СХВАЛЕНО

Рішенням Експертної ради з питань державної експертизи у сфері технічного захисту інформації (Протокол від __.__.2025 року № _____)

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
з формування цільового профілю безпеки інформації

Зміст

1. Загальні положення

1.1. Ці Методичні Рекомендації визначають порядок дій щодо формування цільового профілю безпеки на базі якого створюється комплексна система захисту інформації у визначеній інформаційній, електронній комунікаційній та інформаційно-комунікаційній системі (далі – система).

1.2. Ці Методичні Рекомендації призначені для використання при формуванні цільового профілю безпеки інформації для систем, створених з використанням профілів безпеки.

1.3. Ці Методичні Рекомендації не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і є добровільними для використання.

1.4. Ці Методичні Рекомендації розроблено відповідно до підпункту 7 пункту 4, пункту 10 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, постанови Кабінету Міністрів України від 30 травня 2024 року № 627 «Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, побудованих з використанням профілів безпеки інформації».

1.5. У цих Методичних Рекомендаціях терміни вживаються у значенні, наведеному в Законах України «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні комунікації» «Про Державну службу спеціального зв’язку та захисту інформації України», постанові Кабінету Міністрів України від 30 травня 2024 року № 627 «Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, побудованих з використанням профілів безпеки інформації» та інших нормативних документах сфери захисту інформації.

1.6 Цільовим профілем безпеки інформації (далі - ЦПБ) є взаємопов’язана сукупність заходів із захисту інформації та їх налаштування, визначених для системи її власником (розпорядником) відповідно до базового профілю (далі – БПБ) з урахуванням вимог законодавства та стандартів у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, нормативних документів системи технічного захисту інформації, галузевих вимог, політик безпеки в системах, а також призначення системи, її характеристик та особливостей функціонування, результатів проведеної оцінки ризиків

2. Структура ЦПБ

Рекомендована структура ЦПБ містить:
1) титульний аркуш;
2) загальні відомості про ІКС:
   - назва ІКС;
   - відомості про власника ІКС;
   - відомості про виконавця робіт з розробки ЦПБ;
   - підстава розробки;
   - призначення ІКС та функції ІКС;
   - загальна архітектура ІКС;
   - відомості про обраний БПБ;
   - перелік нормативно-правових актів які використовувались при формуванні ЦПБ, політики безпеки, звіт з оцінки ризиків;
3) ЦПБ.

2.1 На титульному аркуші відображається назва ІКС на яку формується ЦПБ, рік, а також підпис, печатка, прізвище та ім’я власника системи, який затверджує ЦПБ на розробку КСЗІ в ІКС, а також гриф обмеження доступу.

ЦПБ затверджується власником (розпорядником) ІКС де створюється КСЗІ.

2.2 У розділі «назва ІКС» наводиться повна та скорочені назви ІКС.

2.3 У розділі «відомості про власника ІКС» наводяться відомості щодо власника (розпорядника) ІКС (назва організації (підприємства, установи), її місцезнаходження).

2.4 У розділі «відомості про виконавця робіт з розробки ЦПБ» наводиться відомості щодо виконавця (Розробника) ЦПБ (назва організації (підприємства, установи), її місцезнаходження).

2.5 У розділі «підстава розробки» наводиться перелік нормативно-правових актів, а також внутрішніх наказів, розпоряджень, які є підставою на створення КСЗІ з використанням профілів безпеки інформації.

2.6 У розділі «призначення ІКС та функції ІКС» наводяться відомості щодо призначення, основні функції, а саме: функції ІКС та їх технологічні етапи; опис використовуваних заходів та засобів захисту інформації, функціональний опис призначення КСЗІ в ІКС, а також особливості застосування КСЗІ.

2.7 У розділі «загальна архітектура ІКС» наводяться відомості, які детально описують кожну складову апаратної частини ІКС, комунікаційне та програмне забезпечення. Також додається у вигляді рисунків загальна структурна та детальна схема ІКС.

2.8 У розділі «відомості про обраний БПБ» наводяться нормативно-правові акти на підставі яких було обрано БПБ для виду інформації, яка буде оброблятися в системі.

2.9 У розділі «перелік нормативно-правових актів які використовувались при розробці ЦПБ» наводяться нормативно-правові акти та нормативні документи, якими регламентується порядок захисту інформації в ІКС.

2.10 У розділі «ЦПБ» в табличному вигляді наводиться розроблений ЦПБ за формою:

№	Вимога з безпеки інформації	Вимоги БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
1	2	3	4	5

де наводиться наступна інформації:

- 1 - номер вимоги з безпеки інформації у відповідності до обраного БПБ;
- 2 - назва вимоги з безпеки інформації у відповідності до обраного БПБ;
- 3 - зміст вимоги БПБ у відповідності до обраного БПБ;
- 4 - позначення заходу захисту відповідно до НД ТЗІ 3.6-006-24;
- 5 - відповідно до НД ТЗІ 3.6-006-24 з визначеними параметрами.

В разі посилання або доповнення заходу захисту, який не передбачено БПБ, інформація наводиться лише у стовбцях 4 та 5.

Приклад ЦПБ наведений у додатку 1 до цих рекомендацій.

3. Формування цільового профілю безпеки інформації

Під час визначення ЦПБ власник (розпорядник) системи самостійно обирає стандарти у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, які використовуються під час здійснення заходів із захисту інформації, шляхи і способи здійснення таких заходів відповідно до ЦПБ, а також визначає наявність у ньому інформації з обмеженим доступом та забезпечує дотримання встановлених правил роботи з документами, які містять інформацію з обмеженим доступом.

Передбачені у ЦПБ заходи із захисту інформації, обрані стандарти, шляхи і способи здійснення таких заходів повинні включати відповідні вимоги та заходи, визначені базовим профілем безпеки інформації (далі – БПБ).

Формування ЦПБ включає наступні етапи:

1) вибір БПБ;

2) Формування ЦПБ:
   - налаштування параметрів заходів захисту;
   - посилення заходів захисту;
   - доповнення заходів захисту;

3) адаптація ЦПБ.

4. Вибір БПБ

БПБ є вимогами з безпеки інформації та взаємопов’язана сукупність заходів з її захисту, для відкритої інформації та інформації з обмеженим доступом, яка обробляється у системах.

БПБ затверджуються наказом Адміністрації Держспецзв’язку та розміщуються на сайті Держспецзв’язку, крім БПБ які містять інформацію з обмеженим доступом.

4.1 Структура БПБ

Вимоги з безпеки наводяться у табличному вигляді та мають визначену структуру:

- номер вимоги з безпеки інформації;
- назва вимоги з безпеки інформації;
- зміст вимоги;
- захід/заходи захисту яким реалізується вимога.

№	Назва вимоги з безпеки інформації	Зміст вимоги	Заходи захисту інформації відповідно до НД ТЗІ 3.6-006-24
1	2	3	4
…	…	…	…
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*].	АС-7
…	…	…	…

Зміст вимоги з безпеки інформації в цілому відповідає вимогам щодо реалізації окремого або сукупності заходів захисту у відповідності до НД ТЗІ 3.6-006-24 «Порядок вибору захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем», але при формуванні ЦПБ доцільно використовувати окремий зміст визначеного заходу захисту відповідно НД ТЗІ 3.6-006-24.

4.2 Вибір БПБ

Власник обирає БПБ інформації виходячи з виду інформації за рівнем обмеження доступу який буде оброблятися в ІКС.

Обраний БПБ повинен бути затверджений наказом Адміністрації Держспецзв'язку.

5. Налаштування параметрів заходів захисту

Після вибору відповідного базового профілю безпеки інформації необхідно здійснити налаштування з метою узгодження заходів захисту з конкретними потребами організації щодо захисту інформації. Процес налаштування є елементом процесу управління ризиками організації. Рішення щодо визначення параметрів заходів захисту мають враховувати різни фактори управління ризиками безпеки.

Налаштування являє собою циклічну реалізацію заходів захисту, що входять до складу визначених груп заходів захисту. Налаштування заходів захисту здійснюється відповідно до НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

5.1 Структура вимог до реалізації заходів захисту

Структура вимог до засобів захисту має наступний вид:

- Цілі захисту визначають основні інформаційні активи, які потребують захисту, а також визначають загрози, які можуть вплинути на ці активи. Основними завданнями є забезпечення цілісності, конфіденційності та доступності інформації в рамках операційних процесів організації;
- вимоги безпеки.

На рисунку 1 проілюстроване впорядкування заходів захисту (структура каталогу).

Всього визначено 20 класів заходів захисту. Кожний клас містить декілька груп заходів захисту. Своєю чергою захід захисту може мати декілька посилень.

Клас заходів захисту — це сукупність заходів захисту, які стосуються конкретного аспекту забезпечення безпеки інформації. Для позначення класу використовується ідентифікатор з двох літер, наприклад «УПРАВЛІННЯ ДОСТУПОМ (АС)».

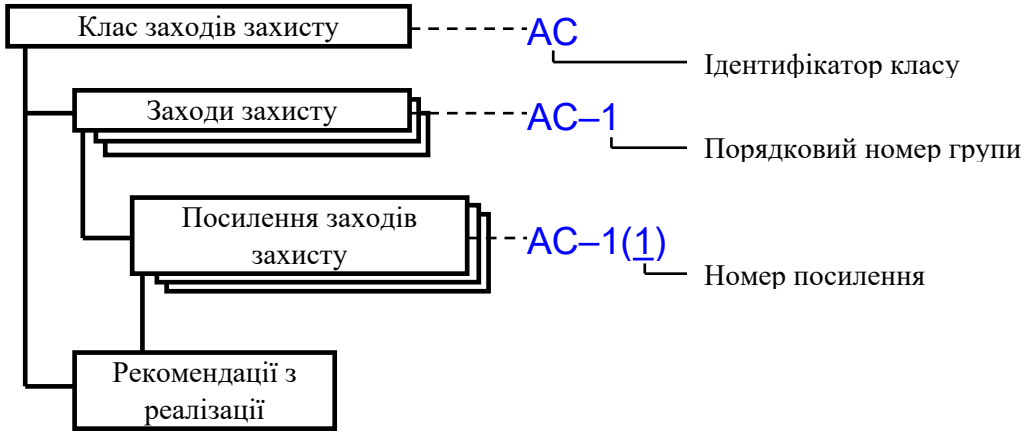

Рисунок 1 — Упорядкування заходів захисту

При налаштуванні параметрів власник системи здійснює посилання на нормативні документи, згідно яких вказане значення, та методи і засоби за допомогою яких це буде реалізоване.

Заходи захисту мають змінні параметри, які треба визначити чи вибрати зі списку запропонованих під час налаштування профілю безпеки інформації з урахуванням конкретних умов діяльності організації та застосування інформаційної системи, структурно-функціональних характеристик інформаційної системи, результатів аналізу ризиків безпеки. Цей механізм надає організаціям можливість налаштувати заходи захисту з урахуванням вимог політики безпеки та конфіденційності конкретних зацікавлених сторін. Результати оцінювання ризиків безпеки також є важливим фактором при визначенні конкретних значень параметрів заходів захисту. Організації, в особі визначених посадових осіб, безпосередньо несуть відповідальність за вибір, обґрунтування та призначення параметрів для кожного заходу захисту.

5.2. Вхідні дані для налаштування

Вхідними даними для налаштування виступають наступні дані:

1. БПБ

2. Нормативно-правові акти;
3. Задокументована стратегія управління ризиками;
4. Задокументовані результати оцінювання ризиків;
5. Політика безпеки.

Перелік вхідних даних не є вичерпним і може бути доповнений в разі необхідності для врахування особливостей ІКС.

5.3 Налаштування параметрів

Заходи захисту мають змінні параметри, які треба визначити чи вибрати зі списку запропонованих під час налаштування профілю безпеки інформації з урахуванням конкретних умов діяльності та застосування інформаційної системи, структурно-функціональних характеристик інформаційної системи, результатів аналізу ризиків безпеки. Цей механізм надає можливість налаштувати заходи захисту з урахуванням вимог політики безпеки та конфіденційності конкретних зацікавлених сторін. Результати оцінювання ризиків безпеки також є важливим фактором при визначенні конкретних значень параметрів заходів захисту. Власник системи безпосередньо несе відповідальність за вибір, обґрунтування та призначення параметрів для кожного заходу захисту

5.3.1 Опис

ODP (Organization-Defined Parameter) – це змінна або значення, яке організація має встановити в рамках реалізації певних заходів безпеки. У багатьох заходах, визначених у НД ТЗІ 3.6-006-24, використовуються параметри, які не встановлені за замовчуванням, а залишаються для визначення організацією. Це робиться для того, щоб організації могли враховувати свої вимоги, ризики, обсяги роботи та ресурси.
В описі заходів захисту НД ТЗІ 3.6-006-24 він записується у квадратних дужках «[]» приклад:

[*Призначення: визначене організацією сповіщення або банер про використання системи*]

5.3.2 Приклади

Приклад 1

№	Вимога з безпеки інформації	Вимоги БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
…	…	…	…	…
1.4.	Розмежування обов’язків	Визначити обов’язки осіб, які потребують розмежування; установити правила авторизації доступу для підтримки розмежування обов’язків.	AC-5	a. Розмежувати і документувати [*Виконавці документів – користувачі, які здійснюють підготовку та відпрацювання електронних документів.* *Реєстратори документів – користувачі, які здійснюють реєстрацію електронних документів.* *Керівники підрозділів – користувачі, які здійснюють розгляд, доопрацювання, погодження та затвердження документів.* *Керівництво – користувачі, які здійснюють розгляд, доопрацювання, погодження та затвердження документів.* *Контролери – користувачі, які забезпечують контроль за виконанням документів.* *Адміністратор – користувачі, які здійснюють створення, видалення, блокування/розблокування, редагування облікових записів*]. b. Установити правила авторизації доступу для підтримки розмежування обов’язків.
…	…	…	…	…

Приклад 2

В політиці безпеки організації, яка затверджена наказом Адміністрації Держспецзв’язку № 282 від 25.02.2025 року, у розділі «Політика блокування» визначено, що завершення сеансу користувача відбувається після періоду відсутньої активності через 15 хв.

…	…	…	…	…
1.11.	Припинення сеансу	Автоматично завершувати сеанс користувача після *[призначення: умови або події, що вимагають відключення сеансу, визначені організацією]*.	AC-12	Сеанс користувача має завершуватися автоматично після [*відсутньої активності протягом 15 хв*].
…	…	…	…	…

Приклад 3

На основі оцінки ризиків організації, яка затверджена наказом Адміністрації Держспецзв'язку № 283 від 16.07.2024 року та спираючись на кращі світові практики, визначено: встановити можливість 3 невдалих спроб входу в систему протягом 15 хвилин, в разі неуспішної спроби, заблокувати користувача доки він не буде розблокований адміністратором.

…	…	…	…	…
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	a. Встановити обмеження на [*3 спроби*] послідовних неуспішних спроб входу користувача в систему впродовж [*15 хв*]. b. Автоматично виконати *[блокування облікового запису, доки він не буде розблокований адміністратором]*; виконати [*перевірку права доступу користувача до системи*], коли перевищено максимальну кількість невдалих спроб входу в систему.
…	…	…	…	…

5.4 Посилення заходів захисту

Після налаштування заходів захисту власником (розпорядник) системи проводиться посилення заходів захисту на підставі:

- вимог нормативно-правових актів, які стосуються функціонування ІКС;
- внутрішніх політик безпеки власника ІКС;
- оцінки ризиків, щодо втрати властивостей інформаційних активів, які оброблюються в ІКС.

5.4.1 Опис

Посилення заходів захисту спрямовується на посилення та розширення функціональності базового заходу захисту. В обох випадках посилення заходу захисту реалізуються (впроваджуються) в інформаційних системах та середовищах, які потребують більшого захисту, ніж забезпечується базовим заходом захисту, або коли організації вимагають доповнення функціональних можливостей базового заходу захисту чи гарантій безпеки за результатами оцінювання ризику та моніторингу безпеки. Кожне посилення заходу захисту має коротку назву, яка вказує на передбачувану функцію або можливість, що надається удосконаленням.

5.4.2 Приклади

Приклад 1

В Законі України «Про електронну ідентифікацію та електронні довірчі послуги» статті 14, пункті 3 зазначено, що, Власники (держателі) інформаційних та інформаційно-комунікаційних систем, з використанням систем яких надаються електронні довірчі послуги, здійснюються відправлення і отримання електронних даних та володільцями інформації в яких є органи державної влади, органи влади Автономної Республіки Крим, органи місцевого самоврядування, інші юридичні особи публічного права, за результатами оцінки ризиків і наслідків неправомірного використання чи підміни ідентифікаційних даних користувачів послуг електронної ідентифікації використовують для здійснення автентифікації в зазначених системах засоби електронної ідентифікації з середнім або високим рівнем довіри.

Використання кваліфікованих електронних підписів та печаток забезпечує високий рівень довіри до засобів електронної ідентифікації, з використанням яких створюються такі електронні підписи та печатки, а також до схем електронної ідентифікації, в рамках яких видаються відповідні засоби електронної ідентифікації.

Використання удосконалених електронних підписів та печаток, які базуються на кваліфікованих сертифікатах відкритих ключів, забезпечує середній рівень довіри до засобів електронної ідентифікації, з використанням яких створюються такі електронні підписи та печатки, а також до схем електронної ідентифікації, в рамках яких видаються відповідні засоби електронної ідентифікації.

Посилення ІА-2(6) було обрано для виконання цих вимог із загального каталогу заходів захисту НД ТЗІ 3.6-006-24.

…	…	…	…	…
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)	Реалізувати багатофакторну автентифікацію для доступу до привілейованих облікових записів. Реалізувати багатофакторну автентифікацію для доступу до непривілейованих облікових записів.
	Ідентифікація та автентифікація (користувачів організації) - мережевий доступ до привілейованих облікових записів — окремий пристрій	**Реалізація багатофакторної автентифікації для [Вибір (один або кілька): локальний; мережевий; віддалений] доступ до [Вибір (один або кілька): привілейовані облікові записи; непривілейовані облікові записи] такі, що: a) Один із факторів забезпечується пристроєм, окремим від системи, який отримує доступ; b) Пристрій відповідає [Призначення: визначені організацією вимоги до міцності механізму].**	**IA-2(6)**	**Реалізація багатофакторної автентифікації для [*мережевий*] доступ до [*привілейовані облікові записи; непривілейовані облікові записи*] такі, що:** **a) Один із факторів забезпечується пристроєм, окремим від системи, який отримує доступ;** **b) Пристрій відповідає [*високий та середній рівень довіри*].**
…	…	…	…	…

Приклад 2

Відповідно до політики безпеки організації, яка затверджена наказом Адміністрації Держспецзв’язку № 282 від 25.02.2025, у розділі «Носії інформації» зазначена необхідність проведення перевірки програмного забезпечення за допомогою якого проводиться форматування USB-носіїв інформації. Захід захисту MP-6 посилено з загального каталогу заходів захисту НД ТЗІ 3.6-006-24 за допомогою MP-6(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	МР-6	a. Очищувати [*USB-носії*] перед утилізацією, випуском за межі організаційного контролю, або перед повторним використанням [*шляхом форматування*]. b. Використовувати механізми очищення зі стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації.
	Знищення інформації на носіях інформації - перевірка обладнання	**Перевіряти обладнання та процедури для очищення [Призначення: з визначеною організацією частотою], щоб переконатися в досягненні запланованого очищення.**	**МР-6(2)**	**Перевіряти обладнання та процедури для очищення [*щорічно*], щоб переконатися в досягненні запланованого очищення.**
…	…	…	…	…

Приклад 3

На основі оцінки ризиків, яка затверджена наказом Адміністрації Держспецзв’язку № 283 від 16.07.2024 року встановлено, що авторизацію користувачів необхідно проводити за допомогою біометрики, захід захисту АС-7 було посилено АС-7(3) з каталогу заходів захисту НД ТЗІ 3.6-006-24

…	…	…	…	…
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	Встановити можливість 3 невдалих спроб входу в систему протягом 15 хвилин.
	Невдалі спроби входу в систему - обмеження на спроби біометричного входу	**Обмежити кількість невдалих спроб входу за допомогою біометрики *[призначення: визначена організацією кількість]*.**	**AC-7(3)**	**Обмежити кількість невдалих спроб входу за допомогою біометрики *[5 спроб]*.**
…	…	…	…	…

5.5 Доповнення заходів захисту

Після налаштування та посилення заходів захисту власником системи проводиться доповнення заходів захисту на підставі:

- вимог нормативно-правових актів, які стосуються функціонування ІКС;
- внутрішніх політик безпеки власника ІКС;
- оцінки ризиків, щодо втрати властивостей інформаційних активів, які оброблюються в ІКС.

5.5.1 Опис

Доповнення заходів захисту спрямовується на збільшення кількості заходів захисту ЦПБ з метою врахування потенційних вразливостей та загроз системи. Доповнення заходу захисту реалізується (впроваджується) в інформаційних системах та середовищах, які потребують більшого захисту, ніж забезпечується БПБ.

5.5.2 Приклади

Для доповнення заходів захисту потрібно вибрати необхідні заходи захисту з НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем» з подальшим їх додаванням в профіль безпеки і формуванням ЦПБ.

Приклад 1

В Законі України «Про електронні документи та електронний документообіг» статті 12 зазначено, що, перевірка цілісності електронного документа проводиться шляхом підтвердження удосконаленого або кваліфікованого електронного підпису чи печатки, а в разі накладання на електронний документ електронного підпису чи печатки іншого виду - із застосуванням інших засобів і методів захисту інформації з дотриманням вимог законодавства у сфері захисту інформації. Захід захисту AU-10 було обрано для виконання цих вимог із загального каталогу заходів захисту НД ТЗІ 3.6-006-24.

…	…	…	…	…
	Неспростовність	**Надавайте неспростовні докази того, що особа (або процес, який діє від імені особи) виконала *[Призначення: дії, визначені організацією, на які поширюється принцип неспростовності]*.**	**AU-10**	**Надавайте неспростовні докази того, що особа (або процес, який діє від імені особи) виконала [*КЕП*].**
…	…	…	…	…

Приклад 2

В політиці безпеки організації, яка затверджена наказом Адміністрації Держспецзв’язку № 282 від 25.02.2025 року, у розділі «Цілісність системи» зазначена необхідність проведення перевірки цілісності програмного забезпечення, що застосовується для управління ключами та сертифікатами. Захід захисту AC-23 було обрано для виконання вимоги політики із загального каталогу заходів захисту НД ТЗІ 3.6-006-24.

…	…	…	…	…
	Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації	**Впровадити інструменти перевірки цілісності для виявлення несанкціонованих змін [Призначення: визначеного організацією програмного забезпечення, вбудованого програмного забезпечення та інформації].**	**SI-7**	**Впровадити інструменти перевірки цілісності для виявлення несанкціонованих змін [*програмного забезпечення для управління ключами та сертифікатами*].**
…	…	…	…	…

Приклад 3

На основі оцінки ризиків, яка затверджена наказом Адміністрації Держспецзв'язку № 283 від 16.07.2024 року встановлено, що місткість сховища повинна бути достатньою для зберігання записів аудиту знижує ймовірність того, що таке сховище буде переповнене, що своєю чергою може призвести до потенційної втрати або зниження ефективності аудиту, профіль був доповнений заходом захисту AU-4 з каталогу заходів захисту НД ТЗІ 3.6-006-24

…	…	…	…	…
3.9.	**Місткість сховища записів аудиту**	**Розподіляти місткість сховища записів аудиту у відповідності до [*Призначення: визначених організацією вимог до зберігання записів аудиту*].**	**AU-4**	**Розподіляти місткість сховища записів аудиту у відповідності до [*обсягу даних, терміну зберігання*].**
…	…	…	…	…

6. Адаптація цільового профілю безпеки інформації

Під час експлуатації ІКС, з метою оперативного реагування на появу нових загроз для системи, проводиться постійний моніторинг з подальшим створенням адаптованого профілю безпеки інформації (далі – АПБ).

У разі внесення змін до БПБ або ЦПБ, до моменту подання нової декларації, ЦПБ вважається АПБ.

Постійний моніторинг безпеки інформаційних систем (далі – ПМ) є одним з етапів життєвого циклу системи в Організації, що ґрунтується на моделі ПВПД (плануй – виконуй – перевіряй – дій), яка визначена в ISO/IEC 27001:2015. (рисунок 2).

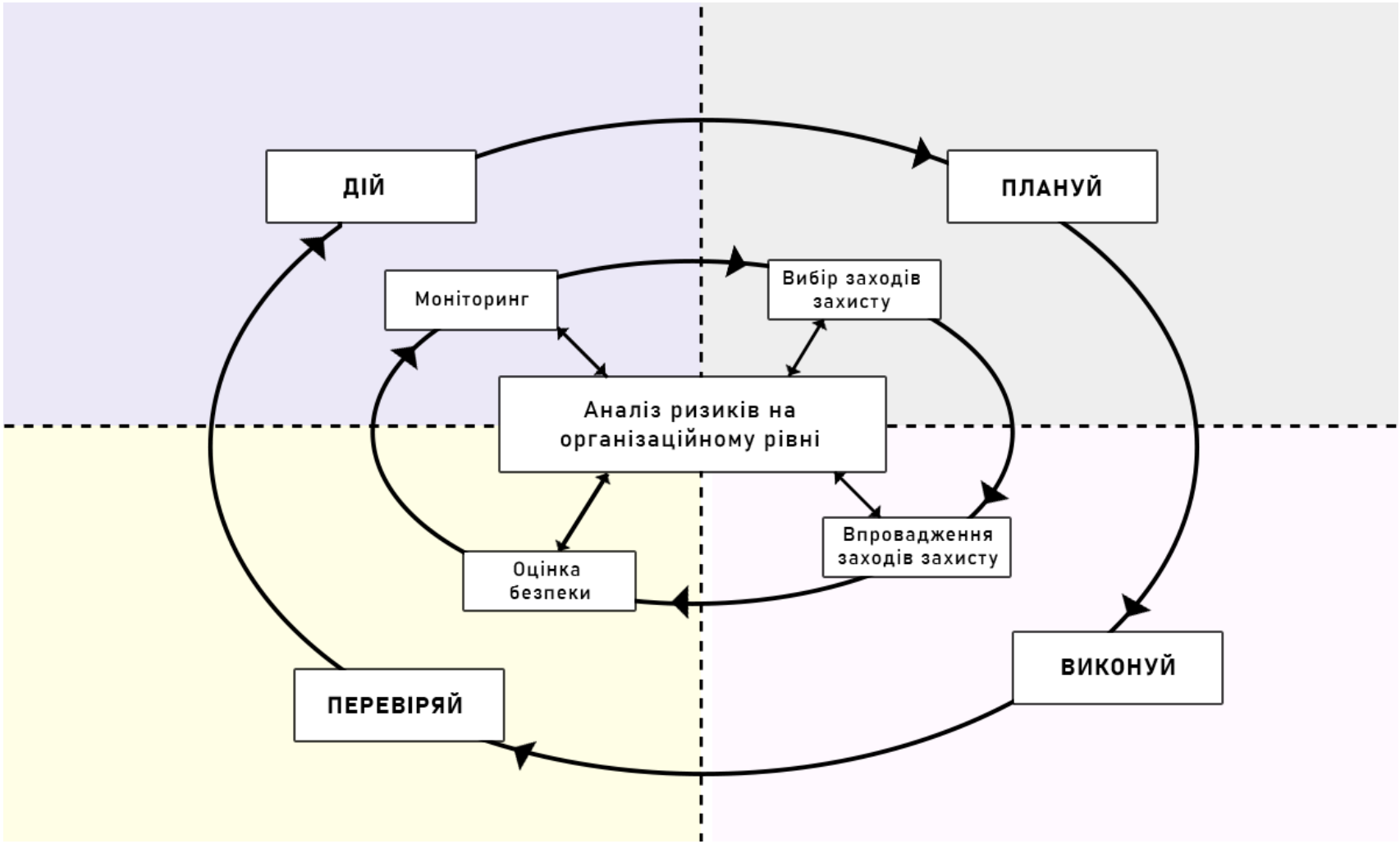

Рисунок 2 – Етапи життєвого циклу системи захисту ІКС

Метою етапу моніторингу безпеки є підтримка обізнаності (поінформованості) про поточний стан безпеки в ІКС та Організації для прийняття рішень щодо вдосконалення ЦПБ.

Відповідальність за проведення постійного моніторингу безпеки покладається на власника (розпорядника) ІКС. Безпосереднє виконання покладається на осіб, на яких покладено функції забезпечення безпеки інформації.

У таблиці наведено короткий опис завдань та очікуваних результатів постійного моніторингу безпеки.

Завдання	Результати
Завдання М-1 Відстеження змін	Виявлені зміни проаналізовані та задокументовані.
Завдання М-2 Формування АПБ	АПБ створений/оновлений. Внесені зміни до політики (політик) безпеки інформації та плану (планів) захисту.
Завдання М-3 Впровадження та оцінка АПБ (змін)	Звіт про оцінку
Завдання М-4 Декларування поточного ЦПБ	Декларація направлена до Адміністрації Держспецзв'язку

Моніторинг безпеки ІКС має проводитися протягом усього етапу експлуатації та підтримки системи. Результати, які отримані в рамках ПМ напряму можуть впливати на:

- рівень критичності інформації, яка циркулює в ІКС;
- вимоги з безпеки до ІКС;
- АПБ.

ПМ проводиться на системному рівні, проте його результати (зокрема результати аналізу ризиків на системному рівні) напряму впливають на процеси організаційного рівня, такі як, формування Концепції безпеки інформації Організації в частині формування стратегії управління ризиками.

Порядок проведення ПМ наведений на рисунку 3.

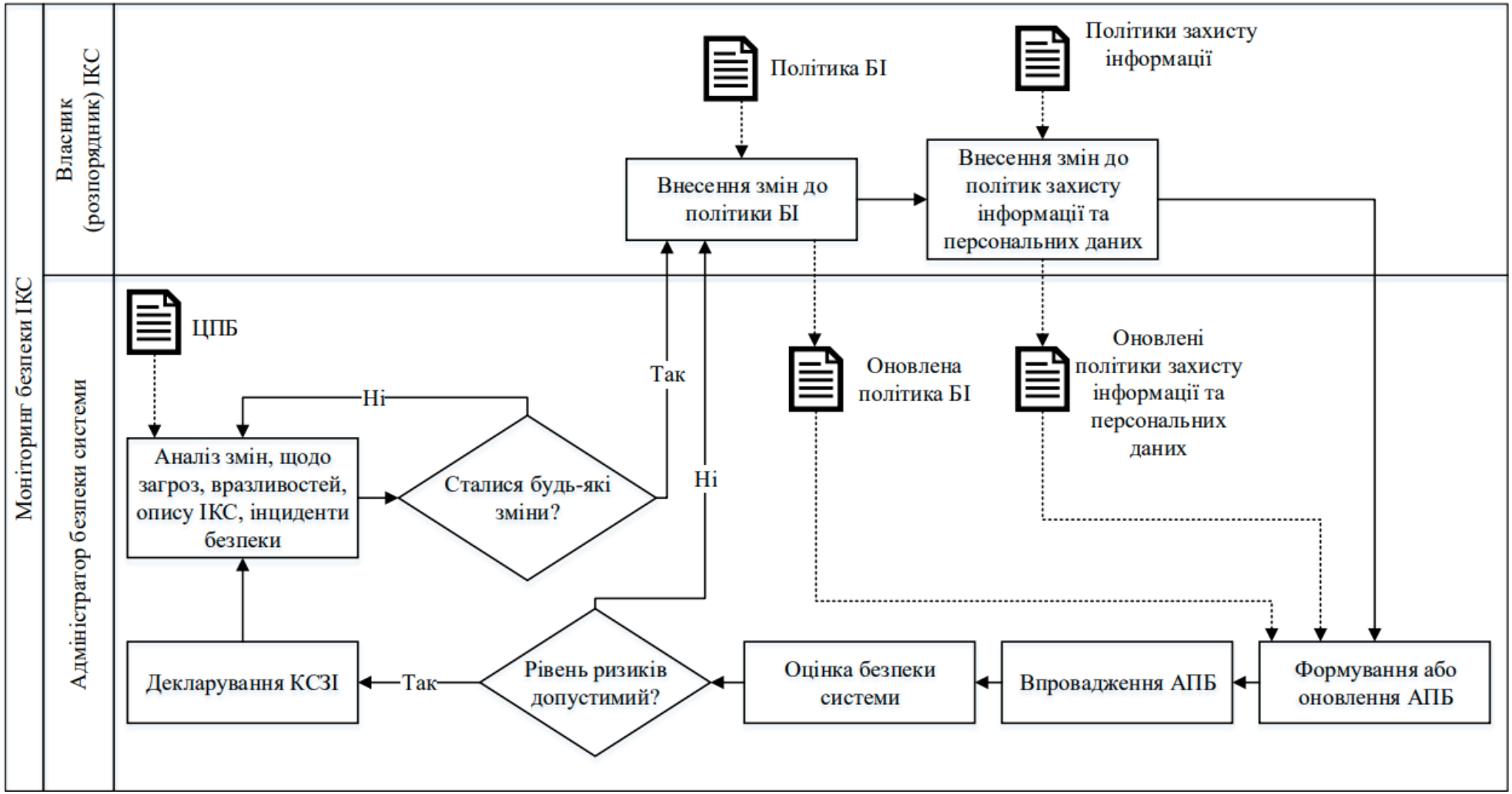

Рисунок 3 – Процес моніторингу безпеки інформаційної системи

Вхідними даними для проведення ПМ виступають:

– концепція БІ (в частині поточної стратегії управління ризиками) затверджена на Організаційному рівні;

- поточні задокументовані результати аналізу ризиків на організаційному та системному рівнях, отримані на етапі аналізу ризиків на організаційному рівні та етапі впровадження заходів захисту(керуючись положеннями НД ТЗІ «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем») відповідно;
- проектна та експлуатаційна документація на ІКС, яка входить до складу власника (розпорядника) ІКС;
- затверджений ЦПБ;
- поточні політики безпеки інформації, які були сформовані та затверджені на етапі впровадження заходів захисту;
- поточні плани заходів захисту, які були сформовані та затверджені на етапі впровадження заходів захисту;
- діючі національні законодавчі акти в сфері безпеки інформації.

Т.в.о. директора Департаменту
полковник Андрій ГОЛОВЕНКО

__.__.2025

Додаток
до методичних рекомендацій з
формування цільового профілю
безпеки інформації
___ _____ 2025 року № ___

Приклад шаблону цільового профілю безпеки на

(Гриф обмеження доступу)

ЗАТВЕРДЖЕНО

_____
(найменування посади керівника або
уповноваженої
особи)

_____
(підпис) (власне ім’я,
прізвище)
___ _____ 202_ р.
МП (у разі наявності)

ЦІЛЬОВИЙ ПРОФІЛЬ БЕЗПЕКИ
СТВОРЕНИЙ НА ОСНОВІ БАЗОВОГО ПРОФІЛЮ БЕЗПЕКИ ДЛЯ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ,
ДЕ ОБРОБЛЯЄТЬСЯ *ВІДКРИТА* ІНФОРМАЦІЯ,

затвердженого наказом Адміністрації Держспецзв’язку від 26.06.2024 № 317

Система електронного документообігу Адміністрації Держспецзв’язку
(найменування об’єкта /унікальний реєстровий номер)

1. Загальні відомості про інформаційно-комунікаційну систему (ІКС)

1.1 Назва ІКС

Система електронного документообігу Адміністрації Держспецзв'язку (далі – ІКС СЕД);

1.2 Відомості про власника ІКС

Адміністрація Держспецзв'язку;

1.3 Відомості про виконавця робіт з розробки ЦПБ

Адміністрація Держспецзв'язку; 03110, Київ, вул. Солом'янська 13, код ЄДРПОУ 34620942;

1.4 Підстава розробки

КСЗІ створюється на підставі *Закону України «Про захист інформації в інформаційно-комунікаційних системах», постанови Кабінету Міністрів України від 30.05.2025 № 627 «Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації», Наказу Адміністрації Держспецзв'язку від 01.01.2025 № 001;*

1.5 Призначення ІКС та функції ІКС

ІКС СЕД призначена для:

- *автоматизації процесів документообігу Адміністрації Держспецзв'язку;*
- *запровадження єдиної централізованої СЕД з автоматизацією безпаперового документообігу в Адміністрації Держспецзв'язку;*
- *підвищення продуктивності праці виконавців, а також рівня виконавчої дисципліни, ефективності управління та оперативності прийняття рішень завдяки прискоренню та оптимізації процесів обміну електронними документами і звітністю;*
- *зменшення термінів підготовки і виконання документів, здійснення постійного моніторингу виконання завдань;*
- *підвищення прозорості процесів розробки та опрацювання документів з можливістю контролю їх виконання на будь-якому етапі;*
- *зберігання електронних документів, разом з їх попередніми версіями у файловому середовищі, що дозволить розділити сховища зберігання метаданих та файлів;*
- *формування електронного архіву справ суб'єктів СЕД, що передбачає складання номенклатури справ структурних підрозділів, узагальнення і погодження зведеної номенклатури справ, складання описів справ постійного, тривалого (понад 10 років) зберігання та з кадрових питань (особового складу), актів про вилучення для знищення документів, не внесених до Національного архівного фонду, їх погодження (схвалення), а також підготовка справ для передачі на державне архівне зберігання, інших документів відповідно до чинних законодавчих та нормативно-правових актів України з питань ведення архівної справи із внесенням відповідної інформації*

до електронної реєстраційно- моніторингової картки;

- зменшення видатків на папір та інші витратні матеріали, економія на поштових відправленнях, телефонному зв'язку, оптимізація використання робочого часу.

1.6 Загальна архітектура ІКС

Загальна та структурна схема ІКС СЕД представлена на рис. 1

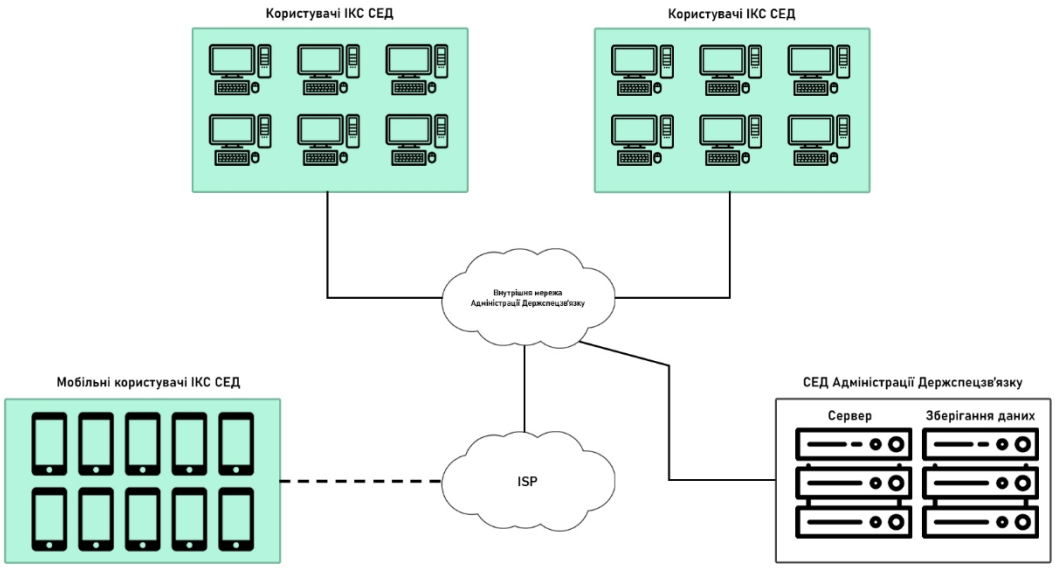

Рис. 1 – Загальна архітектура ІКС СЕД

1.7 Програмна архітектура

Програмна архітектура ІКС СЕД представлена на рис. 2

Рис. 2 – Програмна архітектура ІКС СЕД

1.8 Відомості про обраний БПБ

Порядок захисту інформації в ІКС СЕД регламентується такими нормативно - правовими актами та нормативними документами:

1. *Постанову кабінету Міністрів України від 30.05.2024 № 627 «Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації»;*

2. *Наказ Адміністрації Держспецзв'язку від 24.06.2024 № 317 «Про визначення Базового профілю безпеки інформації»;*

3. *Наказ Адміністрації Держспецзв'язку від 25.02.2025 № 282 «Про затвердження політики безпеки»;*

4. *Наказ Адміністрації Держспецзв'язку «Звіт за результатами проведення оцінки ризиків»;*

5. *Закон України «Про інформацію»;*

6. *Закон України «Про захист інформації в інформаційно-комунікаційних системах»;*

7. *Закон України «Про доступ до публічної інформації»;*

8. *Закон України «Про звернення громадян»;*

9. *Закон України «Про електронні документи та електронний документообіг»;*

10. *Закон України «Про електронну ідентифікацію та електронні довірчі послуги»;*

11. *Закон України «Про основні засади забезпечення кібербезпеки України»;*

12. *Постанова Кабінету Міністрів України «Деякі питання документування управлінської діяльності» від 17.01.2018 № 55;*

13. *Постанова Кабінету Міністрів України «Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації» від 14.04.1997 № 348;*

14. *Постанова Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах»;*

15. *Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;*

16. *Порядок оновлення антивірусних програмних засобів, затверджений наказом Адміністрації Держспецзв'язку від 26 березня 2007 р. № 45.*

17. *Інструкція про порядок доступу і роботи в мережі Інтернет, використання її інформаційних ресурсів і послуг у Державній службі спеціального зв'язку та та захисту інформації України, затверджена наказом Адміністрації*

Держспецзв'язку від 29.09.2014 № 490;

18. *НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;*

19. *НД ТЗІ 3.6-007-21 Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем.*

2.1 ЦПБ ІКС СЕД

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
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	a. Визначити та задокументувати типи облікових записів системи, дозволених для використання в ІС для підтримки цілей, завдань, функцій і процесів організації. b. Призначити менеджерів облікових записів для управління системними обліковими записами. c. Створити умови для групового та рольового членства. d. Визначити авторизованих користувачів інформаційної системи, членство в групі та ролі, а також дозволи доступу (наприклад, привілеї) та інші атрибути (за потреби) для кожного облікового запису. e. Вимагати схвалення ***[службою захисту інформації]*** запитів на створення облікових записів системи. f. Створювати, активувати, змінювати, деактивувати та видаляти системні облікові записи відповідно до ***[Створення****: Облікові записи повинні створюватися на підставі затвердженого наказу з урахуванням політик безпеки. Активування/деактивація: Облікові записи активуються тільки після перевірки відповідності ролі користувача, а також деактивуються в разі, якщо користувач більше не потребує доступу.* ***Видалення****: Якщо обліковий запис більше не потрібен (наприклад, через звільнення або переведення), він має бути видалений відповідно до встановлених процедур.].* g. Впровадити моніторинг використання облікових записів системи. h. Повідомляти адміністраторів облікових записів у межах ***[5 робочих днів з моменту звільнення****]:* 1. коли облікові записи більше не потрібні; 2. коли користувачі звільнені чи переведені; 3. коли використовуються індивідуальні системи або наявні зміни, які потребують нових знань. i. Авторизувати доступ до системи на основі: 1. Дійсної авторизації доступу. 2. Передбачуваного використання системи. 3. Інших атрибутів, що вимагаються організацією. j. Проводити перегляд облікових запис ів на відповідність вимогам управління обліковими записами з ***[щоквартально]***. k. Впровадити процес повторного випуску облікових даних спільного/групового облікового запису (якщо він буде розгорнутий), коли особи виходять з групи. l. Узгодити процеси управління обліковими записами з процесами звільнення та переводу (передачі повноважень) персоналу.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
1.2.	Забезпечення доступу	Застосовувати затверджені повноваження для логічного доступу до конфіденційної інформації та ресурсів у системі.	AC-3	Застосовувати затверджені повноваження для логічного доступу до інформації та ресурсів системи відповідно до чинної політики (правил) управління доступом.
1.3.	Управління інформаційними потоками	Застосовувати затверджені вимоги для управління потоками відкритої та конфіденційної інформації всередині системи та між підключеними системами.	AC-4	Застосувати затверджені повноваження для управління потоком інформації всередині системи та між пов'язаними системами на основі ***[1. Політика щодо обміну документами між підрозділами:*** - *Шифрування: Всі документи, що передаються між підрозділами (наприклад, внутрішні звіти, договірні документи), повинні бути шифровані для забезпечення конфіденційності. Використовувати AES-256 для шифрування даних під час передачі.* - *Авторизація доступу: Доступ до документів надається лише тим користувачам, чия роль дозволяє обробляти конкретний тип документа:* - *Співробітники відділу документообігу мають доступ до стандартних документів для реєстрації і архівування.* - *Керівники підрозділів мають доступ до документів, що стосуються їхнього підрозділу, наприклад, звіти, внутрішня кореспонденція.* - *Служба захисту інформації можуть мати доступ до метаданих для забезпечення правильного функціонування системи.* ***2. Політика управління документами між системами:*** - *Міжсистемна передача: Документи, що передаються між різними системами (наприклад, між СЕД і архівом), повинні бути передані через захищені канали (наприклад, VPN, HTTPS).* - *Стандарти форматів документів: Для передачі документів використовувати PDF/A для довгострокового зберігання та XML для передачі структурованих даних.* - *Аутентифікація та перевірка: Передача документів між системами має відбуватися лише після верифікації користувача або системи, яка ініціює операцію, через двухфакторну аутентифікацію (2FA).* ***3. Обмеження доступу до конфіденційних документів:*** - *Політика мінімальних привілеїв: Кожен користувач має доступ лише до тих документів, що необхідні для виконання його завдань:* - *Звичайні користувачі мають доступ до обмеженого набору документів (наприклад, внутрішня кореспонденція, повідомлення).* - *Керівники мають доступ до документів за їхнім підрозділом, включаючи звіти та інші важливі документи.*

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				- *Часові обмеження доступу: Доступ до певних типів документів може бути обмежений за часом або терміном їх зберігання.* ***4. Процес моніторингу доступу та використання документів:*** - *Аудит: Усі дії з документами (перегляд, зміна, передача) повинні бути задокументовані в журналах аудиту з зазначенням:* - *Дата і час операції.* - *Користувач, що виконав дію.* - *Тип дії (наприклад, перегляд, зміна, передача).* - *Сповіщення: У разі спроби несанкціонованого доступу до документів або порушення правил доступу адміністратори повинні отримувати автоматичні сповіщення.* ***5. Політика обміну документами з зовнішніми організаціями:*** - *Шифрування при передачі зовнішнім організаціям:* - *Для передачі документів до зовнішніх організацій (партнерів, контрагентів) повинно бути застосовано шифрування, наприклад, за допомогою PGP або AES-256.* - *Електронний підпис: Усі документи, які передаються зовнішнім організаціям і потребують підтвердження їх автентичності, повинні бути підписані електронним підписом.* ***6. Політика для документів, що потребують змін:*** - *Редагування та збереження версій: Усі зміни до документів повинні зберігатися як окремі версії.* - *Кожен документ, що змінюється, повинен містити інформацію про:* - *Користувача, що змінив документ.* - *Причину зміни.* - *Попередні версії документа, з можливістю їх відновлення.* ***7. Регулярний перегляд доступу до документів:*** - *Перегляд доступу:* - *Регулярно проводити перегляд доступу до документів з метою визначення, чи відповідає поточний доступ користувачів їхнім ролям та обов'язкам:* - *Перегляд проводиться щоквартально.* - *За результатами перегляду можливе оновлення рівнів доступу для користувачів або зміна політики доступу до певних документів.* ***8. Впровадження процедур для втрати документів:*** - *Відновлення після втрати:* - *У разі втрати або пошкодження документа має бути процедура відновлення із резервної копії:*

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				- *Всі документи повинні бути автоматично архівовані щодня.* - *Для відновлення документів має бути чітко визначено, хто та як може доступати архіви.].*
1.4.	Розмежування обов'язків	Визначити обов'язки осіб, які потребують розмежування; установити правила авторизації доступу для підтримки розмежування обов'язків.	AC-5	a. Розмежувати і документувати ***[Адміністратори системи:*** - *Відповідають за загальну настройку та технічне обслуговування системи.* - *Мають доступ до всіх документів та налаштувань без обмежень.* - *Управляють користувачами та їх ролями.* ***Користувачі, відповідальні за документообіг:*** - *Реєструють, обробляють і зберігають документи в системі.* - *Мають доступ тільки до документів, що стосуються їхньої роботи.* - *Здійснюють контроль за правильним оформленням документів та їх збереженням.* ***Керівники підрозділів**:* - *Переглядають та затверджують документи, які стосуються їхніх підрозділів.* - *Мають доступ до звітних і управлінських документів.* - *Здійснюють контроль за процесами документообігу в межах свого підрозділу.* ***Користувачі, відповідальні за архівування:*** - *Відповідають за зберігання і архівацію документів.* - *Здійснюють контроль за періодичним видаленням або архівуванням документів, що більше не потребують активного використання.* - *Впроваджують політики зберігання та видалення документів відповідно до вимог законодавства та внутрішніх регламентів.].* b. Установити правила авторизації доступу для підтримки розмежування обов'язків.
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*].	AC-6	Впровадити принцип мінімізації повноважень, який дозволяє користувачам (або процесам, що діють від імені користувачів) здійснювати лише такі авторизовані звернення, які необхідні для виконання визначених завдань відповідно до цілей (призначення, місії) організації та функцій.
			AC-6(1)	Авторизуваний доступ для ***[адміністратори]*** до: a) [*Має повний доступ до всіх функцій безпеки, таких як налаштування захисту паролів, моніторингу доступу, оновлень системи безпеки. Можуть змінювати параметри апаратних засобів (наприклад, налаштування серверів чи мережевих пристроїв), програмного забезпечення (наприклад, налаштування СЕД для забезпечення доступу) та мікропрограмного забезпечення (в разі наявності в системі, наприклад, для криптографічних пристроїв).];* b) ***[Журнали аудиту доступу**:* - *Записи про всі спроби доступу до системи та окремих документів.*

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				- *Інформація про невдалі спроби входу, включаючи дані про несанкціоновані спроби доступу.* - *Дані про перегляд документів: хто, коли та які документи переглядав.* ***Журнали безпеки**:* - *Записи про події безпеки: наприклад, спроби злому, несанкціоновані зміни конфігурацій, атаки на мережу тощо.* - *Інформація про системні помилки, що можуть вказувати на потенційні вразливості або порушення безпеки.* ***Інформація, яка містить дані про документи:*** - *Створення документа: хто створив, коли.* - *Остання зміна документа: хто вносив зміни та які саме зміни були зроблені.* - *Доступні версії документа: коли і ким була змінена кожна з версій.* ***Інформація про облікові записи користувачів:*** - *Список всіх активних користувачів системи та їхні ролі.* - *Дані для аутентифікації.* - *Записи про зміни в облікових записах створення, активація, деактивація, зміна прав доступу.* ***Політики доступу та дозволів:*** - *Документація, яка визначає, які групи користувачів мають доступ до яких типів документів або функцій в системі.* - *Інформація про правила доступу (наприклад, рівні доступу до документів, конфіденційність даних).* ***Інформація про налаштування системи безпеки:*** - *Конфігурації шифрування, які використовуються для захисту даних.* - *Налаштування мережевого захисту (фаєрволи, VPN, маршрутизація)* - *Налаштування для двухфакторної аутентифікації (2FA) та інших методів автентифікації користувачів.* ***Інформація щодо оновлень і патчів безпеки**:* - *Записи про встановлені оновлення безпеки в програмному та апаратному забезпеченні.* - *Дані про виконані тестування на вразливості і використані патчі для виправлення.* ***Копії та резервні копії важливих даних:*** - *Дані, що зберігаються в резервних копіях: важливі документи, журнали, налаштування безпеки.* - *Інформація про строки зберігання та відновлення резервних копій для забезпечення безпеки даних.*

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				Інформація про інциденти безпеки: - *Записи про кожен інцидент безпеки, що стався в системі.* - *Деталі про реагування на інцидент, включаючи аналіз причин та вжиті заходи для запобігання подібним подіям у майбутньому.* ***Інформація щодо використання системи:*** - *Логи використання системи для виявлення аномалій у доступі або діяльності користувачів, що можуть вказувати на порушення безпеки.].*
			AU-9(4)	Авторизувати доступ до управління функціональністю аудиту тільки для [***Адміністратор безпеки***].
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)	Вимагати від користувачів облікових записів системи або ролей, які мають доступ до [***адміністративних функцій безпеки, журналів аудиту, конфігурацій системи безпеки, механізмів керування доступом***], використовувати непривілейовані облікові записи чи ролі під час доступу до незахищених функцій.
			AC-6(5)	Обмежити привілейовані облікові записи в системі згідно з [***Адміністратор системи***].
1.7.	Мінімізація повноважень – заборона непривілейованим користувачам виконувати привілейовані функції	Заборонити непривілейованим користувачам виконувати привілейовані функції.	AC-6(10)	Вжити заходи для запобігання можливості виконувати привілейовані функції непривілейованими користувачами.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
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	a. Встановити обмеження на ***[3 спроби]*** послідовних неуспішних спроб входу користувача в систему впродовж ***[15 хвилин]***. b. Автоматично виконати ***[блокування облікового запису на [30 хвилин];*** затримання наступної команди входу в систему за ***[перша невдала спроба - затримка 1 хвилина, після другої — 5 хвилин, після третьої — 10 хвилин];*** виконати [***автоматичне повідомлення адміністратора]***, коли перевищено максимальну кількість невдалих спроб входу в систему.
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	a. Демонструвати користувачам ***[сповіщення про умови використання системи]*** перед тим, як надавати доступ до системи, що забезпечує безпеку та приватність відповідно до чинних законів, нормативних документів, наказів, директив, політик, правил, стандартів і керівних принципів, які зазначають, що: 1. користувачі здійснюють доступ до урядової системи; 2. використання системи може контролюватися, реєструватися та підлягати аудиту;

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				3. несанкціоноване використання системи забороняється та приводить до кримінальної та цивільної відповідальності; 4. використання системи означає згоду на моніторинг і запис дій користувача. b. Зберігати сповіщення або банер на екрані, доки користувачі не визнають умови використання та не приймуть явних дій для входу в систему або подальшого доступу до системи. c. Для загальнодоступних систем: 1. демонструвати інформацію про умови використання системи ***[умови доступу до загальнодоступної системи]***, перш ніж надавати подальший доступ до загальнодоступної системи; 2. демонструвати посилання, якщо такі є, на моніторинг, запис або аудит, які узгоджуються з акомодацією приватності для таких систем, які зазвичай забороняють такі дії; 3. мати опис авторизованого використання системи
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	a. Заборонити подальший доступ до системи шляхом ініціювання блокування пристрою після [***після 15 хвилин]*** бездіяльності або після отримання запиту від користувача. b. Зберігати блокування пристрою, поки користувач не відновить доступ, використовуючи встановлені процедури ідентифікації та автентифікації
			AC-11(1)	Приховувати, через блокування пристрою, інформацію, раніше видиму на дисплеї, із загальнодоступним зображенням.
1.11.	Припинення сеансу	Автоматично завершувати сеанс користувача після [*призначення: умови або події, що вимагають відключення сеансу, визначені організацією*].	AC-12	Сеанс користувача має завершуватися автоматично після ***[30 хвилин бездіяльності].***

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
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	a. Встановити та задокументувати обмеження на використання, вимоги до конфігурації/підключення та рекомендації щодо здійснення кожного типу віддаленого доступу. b. Авторизувати віддалений доступ до системи, перш ніж будуть дозволені такі підключення.
			AC-17(3)	Виконувати маршрутизацію всього віддаленого доступу через авторизовані та керовані точки контролю управління доступом до мережі.
			AC-17(4)	(a) Авторизувати виконання привілейованих команд і доступ до інформації, що стосується безпеки, за допомогою віддаленого доступу тільки для ***[відсутні потреби для виконання команд за допомогою віддаленого доступу]***; (b) Задокументувати обґрунтування такого доступу в плані захисту інформації для системи
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	a. Установити обмеження на використання, вимоги до конфігурації/підключення та рекомендації щодо здійснення бездротового доступу. b. Авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення
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	a. Встановити обмеження на використання, вимоги до конфігурації, вимоги до підключення і рекомендації щодо впровадження мобільних пристроїв, контрольованих організацією. b. Авторизувати підключення мобільних пристроїв до систем, які експлуатуються організацією.
			AC-19(5)	Організація має застосувати ***[повне шифрування пристроїв]*** для захисту конфіденційності та цілісності інформації на ***[мобільних що належать Адміністрації Держспецзв'язку].***
1.15.	Використання зовнішніх систем	1) Заборонити використання зовнішніх систем, крім систем дозволених організацією;	AC-20	a. [Вибір (один або кілька): Встановіть [***мови доступу до системи з довірених зовнішніх систем, зокрема корпоративних VPN та зареєстрованих пристроїв***]; Визначте [***механізми контролю доступу, що реалізуються на зовнішніх хмарних системах***

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		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; 4) обмежити використання портативних пристроїв зберігання даних авторизованими особами на зовнішніх системах.		***відповідно до угод про довіру***], узгоджені з довірчими відносинами, встановленими з іншими організаціями, які володіють, експлуатують та/або обслуговують зовнішні системи, дозволяючи уповноваженим особам: 1. доступ до системи із зовнішніх систем; 2. обробляти, зберігати або передавати керовану організацією інформацію за допомогою зовнішніх систем; b. Заборонити використання [***особистих пристроїв (BYOD), неавторизованих хмарних сховищ (Dropbox, Google Drive без корпоративного контролю), публічних Wi-Fi мереж, анонімних VPN та проксі-серверів***].
			AC-20(1)	Дозволити авторизованим особам використовувати зовнішню систему для доступу до системи або для обробки, зберігання чи передачі інформації, що контролюється організацією, лише після: a) перевірки виконання необхідних заходів безпеки та приватності щодо зовнішніх систем, як зазначено в політиці безпеки та приватності організації, а також планах безпеки та приватності; b) збереження погоджених угод про підключення або обробку системи з організаційною структурою, на якій розміщена зовнішня система.
			AC-20(2)	Обмежити використання портативних пристроїв зберігання даних авторизованими особами на зовнішніх системах за допомогою ***[обмеження на підключення зовнішніх носіїв, які не зареєстровані в Адміністрації держспецзв'язку].***
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	a. Призначити осіб, що уповноважені на розміщення інформації в загальнодоступній системі. b. Навчати уповноважених осіб тому, щоб загальнодоступна інформація не містила інформацію з обмеженим доступом. c. Переглядати запропонований зміст інформації до публікації в загальнодоступній системі, щоб гарантувати, що там не міститься інформація з обмеженим доступом. d. Переглядати вміст загальнодоступної системи на предмет наявності там інформації з обмеженим доступом з ***[щомісяця]***; така інформація має бути видалена в разі її виявлення.
	Обізнаність і навчання (AT)			

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
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	Впровадити базові тренінги з підвищення обізнаності у сфері безпеки та приватності для користувачів системи (включно з менеджерами, керівниками компаній і підрядниками): a. Забезпечити навчання грамотності з питань безпеки та конфіденційності для користувачів системи (включаючи менеджерів, керівників вищої ланки та підрядників): 1. як частину початкового навчання для нових користувачів і ***[щорічно]*** після цього; 2. якщо цього потребують системні зміни або наступні [***оновлення системи безпеки, зміни в політиках або інциденти безпеки]***. b. Використовувати наведені нижче методи, щоб підвищити рівень безпеки та конфіденційності користувачів системи ***[курси, тренінги, семінари, відео уроки]***; c. Оновлювати навчання грамотності та зміст обізнаності ***[щорічно]*** і наступні [***оновлення політики безпеки, або виявлення нових інцидентів***]; d. Включити уроки, отримані з внутрішніх або зовнішніх інцидентів безпеки або порушень, у навчання грамотності та методи підвищення обізнаності.
			AT-2(2)	Ввести до програми навчання вправи з розпізнавання та виявлення потенційних індикаторів внутрішніх загроз.
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	a. Забезпечити проведення навчання з питань безпеки та приватності на основі ролей для працівників з ролями та обов’язками: ***[керівники]***: 1. перед авторизацією доступу до системи, інформації або виконанням призначених обов’язків і ***[щорічно]*** після цього; 2. коли цього потребують системні зміни. b. Оновити навчальний контент на основі ролей ***[щорічно***] і наступні [***в разі змін в системі, або інцидентів***]; c. Включіть у рольове навчання, інформацію, отриману з внутрішніх або зовнішніх інцидентів та порушень безпеки.
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	a. Визначити типи подій, які система може реєструвати для підтримки функції аудиту: ***[уведення/вихід користувачів з системи, неуспішні спроби входу, активність адміністратора (створення/редагування/видалення облікових записів), зміни в конфігураціях системи, зміни в налаштуваннях безпеки, неавторизовані спроби доступу];***

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				b. Координувати функції аудиту безпеки з іншими організаційними підрозділами, які вимагають інформації, пов'язаної з аудитом, для посилення взаємної підтримки та допомоги у виборі типів подій, що перевіряються; c. Визначити, які типи подій підлягають аудиту: - [***Події, що стосуються доступу користувачів: включаючи входи та виходи з системи, спроби несанкціонованого доступу, зміни прав доступу.*** - ***Події, що стосуються адміністрування системи: створення, редагування, видалення облікових записів, зміни в налаштуваннях системи та безпеки.*** - ***Інші події безпеки: спроби маніпулювання логами, зміни в конфігурації безпеки, підключення зовнішніх пристроїв або мереж.*** ***Проведення аудиту щорічно, або в разі виявлення інцидентів***] d. Обґрунтувати, чому типи подій, що перевіряються, вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов'язаних з безпекою та приватністю; e. Перегляньте й оновіть типи подій, вибрані для журналювання ***[щорічно]***.
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; 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	Переконатися, що записи аудиту містять інформацію, яка встановлює наступне: a. який тип події стався; b. коли відбулася подія; c. де відбулася подія; d. джерело події; e. наслідки події; f. результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією.
			AU-3(1)	Формувати записи аудиту, що містять наступну додаткову інформацію: ***[1. Записи аудиту повинні містити інформацію про тип події, ідентифікатор пристрою, час події, адресу IP, тип доступу (успішний чи неуспішний), виконану команду.*** ***2. Для подій, пов'язаних із системними змінами, має бути вказано:*** - ***назву зміненої системи або компонента,*** - ***тип змін,*** - ***підпис користувача або адміністратора, що здійснив зміни.*** ***3. Записи аудиту повинні також включати підтвердження або повідомлення про спробу несанкціонованого доступу, наприклад, з описом помилок авторизації або причинами блокування доступу (в разі неуспішних спроб).*** ***4. Крім цього, для критичних або підозрілих подій повинна бути додана інформація про перевірку або виведення результатів з обробленого аналізу таких подій у разі виявлення підозр або інцидентів безпеки.].***

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
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	Зберігати записи аудиту впродовж ***[1 рік]***, щоб забезпечити підтримку розслідувань (постфактум) інцидентів безпеки та приватності, а також для задоволення вимог нормативних і документів організації щодо збереження даних аудиту.
			AU-12	a. Забезпечити генерацію даних аудиту для типів подій, що перевіряються в AU-2a в [***серверах, мережевих пристроях, брандмауери, точки доступу***]. b. Дозволити [***адміністратору системи***] вибирати, які типи подій, що перевіряються, повинні перевірятися окремими компонентами системи; c. Генерувати записи аудиту для типів подій, визначених в AU-2c. з вмістом згідно з AU-3.
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	a. Сповіщати **[адміністратора безпеки]** у разі збою обробки даних аудиту в ***[протягом 30 хвилин]***. b. Виконати наступні додаткові дії: - ***[Перевірка цілісності даних аудиту.*** - ***Відновлення або повторна обробка даних аудиту.*** - ***Оновлення системи або оновлення компонентів, що відповідають за обробку аудиту.*** - ***Вжиття заходів щодо попередження подібних інцидентів у майбутньому.]***
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	a. Переглядати та аналізувати записи системного аудиту ***[щомісяця***] для виявлення - ***[Несанкціоновані спроби доступу.*** - ***Неочікувані зміни в системних налаштуваннях.*** - ***Аномальні або підозрілі операції користувачів.*** - ***Можливі атаки або спроби порушення цілісності.].*** b. Відправляти звіт про аудит ***[адміністратору безпеки***]. c. Налаштувати рівні огляду аудиту, аналізу та звітності в рамках системи, коли змінюється рівень ризику на основі інформації від правоохоронних органів, розвідувальної інформації або від інших достовірних джерел інформації.
			AU-6(3)	Аналізувати та зіставляти записи аудиту в різних сховищах задля забезпечення ситуативної обізнаності в масштабах організації.
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	AU-7	Забезпечити та реалізувати можливості скорочення записів перевірок аудитом і звітів, до рівня, який: a. підтримує перевірку, аналіз і звітність аудиту на вимогу та розслідування (постфактум) інцидентів безпеки; b. не змінює оригінальний вміст або час упорядкування записів аудиту.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		незаконну або несанкціоновану діяльність у системі; зберігати оригінальний зміст і часовий порядок записів аудиту.		
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	a. Використовувати внутрішньосистемний годинник для створення позначок часу для записів аудиту. b. Застосовувати позначки часу, які відповідають ***[мілісекунд***] і використовують всесвітній координований час, мають фіксоване зміщення місцевого часу відносно всесвітнього координованого часу або включають зміщення місцевого часу як частину позначки часу.
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	a. Захист інформації аудиту та інструментів журналювання аудиту від несанкціонованого доступу, зміни та видалення; b. Сповіщення ***[адміністратора безпеки]*** у разі виявлення несанкціонованого доступу, зміни або видалення інформації аудиту
			AU-9(4)	Авторизувати доступ до управління функціональністю аудиту тільки для ***[служби захисту інформації].***
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	a. Розробити, задокументувати та підтримувати за допомогою заходів конфігурації поточні базові налаштування системи. b. Переглядати та оновлювати базові налаштування системи: 1. з [***щоквартально]***; 2. за потреби внаслідок [***виявлення нових загроз або зміни у нормативних документах***]; 3. коли встановлені нові або оновлені компоненти системи.
4.2.	Налаштування конфігурації	Встановити, задокументувати та впровадити параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам: [*призначення:*	CM-6	a. Встановити та задокументувати параметри конфігурації компонентів, які застосовуються в системі, які відображають найбільш обмежений режим, що відповідає експлуатаційним вимогам, використовуючи [***безпечні конфігурації операційних систем, баз даних, мережевих компонентів та прикладного програмного забезпечення, визначені організацією***].

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		налаштування конфігурації, визначені організацією]; визначити, задокументувати та затвердити будь-які відхилення від встановлених налаштувань конфігурації.		b. Реалізувати конфігураційні установки. c. Визначити, задокументувати та затвердити будь-які відхилення від встановлених конфігураційних параметрів конфігурації для [***файлових серверів, баз даних, мережевих пристроїв***] на основі [***експлуатаційних вимог для забезпечення доступності і ефективності систем***]. d. Відстежувати та керувати змінами конфігураційних параметрів відповідно до організаційної політики та процедур.
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	a. Визначити типи змін у системі, які контролюються конфігурацією. b. Переглядати запропоновані зміни в конфігурації, контрольовані системою, і схвалити або відхилити ці зміни з явним урахуванням аналізу наслідків безпеки. c. Документувати рішення зі зміни конфігурації системи. d. Впровадити схвалені зміни конфігурації в систему. e. Зберігати записи змін конфігурації системі впродовж [***3 роки***]. f. Здійснювати моніторинг і аналіз дій, пов’язаних зі змінами конфігурації системи. g. Координувати та впроваджувати нагляд за діяльністю з управління змінами конфігурації за допомогою [***системи управління змінами конфігурації (CMDB) або іншого визначеного організацією механізму***], який викликається ***[через впровадження нових стандартів безпеки, або змін у політиках конфігурації]***.
4.4.	Аналіз впливу на безпеку та приватність	Проаналізувати вплив змін у системі на безпеку перед їх впровадженням.	CM-4	Аналізувати зміни в системі, щоб визначити потенційну загрозу безпеці та приватності перед реалізацією змін.
4.5.	Обмеження доступу до змін	Визначити, задокументувати, затвердити та впровадити фізичні та логічні обмеження доступу, пов'язані зі змінами в системі.	CM-5	Визначити, задокументувати, затвердити та забезпечити застосування фізичних і логічних обмежень доступу, пов’язаних зі змінами в системі.
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	CM-7	a. Налаштуйте систему для забезпечення лише [***критичних бізнес-функцій електронного документообігу***]; b. Заборонити або обмежити використання таких функцій, портів, протоколів, програмного забезпечення та/або служб: ***[небезпечні або невикористовувані служби, застарілі протоколи зв’язку (наприклад, SMBv1, TLS 1.0/1.1), незатверджене програмне забезпечення, відкриті адміністративні порти (наприклад, 23 (Telnet), 3389 (RDP) без VPN), а також будь-які сторонні додатки, що не відповідають політиці безпеки організації]].***
			CM-7(1)	(a) Проводити перегляд системи [щомісяця] для виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг; (b) Вимкнути [***Вимкнення порту 21 (FTP) для передачі файлів.***

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		функції, порти, протоколи, з'єднання та служби; вимкнути або видалити функції, порти, протоколи, з'єднання та служби, які є непотрібними або небезпечними.		***Вимкнення порту 23 (Telnet).*** ***Вимкнення SMB (Server Message Block).*** ***Вимкнення RDP (Remote Desktop Protocol)*** ***Вимкнення HTTP (порт 80)]***
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.	IA-2	Унікально ідентифікувати та автентифікувати користувачів або процеси, що діють від імені користувачів.
5.2.	Ідентифікація та автентифікація пристроїв	Унікально ідентифікувати та автентифікувати пристрої перед встановленням з'єднання з системою.	IA-3	Унікально ідентифікувати та автентифікувати ***[всі типи пристроїв]*** перед установкою ***[локального, мережного***] підключення.
5.3.	Ідентифікація та автентифікація (користувачів організації) – Багатофакторна автентифікація привілейованих облікових записів	Упровадити багатофакторну автентифікацію для доступу до облікових записів системи.	IA-2(1)	Реалізувати багатофакторну автентифікацію для доступу до привілейованих облікових записів.
			IA-2(2)	Реалізувати багатофакторну автентифікацію для доступу до непривілейованих облікових записів.
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)	Реалізувати стійкі до відтворення механізми автентифікації для доступу до ***[привілейованих облікових записів; непривілейованих облікових записів]***
5.5.	Управління ідентифікацією	Отримати дозвіл від персоналу або ролей організації на призначення ідентифікатора особи, групи, ролі, служби або пристрою;	IA-4	a. отримання дозволу від [***керівника***] для призначення ідентифікатора особі, групі, ролі або пристрою; b. вибору ідентифікатора, який ідентифікує окрему особу, групу, роль або пристрій; c. призначення ідентифікатора особі, групі, ролі або пристрою; d. запобігання повторному використанню ідентифікаторів впродовж ***[1 року].***

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		вибрати та призначити ідентифікатор, який ідентифікує особу, групу, роль, службу або пристрій; запобігати повторному використанню ідентифікаторів для [*призначення: період часу, визначений організацією*].		
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)	Для автентифікації на основі пароля необхідно: (a) вести список часто використовуваних, очікуваних або скомпрометованих паролів та оновлювати його ***[щоквартально]***, а також при підозрі, що паролі організацій скомпрометовані прямо чи опосередковано; (b) перевіряти, коли користувачі створюють або оновлюють паролі, що паролі не перебувають у визначеному організацією списку найчастіше використовуваних, очікуваних або скомпрометованих паролів у IA-5(1)(a); (c) передавати паролі лише через криптографічно захищені канали; (d) зберігати паролі за допомогою затвердженого алгоритму гешування, переважно використовуючи ключову геш-функцію; (e) вимагати негайного вибору нового пароля після відновлення облікового запису; (f) дозволити користувачеві вибирати довгі паролі та фрази, включно з пробілами та всіма друкованими символами; (g) використовувати автоматизовані інструменти для допомоги користувачеві у виборі надійних автентифікаторів паролів; (h) застосовувати наступні правила складу та складності: ***[мінімум 12 символів, включаючи великі і малі літери, цифри і спецсимвол].***
5.7.	Зворотний зв’язок автентифікатора	Забезпечити прихований зворотний зв'язок автентифікаційної інформації під час процесу автентифікації.	IA-6	Забезпечити приховану зворотну передачу інформації автентифікації в процесі автентифікації для забезпечення захисту інформації від можливої експлуатації та використання неавторизованими особами.
5.8.	Управління автентифікатором	Перевіряти ідентичність особи, групи, ролі, служби або пристрою, які отримують автентифікатор під час початкового розповсюдження автентифікатора;	IA-5	Управляти системними автентифікаторами шляхом: a. перевірки, як частини початкового розподілу автентифікатора, особи, групи, ролі або пристрою, який отримує автентифікатор; b. створення вихідного вмісту автентифікатора для будь-яких автентифікаторів, виданих організацією;

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		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.		c. забезпечення того, щоб автентифікатори мали достатню стійкість механізму для їх використання за призначенням; d. створення та реалізація адміністративних процедур для первинного розповсюдження автентифікаторів, для втрачених/скомпрометованих або пошкоджених автентифікаторів, а також для відкликання автентифікаторів; e. зміни типових автентифікаторів перед першим використанням; f. зміни/оновлення автентифікаторів у встановлений ***[6 місяців]*** або коли відбуваються ***[зміни в організації, підозри на компрометацію, або змінюється рівень доступу];*** g. захисту вмісту автентифікатора від несанкціонованого розкриття та модифікацій; h. вимоги до осіб, які використовують пристрої, використовувати спеціальні заходи безпеки для захисту автентифікаторів; i. вимоги змінювати автентифікатори для облікових записів груп/ролей при зміні членства в цих облікових записах.
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	a. Впровадити можливості обробки інцидентів безпеки та приватності, включно з підготовкою, виявленням і аналізом, локалізацією, ліквідацією та відновленням. b. Координувати діяльність з обробки інцидентів із заходами із забезпечення безперервності функціонування. c. Вводити уроки, що отримані з поточних дій з обробки інцидентів, у процедури реагування на інциденти, навчання й тестування та вносити відповідні зміни. d. Забезпечити, щоб строгість, інтенсивність, обсяг і результати діяльності з обробки інцидентів можна було порівняти та передбачити у всій організації.
			IR-8	a. Розробити план реагування на інциденти, який: 1. надає організації дорожню карту для впровадження її можливостей реагування на інциденти; 2. описує структуру та організацію спроможності реагування на інциденти; 3. надає високорівневий підхід до того, як здатність реагування на інциденти вписується в загальну практику організації;

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				4. відповідає унікальним вимогам організації, які пов’язані із завданнями, розміром, структурою і функціями; 5. визначає підзвітні інциденти; 6. надає показники для вимірювання можливостей реагування на інциденти всередині організації; 7. визначає ресурси та управлінську підтримку, необхідну для ефективної підтримки та розвитку можливостей реагування на інциденти; 8. вирішує питання обміну інформацією про інциденти; 9. явно визначає відповідальність за реагування на інциденти ***[керівник відділу, служба захисту інформації]***; 10. явно визначає відповідальність за реагування на інциденти ***[системний адміністратор]***. b. Поширити копії плану реагування на інциденти серед [***адміністраторами безпеки, керівниками відділів].*** c. Оновлювати план реагування на інциденти в разі змін в системі та організації або проблем, що виникають при реалізації, виконанні чи тестуванні плану. d. Повідомляти про зміни плану реагування на інциденти [***адміністраторами безпеки, керівниками відділів***]. e. Захистити план реагування на інциденти від несанкціонованого розкриття та модифікації.
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	Відстежувати та документувати інциденти безпеки та приватності
			IR-6	a. Вимагати від персоналу повідомляти про підозрілі інциденти з безпеки та приватності відповідно до організаційної спроможності реагування на інциденти впродовж ***[24 годин].*** b. Звітувати про інциденти безпеки, приватності та ланцюжки постачання в ***[CERT-UA].***
			IR-7	Надавати ресурси для підтримки реагування на інциденти, що є невіддільною частиною спроможностей організації реагування на інциденти, які являють собою поради та допомогу користувачам інформаційної системи для обробки та формування звітності про інциденти безпеки та приватності.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
6.3.	Перевірка реагувань на інциденти	Періодично перевіряти ефективність системи реагування на інциденти.	IR-3	Перевіряти ефективність реагування системи на інциденти [***щоквартально***] за допомогою [***Моделювання атак (penetration testing).*** ***Тестування на відновлення після інцидентів (disaster recovery testing).*** ***Сценарії реагування на інциденти (incident response drills).*** ***Оцінка уразливостей (vulnerability assessments).].***
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	a. Забезпечити навчання користувачів щодо системи реагування на інциденти, відповідно до призначених ролей та обов'язків: 1. у рамках ***[протягом першого місяця після призначення на відповідну посаду***], впродовж якого авторизована роль або відповідальність за реагування на інциденти; 2. у разі внесення змін у систему; 3. з визначеною ***[щорічно***] у подальшому. b. Переглядайте та оновлюйте навчальний контент із реагування на інциденти ***[щорічно***] та наступні ***[після будь-яких значних інцидентів безпеки або змін у законодавстві, що впливають на вимоги до реагування на інциденти.].***
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	a. Затвердити, контролювати та відстежувати використання засобів технічного обслуговування. b. Переглядати раніше затверджені інструменти технічного обслуговування ***[щоквартально].***
			MA-3(1)	Оглянути інструменти для технічного обслуговування, які доставлені на об'єкт обслуговим персоналом, на предмет неправильних або несанкціонованих модифікацій.
			MA-3(2)	Перед використанням носіїв у системі перевірити носії, що містять діагностичні та тестові програми на наявність шкідливого коду.
7.2.	Віддалене обслуговування	Затверджувати та контролювати віддалені сеанси з технічного обслуговування та діагностики;	MA-4	a. Впровадити та відстежувати віддалені дії з обслуговування та діагностики.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		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.		b. Дозволити використання віддалених засобів технічного обслуговування та діагностики лише відповідно до організаційної політики та в разі, якщо це документально зафіксовано в плані безпеки системи. c. Використовувати надійну автентифікацію при встановленні віддалених технічних та діагностичних сеансів. d. Вести облік віддалених дій з обслуговування та діагностики. e. Припинити сесії та мережеві з'єднання, коли завершено віддалене 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	a. Встановити процедуру авторизації технічного персоналу та вести перелік авторизованих організацій технічного обслуговування або персоналу. b. Перевіряти, що персонал, який не супроводжується та виконує технічне обслуговування в системі, має необхідні дозволи на доступ. c. Визначити персонал організації з необхідними повноваженнями щодо доступу та технічною компетенцією для нагляду за персоналом з технічного обслуговування, який не має необхідних дозволів на доступ.
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	a. Фізично контролювати та безпечно зберігати ***[жорсткі диски, SSD, USB-накопичувачі, оптичні диски]*** в межах [***контрольованої зони***]. b. Захищати системні носії, які визначені в MP-4 до того часу, як носії знищуються або очищаються, з використанням затвердженого обладнання, методів та процедур.
8.2.	Доступ до носіїв інформації	Обмежити доступ до конфіденційної інформації на носіях інформації.	MP-2	Обмежити доступ до [***жорсткі диски, SSD, USB-накопичувачі, оптичні диски***] ***[керівниками, системними адміністраторами].***
8.3.	Знищення інформації на носіях інформації	Очистити носії інформації, що містять відкриту та конфіденційну інформацію, перед утилізацією,	MP-6	a. Очищувати [***жорсткі диски, SSD, USB-накопичувачі, сервери]*** перед утилізацією, випуском за межі організаційного контролю, або перед повторним використанням [***використовуючи спеціальне програмне забезпечення DBAN***].

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		випуском з-під контролю організації або повторним використанням.		b. Використовувати механізми очищення зі стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації.
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	a. Наносити на носії інформації маркування, що вказують на обмеження поширення, обробки, а також застереження та відповідні мітки безпеки (якщо такі є) інформації. b. Звільнити [***жорсткі диски, SSD, USB-накопичувачі, оптичні диски, які містять відкриту інформацію***] від маркування, якщо носії залишаються в межах [***Серверні кімнати, що захищені від несанкціонованого доступу.*** ***Зони для зберігання даних, доступ до яких мають лише уповноважені особи.*** ***Внутрішні архіви, що знаходяться під контролем спеціалізованого персоналу***.].
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	a. Захищати та контролювати ***[жорсткі диски, SSD, магнітні стрічки, USB-накопичувачі, оптичні диски, резервні копії даних, ноутбуки***] під час транспортування за межами контрольованих зон, використовуючи [***захищених контейнерів або сейфів для транспортування;*** ***Використання захищених каналів зв'язку для передачі даних, таких як;*** ***Супроводжуючого персоналу для забезпечення фізичної безпеки під час транспортування].*** b. Вести облік носіїв системи інформації під час транспортування за межами контрольованих зон. c. Документувати дії, пов’язані з транспортуванням носіїв системи. d. Обмежити діяльність уповноваженого персоналу, пов’язану з транспортуванням носіїв системи.
			SC-28	Забезпечити [***конфіденційність; цілісність***] [***технічні дані***] в стані спокою.
			SC-28(1)	Впровадити криптографічні механізми для запобігання несанкціонованому розкриттю та модифікації [***конфіденційної інформації, зокрема документів, персональних даних, журналів аудиту***] у стані спокою на [***серверних сховищах, базах даних, резервних копіях, пристроях користувачів***].
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	a. [***обмежити***] використання [***зовнішніх носіїв інформації, таких як USB-накопичувачі, зовнішні жорсткі диски, SD-карти, CD/DVD***] на [***серверних системах, робочих станціях співробітників, пристроях з доступом до конфіденційних даних***], використовуючи [***групові політики доступу, блокування портів на рівні операційної системи, DLP-системи (Data Loss Prevention), шифрування дозволених носіїв***]. b. Заборонити використання портативних пристроїв зберігання даних в системах організації, якщо такі пристрої не мають визначеного власника.
Кадрова безпека (PS)				
9.1.	Перевірка персоналу	Перевіряти осіб перед тим, як надавати їм доступ до системи;	PS-3	a. Перевіряти окремих осіб перед дозволом на доступ до інформаційної системи. b. Переглядати окремих осіб відповідно до ***[зміна посади, порушення політик безпеки, не рідше ніж раз на 12 місяців.]***.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		проводити повторні перевірки осіб відповідно до [*призначення: умови, що потребують повторної перевірки, визначені організацією*].		
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	При припиненні особою індивідуального трудового договору в організації необхідно: a. відключити доступ до системи протягом ***[24 годин з моменту офіційного припинення трудових відносин]***; b. завершити або скасувати всі засоби автентифікації та облікові дані, пов’язані з цією особою; c. провести співбесіди при звільненні, які містять обговорення ***[знищення даних після звільнення*** ***наслідки щодо несанкціонованого доступу та розповсюдження робочих матеріалів];*** d. отримати все майно, пов’язане із заходами безпеки під час користування системою організації; e. зберігати доступ до інформації та систем організації, які раніше контролювала звільнена особа.
			PS-5	a. Переглядати та підтверджувати поточну оперативну потребу в поточних дозволах логічного та фізичного доступу до систем і об’єктів, коли особи перепризначаються або переводяться на інші посади в організації. b. Ініціювати [***видачі нових облікових записів, проведення інструктажу щодо інформаційної безпеки на новому робочому місці***] в межах ***[3 робочих днів].*** c. Змінювати повноваження доступу, якщо це необхідно, щоб відповідати будь-яким змінам операційної потреби через перепризначення або переведення. d. Повідомляти про переведення персоналу **[*службі захисту інформації*]** в рамках [***1 робочого дня***].
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;	PE-2	a. Розробити, затвердити та вести перелік осіб, які мають право авторизованого доступу до об’єкта, де перебуває система. b. Надати повноваження для доступу до об’єкта. c. Переглядати список доступу, у якому закріплений перелік персоналу або ролей, яким дозволений санкціонований доступ до об’єкта [***щоквартально***].

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		періодично перевіряти список фізичного доступу; видаляти осіб зі списку фізичного доступу, коли доступ більше не потрібен.		d. Видалити персонал зі списку доступу до об’єкта, коли такий доступ більше не потрібний.
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	a. Проводити моніторинг фізичного доступу до об’єкта, де перебуває система, з метою виявлення та реагування на інциденти фізичної безпеки. b. Переглядати журнали фізичного доступу [***раз на тиждень***] на предмет наявності [***невідповідність між обліковими записами та фактичним доступом, спроби несанкціонованого входу, доступ у неробочий час***]. c. Узгоджувати результати перегляду та розслідувань з організаційними можливостями реагування на інциденти.
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	a. Визначити та задокументувати [***відстуні альтернативні робочі місця***], які дозволені для використання працівниками. b. Впровадити [***відсутні***] на альтернативних робочих місцях. c. Оцінити ефективність заходів захисту на альтернативних робочих місцях. d. Надати працівникам засоби комунікації з персоналом служби інформаційної безпеки в разі інцидентів безпеки.
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];	PE-3	a. Забезпечити авторизацію фізичного доступу за адресою [***вхід в будівлю, вул. Максима Залізняка 3, б 6***] шляхом: 1. перевірки індивідуального дозволу доступу до об’єкта; 2. управління входом та виходом на об’єкт за допомогою ***[турнікет, електронні картки; охорона]***. b. Вести журнали контролю фізичного доступу для [***серверних приміщень, та входу в будівлю***]. c. Забезпечити [***вставновлення турнікетів, паролі доступу в приміщення, системи відеоспостереження***] для контролю доступу в зони всередині об’єкта, позначені як загальнодоступні. d. Супроводжувати відвідувачів та контролювати активність відвідувачів [***Відвідувачі допускаються лише у супроводі уповноваженого співробітника.*** ***Вхід реєструється в електронному журналі із записом: Ім'я, прізвище Ціль візиту Особа, яка супроводжує Час входу/виходу***]. e. Забезпечити захист ключів, кодів доступу та інших пристроїв фізичного доступу. f. Проводити інвентаризацію [***електронних ключів, карт доступу, біометричних зчитувачів, кодових панелей, механічних замків***] кожен ***[щоквартально***].

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		4) забезпечити захист ключів, кодів доступу та інших пристроїв фізичного доступу.		g. Здійснювати зміну кодів доступу та ключів [***кожні 90 днів***], коли ключі втрачені, комбінації скомпрометовані або фізичні особи переведені чи звільнені.
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	Контролювати фізичний доступ до [***серверної кімнати, кімнати резервного живлення, комутаційної кімнати***] у рамках можливостей організації, використовуючи [***кодовий замок, відеоспостереження, датчики відкриття дверей, систему контролю доступу із логуванням усіх подій***].
			PE-5	Керувати фізичним доступом до вихідних даних з [***принтерів, копіювальних апаратів, терміналів перегляду документів, USB-портів на робочих станціях***], для запобігання несанкціонованому отриманню користувачами вихідних даних.
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	a. Проводити оцінювання ризику, включно з вірогідністю й величиною шкоди від: 1. несанкціонованого доступу, використання, розголошення, руйнування, модифікації або знищення інформаційної системи, інформації, яку вона обробляє, зберігає та передає; а також будь-якої пов'язаної інформації; 2. проблем, пов'язаних з приватністю фізичних осіб, що виникають у результаті обробки персональних даних. b. Інтегрувати результати оцінювання ризику та рішення з управління ризиками на рівні організації та завдань/процесів з оцінюванням ризиків на рівні інформаційної системи. c. Задокументувати результати оцінювання ризику до [***звітів про оцінювання ризику, планів безпеки та приватності, які включають:*** ***Опис ідентифікованих ризиків (список загроз, атак, уразливостей).*** ***Оцінка впливу та ймовірності кожного ризику.*** ***Заходи для зниження ризику (технічні, адміністративні).*** ***Відповідальні особи за реалізацію заходів.*** ***Дата проведення оцінювання та наступного перегляду***.]. d. Переглядати результати оцінювання ризиків [***щонайменше раз на рік або при виникненні суттєвих змін у системі***]. e. Поширити результати оцінювання ризику серед ***[керівництва служби, служби захисту інформації].*** f. Оновлювати оцінювання ризику [***щонайменше раз на рік або при значних змінах у системі (впровадження нового функціоналу, зміну конфігурації, виявлення нових загроз)***] або коли є суттєві зміни в інформаційній системі, її робочому середовищі чи інших умовах, які можуть вплинути на стан безпеки або приватність інформаційної системи.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
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	a. Сканувати на наявність вразливостей в інформаційній системі та інстальованих застосунках [***щотижня, після критичних оновлень безпеки та випадковим чином у межах процесу безперервного моніторингу***] і коли виявляються нові вразливості, які потенційно впливають на інформаційну систему. b. Використовувати інструменти та методи сканування вразливості, які полегшують сумісність між інструментами та автоматизують частини процесу управління вразливостями, використовуючи стандарти для: 1. обліку платформ, недоліків програмного забезпечення та неправильних конфігурацій; 2. форматування контрольних списків і процедур тестування; 3. вимірювання впливу вразливості. c. Аналізувати звіти про сканування вразливості та результати контрольних оцінювань. d. Виправити наявні вразливості [***протягом 24 годин для критичних вразливостей, 7 днів для високих ризиків, 30 днів для середніх ризиків та 90 днів для низьких ризиків***] відповідно до організаційної оцінки ризику. e. Ділитися інформацією, отриманою в процесі сканування вразливостей та контрольного оцінювання серед [***служби захисту інформації, адміністраторів системи та відповідальних за аудит персоналу***], щоб допомогти усунути подібні вразливі місця в інших системах. f. Використовувати інструменти сканування вразливості, які містять можливість легко оновлювати вразливості, що були просканові.
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	a. Виберіть відповідного оцінювача або команду з оцінки для типу оцінювання, яке буде проводитися; b. Розробіть план контрольної оцінки, який описує обсяг оцінки, в тому числі: 1. заходи захисту та посилені заходи, що підлягають оцінюванню; 2. процедури оцінювання, які використовуватимуться для визначення ефективності заходів; 3. середовище оцінювання, групу оцінювання, ролі й обов’язки з оцінювання. c. Забезпечити розгляд і затвердження плану оцінювання уповноваженою офіційною особою або призначеним для проведення оцінювання представником; d. Оцінити заходи захисту в системі та в її середовищі функціонування з [***щоквартальною або після значних змін у системі***] для визначення, наскільки коректно реалізовані заходи безпеки і чи працюють вони за призначенням і дають бажаний результат щодо дотримання встановлених вимог безпеки та приватності; e. Підготовити звіт оцінювання безпеки, який документує результати оцінювання; f. Надати результати оцінювання з безпеки [***керівництву, службі захисту інформації***].

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
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	a. Розробити для системи план усунення недоліків та контрольні показники з метою документування запланованих коригувальних дій організації для усунення недоліків і зауважень, які виявлені в ході оцінювання заходів захисту, а також для зменшення або усунення відомих вразливостей у системі. b. Оновлювати чинний план усунення недоліків та контрольні показники з [***щоквартально, або після значних змін у системі***] на основі результатів оцінювання заходів, незалежних аудитів та постійного моніторингу.
12.3.	Безперервний моніторинг	Розробити та впровадити стратегію безперервного моніторингу на рівні системи, що передбачає постійний моніторинг та оцінку безпеки.	CA-7	Розробити стратегію безперервного моніторингу безпеки та приватності й упровадити програму безперервного моніторингу безпеки та приватності, яка охоплює: a. встановлення показників безпеки та приватності, які необхідно відстежувати: [***кількість виявлених вразливостей, середній час на усунення інцидентів, кількість несанкціонованих доступів, рівень відповідності нормативним вимогам***]; b. встановлення [***щогодинної частоти для критичних подій, щоденної для загальних подій, щоквартальної для стратегічного аналізу***] для моніторингу та [***щомісячної оцінки ефективності заходів захисту***] для безперервного оцінювання ефективності заходів захисту; c. поточні оцінювання заходів захисту відповідно до стратегії безперервного моніторингу організації; d. постійний моніторинг стану безпеки та приватності відповідно до встановлених організацією метрик і відповідно до стратегії безперервного моніторингу організації; e. зіставлення та аналіз інформації, отриманої в результаті оцінювання та моніторингу безпеки та приватності; f. дії реагування за результатами аналізу інформації, пов’язаної з безпекою та приватністю; g. повідомлення про статус безпеки та приватності системи [**службі захисту інформації, керівництву**] з [***щотижневою періодичністю та негайними сповіщеннями при критичних інцидентах***].
12.4.	Взаємодія систем	Затвердити та керувати обміном конфіденційної інформації між системою та іншими системами, використовуючи [*вибір (один або*	CA-3	a. схвалити та керувати обміном інформацією між системою та іншими системами за допомогою [***угоди безпеки взаємозв’язку (ISA), договорів безпеки обміну інформацією (ISSA), меморандумів про взаєморозуміння (MOU), угод про рівень обслуговування (SLA), угод користувача (UA), угод про нерозголошення (NDA)];.***

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		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.		b. документувати, як частину угоди про обмін, характеристики інтерфейсу, вимоги до безпеки та приватності, засоби контролю та відповідальність для кожної системи, а також характер переданої інформації; c. здійснювати перегляд та оновлення угод з [***щорічною частотою для стандартних угод, щоквартально для критичних взаємозв'язків, або при зміні законодавчих вимог***].
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	a. Контролювати та управляти зв'язком на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи. b. Реалізувати підмережі для загальнодоступних компонентів системи, які є [***логічно***] відділені від внутрішніх мереж організації. c. Підключатися до зовнішніх мереж або систем тільки через керовані інтерфейси, що складаються з пристроїв захисту периметру, і розташованих відповідно до архітектури безпеки та приватності організації.
13.2.	Інформація в загальних ресурсах системи	Запобігати несанкціонованій і ненавмисній передачі інформації за допомогою загальних ресурсів системи.	SC-4	Запобігати несанкціонованій та ненавмисній передачі інформації через спільні системні ресурси.
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)	Заборонити за умовчанням трафік мережевого зв'язку та дозволити трафік мережевого зв'язку за винятком [***керованих інтерфейсів***] для [***СЕД]***.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
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	Забезпечити [***конфіденційність; цілісність***] інформації, що передається.
			SC-8(1)	Реалізувати механізми криптографічного захисту для [***запобігання несанкціонованому розкриттю інформації; вияву зміни в інформації***] під час передачі.
			SC-28	Забезпечити [***конфіденційність; цілісність***] [***документів в системі, метадані документів, база даних документів, журнали аудиту, резервні копії***] в стані спокою.
			SC-28(1)	Впровадити криптографічні механізми для запобігання несанкціонованому розкриттю та модифікації [***службової інформації, персональних даних, журналів аудиту, конфіденційної документації***] у стані спокою на [***сервери баз даних, файлові сховища, резервні копії, лог-сервери***].
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	Завершити з'єднання з мережею, яке пов'язане із сеансом зв'язку в кінці сеансу або після [***15 хвилин***] бездіяльності.
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	Встановити та управляти криптографічними ключами для криптографічних засобів, які використовуються в системі відповідно до [***Призначення: алгоритм для генерації RSA-3072 або більше, метод розповсюдження: автентифіковані канали TLS 1.3***].
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	a. Визначити [***Призначення: засоби КЗІ які мають експертний висновок за результатами державної експертизи у сфері КЗІ та призначені для захисту конфіденційної інформації***]; b. Впровадити [***Завдання: протокол: TLS 1.3, алгоритм: AES-256***].
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	a. Заборонити віддалену активацію спільних обчислювальних пристроїв (хмар) та застосунків з такими виключеннями: [***Призначення: без виключень***]. b. Надати явну вказівку щодо використання користувачами фізично присутніми пристроями.
13.9.	Мобільний код	Визначити прийнятний мобільний код і технології мобільного коду; авторизувати, відстежувати та контролювати використання мобільного коду.	SC-18	a. Визначати прийнятні та неприйнятні мобільні коди та технології мобільних кодів. b. Проводити авторизацію, відстежувати та контролювати використання мобільного коду всередині системи.
13.10	Автентифікація сесії	Захистити автентифікацію сеансів зв'язку.	SC-23	Забезпечити автентифікацію сеансів зв'язку.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
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	a. Виявляти, виправляти та повідомляти про недоліки системи. b. Перед установкою перевірити програмне забезпечення та оновлення вбудованого програмного забезпечення, що пов'язані з усуненням дефектів, на ефективність та можливі побічні ефекти. c. Інсталювати оновлення програмного забезпечення та оновлення вбудованого програмного забезпечення в межах [***30 днів***] випуску оновлень. d. Внести виправлення помилок в процес управління конфігурацією організації.
14.2.	Захист від шкідливого коду	1) Упровадити механізми захисту від шкідливого коду у визначених місцях системи для виявлення та знищення шкідливого коду; 2) оновлювати механізми захисту від шкідливого коду в міру виходу нових версій відповідно до політики та процедур управління конфігурацією; 3) налаштувати механізми захисту від шкідливого коду на: виконання сканування системи [*призначення: частота, визначена організацією*] та сканування файлів із зовнішніх джерел у реальному часі на кінцевих точках або точках входу та виходу з мережі під час завантаження, відкриття або виконання файлів; блокування шкідливого коду, поміщення шкідливого коду в карантин або інші дії у відповідь на виявлення шкідливого коду.	SI-3	a. Впровадити механізми захисту від шкідливого коду [***на основі підпису; не на основі підпису]*** на вході та виході системи для виявлення та знищення шкідливого коду. b. Автоматично оновлювати механізми захисту від шкідливого коду, коли доступні нові випуски відповідно до політики та процедур управління конфігурацією. c. Налаштовувати механізми захисту від шкідливого коду для: 1. Виконання періодичного сканування системи [***раз на 24 години***] і сканування файлів у реальному часі із зовнішніх джерел у [***кінцевій точці; точці входу/виходу в мереж***у], коли файли завантажуються, відкриваються або виконуються відповідно до політики організації. 2. [***Блокування шкідливого коду; Відправлення шкідливого коду в карантин; Надсилання попередження адміністратору***] у відповідь на виявлення шкідливого коду. d. Фіксувати отримання помилкових спрацьовувань під час виявлення й усунення шкідливого коду та, як наслідок, потенційного впливу на доступність системи.
14.3.	Попередження, рекомендації та директиви з безпеки	Отримувати попередження, рекомендації та директиви щодо безпеки системи від зовнішніх організацій на постійній основі;	SI-5	a. Отримувати системні попередження безпеки, рекомендації та директиви від [***Національного центру кібербезпеки, CERT-UA, вендорів безпеки***] на постійній основі. b. Генерувати внутрішні попередження безпеки, рекомендації та директиви (за необхідністю).

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		створювати та розповсюджувати внутрішні попередження системи, рекомендації та директиви щодо безпеки у разі потреби; упроваджувати директиви з безпеки відповідно до встановлених часових рамок.		c. Поширювати попередження, рекомендації та директиви безпеки для: [***Користувачів***] d. Впровадити директиви безпеки відповідно до встановлених термінів і повідомити організацію-емітента про ступінь невідповідності.
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	a. Здійснювати моніторинг системи для виявлення: 1. атак та індикаторів потенційних атак відповідно до [***стратегії кібербезпеки організації, політики реагування на інциденти***]; 2. Неавторизованих локальних, мережевих та віддалених підключень. b. Визначати несанкціоноване використання системи через [***аналіз логів безпеки, поведінковий аналіз користувачів (UEBA), SIEM-систему, контроль доступу, моніторинг підозрілих дій у реальному часі***]. c. Застосовувати можливості внутрішнього моніторингу або розгортати пристрої моніторингу: 1. стратегічно в рамках системи для збору необхідної для організації суттєвої інформації; 2. у спеціальних місцях у системі для відстеження конкретних видів транзакцій, що мають інтерес для організації. d. Захищати інформацію, отриману від засобів моніторингу вторгнень, від несанкціонованого доступу, модифікації та видалення. e. Регулювати рівень активності системного моніторингу при зміні ризику для операцій і активів організації, фізичних осіб, інших організацій або держави. f. Отримувати за результатами моніторингу системи юридичний висновок щодо діяльності. g. Надавати [***звіт про моніторинг системи, індикатори компрометації, інформацію про виявлені інциденти***] до [***Призначення: визначений організацією персонал або посадові особи***] [***за необхідності або щотижнево***].
			SI-4(4)	a) Визначити критерії незвичайної або несанкціонованої діяльності або умов для вхідного та вихідного комунікаційного трафіку; b) Проводити моніторинг вхідного та вихідного комунікаційного трафіку [***у реальному часі***] для виявлення незвичайних або несанкціонованих дій чи умов.
Планування безпеки (PL)				
15.1.	Політика та процедури планування безпеки	Розробити, задокументувати та розповсюдити серед персоналу організації або ролей політики та	AC-1	a. Розробити, задокументувати та поширити [***відповідальних адміністраторів, керівників підрозділів, користувачів з привілейованим доступом***]: 1. [***Рівень організації; Рівень місії/бізнес-процесу; рівень системи***] політики контролю доступу, яка:

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		процедури, необхідні для виконання вимог безпеки; періодично переглядати та оновлювати політики та процедури.		(a) містить мету, сферу застосування, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та систему контролю відповідності (compliances); (b) відповідає чинному законодавству, нормативним документам, директивам, нормам, політикам, стандартам і керівним документам. 2. Процедури, що сприяють реалізації політики управління доступом і відповідних заходів управління доступом. 21 b. Призначити на посаду [***керівник служби захисту***] для управління, документування і розповсюдження політики та процедур контролю доступом. c. Переглянути та оновити: 1. поточну політику управління доступом [***раз на рік***] та [***після зміни у законодавстві, структурі організації чи виявлених інцидентів***]; 2. поточні процедури управління доступом [***щоквартально***] та [***після значних оновлень системи, виявлення порушень безпеки***].
			AT-1	a. Розробити, задокументувати та поширити [***усіх працівників, служби захисту, керівників підрозділів***]: 1. [***Рівень організації; Рівень місії/бізнес-процесу; рівень системи***] політики обізнаності та навчання у сфері забезпечення безпеки та приватності, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам. 2. Процедури, що сприяють реалізації політики підвищення обізнаності та професійної підготовки в галузі безпеки, приватності, а також пов'язаних з ними заходів захисту інформації та персональних даних. b. Призначити [***керівник служби захисту***] для управління політикою та процедурами підвищення обізнаності та навчання у сфері забезпечення безпеки та приватності. c. Переглядати та оновлювати: 1. Поточну політика [***раз на рік***] і наступне [**п*ісля змін у законодавстві, кіберінцидентів чи оновлення технологій***]; 2. Процедури [***кожні півроку***] та наступні [***після виявлення нових загроз чи впровадження нових безпекових заходів***].
			AU-1	a. Розробити, задокументувати та поширити [***усіх працівників, служби захисту, керівників підрозділів***]:

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				1. [***Рівень організації; Рівень місії/бізнес-процесу; рівень системи***] політика аудиту та підзвітності, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам. 2. Процедури, що сприяють здійсненню політики аудиту та підзвітності, а також пов'язані з ними заходи аудиту та підзвітності. b. Призначити [***керівник служби захисту***] для управління політикою та процедурами аудиту та підзвітності. c. Переглядати та оновлювати поточний аудит та підзвітність: 1. політику [***раз на рік***] та наступне [***після змін у законодавстві чи виявлення критичних інцидентів***]; 2. процедури аудиту **[*щоквартал*]** та [***після виявлення порушень чи змін у критичних бізнес-процесах*].**
			CA-1	a. Розробити, задокументувати та поширити серед [***усіх працівників, служби захисту, керівників підрозділів***]: 1. [***Рівень організації; Рівень місії/бізнес-процесу; рівень системи***] політика оцінювання, авторизації та моніторингу, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинним законам, нормативним документам, наказам, положенням, політиці, стандартам і керівним принципам. 2. Процедури, що сприяють реалізації політики оцінювання, авторизації та моніторингу безпеки та приватності, а також пов'язаних з ними заходів оцінювання, авторизації та моніторингу безпеки та приватності. b. Призначити [***керівник служби захисту***] для управління розробкою, документуванням і розповсюдженням політики та процедур оцінювання, авторизації та моніторингу; c. Переглядати та оновлювати поточне оцінювання, авторизацію та моніторинг: 1. Політику [***раз на рік***] та наступне [***після змін у законодавстві чи виявлення критичних інцидентів***]; 2. Процедури [***щоквартал***] та наступні [***після виявлення критичних вразливостей, змін у процесах або значних інцидентів безпеки***].
			CM-1	a. Розробити, задокументувати та поширити серед [***усіх працівників, служби захисту, керівників підрозділів***]:

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				1. [***Рівень організації; Рівень місії/бізнес-процесу; рівень системи***] політики управління конфігурацією, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинним законам, нормативним документам, наказам, положенням, політикам, стандартам і керівним принципам; 2. процедури, що сприяють реалізації політики управління конфігурацією та пов'язаних з нею заходів управління конфігурацією. b. Призначити [***керівник служби захисту***] для управління розробкою, документуванням і розповсюдженням політики та процедур керування конфігурацією. c. Переглядати та оновлювати поточну політику управління конфігурацією: 1. Політика [***раз на рік***] та наступні [**п*ісля змін у законодавстві, кіберінцидентів чи оновлення технологій***]; 2. Процедури [***щоквартал***] та наступні [**п*ісля виявлення критичних вразливостей, змін у процесах або значних оновлень систем***].
			IA-1	a. Розробити, задокументувати та поширити [***усіх працівників, служби захисту, керівників підрозділів***]: 1. 1. [***Рівень організації; Рівень місії/бізнес-процесу; рівень системи***] політики ідентифікації та автентифікації, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим розпорядженням, директивам, положенням, політиці, стандартам і керівним принципам; 2. процедури, що спрямовані на реалізацію політики ідентифікації та автентифікації і пов'язаних з ними заходів ідентифікації та перевірки автентичності. b. Призначити [***керівник служби захисту***] для управління політикою та процедурами ідентифікації та автентифікації. c. Переглянути та оновити поточну політику ідентифікації та автентифікації: 1. політика [***щороку]*** і наступні [**п*ісля значних змін у нормативних вимогах, загрозах або системах автентифікації***]; 2. процедури [***щопівроку*]** і наступні [**у *разі виявлення вразливостей, змін у технологіях або значних інцидентів безпеки***].
			IR-1	a. Розробити, задокументувати та поширити [***усіх працівників, служби захисту, керівників підрозділів***]:

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				1. [***Рівень організації; Рівень місії/бізнес-процесу; рівень системи***] політики реагування на інциденти, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (a) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам; 2. процедури, що забезпечують реалізацію політики реагування на інциденти та пов'язані з нею заходи реагування на інциденти. b. Призначити [***керівник служби захисту***] для управління, документування і розповсюдження політики та процедур реагування на інциденти. c. Переглядати та оновлювати поточні: 1. політику реагування на інциденти [***щороку***] і наступні [**п*ісля значних змін у загрозах, нормативних вимогах чи кіберінцидентах***.]; 2. процедури реагування на інциденти [***щопівроку***] та наступні [***у разі значного інциденту, виявлення нових атак чи змін у технологічному ландшафті***].
			MA-1	a. Розробити, задокументувати та поширити серед [***усіх працівників, служби захисту, керівників підрозділів***]: 1. Політику технічного обслуговування системи, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам. 2. Процедури, що сприяють здійсненню політики та заходів технічного обслуговування систем. b. Призначити [***керівник служби захисту***] для управління політикою та процедурами технічного обслуговування. c. Переглядати та оновлювати: 1. Поточну політику технічного обслуговування систем [***щороку***] та слідувати [**у *разі значних змін у технологічній інфраструктурі, нормативних вимогах чи виявлених вразливостях***.]. 2. Поточні процедури технічного обслуговування систем [***щопівроку***] та слідувати **[у *разі критичних змін у системах, впровадження нового обладнання чи оновлення ПЗ***].
			MP-1	a. Розробити, задокументувати та поширити серед [***усіх працівників, служби захисту, керівників підрозділів***]: 1. політику захисту носіїв інформації, яка:

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам; 2. процедури, які сприяють здійсненню політики та заходів захисту носіїв інформації. b. Призначити [***керівник служби захисту***] для управління розробкою, документування, та розповсюдження політики та процедурами захисту носіїв інформації. c. Переглядати та оновлювати чинну систему захисту носіїв інформації: 1. поточну політику захисту носіїв інформації [***щороку***]; 2. поточні процедури захисту носіїв інформації [***щопівроку***].
			PE-1	a. Розробляє, документує та поширює серед [***усіх працівників, служби захисту, керівників підрозділів***]: 1. політику в галузі фізичного захисту та захисту робочого середовища, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам; 2. процедури, які сприяють виконанню політики та заходів у галузі фізичного захисту та захисту робочого середовища. b. Призначити [***керівник служби захисту***] для управління політикою та процедурами фізичного захисту та захисту робочого середовища. c. Переглядати та оновлювати: 1. поточну політику фізичного захисту та захисту робочого середовища [***щороку***]; 2. поточні процедури фізичного захисту та захисту робочого середовища [***щопівроку***].
			PL-1	a. Розробити, задокументувати та поширити серед [***усіх працівників, служби захисту, керівників підрозділів***]: 1. [***рівень організації; рівень місії/бізнес процесу; рівень системи***] політику планування, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та системою контролю (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам; 2. процедури, що полегшують здійснення планування політики безпеки та приватності й пов'язані з ними заходи.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				b. Призначити [***керівник служби захисту***] для управління політикою та процедурами планування політики безпеки та приватності. c. Переглядати та оновлювати поточне планування: 1. політики планування безпеки та приватності [***щороку***] та наступні [***після значних змін у нормативно-правовому полі***]; 2. поточні процедури планування політики безпеки та приватності [***Щоквартально***] та наступні [***після інцидентів з безпеки***].
			PS-1	a. Розробити, задокументувати та поширити серед [***усіх працівників, служби захисту, керівників підрозділів***]: 1. [***на рівні організації, на рівні місії/бізнес процесу, на рівні системи***] політику кадрової безпеки, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та рекомендаціям. 2. Процедури, що сприяють здійсненню політики кадрової безпеки та пов'язаних з ними заходів кадрової безпеки. b. Призначити [***керівник служби захисту***] для управління розробкою, документуванням та впровадженням політики та процедур кадрової безпеки. c. Переглядати та оновлювати: 1. Поточну політику кадрової безпеки [***щорічно***] та подальші заходи, визначені організацію. 2. Поточні процедури кадрової безпеки [***щоквартально***] та подальші заходи, визначені організацію.
			RA-1	a. Розробити, задокументувати та поширити серед [***усіх працівників, служби захисту, керівників підрозділів***]: 1. Політику оцінювання ризику, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам. 2. Процедури, що сприяють здійсненню політики оцінювання ризику та пов'язаних з ними заходів оцінювання ризику. b. Призначити [***керівник служби захисту***] для управління політикою та процедурами оцінювання ризику.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				с. Переглядати й оновлювати: 1. Поточну політику оцінювання ризику [***щорічно***]. 2. Поточні процедури оцінювання ризику [***щоквартально***].
			SA-1	a. Розробити, задокументувати та поширити серед [***усіх працівників, служби захисту, керівників підрозділів***]: 1. [***рівень організації; рівень місії/бізнес-процесу; рівень системи***] політики придбання систем і послуг, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і рекомендаціям. 2. Процедури, що полегшують впровадження політики та заходів придбання систем і послуг. b. Призначити [***керівник служби захисту***] для управління політикою та процедурами придбання системи та послуг. c. Переглядати й оновлювати поточні політику та процедури придбання систем та послуг: 1. Поточну політику придбання системи та послуг [***щорічно***]. 2. Поточні процедури придбання системи та послуг [***щоквартально***] та наступні [***після значних змін у процесах закупівель чи постачальниках***].
			SC-1	a. Розробити, задокументувати та поширити серед [***усіх працівників, служби захисту, керівників підрозділів***]: 1. Політику захисту системи та комунікацій, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам. 2. Процедури для сприяння впровадженню політики в області захисту систем і комунікацій, а також пов'язаних з ними систем і засобів захисту зв'язку. b. Призначити [***керівник служби захисту***] для управління політикою та процедурами захисту системи та комунікацій. c. Переглядати та оновлювати: 1. поточну політику захисту системи та комунікацій [***щорічно***]; 2. поточні процедури захисту системи та комунікацій [***щоквартально***].
			SI-1	a. Розробити, задокументувати та поширити серед [***усіх працівників, служби захисту, керівників підрозділів***]:

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				1. Політику цілісності системи та інформації, яка: (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince); (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам. 2. Процедури, що сприяють впровадженню політики цілісності системи та інформації, а також пов'язані з нею заходи цілісності системи та інформації. a. Призначити [***керівник служби захисту***] для управління політикою та процедурами цілісності системи та інформації. b. Переглядати й оновлювати: 1. поточну політику цілісності системи та інформації [***щорічно***]; 2. поточні процедури цілісності системи та інформації [***щоквартально***].
			SR-1	a. Розробіть, задокументуйте та поширте [***усіх працівників, служби захисту, керівників підрозділів***]: 1. [***Рівень організації; Рівень місії/бізнес-процесу; рівень системи***] політика управління ризиками ланцюга постачання, яка: a) Розглядає мету, сферу діяльності, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та відповідність; b) Відповідає чинним законам, виконавчим наказам, директивам, положенням, політикам, стандартам і вказівкам; 2. Процедури для сприяння впровадженню політики управління ризиками ланцюга постачання та відповідних засобів контролю управління ризиками ланцюга постачання; b. Призначити [***керівник служби захисту***] для управління розробкою, документуванням і розповсюдженням політики та процедур управління ризиками ланцюга постачання; c. Перегляньте та оновіть поточне управління ризиками ланцюга постачання: 1. Політика [***щорічно*]** та наступне [***після значних змін у законодавстві, бізнес-процесах чи загрозах у ланцюзі постачання***]; 2. Процедури [***щопівроку***] та наступні [***після змін у постачальниках, технологіях чи виявлення нових ризиків***].
15.2.	Плани захисту інформації та персональних даних	1) Розробити план захисту інформації, який: визначає складові компоненти системи; описує робоче середовище системи;	PL-2	a. Розробити план захисту інформації та персональних даних для інформаційної системи, який: 1. узгоджується з архітектурою підприємства організації; 2. чітко визначає складові компоненти системи; 3. описує оперативний контекст інформаційної системи з точки зору завдань та процесів; 4. визначає осіб, які виконують системні ролі та обов'язки; 5. визначає тип інформації, яка обробляється, зберігається та передається системою;

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		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.		6. надає огляд вимог безпеки та приватності інформаційної системи; 7. описує будь які конкретні загрози системи, які викликають стурбованість організації; 8. надає результати оцінки ризику конфіденційності для систем, в яких обробляються персональні дані; 9. описує робоче середовище інформаційної системи та будь які залежності від систем або компонентів систем або підключень до таких систем та їх компонентів; 10. надає огляд вимог безпеки та конфіденційності системи; 11. визначає будь які відповідні контрольні базові рівні або накладання, якщо вони застосовуються; 12. описує чинні або заплановані заходи щодо забезпечення безпеки та приватності, включно з обґрунтуванням рішень щодо налаштування 13. включає виявлення ризиків для архітектури безпеки і приватності, а також проєктних рішень; 14. включає дії, пов’язані з безпекою та конфіденційністю, які впливають на систему, виконання яких вимагає планування та координацію з [***керівником служби захисту***]; 15. розглядається та затверджується уповноваженою посадовою особою або призначеним представником до початку реалізації плану. b. Поширити копії планів захисту інформації та персональних даних і повідомляти про подальші зміни планів серед [***системних адміністраторів, керівників відділів***]. c. Переглядати плани захисту інформації та персональних даних [***щорічно***]. d. Оновлювати плани захисту інформації та персональних даних для врахування змін в інформаційній системі й робочому середовищі або проблем, виявлених у ході реалізації або оцінювання заходів безпеки та приватності. e. забезпечити захист планів захисту інформації та персональних даних від несанкціонованого розголошення та змін.