; користувачі звільняються або переводяться; у системі наявні зміни, які потребують нових знань.	
1.2.	Забезпечення доступу	Застосовувати затверджені повноваження для логічного доступу до службової інформації та ресурсів у системі.	AC-3
1.3.	Управління інформаційними потоками	Застосовувати затверджені вимоги для управління потоками службової інформації всередині системи та між підключеними системами.	AC-4
1.4.	Розмежування обов’язків	Визначити обов'язки осіб, які потребують розмежування; установити правила авторизації доступу для підтримки розмежування обов’язків.	AC-5
1.5.	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*]; періодично перевіряти привілеї, призначені ролям або класам користувачів, щоб підтвердити необхідність таких привілеїв; за необхідності перепризначити або видалити привілеї.	AC-6, AC-6(1), AC-6(7), AU-9(4)
1.6.	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), AC-6(5)
1.7.	Мінімізація повноважень – заборона непривілейованим користувачам виконувати привілейовані функції	Заборонити непривілейованим користувачам виконувати привілейовані функції; реєструвати виконання привілейованих функцій.	AC-6(9), AC-6(10)
1.8.	Невдалі спроби входу в систему	Встановити обмеження на кількість [*призначення: кількість, яка визначена організацією*] невдалих спроб входу в систему	AC-7

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
		протягом певного часу [*призначення: проміжок часу, визначений організацією*].	
1.9.	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
1.10.	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, AC-11(1)
1.11.	Припинення сеансу	Автоматично завершувати сеанс користувача після [*призначення: умови або події, що вимагають відключення сеансу, визначені організацією*].	AC-12
1.12.	Віддалений доступ	Встановити обмеження на використання, вимоги 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)
1.13.	Бездротовий доступ	Встановити обмеження на використання, вимоги до конфігурації та підключення для кожного типу бездротового доступу до системи; авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення; вимкнути перед розгортанням та запуском бездротові мережеві можливості, якщо вони не призначені для використання.	AC-18, AC-18(3)

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
1.14.	Контроль доступу для мобільних пристроїв	Встановити обмеження на використання, вимоги 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)
1.15.	Використання зовнішніх систем	1) Заборонити використання зовнішніх систем, крім систем дозволених організацією; 2) установити такі положення, умови та вимоги щодо безпеки, які повинні бути виконані у зовнішніх системах, перш ніж дозволити використання або доступ до цих систем авторизованим особам: [*призначення: умови, положення та вимоги визначаються організацією*]; 3) дозволити авторизованим особам використовувати зовнішню систему для доступу до системи організації або для обробки, зберігання чи передачі службової інформації, лише після: перевірки реалізації вимог безпеки на зовнішній системі, як зазначено в планах безпеки організації; збереження затверджених угод про підключення або обробку даних з організацією, що розміщує зовнішню систему, з якою укладено відповідну угоду; 4) обмежити використання портативних пристроїв зберігання даних авторизованими особами на зовнішніх системах.	AC-20, AC-20(1), AC-20(2)
1.16.	Публічно доступний контент	Навчати авторизованих осіб щодо нерозголошення службової в загальнодоступних системах; періодично переглядати вміст загальнодоступних систем на предмет наявності службової інформації та видаляти таку інформацію, якщо її виявлено.	AC-22
2.	**Обізнаність і навчання**		**AT**
2.1.	Навчання з підвищення обізнаності	3) 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*];	AT-2, AT-2(2), AT-2(3)

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
		про розпізнавання та повідомлення про ознаки внутрішньої загрози, соціальної інженерії та соціального майнінгу; 4) періодично оновлювати зміст тренінгу з безпекової обізнаності [*призначення*: *визначені організацією події*].	
2.2.	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 призначених обов'язків, а також періодично після цього; коли цього вимагають зміни в системі або після [*призначення: події, визначені організацією*]; 2) періодично оновлювати зміст тренінгів на основі покладених обов'язків, а також після [*призначення: події, визначені організацією*].	АТ-3
3.	**Аудит і підзвітність**		**AU**
3.1.	Події аудиту	Визначити перелік подій, які реєструються в системі: [*призначення: типи подій, визначені організацією*]; періодично переглядати та оновлювати типи подій, обрані для реєстрації.	AU-2
3.2.	Зміст записів аудиту	3) 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; 4) за потреби надавати додаткову інформацію для записів аудиту.	AU-3, AU-3(1)
3.3.	Збереження записів аудиту	Згенерувати записи аудиту для вибраних типів подій згідно з вмістом записів аудиту, вказаних в 3.1 та в 3.2; зберігати записи аудиту протягом періоду часу, який відповідає політиці зберігання записів аудиту.	AU-11, AU-12
3.4.	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

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
3.5.	Огляд, аналіз і звітність аудиту	Переглядати та аналізувати 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, AU-6(3)
3.6.	Скорочення записів аудиту та формування звіту	Упровадити функцію скорочення записів аудиту і створення звітів, яка підтримує перегляд записів аудиту, аналіз, вимоги до звітності та постфактум розслідування інцидентів. Створити та зберігати журнали та записи аудиту системи в обсязі, необхідному для моніторингу, аналізу, розслідування та звітування про незаконну або несанкціоновану діяльність у системі; зберігати оригінальний зміст і часовий порядок записів аудиту.	AU-7
3.7.	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
3.8.	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)
4.	**Управління конфігурацією**		**CM**
4.1.	Базова конфігурація	Розробляти та підтримувати під контролем налаштування поточної базової конфігурації системи; періодично переглядати та оновлювати базову конфігурацію системи, а також при встановленні або модифікації компонентів системи.	CM-2

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
4.2.	Налаштування конфігурації	Встановити, задокументувати та впровадити параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам: [*призначення: налаштування конфігурації, визначені організацією*]; визначити, задокументувати та затвердити будь-які відхилення від встановлених налаштувань конфігурації.	CM-6
4.3.	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; відстежувати та переглядати дії, пов'язані зі змінами в конфігурації системи, які необхідно контролювати.	CM-3
4.4.	Аналіз впливу на безпеку та приватність	Проаналізувати вплив змін у системі на безпеку перед їх впровадженням.	CM-4
4.5.	Обмеження доступу до змін	Визначити, задокументувати, затвердити та впровадити фізичні та логічні обмеження доступу, пов'язані зі змінами в системі.	CM-5
4.6.	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*]; періодично переглядати 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.	CM-7, CM-7(1)
4.7.	Мінімально необхідна функціональність – авторизоване програмне забезпечення – чорний список	Визначити програми, яким дозволено виконуватися в системі; впровадити політику "заборонити все", "дозволити за винятком" для виконання програм у системі; періодично переглядати та оновлювати список дозволених програм	CM-7(5)

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
4.8.	Інвентаризація компонентів системи	Розробити та документувати перелік компонентів системи.; періодично переглядати та оновлювати перелік компонентів системи; оновлювати перелік компонентів системи під час інсталяції, видалення та оновлення системи.	CM-8, CM-8(1)
4.9.	Розташування інформації	Визначити та задокументувати розташування службової інформації та компонентів системи, на яких інформація обробляється та зберігається; ідентифікувати та задокументувати користувачів, які мають доступ до системи та компонентів системи, де обробляється та зберігається службова інформація; документувати зміни в розташуванні (тобто в системі або компонентах системи), де обробляється та зберігається службова інформація.	CM-12
4.10.	Базова конфігурація – конфігурація системи та компонентів для сфер з високим ризиком	Видавати системи або компоненти системи з такими конфігураціями особам, які відряджаються до місць підвищеного ризику: [*призначення: конфігурації систем, визначені організацією*]; застосовувати такі вимоги безпеки до системи та компонентів системи після повернення осіб з відрядження: [*призначення: вимоги безпеки, визначені організацією*].	CM-2(7)
5.	**Ідентифікація та автентифікація**		**IA**
5.1.	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: обставини або ситуації, що вимагають повторної автентифікації, визначені організацією*].	IA-2, IA-11
5.2.	Ідентифікація та автентифікація пристроїв	Унікально ідентифікувати та автентифікувати пристрої перед встановленням з'єднання з системою.	IA-3
5.3.	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)

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
5.4.	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)
5.5.	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*]; унікально ідентифікувати статус кожної особи за допомогою ідентифікаційної характеристики.	IA-4, IA-4(4)
5.6.	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)
5.7.	Зворотний зв'язок автентифікатора	Забезпечити прихований зворотний зв'язок автентифікаційної інформації під час процесу автентифікації.	IA-6
5.8.	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;	IA-5

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
		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.	
6.	**Реагування на інциденти**		**IR**
6.1.	Обробка інциденту	Розробити план реагування на інциденти, який забезпечить організацію стратегії для реалізації її можливостей реагування на інциденти; упровадити систему реагування на інциденти, яка відповідає плану реагування на інциденти і передбачає підготовку, виявлення та аналіз, локалізацію, ліквідацію та відновлення інцидентів; оновити план реагування на інциденти, щоб врахувати зміни в системі та зміни в організації або проблеми, що виникли під час впровадження, виконання або тестування плану.	IR-4, IR-8
6.2.	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, IR-7
6.3.	Перевірка реагувань на інциденти	Періодично перевіряти ефективність системи реагування на інциденти.	IR-3
6.4.	Навчання з реагування на інциденти	3) 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	IR-2

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
		чи відповідальності за реагування на інцидент або отримання доступу до системи; коли цього вимагають зміни в системі; періодично після змін у системі; 4) періодично переглядати та оновлювати зміст навчання з реагування на інциденти [*призначення: події, визначені організацією*].	
7.	**Технічне обслуговування**		**МА**
7.1.	Інструменти для обслуговування	1) Затверджувати, контролювати та відстежувати використання інструментів технічного обслуговування системи; 2) перевіряти інструменти для технічного обслуговування на наявність неналежних або несанкціонованих модифікацій; 3) перевіряти носії, що містять діагностичні та тестові програми, на наявність шкідливого коду, перш ніж використовувати їх у системі; 4) запобігати вилученню обладнання для обслуговування системи, що містить службову інформацію: переконатися, що на обладнанні немає службової інформації; процедура очистки або знищення обладнання; збереження обладнання в межах об'єкта.	МА-3, МА-3(1), МА-3(2), МА-3(3)
7.2.	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
7.3.	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	МА-5

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
		персоналу з технічного обслуговування, який не має необхідних повноважень доступу.	
8.	**Захист носіїв інформації**		**MP**
8.1.	Зберігання носіїв інформації	Фізично контролювати та безпечно зберігати носії інформації, що містять службову інформацію, до моменту їх знищення або очищення за допомогою затвердженого обладнання, методів і процедур.	MP-4
8.2.	Доступ до носіїв інформації	Обмежити доступ до службової інформації на носіях інформації.	MP-2
8.3.	Знищення інформації на носіях інформації	Очистити носії інформації, що містять службову інформацію, перед утилізацією, випуском з-під контролю організації або повторним використанням.	MP-6
8.4.	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
8.5.	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.	MP-5, SC-28, SC-28(1)
8.6.	Використання носіїв інформації	Обмежити або заборонити використання [*призначення: типи носіїв інформації, визначені організацією*]; заборонити використання знімних носіїв інформації без ідентифікованого власника.	MP-7
8.7.	Резервне копіювання - криптографічний захист	Упровадити криптографічні механізми для запобігання несанкціонованому розкриттю службової інформації в місцях зберігання резервних копій.	CP-9(8)
9.	**Кадрова безпека**		**PS**
9.1.	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
9.2.	Звільнення персоналу. Переведення персоналу	3) Коли припиняється індивідуальна трудова діяльність:	PS-4, PS-5

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
		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; 4) 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.	
10.	**Фізичний захист і захист робочого середовища**		**PE**
10.1.	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; видаляти осіб зі списку фізичного доступу, коли доступ більше не потрібен.	PE-2
10.2.	Моніторинг фізичного доступу	Моніторити фізичний доступ до місця розташування системи, щоб виявляти та реагувати на інциденти фізичної безпеки; періодично переглядати журнали фізичного доступу.	PE-6
10.3.	Альтернативне робоче місце	Визначити альтернативні робочі місця, дозволені для використання працівниками; застосовувати вимоги безпеки на альтернативних робочих місцях [*призначення: вимоги безпеки, визначені організацією*].	PE-17
10.4.	Керування фізичним доступом	5) 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;	PE-3

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
		6) вести журнали контролю фізичного доступу для точок входу та виходу; 7) супроводжувати відвідувачів і контролювати їхню діяльність [призначення: обставини, що вимагають супроводу відвідувачів та контролю за їхньою діяльністю, визначені організацією]; 8) забезпечити захист ключів, кодів доступу та інших пристроїв фізичного доступу.	
10.5.	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; контролювати фізичний доступ до пристроїв виводу, щоб запобігти доступу сторонніх осіб до службової інформації.	PE-4, PE-5
11.	**Оцінка ризику**		**RA**
11.1.	Оцінювання ризику	Оцінити ризик несанкціонованого розголошення в результаті обробки, зберігання або передачі службової інформації; періодично оновлювати оцінки ризиків.	RA-3, RA-3(1), SR-6
11.2.	Сканування вразливостей	Періодично проводити перевірку, відстеження та сканування системи на наявність вразливостей, а також при виявленні нових вразливостей, що впливають на систему; усунути вразливості системи протягом часу [*призначення: час на реагування, визначений організацією*]; періодично оновлювати список вразливостей системи для сканування, а також при виявленні нових вразливостей та повідомляти про них.	RA-5, RA-5(2)
12.	**Оцінювання, акредитація та моніторинг безпеки**		**CA**
12.1.	Оцінювання	Періодично оцінювати вимоги до безпеки системи та середовища її функціонування, щоб визначити, чи були ці вимоги виконані.	CA-2
12.2.	План усунення недоліків та контрольні показники	3) 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; 4) періодично оновлювати існуючий план дій і показників на основі результатів оцінки безпеки, незалежних аудитів або оглядів, а також безперервного моніторингу.	CA-5

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
12.3.	Безперервний моніторинг	Розробити та впровадити стратегію безперервного моніторингу на рівні системи, що передбачає постійний моніторинг та оцінку безпеки.	CA-7
12.4.	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, вимоги до безпеки та обов'язки для кожної системи як частину договорів про обмін; періодично переглядати та оновлювати договори про обмін.	CA-3
13.	**Захист інформаційної системи та комунікацій**		**SC**
13.1.	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
13.2.	Інформація в загальних ресурсах системи	Запобігати несанкціонованій і ненавмисній передачі інформації за допомогою загальних ресурсів системи.	SC-4
13.3.	Захист периметра - Відмова за замовчуванням - Дозвіл за винятком	Заборонити трафік мережевих комунікацій за замовчуванням і дозволити трафік мережевих комунікацій за винятком.	SC-7(5)
13.4.	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), SC-28, SC-28(1)
13.5.	Відключення мережі	Завершити з’єднання з мережею, яке пов’язане із сеансом зв’язку в кінці сеансу або після періоду бездіяльності.	SC-10

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
13.6.	Встановлення та управління криптографічними ключами	Встановити криптографічні ключі в системі та керувати ними відповідно до наведених нижче вимог [*призначення: вимоги до встановлення та управління ключами, визначені організацією*].	SC-12
13.7.	Криптографічний захист	Впровадити типи криптографічного захисту при використанні системи для захисту конфіденційності службової інформації [*призначення: типи криптографії, визначені організацією*].	SC-13
13.8.	Спільні обчислювальні пристрої та застосунки	Заборонити віддалену активацію спільних обчислювальних пристроїв і програмного забезпечення; надавати чіткі вказівки щодо використання користувачам, які фізично наявні біля пристроїв.	SC-15
13.9.	Мобільний код	Визначити прийнятний мобільний код і технології мобільного коду; авторизувати, відстежувати та контролювати використання мобільного коду.	SC-18
13.10.	Автентифікація сесії	Захистити автентифікацію сеансів зв’язку.	SC-23
14.	**Цілісність системи та інформації**		**SI**
14.1.	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
14.2.	Захист від шкідливого коду	4) Упровадити механізми захисту від шкідливого коду у визначених місцях системи для виявлення та знищення шкідливого коду; 5) оновлювати механізми захисту від шкідливого коду в міру виходу нових версій відповідно до політики та процедур управління конфігурацією; 6) 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

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
		блокування шкідливого коду, поміщення шкідливого коду в карантин або інші дії у відповідь на виявлення шкідливого коду.	
14.3.	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
14.4.	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)
14.5.	Управління та збереження інформації	Управляти та зберігати службову інформацію в системі та виводити службову інформацію з системи відповідно до чинного законодавства, виконавчих наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог.	SI-12
15.	**Планування безпеки**		**PL**
15.1.	Політика та процедури планування безпеки	Розробити, задокументувати та розповсюдити серед персоналу організації або ролей політики та процедури, необхідні для виконання вимог безпеки; періодично переглядати та оновлювати політики та процедури.	AC-1, AT-1, AU-1, CA-1, CM-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1, SR-1
15.2.	Плани захисту інформації та персональних даних	1) Розробити план захисту інформації, який: визначає складові компоненти системи; описує робоче середовище системи; описує конкретні загрози для системи, які викликають занепокоєння в організації; надає огляд вимог до безпеки системи; визначає з'єднання з іншими системами; визначає осіб, які виконують ролі та обов'язки в системі;	PL-2

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
		містить іншу інформацію, необхідну для захисту службової інформації; 2) періодично переглядати та оновлювати план захисту інформації; 3) захистити план захисту інформації від неавторизованого розголошення.	
15.3.	Правила поведінки	Створити та надати особам, що потребують доступу до інформаційної системи, правила, які описують їхні обов'язки й очікувану поведінку при роботі зі службовою інформацією та використанням системи; отримати документальне підтвердження від таких осіб про те, що вони прочитали, зрозуміли та погодилися дотримуватися правил поведінки, перш ніж дозволяти доступ до службової інформації та системи; періодично переглядати та оновлювати правила поведінки.	PL-4
16.	**Придбання систем та послуг**		**SA**
16.1.	Процес закупівель	Внести наступні вимоги щодо безпеки, прямо або шляхом посилання, до договору про закупівлю системи, компоненту системи або послуги: [*призначення: вимоги безпеки, визначені організацією*].	SA-4
16.2.	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
16.3.	Зовнішні послуги для системи	Вимагати від постачальників зовнішніх послуг для системи, що використовуються для обробки, зберігання або передачі службової інформації, дотримання наступних вимог безпеки: [*призначення: вимоги 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 вимог безпеки зовнішніми постачальниками послуг.	SA-9
17.	**Управління ризиками ланцюга постачання**		**SR**

№	Назва вимоги	Зміст вимоги	Заходи захисту відповідно до НД ТЗІ 3.6-006-24
17.1.	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; періодично переглядати та оновлювати план управління ризиками ланцюга постачання; захистити план управління ризиками ланцюга постачання від несанкціонованого розголошення.	SR-2
17.2.	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
17.3.	Контроль ланцюга постачання і процесів	Запровадити процес виявлення та усунення слабких місць або недоліків в елементах та процесах ланцюга постачання; упровадити наведені нижче вимоги безпеки для захисту від ризиків ланцюга постачання для системи, компонентів системи або послуг для системи, а також для обмеження шкоди або наслідків від подій, пов'язаних з ланцюгом постачання: [*призначення: вимоги безпеки, визначені організацією*].	SR-3

Т.в.о. директора
ДЗІ Адміністрації Держспецзв’язку
лейтенант Олександр ГРИЩЕНКО