ЗАТВЕРДЖЕНО
Наказ Міністерства культури України
___._____ 202__ року № _____

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА «ДЕРЖАВНИЙ РЕЄСТР ВИДАВЦІВ, ВИГОТОВЛЮВАЧІВ І РОЗПОВСЮДЖУВАЧІВ ВИДАВНИЧОЇ ПРОДУКЦІЇ»

ЦІЛЬОВИЙ ПРОФІЛЬ БЕЗПЕКИ

UA.43220275.СЗІ.ЦПБ-02

1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНУ СИСТЕМУ

1.1. Назва інформаційно-комунікаційної системи (ІКС)

Інформаційно-комунікаційна система «Державний реєстр видавців, виготовлювачів і розповсюджувачів видавничої продукції».

1.2. Відомості про суб'єктів відносин ІКС

Розпорядник ІКС, адміністратор ІКС:

Міністерство культури України (01601, м. Київ, вул. Івана Франка, буд. 19 (Шевченківський р-н), код ЄДРПОУ 43220275).

В подальшому викладі використовується таке позначення:

А_ІКС – Адміністратор ІКС.

1.3. Призначення та функції ІКС

ІКС призначена для автоматизації наступних процесів:

- обліку інформації про суб'єктів видавничої справи;
- надання адміністративних послуг із внесення суб'єкта господарювання до «Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції» (далі – Реєстр) та видачі свідоцтва про внесення суб'єкта господарювання до Реєстру (далі – свідоцтво), а також видачі дубліката, переоформлення, анулювання свідоцтва;
- забезпечення доступу до відомостей Реєстру;
- проведення аналізу інформації, яка обробляється в Реєстрі;
- електронної інформаційної взаємодії між інформаційно-комунікаційними системами та Реєстром.

1.4. Опис обчислювальної системи ІКС

1.4.1. Структурна схема та склад обчислювальної системи

ІКС побудована на базі локальної обчислювальної мережі центрального вузлу ІКС, яка має підключення до мережі загального користування Інтернет.

Структурна схема ІКС наведена на рис. 1.1.

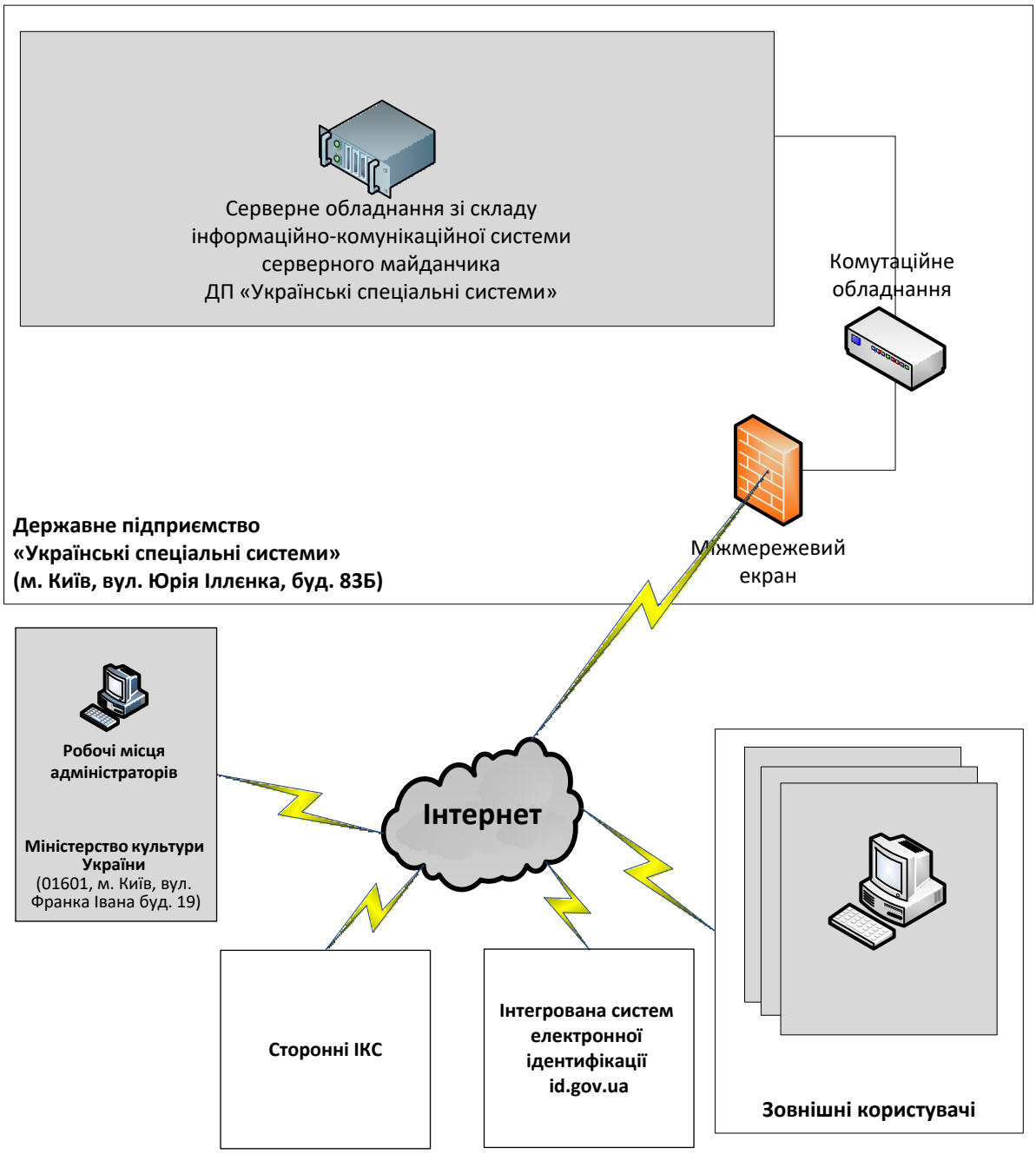

Рис. 1.1. Структурна схема ІКС

До складу ІКС входять:

– центральний вузол ІКС;

– робочі місця адміністраторів Міністерства культури України.

До складу центрального вузлу ІКС входять:

– серверне обладнання зі складу інформаційно-комунікаційної системи «Інформаційна система «Програмна платформа для розгортання та супроводження державних електронних реєстрів» Державного підприємства «Українські спеціальні системи» (далі – серверний майданчик ДП «Українські спеціальні системи»);

– комутаційне обладнання (в тому числі, міжмережевий екран).

Інформаційними послугами ІКС користуються наступні користувачі (далі разом – зовнішні користувачі):

– суб’єкти господарювання, які після проходження авторизації відповідно до цього Порядку подають заяву про внесення їх до Реєстру;

– суб’єкти видавничої справи, які пройшли авторизацію відповідно до цього Порядку;

– публічні реєстратори (посадові особи Державного комітету телебачення і радіомоовлення України (далі – Держкомтелерадіо), які взаємодіють з Реєстром відповідно до своїх посадових обов’язків).

Робочі місця адміністраторів призначені для:

– управління налаштуваннями прикладного програмного забезпечення, обліковими записами зовнішніх користувачів та правами доступу до інформаційних об’єктів;

– управління обліковими записами адміністраторів на технічних засобах ІКС, а також для перегляду протоколів подій в ІКС;

– оновлення системного, антивірусного та прикладного програмного забезпечення.

До складу ІКС не входять, але взаємодіють з нею віддалені АРМ зовнішніх користувачів, які побудовані на базі персональних та мобільних ЕОМ (ноутбуків, нетбуків). Віддалені АРМ зовнішніх користувачів призначені для виконання функцій, визначених постановою Кабінету Міністрів України від 10.03.2017 № 135 «Про затвердження Порядку ведення Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції». Віддалені АРМ зовнішніх користувачів працюють у режимі «тонкого» клієнта, які не передбачають можливості зберігання будь-яких даних на таких робочих місцях, за виключенням адміністративних даних. Всі дані, що обробляються в ІКС, зберігаються виключно в межах центрального вузла ІКС.

В рамках функціонування ІКС взаємодіє з іншими інформаційно-комунікаційними системами (див. рис. 1.1). Така взаємодія здійснюється в порядку, визначеному в документі «Інструкція з оцінювання, акредитації та моніторингу безпеки. UA.44760433.СЗІ.ІОАМ-02».

1.4.2. Характеристика апаратного та програмного забезпечення

На центральному вузлі ІКС використовується наступне програмне забезпечення:

– операційні системи робочих місць адміністраторів – Microsoft Windows 11;

– прикладне програмне забезпечення:

  – прикладне програмне забезпечення «Державний реєстр видавців, виготовлювачів і розповсюджувачів видавничої продукції» (далі – прикладне програмне забезпечення);

– антивірусне програмне забезпечення Microsoft Defender (на робочих місцях адміністраторів).

Операційні системи, прикладне та антивірусне програмне забезпечення містять програмні механізми захисту інформації, які використовуються для захисту інформації, що циркулює в ІКС.

Для мережевого захисту використовуються апаратно-програмні міжмережеві екрани (зі складу інформаційно-комунікаційної системи серверного майданчика Державного підприємства «Українські спеціальні системи»), які забезпечують виконання наступних функцій:

– фільтрацію та аналіз трафіку на рівнях L3-L4 моделі OSI;

– розмежування доступу між ІКС та зовнішніми мережами;

– інспекцію (в тому числі антивірусну перевірку) мережевого трафіку та блокування пакетів або сесій, що є підозрілими;

– маскування топології і мережевих адрес ІКС від публічного перегляду;

– контроль інформаційних потоків між ІКС та Інтернет з метою виявлення спроб мережевих вторгнень та несанкціонованого доступу до мережевих ресурсів, в т.ч. атак типу «відмова в обслуговуванні», забезпечення реєстрації, попередження та протидії таким спробам;

– виявлення комп'ютерних атак і несанкціонованої мережевої активності;

– фільтрацію та аналіз мережевого трафіку за протоколами, портами і IP-адресами відправника й одержувача;

– завершення з'єднання з вузлом, у разі атаки;

– протоколювання (реєстрація) подій, що мають відношення до безпеки;

– інші функції, визначені політикою безпеки.

Живлення всіх серверів та комутаційного обладнання здійснюється від джерел безперебійного живлення (зі складу інформаційно-комунікаційної системи серверного майданчика ДП «Українські спеціальні системи»).

Центральний вузол ІКС розгортається з використанням серверного обладнання з розгорнутою платформою віртуалізації, іншим необхідним прикладним програмним забезпеченням зі складу інформаційно-комунікаційної системи серверного майданчика ДП «Українські спеціальні системи», комплексна система захисту інформації якої має чинний атестат відповідності вимогам нормативних документів системи технічного захисту інформації № 121В від 16.12.2022.

Надання наведених послуг здійснюється ДП «Українські спеціальні системи» на підставі договору № 11.1275/25/НЦ від 05.09.2025.

ДП «Українські спеціальні системи» відповідно до наведеного договору несе відповідальність за:

– забезпечення безперебійного живлення, холодопостачання, сервісу контролю і управління доступом, сервісу пожежної безпеки;

– підтримку обчислювального середовища та мережевої інфраструктури

для забезпечення надійного та безперебійного функціонування системного та прикладного програмного забезпечення ІКС;

– надання послуги з підключення до інформаційно-комунікаційної системи серверного майданчика ДП «Українські спеціальні системи»;

– надання послуги доступу до мережі Інтернет через захищений вузол інтернет-доступу;

– захищеність фізичного середовища з метою виключення можливості несанкціонованого доступу до серверного та мережевого обладнання;

– адміністративну технічну підтримку функціонування серверного та мережевого обладнання;

– розмежування доступу до віртуального середовища, в якому обробляється інформація, що циркулює в ІКС, з боку авторизованого адміністративного персоналу ДП «Українські спеціальні системи»; неможливість доступу такого персоналу до даних, що обробляються в ІКС на рівні прикладного програмного забезпечення;

– створення облікового запису системного адміністратора Міністерства культури України;

– виконання резервного копіювання даних відповідно до налаштувань власника ІКС.

Можливість надання наведених вище інформаційних послуг підтверджується результатами державної експертизи в сфері технічного захисту інформації комплексної системи захисту інформації інформаційно-комунікаційної системи серверного майданчика ДП «Українські спеціальні системи».

Міністерство культури України (замовник послуг розміщення та обробки даних) відповідно до зазначеного договору несе відповідальність за:

– налаштування виділених ресурсів з використанням наданого облікового запису;

– створення облікових записів адміністраторів Міністерства культури України та зовнішніх користувачів.

Контроль за доступом до приміщень, де розміщуються компоненти центрального вузлу ІКС, забезпечується ДП «Українські спеціальні системи» в порядку, визначеному документацією на комплексну систему захисту інформації інформаційно-комунікаційної системи серверного майданчика ДП «Українські спеціальні системи».

1.4.3. Технічні характеристики каналів зв'язку

Для зв'язку технічних засобів локальної обчислювальної мережі центрального вузла ІКС між собою, а також для підключення до мережі Інтернет використовуються канали передачі даних Ethernet та оптоволоконні лінії зв'язку зі швидкістю передачі даних не менше, ніж 100 Мб/с.

Надання послуг інтернет-доступу здійснюється ДП «Українські спеціальні системи» за договором № 11.1275/25/НЦ від 05.09.2025 з використанням захищеного вузлу інтернет-доступу (атестат відповідності комплексної системи захисту інформації вимогам нормативних документів системи технічного захисту інформації № 21662 від 09.06.2020).

Для зв'язку робочих місць адміністраторів та АРМ зовнішніх користувачів із центральним вузлом ІКС, а також для зв'язку центрального вузлу ІКС із сторонніми ІКС та системою електронної ідентифікації id.gov.ua використовується мережа Інтернет.

1.5. Опис інформаційного середовища ІКС

1.5.1. Перелік та класифікація інформаційних ресурсів ІКС

Узагальнені відомості про інформацію, що обробляється та зберігається в ІКС, наведені в табл. 1.1.

Таблиця 1.1

№ з/п	Вид інформації	Ступінь обмеження доступу інформації	Вид представлення даних
1	Журнали реєстрації подій, що ведуться апаратними та програмними засобами ІКС	конфіденційна (технологічна)	у вигляді файлів та об'єктів баз даних
2	Файли конфігурації програмного та апаратного забезпечення, що необхідні для коректної роботи ІКС		
3	Дані облікових записів адміністраторів		
4	Інформація, що зберігається в базі даних та розміщується в Реєстрі		
4.1	Інформація про суб'єктів видавничої справи	відкрита (державні інформаційні ресурси)	у вигляді об'єктів бази даних
4.2	Інформація про суб'єктів господарювання	конфіденційна	у вигляді об'єктів бази даних
4.3	Відомості про свідоцтва про внесення суб'єкта господарювання до Реєстру	відкрита (державні інформаційні ресурси)	у вигляді файлів та об'єктів бази даних
4.4	Заяви про внесення суб'єкта господарювання до Реєстру свідоцтва про внесення суб'єкта господарювання до Реєстру	конфіденційна	у вигляді файлів та об'єктів бази даних
4.5	Заяви суб'єктів видавничої справи, зокрема, про зміну статусу, видачу дубліката тощо	конфіденційна	у вигляді файлів та об'єктів бази даних

№ з/п	Вид інформації	Ступінь обмеження доступу інформації	Вид представлення даних
4.6	Довідники, необхідні для функціонування Реєстру	відкрита (державні інформаційні ресурси)	у вигляді об’єктів бази даних
4.7	Електронні документи, зокрема заяви суб’єктів господарювання та суб’єктів видавничої справи	конфіденційна	у вигляді файлів
4.8	Звернення громадян (в тому числі запити на публічну інформацію)	конфіденційна (персональні дані)	у вигляді файлів та об’єктів бази даних
4.9	Дані облікових записів зовнішніх користувачів ІКС	конфіденційна (персональні дані)	у вигляді об’єктів бази даних
5	Резервна копія інформації, що обробляється та зберігається в ІКС	конфіденційна	у вигляді файлів
6	Особисті ключі, необхідні для формування кваліфікованого електронного підпису	конфіденційна	на носіях ключової інформації
7	Кваліфіковані сертифікати відкритих ключів, необхідні для перевірки кваліфікованого електронного підпису	відкрита	у вигляді файлів

1.5.2. Порядок обробки та зберігання інформації в ІКС

Функціонування Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції регламентується постановою Кабінету Міністрів України від 10.03.2017 № 135 «Про затвердження Порядку ведення Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції».

Реєстр ведеться з метою:

- обліку інформації про суб’єктів видавничої справи;
- надання адміністративних послуг із внесення суб’єкта господарювання до Реєстру та видачі свідоцтва про внесення суб’єкта господарювання до Реєстру (далі – свідоцтво), а також видачі дубліката, переоформлення, анулювання свідоцтва;
- забезпечення доступу до відомостей Реєстру;
- проведення аналізу інформації, яка обробляється в Реєстрі;
- електронної інформаційної взаємодії між інформаційно-комунікаційними системами та Реєстром.

Адміністратором Реєстру є Держкомтелерадіо, яке забезпечує:

- проведення технічних та технологічних заходів з надання, блокування та анулювання доступу користувачів до Реєстру, що здійснюються у порядку, затвердженому держателем Реєстру;
- організацію та проведення навчання щодо роботи з Реєстром.

Технічним адміністратором Реєстру є структурний підрозділ Міністерства культури України, який у межах своїх повноважень забезпечує адміністрування Реєстру, відповідно до статей 36-39 Закону України «Про публічні електронні реєстри» та Порядку використання програмного забезпечення «Програмна платформа для розгортання та супроводження державних електронних реєстрів», затвердженого постановою Кабінету Міністрів України від 18.04.2023 № 356 «Деякі питання створення та функціонування державних електронних платформ для ведення публічних електронних реєстрів».

Користувачами Реєстру є:

- неавторизовані користувачі;

- суб'єкти господарювання, які після проходження авторизації відповідно до цього Порядку подають заяву про внесення їх до Реєстру;

- суб'єкти видавничої справи, які пройшли авторизацію відповідно до цього Порядку;

- публічні реєстратори (посадові особи Держкомтелерадіо, які взаємодіють з Реєстром відповідно до своїх посадових обов'язків).

Інформація, що міститься в Реєстрі (крім інформації з обмеженим доступом), є відкритою і загальнодоступною з можливістю безоплатного цілодобового вільного доступу та копіювання, оприлюднюється і підтримується в актуальному стані на офіційному веб-сайті Держкомтелерадіо.

Електронна інформаційна взаємодії між Реєстром та іншими електронними інформаційними ресурсами забезпечується за допомогою засобів системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта», відповідно до Порядку електронної (технічної та інформаційної) взаємодії, затвердженого постановою Кабінету Міністрів України від 08.09.2016 № 606 «Деякі питання електронної взаємодії електронних інформаційних ресурсів», з використанням засобів криптографічного захисту інформації, що входять до складу інформаційно-комунікаційної системи «Ядро Системи електронної взаємодії державних електронних інформаційних ресурсів» («Трембіта»), що має комплексну систему захисту інформації з підтвердженою відповідністю (атестат відповідності № 20953 від 20.12.2019).

У разі відсутності технічної можливості передачі даних із використанням системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» електронна інформаційна взаємодія між суб'єктами електронної взаємодії може здійснюватися з використанням інших інформаційно-комунікаційних систем за умови застосування комплексних систем захисту інформації, відповідність яких підтверджується результатами державної експертизи у сфері технічного та криптографічного захисту інформації.

Під час формування реєстрової інформації Реєстру та підтримки реєстрової інформації в актуальному стані забезпечується електронна інформаційна взаємодія з

Єдиним державним реєстром юридичних осіб, фізичних осіб - підприємців та громадських формувань, Єдиним державним демографічним реєстром.

Обсяг та структура даних, якими обмінюються суб'єкти електронної взаємодії через програмні інтерфейси електронних інформаційних ресурсів (сервіси), визначаються договорами про інформаційну взаємодію, укладеними відповідно до законодавства.

Відомості про реєстрацію суб'єкта господарювання, наявність відповідних видів економічної діяльності, отримання установчого документа юридичної особи в електронній формі отримуються шляхом електронної інформаційної взаємодії між Реєстром та Єдиним державним реєстром юридичних осіб, фізичних осіб - підприємців та громадських формувань.

Відомості про унікальний номер запису в Єдиному державному демографічному реєстрі отримуються шляхом електронної інформаційної взаємодії між Реєстром та Єдиним державним демографічним реєстром.

Подання заяви про внесення суб'єкта господарювання до Реєстру здійснюється з використанням програмного забезпечення Реєстру, для чого суб'єкт господарювання авторизується в Реєстрі за допомогою кваліфікованого електронного підпису або вдосконаленого електронного підпису, що базується на кваліфікованому сертифікаті електронного підпису керівника суб'єкта господарювання (уповноваженої ним особи), що є юридичною особою, або суб'єкта господарювання, який є фізичною особою - підприємцем, з дотриманням вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

На підставі інформації, отриманої з використанням програмного забезпечення Реєстру, за кодом згідно з ЄДРПОУ перевіряється наявність у Реєстрі поданої суб'єктом господарювання заяви про внесення суб'єкта господарювання до Реєстру.

У разі наявності заяви про внесення суб'єкта господарювання до Реєстру суб'єкт господарювання інформується про це відповідним повідомленням.

У разі відсутності заяви в Реєстрі за кодом згідно з ЄДРПОУ суб'єкта господарювання засобами програмного забезпечення Реєстру перевіряється наявність у Реєстрі свідоцтва, що є об'єктом Реєстру.

Суб'єкт видавничої справи отримує доступ до Реєстру після проходження авторизації за допомогою кваліфікованого електронного підпису або вдосконаленого електронного підпису, що базується на кваліфікованому сертифікаті електронного підпису, відповідно до вимог Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

У разі наявності свідоцтва в Реєстрі суб'єкту видавничої справи надається можливість:

- подати заяву про переоформлення свідоцтва;
- подати заяву про видачу дубліката свідоцтва;
- подати заяву про анулювання свідоцтва;
- внести зміни в контактні дані.

У разі відсутності свідоцтва в Реєстрі або наявності у свідоцтва статусу «анульовано» програмним забезпеченням Реєстру формується запит до Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань за кодом згідно з ЄДРПОУ та автоматично проводиться перевірка інформації про:

1) відсутність відомостей про перебування у процесі припинення; про застосування до суб'єкта господарювання судових процедур банкрутства (неплатоспроможності), про процедури санації до відкриття провадження у справі про банкрутство, передбачені Кодексом України з процедур банкрутства; про дату відкриття виконавчого провадження (для незавершених виконавчих проваджень);

2) наявність видів економічної діяльності для провадження діяльності суб'єкта видавничої справи (для видавничої діяльності - КВЕД 58.11 «Видання книг», та/або 58.12 «Видання довідників і каталогів», та/або 58.13 «Видання газет», та/або 58.14 «Видання журналів і періодичних видань», та/або 58.19 «Інші види видавничої діяльності»; для виготовлення видавничої продукції - КВЕД 18.11 «Друкування газет», та/або 18.12 «Друкування іншої продукції», та/або 18.13 «Виготовлення друкарських форм і надання інших поліграфічних послуг», та/або 18.14 «Брошурувально-палітурна діяльність і надання пов'язаних із нею послуг»; для розповсюдження видавничої продукції - КВЕД 46.49 «Оптова торгівля іншими товарами господарського призначення», та/або 47.19 «Інші види роздрібної торгівлі в неспеціалізованих магазинах», та/або 47.61 «Роздрібна торгівля книгами в спеціалізованих магазинах», та/або 47.62 «Роздрібна торгівля газетами та канцелярськими товарами в спеціалізованих магазинах»).

У разі непідтвердження в порядку електронної інформаційної взаємодії з Єдиним державним реєстром юридичних осіб, фізичних осіб - підприємців та громадських формувань відомостей про суб'єкта господарювання, зазначених у вище, суб'єкт господарювання отримує про це відповідне повідомлення.

Після підтвердження в порядку електронної інформаційної взаємодії з Єдиним державним реєстром юридичних осіб, фізичних осіб - підприємців та громадських формувань відомостей про суб'єкта господарювання, зазначених у пункті 18 цього Порядку, суб'єкт господарювання додає до заяви про внесення суб'єкта господарювання до Реєстру копії установчих документів (у разі, коли установчі документи відсутні в Єдиному державному реєстрі юридичних осіб, фізичних осіб - підприємців та громадських формувань). Сформованій заяві присвоюється номер, про що суб'єкт господарювання отримує відповідне повідомлення.

На заяву про внесення суб'єкта господарювання до Реєстру з присвоєним номером, що є інформаційним джерелом для внесення інформації до Реєстру, накладається кваліфікований електронний підпис публічного реєстратора і програмним забезпеченням Реєстру автоматично генерується номер свідоцтва. При цьому заява про внесення суб'єкта господарювання до Реєстру отримує статус

«схвалено», свідоцтво отримує статус «актуальне», про що суб'єкт господарювання отримує відповідне повідомлення.

Інформація про об'єкт Реєстру вноситься до Реєстру протягом п'яти робочих днів з дати отримання інформації від суб'єкта господарювання.

Під час подання суб'єктом видавничої справи заяви про переоформлення свідоцтва та опрацювання її публічним реєстратором програмним забезпеченням Реєстру статус свідоцтва «актуальне» змінюється на статус «переоформлено» і запис про переоформлення свідоцтва архівується в Реєстрі.

Під час подання суб'єктом видавничої справи заяви про припинення діяльності у сфері видавничої справи та опрацювання її публічним реєстратором програмним забезпеченням Реєстру змінюється статус свідоцтва на «анульовано» і запис про анулювання свідоцтва архівується в Реєстрі.

Суб'єкти видавничої справи несуть відповідальність за подання недостовірної інформації до Реєстру.

Сформоване свідоцтво зберігається в Реєстрі та містить такі відомості:

- код згідно з ЄДРПОУ суб'єкта видавничої справи;
- найменування юридичної особи, у тому числі скорочене (за наявності), або прізвище, власне ім'я, по батькові (за наявності) для фізичної особи - підприємця;
- номер свідоцтва;
- дата видачі свідоцтва;
- місцезнаходження юридичної особи або адреса місця проживання (перебування), за якою здійснюється зв'язок з фізичною особою - підприємцем);
- перелік засновників та учасників (для юридичної особи);
- види діяльності у сфері видавничої справи.

До Реєстру вноситься така реєстрова інформація:

1) відомості про суб'єкта видавничої справи;
2) відомості про видачу свідоцтва;
3) відомості про видачу дубліката свідоцтва;
4) відомості про анулювання свідоцтва.

У Реєстрі містяться такі реєстрові дані про суб'єкта видавничої справи:

1) реєстровий номер суб'єкта видавничої справи у Реєстрі;
2) серія, номер та дата видачі свідоцтва;
3) номер і дата рішення Держкомтелерадіо про видачу дубліката свідоцтва;
4) номер і дата рішення Держкомтелерадіо про переоформлення свідоцтва;
5) відомості про припинення діяльності суб'єкта видавничої справи (залежно від підстав припинення): номер і дата рішення Держкомтелерадіо про анулювання свідоцтва або номер і дата рішення суду;
6) статус суб'єкта видавничої справи (юридична особа / фізична особа - підприємець);
7) для фізичної особи - підприємця:
- прізвище, власне ім'я, по батькові (за наявності);

- вид (види) діяльності у видавничій справі;

- реєстраційний номер облікової картки платника податків або серія та номер паспорта громадянина України (для фізичних осіб, які мають відмітку в паспорті про право здійснювати платежі за серією та номером паспорта);

- місцезнаходження (адреса місця проживання (перебування), за якою здійснюється зв'язок з фізичною особою - підприємцем);

- інформація для зв'язку: номер телефону та/або адреса електронної пошти;

- унікальний номер запису в Єдиному державному демографічному реєстрі;

8) для юридичної особи:

- найменування, у тому числі скорочене (за наявності);

- код згідно з ЄДРПОУ;

- організаційно-правова форма;

- перелік засновників та учасників;

- вид (види) діяльності у видавничій справі;

- місцезнаходження;

- інформація для зв'язку: номер телефону та/або адреса електронної пошти.

Також є можливість подання звернень громадян (в тому числі, запитів на публічну інформацію).

Найвищий ступінь обмеження доступу до інформації, що циркулює в ІКС, – конфіденційна (персональні дані).

Для шифрування даних використовуються засоби криптографічного захисту інформації, наведені в табл. 1.2.

Таблиця 1.2

№ з/п	Ділянка захисту інформації	Засіб криптографічного захисту інформації	Відомості про експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації
1	центральний вузол ІКС ↔ робочі місця адміністраторів	програмний комплекс криптографічного захисту мережевих з'єднань «Шифр-VPN»	№ 04/05/02-1192/ВС1 від 29.12.2023 щодо можливості використання для криптографічного захисту інформації з обмеженим доступом (крім службової інформації та інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом
2	центральний вузол ІКС ↔ АРМ зовнішніх користувачів	програмний комплекс криптографічного захисту мережевих TLS-з'єднань «Шифр-Web»	№ 04/05/02-872/ВС1 від 26.04.2023 щодо можливості використання для криптографічного захисту інформації з обмеженим доступом (крім службової інформації та інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом
3	центральний вузол ІКС ↔ сторонні інформаційно-комунікаційні	засоби криптографічного захисту інформації, що входять до складу інформаційно-комунікаційної системи «Ядро Системи електронної взаємодії державних електронних інформаційних ресурсів» («Трембіта»), що має комплексну систему захисту інформації з підтвердженою відповідністю	

№ з/п	Ділянка захисту інформації	Засіб криптографічного захисту інформації	Відомості про експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації
	системи	(атестат відповідності № 20953 від 20.12.2019)	

Для формування та перевірки кваліфікованого електронного підпису на даних в складі ІКС використовуються засоби криптографічного захисту інформації (засоби кваліфікованого електронного підпису чи печатки), наведені в табл. 1.3.

Таблиця 1.3

№ з/п	Призначення	Засіб криптографічного захисту інформації	Відомості про експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації
1	обчислення геш-функції від даних, для яких формується кваліфікований електронний підпис, та для перевірки кваліфікованого електронного підпису	здійснюється з використанням інформаційних сервісів інтегрованої системи електронної ідентифікації id.gov.ua, що має комплексну систему захисту інформації з підтвердженою відповідністю (атестат відповідності № 18213 від 18.12.2018) та засобів кваліфікованого електронного підпису чи печатки, які відповідають вимогам Закону України «Про електронну ідентифікацію та електронні довірчі послуги»	
2	безпосереднє формування кваліфікованого електронного підпису	засоби кваліфікованого електронного підпису чи печатки, які відповідають вимогам Закону України «Про електронну ідентифікацію та електронні довірчі послуги» та мають чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості використання в якості засобів кваліфікованого електронного підпису чи печатки для надання електронних довірчих послуг	

Адміністрування, в частині, оновлення системного, антивірусного та прикладного програмного забезпечення виконується системним адміністратором.

Адміністрування прикладного програмного забезпечення та баз даних виконується адміністратором прикладного програмного забезпечення.

1.6. Опис середовища користувачів ІКС

1.6.1. Характеристика ролей адміністраторів

За рівнем повноважень щодо виконання завдань із забезпечення функціонування ІКС та забезпечення безпеки інформації, що в ній обробляється та зберігається, обслуговуючий персонал (адміністратори) поділяється на такі категорії:

- *адміністратор прикладного програмного забезпечення* – доступ до налаштувань прикладного програмного забезпечення та механізмів управління обліковими записами та правами доступу користувачів ІКС на рівні прикладного

програмного забезпечення;

- *адміністратор безпеки* – доступ до механізмів управління обліковими записами користувачів на рівні системного програмного забезпечення ІКС;

- *системний адміністратор* – доступ до налаштувань системного, антивірусного та прикладного програмного забезпечення робочих місць адміністраторів.

1.6.2. Характеристика ролей користувачів

За рівнем повноважень щодо доступу до інформації та характером робіт, що виконуються у процесі функціонування ІКС, користувачі, які мають доступ до її ресурсів, поділяються на такі категорії:

- *суб'єкти господарювання* – юридичні особи, які після проходження авторизації відповідно до цього Порядку подають заяву про внесення їх до Реєстру;

- *суб'єкти видавничої справи* – користувачі, які пройшли авторизацію відповідно до цього Порядку та отримують можливість:

  - подати заяву про переоформлення свідоцтва;
  - подати заяву про видачу дубліката свідоцтва;
  - подати заяву про анулювання свідоцтва;
  - внести зміни в контактні дані.

- *публічні реєстратори* – посадові особи Держкомтелерадіо, які взаємодіють з Реєстром відповідно до своїх посадових обов'язків*;*

- *неавторизовані користувачі* – користувачі комунікаційних мереж загального користування, які отримують доступ до загальнодоступних ресурсів ІКС з використанням мережі загального користування Інтернет.

1.7. Опис фізичного середовища ІКС

1.7.1. Фізичне розташування компонентів ІКС

Центральний вузол ІКС розташований в межах серверного майданчика Державного підприємства «Українські спеціальні системи» за адресою: м. Київ, вул. Юрія Іллєнка, буд. 83Б.

Робочі місця адміністраторів розташовані в межах будівлі Міністерства культури України за адресою: м. Київ, вул. Івана Франка, буд. 19 (Шевченківський р-н).

Робочі місця зовнішніх користувачів ІКС знаходяться за місцем їх фактичного місцезнаходження.

1.7.2. Загальна характеристика режиму доступу до компонентів ІКС

Контрольована територія обмежена пропускним пунктом на вході у відповідну будівлю та зовнішніми стінами.

Вхід у будівлі, де розміщені компоненти ІКС, здійснюється через пропускні пункти, обладнані перепускними системами, за персональними перепустками співробітників або тимчасовими перепустками відвідувачів. Порядок відвідування приміщень забезпечує неможливість безконтрольного перебування в приміщеннях, де розміщені компоненти ІКС, сторонніх осіб.

У приміщеннях, в яких розташовані компоненти ІКС, діє пропускний та внутрішньооб'єктовий режими. Доступ до компонентів ІКС має лише обслуговуючий персонал. Доступ інших осіб до компонентів ІКС можливий лише в супроводі осіб, яким надано такий доступ. Забезпечується контроль виконання пропускного та внутрішньооб'єктового режимів та протипожежної безпеки в межах контрольованої території, а також цілодобовий контроль доступу в приміщення, в яких розташовані компоненти центральних вузлів ІКС.

Організація фізичної охорони серверних приміщень, в яких розташовані компоненти центрального вузлу ІКС, пожежної та охоронної сигналізації, систем відеоспостереження, забезпечення електроживлення та інших систем життєзабезпечення, а також пропускного режиму здійснюється в порядку, визначеному нормативно-розпорядчою документацією на комплексну систему захисту інформації інформаційно-комунікаційної системи серверного майданчика ДП «Українські спеціальні системи», яка має чинний атестат відповідності вимогам нормативних документів системи технічного захисту інформації № 121В від 16.12.2022.

Доступ персоналу до приміщень, в яких розміщуються технічні засоби центрального вузлу ІКС, здійснюється в порядку, визначеному нормативно-розпорядчою документацією на комплексну систему захисту інформації інформаційно-комунікаційної системи серверного майданчика ДП «Українські спеціальні системи», яка має чинний атестат відповідності вимогам нормативних документів системи технічного захисту інформації № 121В від 16.12.2022, та полягає в наданні права доступу до цих приміщень лише обслуговуючого персоналу ІКС, функціональними обов'язками якого передбачено необхідність роботи із технічними засобами, розміщеними в цих приміщеннях. Відвідування цих приміщень сторонніми особами не допускається.

Організація фізичної охорони приміщень, в яких розташовані компоненти технічного майданчика віддаленого адміністрування, пожежної та охоронної сигналізації, систем відеоспостереження, забезпечення електроживлення та інших систем життєзабезпечення, а також пропускного режиму здійснюється в порядку, визначеному внутрішньою нормативно-розпорядчою документацією Міністерства культури України.

1.8. Нормативно-правове забезпечення

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

1. Постанова Кабінету Міністрів України від 18.06.2025 № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем».

2. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України (далі – Адміністрація Держспецзв'язку) від 30.06.2025 № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація».

3. Закон України «Про інформацію».

4. Закон України «Про захист інформації в інформаційно-комунікаційних системах».

5. Закон України «Про електронну ідентифікацію та електронні довірчі послуги».

6. Закон України «Про основні засади забезпечення кібербезпеки України».

7. Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах».

8. Постанова Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».

9. 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.

10. 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.

1.9. Відомості про обраний базовий профіль безпеки

Виходячи з найвищого грифу (ступеня обмеження) доступу до інформації, яка обробляється та зберігається в ІКС (див. п. 1.5.1 цього документу), в якості базового профіля безпеки обрано Базовий профіль безпеки системи, де обробляється відкрита або конфіденційна інформація, затверджений наказом Адміністрації Держспецзв'язку від 30.06.2025 № 409.

2. ЦІЛЬОВИЙ ПРОФІЛЬ БЕЗПЕКИ ІНФОРМАЦІЇ

В подальшому викладі використовуються такі позначення:

звичайним шрифтом – наводяться положення базового профіля безпеки (БПБ);

[курсивом в квадратних дужках] – наводяться уточнені (налаштовані) варіативні параметри БПБ в цільовому профілі безпеки (ЦПБ);

жирним шрифтом – наводяться посилення БПБ (додаткові заходи захисту), обгрунтовані результатами оцінки ризиків інформаційної безпеки в ІКС та вимогами діючого законодавства;

[жирним курсивом в квадратних дужках] – наводяться уточнені (налаштовані) варіативні параметри додаткових заходів захисту в ЦПБ.

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	**Налаштований зміст заходу захисту**
1	**Управління доступом (АС)**			
1.1.1	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: *[призначення: визначений організацією період часу]* облікові записи більше не потрібні; *[призначення: визначений організацією період часу]* користувачі звільняються або переводяться; *[призначення: визначений організацією період часу]* у системі наявні зміни, які потребують нових знань.	АС-2	визначити та задокументувати типи (ролі) облікових записів користувачів ІКС, дозволених для використання в ІКС для забезпечення її функціонування: ролі адміністраторів та ролі користувачів (див. п. 1.6.2 цього документу)
1.1.2				створювати, активувати, змінювати, деактивувати та видаляти облікові записи користувачів в ІКС відповідно до політики та процедур, встановлених А_ІКС
1.1.3				визначити (створити умови для групового та рольового членства) та призначити адміністраторів (обслуговуючий персонал) ІКС та їх повноваження щодо адміністрування (обслуговування) компонентів ІКС (див. п. 1.6.1 цього документу): *[- адміністратор прикладного програмного забезпечення* – доступ до налаштувань прикладного програмного забезпечення та механізмів управління обліковими записами та правами доступу користувачів ІКС на рівні прикладного програмного забезпечення; - *адміністратор безпеки* – доступ до механізмів управління обліковими записами користувачів на рівні системного програмного забезпечення ІКС; - *системний адміністратор* – доступ до налаштувань системного, антивірусного та прикладного програмного забезпечення робочих місць адміністраторів.*]*

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
1.1.4				вимагати схвалення запитів на створення облікових записів в ІКС в порядку, визначеному політикою управління доступом А_ІКС
1.1.5				авторизувати доступ адміністраторів та користувачів до ІКС на основі наданого встановленим порядком дозволу та передбачуваного використання ІКС
1.1.6				контролювати використання облікових записів користувачів в ІКС, проводити *[щоквартально]* перегляд облікових записів користувачів
1.1.7				оповістити *[адміністраторів прикладного програмного забезпечення, адміністраторів безпеки]* протягом *[24 годин]*, коли: - облікові записи більше не потрібні; - користувачі звільняються або переводяться; - в ІКС наявні зміни, які потребують зміни встановлених правил розмежування доступу.
1.1.8				впровадити процес повторного випуску облікових даних облікового запису (якщо він буде розгорнутий), коли обслуговуючий персонал виходять з групи / звільняється з ролі
1.1.9				узгодити процеси управління обліковими записами з процесами звільнення та переводу (передачі повноважень) обслуговуючого персоналу
1.1.10	**Управління обліковими записами - деактивація облікових записів**	**б) деактивувати облікові записи в системі, коли:** **термін дії облікових записів закінчився;** **облікові записи були неактивні протягом [*призначення: період часу, визначений організацією*];** **облікові записи більше не пов'язані з користувачем або фізичною особою;** **облікові записи порушують політику організації.**	**АС-2(3)**	**деактивувати облікові записи користувачів в ІКС, коли:** **- термін дії облікових записів закінчився;** **- облікові записи були неактивні протягом *[90 днів]*;** **- облікові записи більше не пов'язані з користувачем;** **- облікові записи порушують політику управління доступом А_ІКС.**
1.1.11	Управління обліковими записами - вихід із системи за відсутності активності	вимагати, щоб користувачі виходили із системи, коли *[призначення: визначений організацією період часу]* очікуваної бездіяльності або за *[призначення: визначені організацією обставини]*	АС-2(5)	вимагати від користувачів виходити з ІКС у таких випадках: - примусове завершення сесій роботи користувачів на рівні *[прикладного програмного забезпечення]* після *[30 хвилин]* бездіяльності, - необхідність залишити власне робоче місце без нагляду.
1.1.12	**Управління обліковими записами**	**а) створювати й адмініструвати привілейовані облікові записи користувачів**	**АС-2(7)**	**створювати та адмініструвати облікові записи адміністраторів на основі ролей обслуговуючого**

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
	– схеми, засновані на ролях	**відповідно до схеми доступу на основі ролей (role-based), яка реалізує дозволений доступ до системи та призначення привілеїв для ролей; b) проводити моніторинг призначення привілейованих ролей; c) відстежувати зміни ролей або атрибутів; d) скасовувати доступ, коли призначені привілейовані ролі більше не потрібні.**		**персоналу (див. п. 1.6.1 цього документу)**
1.1.13				**проводити моніторинг призначення обслуговуючого персоналу на ролі адміністраторів**
1.1.14				**відстежувати зміни ролей або атрибутів адміністраторів**
1.1.15				**скасовувати доступ, коли призначені ролі адміністраторів більше не потрібні**
1.2.1	Забезпечення доступу	застосовувати затверджені повноваження для логічного доступу до конфіденційної інформації та ресурсів у системі	AC-3	застосовувати затверджені повноваження користувачів для логічного доступу до інформації (див. п. 1.6.2 цього документу) в ІКС відповідно до встановленої А_ІКС політики (процедури) управління доступом
1.2.2	Забезпечення доступу - управління доступом на основі ролей	**застосовувати політику управління доступом на основі ролей щодо визначених суб'єктів і об'єктів та управління доступом на основі *[призначення: визначених організацією ролей та користувачів, уповноважених приймати такі ролі]***	**AC-3(7)**	**застосовувати політику (процедуру) управління доступом на основі ролей користувачів інформаційних послуг щодо визначених інформаційних об'єктів та управління доступом на основі відповідних матриць /рольових моделей та правил (процедур) надання доступу**
1.3	Управління інформаційними потоками	застосовувати затверджені дії для управління потоками відкритої та конфіденційної інформації всередині системи та між підключеними системами	AC-4	управління потоками відкритої та конфіденційної інформації між компонентами ІКС, між ІКС та зовнішніми інформаційними системами здійснювати відповідно до встановлених А_ІКС політик (процедур) з урахуванням вимог нормативно-правових актів та нормативних документів з питань захисту конфіденційної інформації
1.4.1	Розмежування обов'язків	визначити обов'язки осіб, які потребують розмежування; установити правила авторизації доступу для підтримки розмежування обов'язків	AC-5	розмежувати і документувати ролі адміністраторів та користувачів відповідно до п. 1.6 цього документу
1.4.2				авторизацію доступу адміністраторів та користувачів інформаційних послуг до ІКС здійснювати на основі дозволу, наданого за встановленою А_ІКС процедурою
1.5.1	Мінімізація повноважень	надавати користувачам (або процесам, що діють від імені користувачів) лише авторизований доступ до системи, необхідний для виконання поставлених завдань організації	AC-6	впровадити принцип мінімізації повноважень, який дозволяє користувачам (або процесам, що діють від імені користувачів) здійснювати лише такі операції з доступу до інформації в ІКС, які визначені їх функціональними обов'язками (див. п. 1.6.2 цього документу)
1.5.2	Мінімізація повноважень - мережевий доступ	авторизувати доступ до *[призначення: функції безпеки, визначені організацією, та важлива для безпеки інформація]*	AC-6(1), AU-9(4)	авторизувати доступ адміністраторів до *[функцій безпеки компонентів ІКС та інформації, необхідної для забезпечення її інформаційної безпеки]* у відповідності до встановлених прав доступу їх ролей (див. п. 1.5.2, 1.6.1 цього документу та AC-2)
1.5.3	Мінімізація	вимагати, щоб користувачі (або ролі) з	AC-6(2)	вимагати від адміністраторів, які мають доступ до

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
	повноважень – непривілейований доступ до незахищених функцій	привілейованими обліковими записами використовували непривілейовані облікові записи для доступу до незахищених функцій або інформації		адміністративних функцій**,** в тому числі здійснюють перегляд журналів реєстрації подій та управляють конфігураційними та технологічними налаштуваннями компонентів ІКС використовувати неадміністративні облікові записи (ролі) під час доступу до звичайних (не адміністративних) функцій ІКС
1.5.4	Мінімізація повноважень - привілейовані облікові записи	обмежити привілейовані облікові записи в системі для [*призначення: персонал або ролі, що визначається організацією*]	AC-6(5)	обмежити можливість використання адміністративних функцій в ІКС лише для адміністраторів
1.5.5	**Мінімізація повноважень – привілейований доступ користувачами, що не належать до організації**	**заборонити привілейований доступ до системи користувачам, які не належать до організації**	**AC-6(6)**	**заборонити адміністративний доступ до ІКС користувачам зовнішніх організацій, які не є користувачами А_ІКС**
1.5.6	**Мінімізація повноважень - перегляд повноважень користувача**	**періодично перевіряти привілеї, призначені ролям або класам користувачів, щоб підтвердити необхідність таких привілеїв;**	**AC-6(7)**	**періодично перевіряти права доступу, призначені відповідним ролям адміністраторів, щоб підтвердити необхідність наявності таких прав доступу**
1.5.7		**за необхідності перепризначити або видалити привілеї**		**за необхідності перепризначити або видалити права доступу відповідних ролей адміністраторів**
1.5.8	**Мінімізація повноважень - аудит використання привілейованих функцій**	**реєструвати виконання привілейованих функцій.**	**AC-6(9)**	**реєструвати виконання адміністративних функцій в журналах реєстрації подій відповідних компонентів ІКС**
1.5.9	Мінімізація повноважень - заборона непривілейованим користувачам виконувати привілейовані функції	заборонити непривілейованим користувачам виконувати привілейовані функції	AC-6(10)	вжити заходів для запобігання виконувати адміністративні функції в ІКС користувачами (не адміністраторами)
1.6.1	Невдалі спроби входу в систему	встановити обмеження на кількість [*призначення: кількість, яка визначена організацією*] невдалих спроб входу в систему протягом певного часу [*призначення: проміжок часу, визначений організацією*]; автоматично *[(вибір (один або декілька):*	AC-7	встановити обмеження на кількість *[10]* невдалих спроб входу до *[прикладного програмного забезпечення]* поспіль

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
1.6.2		*заблокувати обліковий запис або вузол на [призначення: період часу, визначений організацією]; заблокувати обліковий запис або вузол до зняття адміністратором; відкласти наступний запит на вхід; повідомити системного адміністратора; вжити інших заходів]*, коли перевищено максимальну кількість невдалих спроб входу в систему.		після досягнення наведеної кількості невдалих спроб входу заблокувати обліковий запис відповідного користувача на рівні *[прикладного програмного забезпечення] [протягом 10 хвилин]* та повідомити *[адміністратора прикладного програмного забезпечення]*
1.7	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	демонструвати користувачам інформаційних послуг перед тим, як надавати доступ до ІКС на рівні *[операційної системи]* сповіщення про умови використання ІКС, яке визначає, що: - користувачі здійснюють доступ до системи, в якій обробляється інформація з відповідним ступенем обмеження доступу; - несанкціоноване використання системи або її використання з порушенням встановлених правил забороняється та приводить до кримінальної та цивільної відповідальності; - використання системи означає згоду на реєстрацію та контроль дій користувача.
1.8.1	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.	AC-11	заборонити подальший доступ до ІКС шляхом блокування сеансу роботи користувача на рівні *[прикладного програмного забезпечення]* після *[30 хвилин]* бездіяльності;
1.8.2				вимагати від користувача ініціювати блокування сеансу своєї роботи в ІКС (на рівні *[операційної системи, прикладного програмного забезпечення]*) перед тим, як залишити власне робоче місце без нагляду
1.8.3				зберігати блокування сеансу роботи користувача до відновлення ним доступу за допомогою встановлених процедур ідентифікації та автентифікації
1.8.4	Блокування пристрою - приховані дисплеї	приховати за допомогою блокування пристрою інформацію, яку раніше було видно на дисплеї, за допомогою публічно доступного зображення	AC-11(1)	приховувати через блокування робочого місця інформацію, яку раніше було видно на пристрої відображення (дисплеї, екрані), шляхом відображення публічного (загальнодоступного) зображення
1.9	Припинення сеансу	автоматично завершувати сеанс користувача після [*призначення: умови або події, що вимагають відключення сеансу, визначені організацією*]	AC-12	сесія роботи користувачів на рівні *[прикладного програмного забезпечення]* має завершуватися автоматично після *[30 хвилин]* бездіяльності
1.10.1	Віддалений доступ	встановити обмеження на використання, дії до	AC-17	встановити та задокументувати обмеження на

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		конфігурації та підключення для кожного типу допустимого віддаленого доступу до системи		використання, вимоги до конфігурації / підключення та рекомендації щодо здійснення кожного типу віддаленого доступу до ІКС
1.10.2		авторизувати кожен тип віддаленого доступу до системи перед встановленням таких з'єднань.		авторизувати віддалений доступ до ІКС, перш ніж будуть дозволені такі підключення
1.10.3	**Віддалений доступ - захист конфіденційності та цілісності за допомогою шифрування**	**запровадити криптографічні механізми для захисту конфіденційності та цілісності сесій віддаленого доступу**	**AC-17(2)**	**для захисту конфіденційності та цілісності інформації, обмін якою здійснюється через незахищене середовище запровадити засоби криптографічного захисту інформації, які відповідають вимогам законодавства України з питань криптографічного захисту інформації**
1.10.4	Віддалений доступ - керовані точки контролю доступу	виконувати маршрутизацію всього віддаленого доступу до системи через авторизовані та керовані точки контролю управління доступом до мережі;	AC-17(3)	виконувати маршрутизацію всього віддаленого доступу через *[пристрої мережевого захисту центрального вузлу ІКС]*
1.10.5	Віддалений доступ - привілейовані команди та доступ	авторизувати віддалене виконання привілейованих команд і віддалений доступ до інформації, важливої для безпеки	AC-17(4)	авторизувати виконання адміністративних функцій за допомогою віддаленого доступу тільки для адміністраторів
1.11.1	Бездротовий доступ	встановити обмеження на використання, дії до конфігурації та підключення для кожного типу бездротового доступу до системи;	AC-18	встановити обмеження на використання, вимоги до конфігурації та підключення для кожного типу бездротового доступу до ІКС
1.11.2		авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення		авторизувати бездротовий доступ до ІКС, перш ніж будуть дозволені такі підключення
1.11.3	**Бездротовий доступ - відключення бездротової мережі**	**вимкнути перед розгортанням та запуском бездротові мережеві можливості, якщо вони не призначені для використання**	**AC-18(3)**	**вимкнути на робочих місцях користувачів перед розгортанням та запуском бездротові мережеві можливості, якщо вони не призначені для використання для доступу до ІКС**
1.12.1	Контроль доступу для мобільних пристроїв	встановити обмеження на використання, вимоги до конфігурації та підключення для мобільних пристроїв;	AC-19	*[використання мобільних пристроїв для роботи в ІКС не передбачається]*
1.12.2		авторизувати підключення мобільних пристроїв до системи.		
1.12.3	Контроль доступу для мобільних пристроїв - повне шифрування пристроїв та сховищ інформації	застосувати повне шифрування носія інформації пристрою або шифрування на основі шифрування сховищ інформації (контейнерів)	AC-19(5)	
1.13.1	Використання зовнішніх систем	1) заборонити використання зовнішніх систем, крім систем дозволених організацією; 2) установити такі положення, умови та дії щодо безпеки, які повинні бути виконані у зовнішніх	AC-20	визначити умови та порядок підключення та обміну даними із зовнішніми інформаційними системами, зокрема: - правові підстави; - технічні специфікації обміну даними;

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		системах, перш ніж дозволити використання або доступ до цих систем авторизованим особам *[призначення: положення та дії визначаються організацією]*.		- вимоги до засобів криптографічного захисту даних, обмін якими здійснюється; - зони відповідальності А_ІКС та власників (розпорядників) зовнішніх інформаційних систем; - відповідність зовнішніх інформаційних систем встановленим вимогам до забезпечення захисту інформації
1.13.2	Використання зовнішніх систем - обмеження на авторизоване використання	дозволити авторизованим особам використовувати зовнішню систему для доступу до системи організації або для обробки, зберігання чи передачі відкритої та конфіденційної інформації, лише після: перевірки реалізації вимог безпеки на зовнішній системі, як зазначено в планах безпеки організації; збереження затверджених угод про підключення або обробку даних з організацією, що розміщує зовнішню систему, з якою укладено відповідну угоду.	AC-20(1)	дозволити обмін відкритої та конфіденційної інформацією між ІКС та зовнішніми інформаційними системами лише після: - перевірки реалізації зовнішньою інформаційною системою встановлених вимог безпеки; - укладання договорів (угод, протоколів взаємодії тощо) про підключення та обмін даними із власником (розпорядником) зовнішньої інформаційної системи; - тестування коректності інформаційної взаємодії між ІКС та зовнішньою інформаційною системою.
1.13.3	Використання зовнішніх систем - переносні пристрої зберігання даних	обмежити використання портативних пристроїв зберігання даних авторизованими особами на зовнішніх системах	AC-20(2)	обмежити використання користувачами зовнішніх інформаційних систем для зберігання / експорту відкритої та конфіденційної інформації, отриманої від ІКС, носіїв даних, які не зареєстровані у встановленому порядку як електронні носії інформації з відповідним грифом обмеження доступу
1.14.1	Публічно доступний контент	навчати авторизованих осіб щодо нерозголошення конфіденційної в загальнодоступних системах; періодично переглядати вміст загальнодоступних систем на предмет наявності конфіденційної інформації та видаляти таку інформацію, якщо її виявлено.	AC-22	призначити осіб, уповноважених на розміщення інформації, що обробляється та зберігається в ІКС, в загальнодоступних системах
1.14.2				навчати уповноважених осіб тому, щоб інформація, розміщена в загальнодоступних системах, не містила конфіденційної інформації
1.14.3				перевіряти запропонований зміст інформації до публікації в загальнодоступних системах на відсутність в ній конфіденційної інформації
1.14.4				*[щоквартально або в міру надходження нової інформації]* переглядати вміст загальнодоступної системи на предмет наявності там конфіденційної інформації; в разі виявлення така інформація має бути негайно видалена з загальнодоступної системи
2	**Обізнаність і навчання (АТ)**			
2.1	Навчання з питань безпеки	1) забезпечити навчання користувачів системи з	AT-2	забезпечити навчання користувачів з питань безпеки:

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
	обізнаності	питань безпеки: як частину початкового навчання для нових користувачів і періодично після цього; якщо цього потребують зміни в системі або наступні [*призначення: події, визначені організацією*]; щодо розпізнавання та повідомлення про індикатори внутрішньої загрози, соціальної інженерії, та соціального шпіонажу; 2) оновлювати зміст тренінгу з безпекової обізнаності *[призначення: визначена організацією періодичність]* та після [*призначення*: *визначені організацією події*].		- як частину початкового навчання для нових користувачів і *[щорічно]* після цього; - якщо цього потребують зміни в ІКС, оновлення системи безпеки, зміни в політиках або інциденти безпеки; використовувати при цьому наведені нижче методи, щоб підвищити рівень користувачів з безпеки: *[навчальні теоретичні та практичні заняття, тренінги, тестування знань тощо]*.
2.1.2				*[щорічно]* оновлювати зміст програм навчань користувачів з питань безпеки
2.1.3				включити уроки, отримані з внутрішніх або зовнішніх інцидентів безпеки або порушень, у навчання грамотності та методи підвищення обізнаності
2.1.4			AT-2(2)	ввести до програми навчання відомості з розпізнавання та виявлення потенційних індикаторів внутрішніх загроз, соціальної інженерії та соціального шпіонажу
2.2.1	Рольове навчання	1) провести тренінги з безпеки для персоналу організації на основі покладених обов’язків: перед авторизацією доступу до системи або відкритої та конфіденційної інформації, перед виконанням призначених обов'язків, а також *[призначення: частота визначається організацією]* після цього; коли цього вимагають зміни в системі або після [*призначення: події, визначені організацією*]; 2) оновлювати зміст тренінгів *[призначення: частота, визначена організацією]* на основі покладених обов’язків, а також після [*призначення: події, визначені організацією*].	AT-3	проводити навчання адміністраторів з питань безпеки на основі покладених обов’язків: - перед авторизацією доступу до ІКС, відкритої та конфіденційної інформації, перед виконанням призначених обов'язків, а також *[щорічно]* після цього; - коли цього вимагають зміни в ІКС або після критичних інцидентів інформаційної безпеки. *Примітка: тут та надалі під критичними інцидентами інформаційної безпеки розуміються інциденти з рівнем 9.0 – 10.00 згідно Common Vulnerability Scoring System (CVSS)*
2.2.2				оновлювати зміст програм навчання обслуговуючого персоналу з питань безпеки на основі покладених обов’язків *[щорічно]* та *[після критичних інцидентів інформаційної безпеки]*
2.2.3				включити у рольове навчання, інформацію, отриману з внутрішніх або зовнішніх інцидентів та порушень безпеки
3	**Аудит і підзвітність (AU)**			
3.1.1	Події аудиту	визначити перелік подій, які реєструються в системі: [*призначення: типи подій, визначені організацією*]; переглядати та оновлювати *[призначення: частота визначається організацією]* типи подій, обрані для реєстрації.	AU-2	визначити перелік подій, які реєструються в ІКС: - успішні/неуспішні спроби входу; - дії адміністраторів щодо управління обліковими записами та правами доступу користувачів, скидання даних автентифікації; - зміни в конфігурації компонентів ІКС; - зміни в налаштуваннях безпеки компонентів ІКС;

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				- спроби неавторизованого доступу; - доступ користувачів до інформаційних об'єктів.
3.1.2				координувати функції реєстрації подій з іншими підрозділами А_ІКС, які вимагають інформації, пов'язаної з реєстрацією подій, для посилення взаємної підтримки та допомоги у виборі типів подій, що перевіряються
3.1.3				обґрунтувати, чому типи подій, що перевіряються, вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов'язаних з безпекою
3.1.4				*[щорічно]* переглядати та оновлювати типи подій, обрані для реєстрації
3.2.1	Зміст записів аудиту	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.	AU-3	записи в журналах реєстрації подій (див. п. 1.5.1 цього документу) 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.
3.2.2	Зміст записів аудиту - додаткова інформація про аудит	за потреби надавати додаткову інформацію для записів аудиту.	AU-3(1)	формувати записи в журналах реєстрації подій, що містять таку додаткову інформацію: *[потреба у додатковій інформації відсутня]*
3.3.1	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	сповіщати *[адміністратора безпеки] [майже в реальному часі]* у разі збою засобів реєстрації подій та засобів обробки зареєстрованих подій
3.3.2				виконати додаткові дії: - перевірка цілісності даних про зареєстровані події; - відновлення або повторна обробка даних про зареєстровані події; - оновлення системи або оновлення компонентів, що відповідають за обробку даних про зареєстровані події; - вжиття заходів щодо попередження подібних інцидентів у майбутньому.
3.4.1	Огляд, аналіз і звітність аудиту	переглядати та аналізувати *[призначення: частота, визначена організацією]* записи аудиту системи на предмет виявлення ознак і потенційного впливу не властивої або незвичної діяльності; повідомляти про результати аудиту співробітникам організації або ролям.	AU-6	переглядати та аналізувати записи системних журналів реєстрації подій *[щотижня]* для виявлення: - несанкціонованих спроб доступу; - неочікуваних змін в системних налаштуваннях; - аномальних або підозрілих операцій користувачів; - можливих атак або спроб порушення цілісності.
3.4.2				результати аналізу журналів реєстрації подій доводити до

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				відома *[адміністратора безпеки]*
3.4.3				налаштувати рівні перегляду журналів реєстрації подій, коли змінюється рівень ризику на основі інформації від правоохоронних органів, розвідувальної інформації або від інших достовірних джерел інформації
3.4.4	Огляд, аналіз і звітність аудиту - зіставляння сховищ аудиту	аналізувати та зіставляти записи аудиту в різних сховищах задля забезпечення ситуативної обізнаності в масштабах організації	AU-6(3)	аналізувати та зіставляти записи журналів реєстрації подій різних компонент ІКС, з метою забезпечення ситуативної обізнаності в масштабах ІКС в цілому
3.5	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; зберігати оригінальний зміст і часовий порядок записів аудиту.	AU-7	забезпечити та реалізувати можливості скорочення записів про зареєстровані події до рівня, який: - підтримує перевірку, аналіз і звітність на вимогу та розслідування (постфактум) інцидентів безпеки; - не змінює оригінальний вміст або час упорядкування записів в журналах реєстрації подій.
3.6.1	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	використовувати внутрішній годинник компонентів ІКС для створення позначок часу для записів в журналах реєстрації подій
3.6.2				застосовувати позначки часу з деталізацією до *[секунд]*, і використовують: - всесвітній координований час (UTC); - фіксоване зміщення місцевого часу відносно UTC або зміщення місцевого часу як частину позначки часу.
3.7.1	Захист інформації аудиту	захистити інформацію аудиту та інструментів журналювання аудиту від несанкціонованого доступу, зміни та видалення	AU-9	дані про події, зареєстровані на компонентах ІКС, та механізми реєстрації подій компонентів ІКС повинні бути захищені від несанкціонованого доступу, зміни та видалення
3.7.2				*[адміністратори безпеки]* повинні отримувати сповіщення у разі виявлення несанкціонованого доступу, зміни або видалення даних про зареєстровані події
3.7.3	Захист інформації аудиту - доступ, який надається через членство в підмножині привілейованих користувачів	надавати доступ до управління функціями аудиту тільки підмножині привілейованих користувачів або ролей	AU-9(4)	доступ до управління функціями реєстрації подій повинен надаватися лише адміністраторам по відношенню до відповідних компонентів ІКС
3.8	Збереження записів аудиту	зберігати записи аудиту протягом періоду часу, який відповідає політиці зберігання записів аудиту	AU-11	зберігати журнали реєстрації подій впродовж *[1 року]*, щоб забезпечити можливість проведення розслідувань інцидентів безпеки
3.9.1	Генерація даних аудиту	згенерувати записи аудиту для вибраних типів подій згідно з вмістом записів аудиту, вказаних	AU-12	забезпечити формування даних про зареєстровані події для типів подій, що реєструються згідно вимог AU-2, на рівні

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	**Налаштований зміст заходу захисту**
		в п. 3.1 та 3.2		*[гіпервізора, операційних систем, прикладного програмного забезпечення, мережевого обладнання]* із реєстрацією даних щодо кожної зареєстрованої події згідно вимог AU-3
3.9.2				дозволити *[адміністратору безпеки]* вибирати, які типи подій повинні реєструватися на відповідних компонентах ІКС
4	**Управління конфігурацією (CM)**			
4.1.1	Базова конфігурація	розробляти та підтримувати під контролем налаштування поточної базової конфігурації системи; переглядати та оновлювати *[призначення: частота, визначена організацією]* базову конфігурацію системи, а також при встановленні або модифікації компонентів системи.	CM-2	розробити, задокументувати та підтримувати поточні базові налаштування компонентів ІКС (див. п. 1.5.1 цього документу)
4.1.2				переглядати та оновлювати базові налаштування компонентів ІКС (див. п. 1.5.1 цього документу): - *[щорічно]*; - за потреби, внаслідок виявлення нових загроз або зміни в законодавстві або внутрішніх нормативних документах А_ІКС; - коли встановлені нові або оновлені існуючі компоненти ІКС.
4.2.1	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	визначити типи змін в ІКС, які потрібно контролювати
4.2.2				переглядати запропоновані зміни в конфігурації ІКС і схвалити або відхилити ці зміни з урахуванням аналізу наслідків для безпеки
4.2.3				документувати рішення зі зміни конфігурації ІКС
4.2.4				впровадити схвалені зміни конфігурації в ІКС
4.2.5				зберігати записи змін конфігурації ІКС впродовж *[1 року]*
4.2.6				здійснювати моніторинг і аналіз дій, пов’язаних зі змінами конфігурації ІКС
4.2.7				координувати та впроваджувати нагляд за діяльністю з управління змінами конфігурації за допомогою *[наявних засобів управління змінами конфігурації]*, який здійснюється *[щорічно або при змінах в конфігурації компонентів ІКС]*
4.2.8	**Управління змінами конфігурації - управління засобами криптографічного захисту**	**забезпечити, щоб криптографічні механізми, які використовуються для забезпечення відповідних заходів захисту перебували під управлінням конфігурацією *[призначення: визначених організацією заходів безпеки]***	**CM-3(6)**	**управління конфігурацією засобів криптографічного захисту інформації повинно здійснюватися лише *[адміністратором безпеки]***
4.2.9	**Управління змінами конфігурації**	**переглянути зміни в системі *[призначення: частота, визначена організацією]* або коли**	**CM-3(7)**	**переглядати зміни в ІКС: - *[щоквартально]*;**

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
	перегляд змін у системі	***[призначення: обставини, визначені організацією]*, щоб визначити, чи відбулися неавторизовані зміни.**		**- за потреби, внаслідок внесення позапланових змін; - коли встановлені нові або оновлені існуючі компоненти ІКС.**
4.3	Аналіз впливу на безпеку та приватність	проаналізувати вплив змін у системі на безпеку перед їх впровадженням	CM-4	проводити аналіз запропонованих зміни в компонентах ІКС, щоб визначити потенційні загрози безпеці інформації перед внесенням таких змін
4.4	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 із внесенням змін до компонентів ІКС
4.5.1	Налаштування конфігурації	встановити, задокументувати та впровадити параметри конфігурації системи, які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам: [*призначення: налаштування конфігурації, визначені організацією*]; визначити, задокументувати та затвердити будь-які відхилення від встановлених налаштувань конфігурації.	CM-6	встановити, задокументувати та впровадити параметри конфігурації компонентів ІКС (див. п. 1.5.1 цього документу), які відображають найбільш обмежувальний режим, що відповідає експлуатаційним вимогам та відповідним політикам А_ІКС
4.5.2				визначити, задокументувати та затвердити будь-які відхилення від встановлених налаштувань конфігурації *[для всіх конфігурованих компонентів ІКС]* на основі *[політики управління конфігурацією А_ІКС]*
4.5.3				реалізувати конфігураційні налаштування на компонентах ІКС
4.5.4				відстежувати та керувати змінами конфігураційних параметрів відповідно до організаційної політики та процедур А_ІКС
4.6.1	Мінімально необхідна функціональність	налаштувати систему так, щоб вона надавала лише необхідні для виконання завдань функції; заборонити або обмежити використання таких функцій, портів, протоколів, підключень і служб: [*призначення: функції, порти, протоколи, з'єднання та служби, визначені організацією*].	CM-7	налаштувати ІКС так, щоб вона виконувала функції, необхідні лише для виконання покладених функціональних завдань
4.6.2				заборонити або обмежити використання таких функцій, портів, протоколів, підключень і служб: *[небезпечні або невикористовувані служби, застарілі протоколи зв’язку (наприклад, SMBv1, SSL, TLS 1.0/1.1), недозволене програмне забезпечення, усі зовнішні неавторизовані мережеві підключення тощо]*
4.6.3	Мінімально необхідна функціональність - періодичний перегляд	переглядати *[призначення: частота, визначена організацією]* систему, щоб виявити непотрібні або небезпечні функції, порти, протоколи, з’єднання та служби; вимкнути або видалити функції, порти, протоколи, з’єднання та служби, які є непотрібними або небезпечними.	CM-7(1)	*[щорічно або в разі внесення змін до налаштувань компонентів ІКС чи виникнення інцидентів]* проводити перегляд налаштувань компонентів ІКС для виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг
4.6.4				вимкнути або видалити функції, порти, протоколи, з’єднання та служби, які є непотрібними або небезпечними
4.6.5	**Мінімально необхідна функціональність –**	**визначити програми, яким дозволено виконуватися в системі;**	**CM-7(5)**	**визначити та затвердити перелік програмного забезпечення, яке дозволено до використання в ІКС**

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
4.6.6	**авторизоване програмне забезпечення – чорний список**	**впровадити політику «заборонити все», «дозволити за винятком» для виконання програм у системі; періодично переглядати та оновлювати список дозволених програм.**		**впровадити політику «заборонити все», «дозволити за винятком» для використання (виконання) програмного забезпечення в ІКС**
4.6.7				***[щоквартально]* переглядати та оновлювати список дозволеного програмного забезпечення в ІКС**
4.7.1	**Інвентаризація компонентів системи**	**розробити та документувати перелік компонентів системи; періодично переглядати та оновлювати перелік компонентів системи.**	**СМ-8**	**розробити та задокументувати процес інвентаризації компонентів ІКС, який: 1. точно описує поточну конфігурації ІКС; 2. охоплює всі компоненти ІКС в межах авторизації; 3. не включає повторний облік компонентів ІКС або компонентів будь-якої іншої системи; 4. визначає рівень деталізації, який є необхідним для відстеження та звітування; 5. включає інформацію для обліку компонентів ІКС: *[технічні характеристики обладнання (виробник, тип, модель, серійний номер, фізичне місцезнаходження), програмне забезпечення, відповідальний обслуговуючий персонал]*.**
4.7.2				***[щоквартально]* переглядати та оновлювати перелік компонентів ІКС**
4.7.3	**Інвентаризація компонентів системи - оновлення під час встановлення та видалення**	**оновлювати перелік компонентів системи під час інсталяції, видалення та оновлення системи**	**СМ-8(1)**	**оновлювати перелік компонентів ІКС під час інсталяції, видалення та оновлення таких компонентів**
4.8.1	**Встановлене користувачем програмне забезпечення**	**встановити [*призначення: визначені організацією правила (політики)*], що регулюють встановлення програмного забезпечення користувачами; застосувати правила (політики) встановлення програмного забезпечення за допомогою таких методів: *[призначення: визначені організацією методи]*; відстежувати відповідність правилам (політики) з *[призначення: визначеною організацією частотою]*.**	**СМ-11**	**заборонити користувачам самостійно встановлювати програмне забезпечення на робочих місцях користувачів; дозволити користувачам встановлювати програмне забезпечення на робочих місцях користувачів лише за дозволом, наданим встановленим порядком**
4.8.2				**обмежити права користувачів на самостійне встановлення програмного забезпечення організаційними заходами**
4.8.3				***[щоквартально]* здійснювати контроль робочих місць користувачів з метою перевірки відсутності самостійно встановленого програмного забезпечення**

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
5	**Ідентифікація та автентифікація (ІА)**			
5.1.1	Ідентифікація та автентифікація (користувачів організації)	унікально ідентифікувати та автентифікувати користувачів організації і пов'язувати цю унікальну ідентифікацію з процесами, що діють від імені цих користувачів;	ІА-2	унікально ідентифікувати та автентифікувати користувачів (див. п. 1.6.2 цього документу) і пов'язувати цю унікальну ідентифікацію з процесами, що діють від імені цих користувачів
5.1.2	Ідентифікація та автентифікація (користувачів організації) – багатофакторна автентифікація привілейованих облікових записів	упровадити багатофакторну автентифікацію для доступу до привілейованих облікових записів системи	ІА-2(1)	упровадити багатофакторну автентифікацію *[системного адміністратора, адміністратора безпеки]* при доступі до *[операційних систем серверів (1 фактор), технологічного програмного забезпечення (2 фактор)]*
5.1.3	Ідентифікація та автентифікація (користувачів організації) – багатофакторна автентифікація непривілейованих облікових записів	упровадити багатофакторну автентифікацію для доступу до непривілейованих облікових записів системи	ІА-2(2)	упровадити багатофакторну автентифікацію *[користувачів]* при доступі до *[прикладного програмного забезпечення] [з використанням кваліфікованого / удосконаленого електронного підпису]*
5.1.4	Ідентифікація та автентифікація (користувачів організації) – доступ до облікових записів – стійкість до відтворення	упровадити механізми автентифікації, стійкі до повторного відтворення, для доступу до облікових записів у системі	ІА-2(8)	упровадити стійкі до повторного відтворення механізми автентифікації для доступу до облікових записів користувачів
5.2	Ідентифікація та автентифікація пристроїв	унікально ідентифікувати та автентифікувати пристрої перед встановленням з'єднання з системою	ІА-3	унікально ідентифікувати та автентифікувати *[робочі місця адміністраторів] [перед встановленням з'єднання з центральним вузлом ІКС за ключовими даними відповідних засобів криптографічного захисту інформації]*
5.3.1	Управління ідентифікацією	отримати дозвіл від персоналу або ролей організації на призначення ідентифікатора особи, групи, ролі, служби або пристрою;	ІА-4	встановленим порядком отримати дозвіл для призначення ідентифікатора особі, групі, ролі або пристрою
5.3.2		вибрати та призначити ідентифікатор, який ідентифікує особу, групу, роль, службу або пристрій;		обрати ідентифікатор, який ідентифікує окрему особу, групу, роль або пристрій
5.3.3		запобігати повторному використанню ідентифікаторів для [*призначення: період часу,*		призначити ідентифікатор особі, групі, ролі або пристрою; запобігати повторному використанню цього ідентифікатора впродовж *[1 року]*

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	**Налаштований зміст заходу захисту**
		визначений організацією].		
5.3.4	**Управління ідентифікацією - заборона використання ідентифікаторів облікових записів таких самих, як і публічні ідентифікатори**	**заборонити використання ідентифікаторів облікових записів системи, які збігаються із загальнодоступними ідентифікаторами для індивідуальних облікових записів**	**IA-4(1)**	**заборонити використання вбудованих облікових записів адміністраторів в операційних системах робочих місць адміністраторів та користувачів**
5.3.5	**Управління ідентифікацією - ідентифікація статусу користувача**	**унікально ідентифікувати статус кожної особи за допомогою ідентифікаційної характеристики.**	**IA-4(4)**	**унікально ідентифікувати статус кожного користувача за допомогою ідентифікаційної характеристики**
5.4.1	Управління автентифікатором	перевіряти ідентичність особи, групи, ролі, служби або пристрою, які отримують автентифікатор під час початкового розповсюдження автентифікатора; встановити початковий вміст автентифікатора для всіх автентифікаторів, виданих організацією; створити та впровадити адміністративні процедури для початкового розподілу автентифікаторів для втрачених, скомпрометованих або пошкоджених автентифікаторів, а також для відкликання автентифікаторів; змінити автентифікатори за замовчуванням під час першого використання; змінювати або оновлювати автентифікатори періодично або коли відбуваються події: *[призначення: події, визначені організацією]*; захистити вміст автентифікатора від несанкціонованого розкриття та модифікації.	IA-5	перевіряти ідентичність особи, групи, ролі, служби або пристрою, які отримують автентифікатор під час початкового розповсюдження автентифікатора
5.4.2				встановити початковий вміст автентифікатора для всіх автентифікаторів, виданих організацією; забезпечити, щоб автентифікатори мали достатню стійкість механізму для їх використання за призначенням
5.4.3				створити та впровадити адміністративні процедури для початкового розподілу автентифікаторів для втрачених, скомпрометованих або пошкоджених автентифікаторів, а також для відкликання автентифікаторів
5.4.4				змінити автентифікатори за замовчуванням під час першого використання
5.4.5				змінювати або оновлювати автентифікатори *[кожні 180 днів]* або у разі підозри на компрометацію
5.4.6				захистити вміст автентифікатора від несанкціонованого розкриття та модифікації
5.4.7				встановити вимоги до осіб використовувати заходи безпеки для захисту автентифікаторів від несанкціонованого розкриття

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
5.4.8				встановити вимоги змінювати автентифікатори для облікових записів груп/ролей обслуговуючого персоналу при зміні його членства в цих облікових записах
5.4.9	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)	вести перелік часто використовуваних, очікуваних або скомпрометованих паролів і *[щоквартально]* оновлювати його, а також у разі виникнення підозри, що паролі організації були скомпрометовано
5.4.10				перевіряти, коли користувачі створюють або оновлюють паролі, чи не містяться вони у списку загальновживаних, очікуваних або скомпрометованих паролів
5.4.11				передавати паролі тільки криптографічно захищеними каналами
5.4.12				зберігати паролі в криптографічно захищеному *[(з використанням механізмів гешування)]* вигляді
5.4.13				встановити новий пароль при першому використанні після відновлення облікового запису
5.4.14				дозволити вибирати довгі паролі та фрази, включно з пробілами та всіма друкованими символами
5.4.15				використовувати автоматизовані інструменти для допомоги у виборі надійних паролів
5.4.16				упровадити правила складу та складності паролів: *[12-символьний набір з великих, малих літер, цифр та спеціальних символів, що включає принаймні по одному символу кожного регістру; змінювати принаймні 50% символів при створенні нових паролів]*
5.4.17	**Управління автентифікатором – автентифікація на основі відкритого ключа**	**(a) для автентифікації на основі відкритого ключа:** **1) забезпечити авторизований доступ до відповідного закритого ключа;** **2) зіставити автентифіковану особу з обліковим записом особи чи групи;** **(b) при використанні інфраструктури відкритого ключа (PKI):** **1) перевіряти сертифікати шляхом створення та перевірки шляху сертифікації до прийнятої довіреної прив'язки, включно з перевіркою інформації про статус сертифіката;** **2) впровадити локальний кеш даних для підтримки виявлення та перевірки шляху.**	**IA-5(2)**	**для автентифікації на основі відкритого ключа:** ***[механізми автентифікації на основі відкритого ключа не використовуються]***
5.4.18				**при використанні інфраструктури відкритого ключа (PKI) *[для ідентифікації та автентифікації на рівні прикладного програмного забезпечення]*:** **1) перевіряти сертифікати з використанням сервісів відповідного надавача електронних довірчих послуг, включно з перевіркою інформації про статус сертифіката;** **2) зберігати доменні адреси надавачів електронних довірчих послуг для обміну даними з ними при перевірці статусу сертифікатів.**
5.5	Зворотний зв'язок	забезпечити прихований зворотний зв'язок	IA-6	забезпечити введення даних автентифікації в

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
	автентифікатора	автентифікаційної інформації під час процесу автентифікації		замаскованому вигляді із можливістю контролю факту введення символів та одночасного захисту від можливого підглядання за значенням введеного паролю сторонніми особами
5.6	**Ідентифікація та автентифікація (користувачі, що не належать до організації)**	**унікально ідентифікувати та автентифікувати користувачів, що не належать до організації або процеси (що не належать організації), які діють від імені користувачів**	**ІА-8**	**унікально ідентифікувати та автентифікувати користувачів зовнішніх організацій, які не є користувачами А_ІКС на рівні *[прикладного програмного забезпечення]***
5.7	**Повторна автентифікація**	**повторно автентифікувати користувачів, коли *[призначення: обставини або ситуації, що вимагають повторної автентифікації, визначені організацією]***	**ІА-11**	**повторно автентифікувати користувачів у випадках, передбачених вимогами АС-2(5)**
6	**Реагування на інциденти (IR)**			
6.1.1	Навчання з реагування на інциденти	1) проводити навчання з реагування на інциденти для користувачів системи відповідно до призначених ролей та обов'язків: протягом *[призначення: період часу, визначений організацією]* з моменту прийняття на себе ролі чи відповідальності за реагування на інцидент або отримання доступу до системи; коли цього вимагають зміни в системі; *[призначення: частота, визначена організацією]* надалі; 2) переглядати та оновлювати зміст навчання з реагування на інциденти *[призначення: періодичність, визначена організацією]* та наступні *[призначення: події, визначені організацією]*.	IR-2	проводити навчання з реагування на інциденти для *[адміністраторів]* відповідно до призначених ролей та обов'язків: - протягом *[30 робочих днів]* з моменту прийняття на себе ролі чи відповідальності за реагування на інцидент або отримання доступу до ІКС; - коли цього вимагають зміни в ІКС; - *[щорічно]* в подальшому.
6.1.2				переглядати та оновлювати зміст навчання з реагування на інциденти *[щорічно]*, а також у разі виявлення інцидентів, не охоплених чинним обсягом (змістом) програми навчання з реагування
6.2	Перевірка реагувань на інциденти	перевіряти ефективність системи реагування на інциденти *[призначення: частота, визначена організацією]*	IR-3	*[щорічно]* перевіряти ефективність системи реагування на інциденти
6.3.1	Обробка інциденту	упровадити систему реагування на інциденти, яка відповідає плану реагування на інциденти і передбачає підготовку, виявлення та аналіз, локалізацію, ліквідацію та відновлення інцидентів.	IR-4	упровадити систему реагування на інциденти, яка відповідає плану реагування на інциденти і передбачає підготовку, виявлення та аналіз, локалізацію, ліквідацію та відновлення після інцидентів
6.3.2				координувати діяльність з обробки інцидентів із заходами із забезпечення безперервності функціонування
6.3.3				вводити уроки, що отримані з поточних дій з обробки інцидентів, у процедури реагування на інциденти, навчання

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				й тестування та вносити відповідні зміни
6.3.4				забезпечити, щоб ретельність, інтенсивність, обсяг і результати діяльності з обробки інцидентів можна було порівняти та передбачити на рівні А_ІКС
6.4	Моніторинг інциденту	відстежувати та документувати інциденти, пов'язані з безпекою системи	IR-5	відстежувати та документувати інциденти, пов'язані з безпекою ІКС
6.5.1	Звітність про інциденти	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*].	IR-6	повідомляти про підозрілі інциденти до *[адміністратора безпеки] [у найкоротший можливий термін]*
6.5.2				повідомляти інформацію про інцидент до CERT-UA відповідно до визначеного переліку типів інцидентів
6.6	Підтримка реагування на інциденти	забезпечити ресурс підтримки реагування на інциденти, який пропонує поради та допомогу користувачам системи щодо обробки та звітування про інциденти.	IR-7	забезпечити ресурс підтримки реагування на інциденти, який надає рекомендації та допомогу користувачам щодо обробки та звітування про інциденти
6.7.1	План реагування на інциденти	1) Розробити план реагування на інцидент, який: надає організації план дій для реалізації її можливостей реагування на інциденти; описує структуру та організацію системи реагування на інциденти; забезпечує високорівневий підхід до того, як спроможність реагування на інциденти вписується в загальну структуру організації; визначає інциденти, про які необхідно повідомляти, вирішує питання обміну інформацією про інциденти, і розподіляє обов'язки між структурними підрозділами, персоналом або ролями; 2) розповсюдити копії плану реагування на інцидент серед призначеного персоналу, відповідального за реагування на інцидент (ідентифікованого за іменами та/або за ролями), та організаційних елементів; 3) оновлювати план реагування на інциденти з урахуванням змін в системі та організації або проблем, що виникли під час впровадження, виконання або тестування плану; 4) захистити план реагування на інциденти від несанкціонованого розголошення.	IR-8	розробити план реагування на інциденти для реалізації можливостей реагування на інциденти, який: 1. надає дорожню карту для впровадження 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 А_ІКС; 4. відповідає унікальним вимогам А_ІКС, які пов’язані із завданнями, розміром, структурою і функціями; 5. визначає підзвітні інциденти; 6. надає показники для вимірювання можливостей реагування на інциденти всередині А_ІКС; 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 *[уповноваженими посадовими особами А_ІКС]*.
6.7.2				розповсюдити копії плану реагування на інциденти серед призначеного персоналу, відповідального за реагування на інцидент (ідентифікованого за іменами та/або за ролями), та організаційних елементів
6.7.3				*[щорічно]* оновлювати план реагування на інциденти, щоб

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				врахувати зміни в ІКС та зміни в організації або проблеми, що виникли під час впровадження, виконання або тестування плану
6.7.4				повідомляти про зміни плану реагування на інциденти *[весь персонал, який має роль або відповідальність за впровадження плану реагування на інциденти]*
6.7.5				захистити план реагування на інциденти від несанкціонованого розголошення.
7	**Технічне обслуговування (МА)**			
7.1.1	Інструменти для обслуговування	затверджувати, контролювати та відстежувати використання інструментів технічного обслуговування системи.	МА-3	затвердити, контролювати та відстежувати використання засобів технічного обслуговування
7.1.2				переглядати раніше затверджені інструменти технічного обслуговування *[щорічно]*
7.1.3	Інструменти для обслуговування - перевірка інструментів	перевіряти інструменти для технічного обслуговування на наявність неналежних або несанкціонованих модифікацій	МА-3(1)	оглянути інструменти для технічного обслуговування, які доставлені на об'єкт обслуговуючим персоналом, на предмет неправильних або несанкціонованих модифікацій
7.1.4	Інструменти для обслуговування - перевірка носіїв інформації	перевіряти носії, що містять діагностичні та тестові програми, на наявність шкідливого коду, перш ніж використовувати їх у системі	МА-3(2)	перед використанням носіїв в ІКС перевірити носії, що містять діагностичні та тестові програми на наявність шкідливого коду
7.1.5	**Інструменти для обслуговування - запобігання несанкціонованому переміщенню**	**запобігати вилученню обладнання для обслуговування системи, що містить відкриту та конфіденційну інформацію: переконатися, що на обладнанні немає відкритої та конфіденційної інформації; процедура очистки або знищення обладнання; збереження обладнання в межах об'єкта.**	**МА-3(3)**	**запобігати вилученню обладнання для обслуговування ІКС, що містить конфіденційну інформацію: - переконатися, що на обладнанні немає конфіденційної інформації; - застосувати процедури очистки або знищення обладнання; - забезпечити збереження обладнання в межах об'єкта А_ІКС; - отримати дозвіл від керівника А_ІКС (або уповноваженої ним посадової особи), який явно дозволяє переміщення обладнання з об'єкта**
7.2.1	Віддалене обслуговування	затверджувати та контролювати віддалені сеанси з технічного обслуговування та діагностики; упровадити багатофакторну автентифікацію та стійкість до повторного відтворення при створенні віддалених сеансів технічного обслуговування та діагностики; забезпечити завершення сеансу та мережевих	МА-4	впровадити та відстежувати віддалені дії з обслуговування та діагностики
7.2.2				дозволити використання віддалених засобів технічного обслуговування та діагностики лише відповідно до політики технічного обслуговування А_ІКС та в разі, якщо це документально зафіксовано в нормативно-розпорядчій документації ІКС
7.2.3				використовувати надійну автентифікацію при встановленні

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		з'єднань після завершення віддаленого технічного обслуговування.		віддалених технічних та діагностичних сеансів
7.2.4				вести облік віддалених дій з обслуговування та діагностики
7.2.5				забезпечити завершення сеансу та мережевих з'єднань після завершення віддаленого технічного обслуговування
7.2.6	**Віддалене обслуговування - криптографічний захист**	**запровадити криптографічні механізми для захисту цілісності та конфіденційності віддаленого обслуговування та діагностичних комунікацій**	**МА-4(6)**	**в разі необхідності проведення віддаленого технічного обслуговування використовувати засоби криптографічного захисту інформації, що відповідають вимогам законодавства України з питань криптографічного захисту інформації**
7.3.1	Технічний персонал	встановити процес авторизації персоналу з технічного обслуговування; вести список уповноважених організацій або персоналу з технічного обслуговування; переконатися, що персонал без супроводу, який виконує технічне обслуговування системи, має необхідні дозволи на доступ; призначити персонал організації з необхідними повноваженнями доступу та технічною компетентністю для нагляду за діяльністю персоналу з технічного обслуговування, який не має необхідних повноважень доступу.	МА-5	визначити порядок авторизації персоналу з технічного обслуговування
7.3.2				вести список уповноважених організацій або персоналу з технічного обслуговування
7.3.3				переконатися, що персонал без супроводу, який виконує технічне обслуговування ІКС, має необхідні дозволи на доступ
7.3.4				призначити персонал з необхідними повноваженнями доступу та технічною компетентністю для нагляду за діяльністю персоналу з технічного обслуговування, який не має необхідних повноважень доступу
8	**Захист носіїв інформації (МР)**			
8.1	Доступ до носіїв інформації	обмежити доступ до конфіденційної інформації на носіях інформації	МР-2	заборонити доступ до будь-яких носіїв інформації, що містять конфіденційну інформацію, для осіб, яким не надано встановленим порядком дозвіл на доступ до конфіденційної інформації
8.2.1	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	МР-3	маркувати носії інформації, на яких зберігається конфіденційна інформація в стані спокою (див. п. 1.5.1 цього документу), для позначення обмежень щодо розповсюдження, застережень стосовно поводження з ними та позначок безпеки
8.2.2				дозволити не здійснювати маркування *[незнімних носіїв відкритої інформації, що використовуються в складі компонентів ІКС]*, якщо вони залишаються в межах контрольованої зони А_ІКС
8.3	Зберігання носіїв інформації	фізично контролювати та безпечно зберігати носії інформації, що містять відкриту та конфіденційну інформацію	МР-4	фізично контролювати та безпечно зберігати будь-які носії інформації, що містять конфіденційну інформацію, до моменту їх знищення або очищення за допомогою затвердженого обладнання, методів і процедур
8.4	Транспортування носіїв інформації	захистити і контролювати носії інформації, що	МР-5	захищати та контролювати будь-які носії інформації під час

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
	інформації	містять відкриту та конфіденційну інформацію, під час транспортування за межі контрольованих територій; вести облік носіїв інформації, що містять відкриту та конфіденційну інформацію, під час транспортування за межі контрольованих територій; документувати дії, пов'язані з транспортуванням системних носіїв, які містять відкриту та конфіденційну інформацію.		транспортування за межами контрольованих територій, використовуючи: *[захищені контейнери (валізи) для транспортування, супроводжуючий персонал для забезпечення фізичної безпеки під час транспортування]*
8.4.2				вести облік носіїв інформації під час транспортування за межами контрольованих територій
8.4.3				документувати дії, пов’язані з транспортуванням носіїв інформації
8.4.4				обмежити діяльність персоналу, пов’язану з транспортуванням носіїв інформації
8.4.5			SC-28	забезпечити конфіденційність конфіденційної інформації, що зберігається на носіях інформації в стані спокою під час їх транспортування
8.5	Знищення інформації на носіях інформації	очистити носії інформації, що містять відкриту та конфіденційну інформацію, перед утилізацією, випуском з-під контролю організації або повторним використанням	MP-6	очистити будь-які носії інформації, що містять конфіденційну інформацію, перед утилізацією, випуском з-під контролю А_ІКС або повторним використанням
8.6.1	Використання носіїв інформації	обмежити або заборонити використання [*призначення: типи носіїв інформації, визначені організацією*]; заборонити використання знімних носіїв інформації без ідентифікованого власника.	MP-7	обмежити використання *[знімних носіїв інформації будь-якого типу на серверах центрального вузлу ІКС]*
8.6.2				заборонити використання знімних носіїв інформації без ідентифікованого власника.
9	**Кадрова безпека (PS)**			
9.1.1	Перевірка персоналу	перевіряти осіб перед тим, як надавати їм доступ до системи; проводити повторні перевірки осіб відповідно до [*призначення: умови, що потребують повторної перевірки, визначені організацією*]	PS-3	перевіряти осіб перед тим, як надавати їм доступ до ІКС за встановленою А_ІКС процедурою
9.1.2				проводити повторні перевірки осіб у випадках, встановлених А_ІКС
9.2.1	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	PS-4	1) коли припиняється індивідуальна трудова діяльність: - заборонити доступ до ІКС *[у разі добровільного звільнення - якомога швидше, але не більше ніж за 5 робочих днів; у разі примусового звільнення - у той самий день, що й припинення трудових відносин]*; - припинити дію або відкликати автентифікатори та облікові записи, пов’язані з особою, з обов’язковим документальним підтвердженням; - отримати всі матеріальні засоби (цінності), пов’язані із використанням ІКС, з обов’язковим документальним підтвердженням; - зберігати доступ до ІКС, який раніше контролювала

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		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.		звільнена особа.
9.2.2			PS-5	2) коли працівників призначають або переводять на інші посади: - переглянути та підтвердити поточну оперативну потребу в поточних логічних і фізичних дозволах доступу до ІКС та об'єкта A_ІКС; - ініціювати *[надання нового набору доступів відповідно до матриці доступів та рольової моделі]* протягом *[3 робочих днів]*; - змінювати авторизацію доступу відповідно до будь-яких змін в процесах (технології) обробки інформації в ІКС; - повідомляти про переведення обслуговуючого персоналу *[адміністратора прикладного програмного забезпечення]* в рамках *[1 робочого дня]*.
10	**Фізичний захист і захист робочого середовища (PE)**			
10.1.1	Авторизація фізичного доступу	розробити, затвердити та підтримувати список осіб, які мають право доступу до фізичного місця розташування системи; надавати повноваження для доступу до об'єкта; періодично перевіряти список фізичного доступу; переглядати список доступу до об'єктів *[призначення: частота, визначена організацією]*; видаляти осіб зі списку фізичного доступу, коли доступ більше не потрібен.	PE-2	розробити, затвердити та підтримувати список осіб, які мають право доступу до фізичного місця розташування компонентів ІКС (список фізичного доступу)
10.1.2				надавати повноваження для фізичного доступу до об'єкта A_ІКС
10.1.3				*[щорічно]* перевіряти список фізичного доступу
10.1.4				видаляти осіб зі списку фізичного доступу, коли їх доступ більше не потрібен
10.2.1	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;	PE-3	забезпечити авторизацію фізичного доступу на об'єкт A_ІКС шляхом: 1. перевірки індивідуального дозволу доступу до об'єкта; 2. управління входом та виходом на об'єкт за допомогою *[турнікетів та персональних електронних карток]*.
10.2.2				вести журнали контролю фізичного доступу *[засобами системи контролю та управління доступом]*
10.2.3				забезпечити *[використання турнікетів, системи відеоспостереження]* для контролю доступу в зони всередині об'єкта A_ІКС

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
10.2.4		4) забезпечити захист ключів, кодів доступу та інших пристроїв фізичного доступу.		супроводжувати будь-яких відвідувачів та контролювати їх активність на об'єкті А_ІКС
10.2.5				забезпечити захист *[ключів від приміщень та персональних електронних карток]*
10.2.6				проводити інвентаризацію *[ключів від приміщень та персональних електронних карток (за наявності)] [щорічно]*
10.2.7				здійснювати зміну кодів доступу щорічно, коли ключі втрачені, комбінації скомпрометовані або фізичні особи переведені чи звільнені.
10.3	Контроль доступу до джерел і ліній електроживлення.	контролювати фізичний доступ до розподільчих ліній системи і ліній електропередач на об'єктах організації	PE-4	контролювати фізичний доступ до розподільчих ліній і ліній електропередач використовуючи *[електронні замки, систему відеоспостереження]*
10.4	Контроль доступу до пристроїв виведення інформації	контролювати фізичний доступ до пристроїв виводу, щоб запобігти доступу сторонніх осіб до конфіденційної інформації	PE-5	керувати фізичним доступом до принтерів, копіювальних апаратів, терміналів перегляду документів, USB-портів на робочих місцях для запобігання несанкціонованому отриманню сторонніми особами даних, що містять конфіденційну інформацію
10.5.1	Моніторинг фізичного доступу	моніторити фізичний доступ до місця розташування системи, щоб виявляти та реагувати на інциденти фізичної безпеки; переглядати журнали фізичного доступу *[призначення: частота, визначена організацією]* та при виникненні *[призначення: події, визначені організацією, або потенційні ознаки подій]*.	PE-6	моніторити фізичний доступ до місця розташування компонентів ІКС, щоб виявляти та реагувати на інциденти фізичної безпеки
10.5.2				переглядати журнали фізичного доступу *[щоквартально]* на предмет наявності невідповідності між обліковими записами та фактичним доступом, спроб несанкціонованого входу, доступу у неробочий час та при виявленні ознак несанкціонованого фізичного доступу до місць розташування ІКС
10.6	**Аварійне енергозабезпечення**	**впровадити тимчасове джерело безперебійного живлення для забезпечення *[Вибір (один або кілька): впорядковане виключення системи; перехід системи на довгостроковy альтернативну систему живлення]* в разі втрати первинного джерела живлення**	**PE-11**	**забезпечити електроживлення *[серверного та мережевого обладнання центрального вузлу ІКС]* від промислової електромережі через відповідні системи (джерела) безперебійного живлення**
10.7.1	Альтернативне робоче місце	визначити альтернативні робочі місця, дозволені для використання працівниками; застосовувати дії безпеки на альтернативних робочих місцях *[призначення: дії безпеки, визначені організацією]*.	PE-17	визначити альтернативні робочі місця, дозволені для використання працівниками
10.7.2				застосовувати альтернативні робочі місця з відповідними підвищеними вимогами безпеки
10.7.3				оцінити ефективність заходів захисту на альтернативних робочих місцях

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
10.7.4				надати працівникам засоби комунікації з персоналом, відповідальним за інформаційну безпеку, в разі інцидентів безпеки
11	**Оцінка ризику (RA)**			
11.1.1	Оцінювання ризику	оцінити ризик несанкціонованого розголошення в результаті обробки, зберігання або передачі конфіденційної інформації	RA-3	оцінити ризик несанкціонованого розголошення в результаті несанкціонованого доступу, використання, розголошення, руйнування, модифікації або знищення ІКС, інформації, яку вона обробляє, зберігає та передає, а також будь-якої пов'язаної інформації
11.1.2				інтегрувати результати оцінювання ризику та рішення з управління ризиками на рівні А_ІКС та завдань/процесів з оцінюванням ризиків на рівні ІКС
11.1.3				задокументувати результати оцінювання ризику до *[планів обробки ризиків]*
11.1.4				*[щорічно]* оновлювати оцінки ризиків
11.1.5				поширити результати оцінювання ризику серед *[адміністраторів безпеки]*
11.1.6				оновлювати оцінювання ризику, коли є суттєві зміни в ІКС, її робочому середовищі чи інших умовах, які можуть вплинути на її стан безпеки
11.2.1	Сканування вразливостей	моніторити та сканувати систему на наявність вразливостей *[призначення: частота, визначена організацією]* та при виявленні нових вразливостей, що впливають на систему; усунути вразливості системи протягом часу *[призначення: час на реагування, визначений організацією]*.	RA-5	*[щомісячно]* проводити сканування ІКС на наявність вразливостей, а також при виявленні нових вразливостей, що впливають на ІКС
11.2.2				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
11.2.3				аналізувати звіти про сканування вразливості та результати контрольних оцінювань
11.2.4				усунути вразливості системи протягом: *[- для вразливостей критичного рівня - 48 год (2 доби);- для вразливостей високого рівня - 96 год (4 доби);- для вразливостей середнього рівня - 120 год (5 діб);- для вразливостей низького рівня – 240 год (10 діб).]*
11.2.5				ділитися інформацією, отриманою в процесі сканування

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				вразливостей та контрольного оцінювання, серед *[адміністраторів безпеки]*, щоб допомогти усунути подібні вразливі місця в інших інформаційно-комунікаційних системах А_ІКС
11.2.6				використовувати інструменти сканування вразливості, які містять можливість легко оновлювати вразливості, що були просканові
12	**Оцінювання, акредитація та моніторинг безпеки (CA)**			
12.1.1	Оцінювання	оцінювати дії *[призначення: частота, визначена організацією]* до безпеки системи та середовища її функціонування, щоб визначити, чи були ці дії виконані	CA-2	обрати відповідного оцінювача або команду з оцінки для типу оцінювання, яке буде проводитися
12.1.2				розробити план контрольної оцінки, який описує обсяг оцінки, в тому числі: 1. заходи захисту, що підлягають оцінюванню; 2. процедури оцінювання, які використовуватимуться для визначення ефективності заходів; 3. середовище оцінювання, групу оцінювання, ролі й обов'язки з оцінювання.
12.1.3				забезпечити розгляд і затвердження плану оцінювання уповноваженою офіційною особою або призначеним для проведення оцінювання представником
12.1.4				*[щорічно]* оцінювати заходи захисту в ІКС та в її середовищі функціонування для визначення, наскільки коректно реалізовані заходи безпеки і чи працюють вони за призначенням і дають бажаний результат щодо дотримання встановлених вимог безпеки
12.1.5				підготовити звіт оцінювання безпеки, який документує результати оцінювання
12.1.6				надати результати оцінювання з безпеки *[адміністраторам безпеки]*
12.2.1	Взаємодія систем	затвердити та керувати обміном конфіденційної інформації між системою та іншими системами, використовуючи *[вибір (один або декілька): угоди про безпеку з'єднання; угоди про безпеку обміну інформацією; меморандуми або угоди про взаєморозуміння; угоди про рівень обслуговування; угоди з користувачами; угоди про нерозголошення інформації]*;	CA-3	затвердити та керувати обміном конфіденційної інформації між ІКС та іншими зовнішніми інформаційними системами, використовуючи *[законодавство / договори / угоди / протоколи про обмін даними (технічної взаємодії), меморандуми або угоди про взаєморозуміння, угоди про рівень обслуговування, угоди з користувачами, угоди про нерозголошення інформації]*
12.2.2		документувати характеристики інтерфейсу, вимоги до безпеки та обов'язки для кожної системи як частину договорів про обмін;		документувати характеристики інтерфейсу, вимоги до безпеки та обов'язки для кожної зовнішньої інформаційної системи як частину *[законодавства / договорів / угод / протоколів про обмін даними (технічної взаємодії)]*

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
12.2.3		переглядати та оновлювати *[призначення: частота, визначена організацією]* договори про обмін.		*[щорічно]* переглядати та за потреби оновлювати *[законодавство / договори / угоди / протоколи про обмін даними (технічної взаємодії), меморандуми або угоди про взаєморозуміння, угоди про рівень обслуговування, угоди з користувачами, угоди про нерозголошення інформації]*
12.3.1	План усунення недоліків та контрольні показники	1) розробити план дій і контрольні показники для системи: задокументувати заплановані заходи з виправлення слабких місць або недоліків, виявлених під час оцінювання безпеки; зменшити або усунути відомі недоліки системи; 2) Оновити існуючий план дій і показників на основі результатів оцінки безпеки, незалежних аудитів або оглядів, а також безперервного моніторингу.	CA-5	розробити план дій і контрольні показники для ІКС: - задокументувати заплановані заходи з виправлення слабких місць або недоліків, виявлених під час оцінювання безпеки; - зменшити або усунути відомі недоліки ІКС.
12.3.2				*[щорічно]* або після значних змін в ІКС оновлювати існуючий план дій і показників на основі результатів оцінки безпеки, незалежних аудитів або оглядів, а також безперервного моніторингу
12.4	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, яка охоплює: - встановлення показників безпеки, які необхідно відстежувати: *[кількість виявлених вразливостей, кількість спроб несанкціонованих доступів]*; - *[щоквартально]* проводити моніторинг та *[щорічно]* безперервне оцінювання ефективності заходів захисту; - поточні оцінювання заходів захисту відповідно до стратегії безперервного моніторингу; - постійний моніторинг стану безпеки відповідно до встановлених метрик; - зіставлення та аналіз інформації, отриманої в результаті оцінювання та моніторингу безпеки; - дії реагування за результатами аналізу інформації, пов'язаної з безпекою; - повідомлення про статус безпеки ІКС *[керівника А_ІКС]* з *[негайними сповіщеннями при критичних інцидентах]*.
13	**Захист інформаційної системи та комунікацій (SC)**			
13.1.1	**Розділення функцій**	**розділяти функціональність користувача, включно зі службами, що призначені для користувача інтерфейсу, від функціональності системного управління**	**SC-2**	**розділити функціональні можливості користувачів (не адміністраторів) та адміністративні функції ІКС**
13.1.2	**Розділення функцій – Інтерфейси для непривілейованих**	**запобігати наданню функціональності системного управління в інтерфейсі для непривілейованих користувачів**	**SC-2(1)**	**обмежити користувачам (не адміністраторам) доступ до адміністративних функцій (механізмів адміністрування) ІКС**

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
	користувачів			
13.2	Інформація в загальних ресурсах системи	запобігати несанкціонованій і ненавмисній передачі інформації за допомогою загальних ресурсів системи	SC-4	запобігати несанкціонованій і ненавмисній передачі інформації через спільні системні ресурси
13.3.1	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	контролювати та управляти мережевим трафіком на зовнішньому мережевому периметрі *[пристрої мережевого захисту центрального вузлу ІКС]* та на ключових внутрішніх мережевих периметрах ІКС
13.3.2				реалізувати підмережі для загальнодоступних компонентів ІКС, які є *[логічно]* відділені від інших внутрішніх мереж
13.3.3				підключатися до зовнішніх мереж або систем тільки через керовані інтерфейси, що складаються з пристроїв захисту периметру, і розташовані відповідно до архітектури безпеки
13.3.4	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 мережевий трафік за умовчанням та дозволити мережевий трафік виключно для керованих інтерфейсів для ІКС
13.4.1	Конфіденційність і цілісність передачі.	реалізувати механізми криптографічного захисту для запобігання несанкціонованому розкриттю конфіденційної інформації під час передачі та зберігання	SC-8	забезпечити *[конфіденційність, цілісність]* інформації, що передається через незахищене середовище *[між компонентами ІКС]*
13.4.2	Конфіденційність та цілісність передачі - криптографічний захист	реалізувати механізми криптографічного захисту для запобігання несанкціонованому розкриттю конфіденційної інформації під час передачі та зберігання	SC-8(1) AC-17(2)	реалізувати механізми криптографічного захисту для запобігання несанкціонованому розкриттю конфіденційної інформації; виявленню змін в цій інформації під час обміну даними через незахищене середовище *[між компонентами ІКС]*
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 дій [*призначення: дії до встановлення та управління ключами, визначені організацією*]	SC-12	встановити та управляти криптографічними ключами для засобів криптографічного захисту інформації, які використовуються в ІКС для *[криптографічного захисту каналів зв'язку із використанням захищеного протоколу TLS 1.2 / 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 AC-17(2)	впровадити засоби криптографічного захисту інформації, які використовуються для *[криптографічного захисту каналів зв'язку із використанням захищеного протоколу TLS 1.2 / 1.3]*
13.8.1	Спільні обчислювальні	заборонити віддалену активацію спільних	SC-15	заборонити віддалену активацію обчислювальних

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
	пристрої та застосунки	обчислювальних пристроїв і програмного забезпечення з такими винятками: *[призначення: визначені організацією винятки, коли дозволяється віддалена активація]*; надавати чіткі вказівки щодо використання користувачам, які фізично наявні біля пристроїв.		пристроїв та застосунків на робочих місцях користувачів *[крім підключень системним адміністратором з метою використання для адміністрування ІКС]*
13.8.2				надавати чіткі вказівки користувачам, які фізично наявні біля робочих місць користувачів, щодо контролю за їх віддаленою активацією
13.9.1	Мобільний код	визначити прийнятний мобільний код і технології мобільного коду; авторизувати, відстежувати та контролювати використання мобільного коду.	SC-18	визначити прийнятний мобільний код і технології мобільного коду
13.9.2				авторизувати, відстежувати та контролювати використання мобільного коду
13.10	Автентифікація сесії	захистити автентифікацію сеансів зв'язку	SC-23	забезпечити автентифікацію сеансів зв'язку
13.11.1	Захист інформації у стані спокою	забезпечити *[вибір (один або кілька): конфіденційність; цілісність] [призначення: визначена організацією інформація]* в стані спокою	SC-28	забезпечити *[конфіденційність та цілісність інформації, що зберігається в ІКС]* в стані спокою
13.11.2	Захист інформації в стані спокою - криптографічний захист	впровадити криптографічні механізми для запобігання несанкціонованому розкриттю та модифікації *[призначення: визначена організацією інформація]* у стані спокою на *[призначення: визначені організацією компоненти системи]*	SC-28(1)	впровадити криптографічні механізми для запобігання несанкціонованому розкриттю та модифікації *[конфіденційної інформації]*, що зберігається у стані спокою в *[базах даних ІКС]*.
14	**Цілісність системи та інформації (SI)**			
14.1.1	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	виявляти, виправляти та повідомляти про виявлені недоліки в ІКС
14.1.2				перед установкою перевірити програмне забезпечення та оновлення вбудованого програмного забезпечення, що пов'язані з усуненням дефектів, на ефективність та можливі побічні ефекти
14.1.3				інсталювати оновлення програмного забезпечення, що використовується в ІКС, в межах *[30 днів]* випуску оновлень
14.1.4				внести виправлення помилок в процес управління конфігурацією А ІКС
14.2.1	Захист від шкідливого	1) упровадити механізми захисту від шкідливого коду у визначених місцях системи для виявлення та знищення шкідливого коду;	SI-3	упровадити механізми захисту від шкідливого коду *[в усіх точках введення та виведення інформації в ІКС]* для виявлення та знищення шкідливого коду
14.2.2		2) оновлювати механізми захисту від шкідливого коду в міру виходу нових версій		оновлювати механізми захисту від шкідливого коду в міру виходу нових версій відповідно до політики та процедур

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
		відповідно до політики та процедур управління конфігурацією;		управління конфігураціє
14.2.3		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.		налаштовувати механізми захисту від шкідливого коду на: 1) *[щотижневе]* сканування і сканування файлів у реальному часі із зовнішніх джерел на *[робочих місцях користувачів]*, коли файли завантажуються, відкриваються, виконуються, імпортуються або експортуються; 2) автоматичне сповіщення, блокування шкідливого коду, відправлення шкідливого коду в карантин в разі виявлення шкідливого коду.
14.2.4	**Захист від шкідливого коду – оновлення тільки привілейованими користувачами**	**здійснювати оновлення механізмів захисту від шкідливого коду лише привілейованими користувачами**	**SI-3(4)**	**здійснювати оновлення механізмів захисту від шкідливого коду на робочих місцях користувачів лише *[системним адміністратором]***
14.3.1	Моніторинг системи	1) проводити моніторинг системи для виявлення: атак та індикаторів потенційних атак; неавторизованих підключень; 2) виявляти неавторизоване використання системи.	SI-4	здійснювати моніторинг ІКС для виявлення: - атак та індикаторів потенційних атак відповідно до встановленої А_ІКС політики реагування на інциденти; - неавторизованих локальних, мережевих та віддалених підключень.
14.3.2				визначати несанкціоноване використання ІКС шляхом аналізу журналів реєстрації подій з метою виявлення підозрілих дій
14.3.3				застосовувати можливості внутрішнього моніторингу ІКС для збору необхідної інформації
14.3.4				захищати інформацію, отриману від засобів моніторингу, від несанкціонованого доступу, модифікації та видалення
14.3.5				регулювати рівень активності системного моніторингу при зміні ризику для А_ІКС, фізичних осіб, інших організацій або держави
14.3.6				отримувати за результатами моніторингу ІКС звіт про моніторинг ІКС
14.3.7				надавати звіт про моніторинг ІКС (інформацію про виявлені інциденти) до *[адміністратора безпеки]* за необхідності або *[щомісячно]*
14.3.8	Моніторинг системи – трафік вхідних і вихідних комунікацій	проводити моніторинг вхідного та вихідного комунікаційного трафіка для виявлення незвичних або несанкціонованих дій чи умов	SI-4(4)	визначити критерії незвичайної або несанкціонованої мережевої активності для вхідного та вихідного мережевого трафіку

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
14.3.9				проводити моніторинг вхідного та вихідного мережевого трафіку *[у реальному часі]* для виявлення незвичайної або несанкціонованої активності
14.4.1	Попередження, рекомендації та директиви з безпеки	отримувати попередження, рекомендації та директиви щодо безпеки системи від зовнішніх організацій на постійній основі; створювати та розповсюджувати внутрішні попередження системи, рекомендації та директиви щодо безпеки у разі потреби; упроваджувати директиви з безпеки відповідно до встановлених часових рамок.	SI-5	отримувати попередження, рекомендації та директиви щодо безпеки від *[CERT-UA]* на постійній основі
14.4.2				генерувати внутрішні попередження безпеки, рекомендації та директиви (за необхідністю)
14.4.3				поширювати попередження, рекомендації та директиви безпеки для користувачів
14.4.4				упроваджувати директиви з безпеки відповідно до встановлених часових рамок
14.5	**Управління та збереження інформації**	**управляти та зберігати конфіденційну інформацію в системі та виводити конфіденційну інформацію з системи відповідно до чинного законодавства, виконавчих наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог**	**SI-12**	**обробляти та зберігати конфіденційну інформацію в ІКС, експортувати конфіденційну інформацію з ІКС відповідно до чинного законодавства, виконавчих наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог**
15	**Планування безпеки (PL)**			
15.1.1	Політика та процедури планування безпеки	розробити, задокументувати та розповсюдити серед персоналу організації або ролей політики та процедури, необхідні для виконання вимог безпеки	AC-1	розробити, задокументувати та поширити серед адміністраторів та користувачів: - політику управління доступом; - процедури реалізації положень політики управління доступом і відповідних заходів управління доступом
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур контролю доступом
				переглядати та оновлювати: - політику управління доступом *[щорічно]* та після зміни у законодавстві чи виявлених інцидентів; - процедури (інструкції) управління доступом *[щорічно]* та після значних оновлень системи, виявлення порушень безпеки.
15.1.2			AT-1	розробити, задокументувати та поширити серед адміністраторів та персоналу А_ІКС, який відповідає за навчання користувачів: - політику обізнаності і навчання; - процедури (інструкції) щодо обізнаності і навчання і відповідних заходів захисту інформації
				призначити на посаду відповідальну посадову особу для

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				управління, документування і розповсюдження політики та процедур обізнаності і навчання
				переглядати та оновлювати: - політику обізнаності і навчання *[щорічно]* та після зміни у законодавстві чи виявлених інцидентів; - процедури (інструкції) щодо обізнаності і навчання *[щорічно]* та після виявлення нових загроз, впровадження нових заходів безпеки.
15.1.3			AU-1	розробити, задокументувати та поширити серед адміністраторів: - політику аудиту та підзвітності; - процедури (інструкції) щодо аудиту та підзвітності і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур аудиту та підзвітності
				переглядати та оновлювати: - політику аудиту та підзвітності *[щорічно]* та після зміни у законодавстві чи виявлених інцидентів; - процедури (інструкції) щодо аудиту та підзвітності *[щорічно]* та після виявлення порушень, змін у процесах.
15.1.4			CA-1	розробити, задокументувати та поширити серед адміністраторів та персоналу А_ІКС, який відповідає за контроль відповідності: - політику оцінювання, акредитації та моніторингу безпеки; - процедури (інструкції) щодо оцінювання, акредитації та моніторингу безпеки і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур оцінювання, акредитації та моніторингу безпеки
				переглядати та оновлювати: - політику оцінювання, акредитації та моніторингу безпеки *[щорічно]* та після зміни у законодавстві чи виявлених інцидентів; - процедури (інструкції) щодо оцінювання, акредитації та моніторингу безпеки *[щорічно]* та після виявлення критичних вразливостей, змін у процесах або критичних інцидентів безпеки.
15.1.5			CM-1	розробити, задокументувати та поширити серед адміністраторів:

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				- політику управління конфігурацією; - процедури (інструкції) щодо управління конфігурацією і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур управління конфігурацією
				переглядати та оновлювати: - політику управління конфігурацією *[щорічно]* та після зміни у законодавстві, виявлених інцидентів, змін у процесах; - процедури (інструкції) щодо управління конфігурацією *[щорічно]* та після виявлення критичних вразливостей, змін у процесах або значних оновлень ІКС.
15.1.6			IA-1	розробити, задокументувати та поширити серед адміністраторів та користувачів: - політику ідентифікації та автентифікації; - процедури (інструкції) щодо ідентифікації та автентифікації і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур ідентифікації та автентифікації
				переглядати та оновлювати: - політику ідентифікації та автентифікації *[щорічно]* та після зміни у законодавстві, виявлених інцидентів, змін у процесах; - процедури (інструкції) щодо ідентифікації та автентифікації *[щорічно]* та після виявлення критичних вразливостей, змін у процесах або критичних інцидентів безпеки.
15.1.7			IR-1	розробити, задокументувати та поширити серед адміністраторів та персоналу А_ІКС, який відповідає за реагування на інциденти: - політику реагування на інциденти; - процедури (інструкції) щодо реагування на інциденти і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур реагування на інциденти
				переглядати та оновлювати: - політику реагування на інциденти *[щорічно]* та після зміни у законодавстві, виявлених інцидентів;

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	**Налаштований зміст заходу захисту**
				- процедури (інструкції) щодо реагування на інциденти *[щорічно]* та після виявлення критичних вразливостей, змін у процесах або критичних інцидентів безпеки.
15.1.8			МА-1	розробити, задокументувати та поширити серед адміністраторів, персонал А_ІКС, який відповідає за технічне обслуговування: - політику технічного обслуговування; - процедури (інструкції) щодо технічного обслуговування і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур технічного обслуговування
				переглядати та оновлювати: - політику технічного обслуговування *[щорічно]* та після зміни у законодавстві, виявлених інцидентів; - процедури (інструкції) щодо технічного обслуговування *[щорічно]* та після виявлення критичних вразливостей, змін у процесах, впровадження нового обладнання або суттєвого оновлення програмного забезпечення.
15.1.9			МР-1	розробити, задокументувати та поширити серед адміністраторів та користувачів: - політику захисту носіїв інформації; - процедури (інструкції) щодо захисту носіїв інформації і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур захисту носіїв інформації
				переглядати та оновлювати: - політику захисту носіїв інформації *[щорічно]* та після зміни у законодавстві, виявлених інцидентів; - процедури (інструкції) щодо захисту носіїв інформації *[щорічно]* та після змін у законодавстві, змін у процесах.
15.1.10			РЕ-1	розробити, задокументувати та поширити серед адміністраторів та персоналу А_ІКС, який відповідає за фізичний захист середовища ІКС: - політику фізичного захисту і захисту робочого середовища; - процедури (інструкції) щодо фізичного захисту і захисту робочого середовища і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				управління, документування і розповсюдження політики та процедур фізичного захисту і захисту робочого середовища
				переглядати та оновлювати: - політику фізичного захисту і захисту робочого середовища *[щорічно]* та після виявлених інцидентів; - процедури (інструкції) щодо фізичного захисту і захисту робочого середовища *[щорічно]* та після виявлення критичних інцидентів.
15.1.11			PL-1	розробити, задокументувати та поширити серед адміністраторів та персоналу А_ІКС, який відповідає за планування безпеки: - політику планування безпеки; - процедури (інструкції) щодо планування безпеки і відповідних заходів захисту інформації .
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур планування безпеки
				переглядати та оновлювати: - політику планування безпеки *[щорічно]* та після змін у законодавстві, виявлених інцидентів; - процедури (інструкції) щодо планування безпеки *[щорічно]* та після змін у законодавстві, виявлення критичних інцидентів.
15.1.12			PS-1	розробити, задокументувати та поширити серед адміністраторів та персоналу А_ІКС, який відповідає за кадрове забезпечення: - політику кадрової безпеки; - процедури (інструкції) щодо кадрової безпеки і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур кадрової безпеки
				переглядати та оновлювати: - політику кадрової безпеки *[щорічно]* та після змін у законодавстві, виявлених інцидентів; - процедури (інструкції) щодо кадрової безпеки *[щорічно]* та після змін у законодавстві, виявлення критичних інцидентів.
15.1.13			RA-1	розробити, задокументувати та поширити серед персоналу А_ІКС, який відповідає за оцінку ризиків інформаційної безпеки:

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	**Налаштований зміст заходу захисту**
				- політику оцінки ризиків; - процедури (методики) щодо оцінки ризиків і відповідних заходів захисту інформації .
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур оцінки ризиків
				переглядати та оновлювати: - політику оцінки ризиків *[щорічно]* та після змін у законодавстві, виявлених інцидентів, змін у процесах; - процедури (методики) щодо оцінки ризиків *[щорічно]* та після змін у законодавстві, виявлення критичних інцидентів, змін у процесах.
15.1.14			SC-1	розробити, задокументувати та поширити серед адміністраторів та персоналу А_ІКС, який відповідає за фізичний захист середовища ІКС: - політику захисту системи та комунікацій; - процедури (інструкції) щодо захисту системи та комунікацій і відповідних заходів захисту інформації .
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур захисту системи та комунікацій
				переглядати та оновлювати: - політику захисту системи та комунікацій *[щорічно]* та після змін у законодавстві, виявлених інцидентів, змін у процесах; - процедури (інструкції) щодо захисту системи та комунікацій *[щорічно]* та після змін у законодавстві, виявлення критичних інцидентів, змін у процесах.
15.1.15			SI-1	розробити, задокументувати та поширити серед адміністраторів: - політику цілісності системи та інформації; - процедури (інструкції) щодо цілісності системи та інформації і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур цілісності системи та інформації
				переглядати та оновлювати: - політику цілісності системи та інформації *[щорічно]* та після змін у законодавстві, виявлених інцидентів, змін у процесах; - процедури (інструкції) щодо цілісності системи та

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	Налаштований зміст заходу захисту
				інформації *[щорічно]* та після змін у законодавстві, виявлення критичних інцидентів, змін у процесах.
			SR-1	розробити, задокументувати та поширити серед персоналу А_ІКС, який відповідає за оцінку ризиків інформаційної безпеки: - політику управління ризиками ланцюга постачання
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики управління ризиками ланцюга постачання
				переглядати та оновлювати: - політику управління ризиками ланцюга постачання *[щорічно]* та після змін у законодавстві, виявлених інцидентів, змін у процесах
15.1.16			CP-1	розробити, задокументувати та поширити серед адміністраторів: - політику резервного копіювання; - процедури (інструкції) щодо резервного копіювання і відповідних заходів захисту інформації.
				призначити на посаду відповідальну посадову особу для управління, документування і розповсюдження політики та процедур резервного копіювання
				переглядати та оновлювати: - політику резервного копіювання *[щорічно]* та після змін у законодавстві, виявлених інцидентів, змін у процесах; - процедури (інструкції) щодо резервного копіювання *[щорічно]* та після змін у законодавстві, виявлення критичних інцидентів, змін у процесах.
15.2.1	Плани захисту інформації та персональних даних	1) розробити план захисту інформації, який: визначає складові компоненти системи; описує робоче середовище системи; описує конкретні загрози для системи, які викликають занепокоєння в організації; надає огляд вимог до безпеки системи; визначає з'єднання з іншими системами; визначає осіб, які виконують ролі та обов'язки в системі; містить іншу інформацію, необхідну для захисту відкритої та конфіденційної інформації; 2) періодично переглядати та оновлювати план захисту інформації *[призначення: частота, визначена організацією]*;	PL-2	розробити план захисту інформації в ІКС, який: - узгоджується з архітектурою ІКС; - чітко визначає складові компоненти ІКС; - описує оперативний контекст ІКС з точки зору завдань та технології обробки інформації; - визначає осіб, які виконують системні ролі, та їх обов'язки; - визначає тип інформації, яка обробляється, зберігається та передається системою; - надає огляд вимог безпеки для ІКС; - описує загрози для інформації в ІКС; - описує робоче середовище ІКС та будь-які залежності від систем або компонентів систем або підключень до таких систем та їх компонентів;

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	**Налаштований зміст заходу захисту**
		3) захистити план захисту інформації від неавторизованого розголошення.		- надає огляд вимог безпеки та конфіденційності ІКС; - визначає будь-які відповідні контрольні базові рівні (в разі використання); - описує чинні або заплановані заходи щодо забезпечення безпеки, включно з обґрунтуванням рішень щодо налаштування; - включає виявлення ризиків для архітектури безпеки і приватності, а також проєктних рішень; - включає дії, пов'язані з безпекою та конфіденційністю, які впливають на ІКС, виконання яких вимагає планування та координацію з *[призначеними особами та/або обслуговуючим персоналом]*; - розглядається та затверджується уповноваженою посадовою особою А_ІКС до початку реалізації плану.
15.2.2				поширити копії плану захисту інформації серед *[обслуговуючого персоналу]* і повідомляти їх про подальші зміни планів
15.2.3				*[щорічно]* або в разі необхідності переглядати план захисту інформації
15.2.4				оновлювати план захисту інформації для врахування змін в ІКС та робочому середовищі або проблем, виявлених у ході реалізації або оцінювання заходів безпеки
15.2.5				забезпечити захист плану захисту інформації від неавторизованого розголошення
15.2.6				оновлювати плани захисту інформації для врахування змін в ІКС й робочому середовищі або проблем, виявлених у ході реалізації або оцінювання заходів безпеки
15.3.1	**Правила поведінки**	**створити та надати особам, що потребують доступу до інформаційної системи, правила, які описують їхні обов'язки й очікувану поведінку при роботі з конфіденційною інформацією та використанням системи;**	**PL-4**	**створити та надати користувачам правила, які описують їхні обов'язки й очікувану поведінку при роботі з конфіденційною інформацією та використанням ІКС**
15.3.2		**отримати документальне підтвердження від таких осіб про те, що вони прочитали, зрозуміли та погодилися дотримуватися правил поведінки, перш ніж дозволяти доступ до службової інформації та системи;**		**отримати документальне підтвердження від користувачів про те, що вони прочитали, зрозуміли та погодилися дотримуватися правил поведінки, перш ніж дозволяти доступ до конфіденційної інформації та ІКС**
15.3.3		**періодично переглядати та оновлювати правила поведінки.**		***[щорічно]*** **переглядати та оновлювати правила поведінки**
15.3.4				**вимагати від осіб, які ознайомилися під підпис з поточною редакцією правил поведінки, повторно ознайомитися під підпис з поточною редакцією правил** ***[щорічно або коли правила переглядаються чи***

№	Вимога з безпеки інформації	Вимога БПБ	ЦПБ	
			Захід захисту	**Налаштований зміст заходу захисту**
				оновлюються]
16	**Планування безперервної роботи (CP)**			
16.1.1	Резервне копіювання	захистити конфіденційність резервної копії	CP-9	*[щотижня]* проводити резервне копіювання інформації користувачів, що обробляється та зберігається в ІКС
16.1.2				*[щомісячно та перед внесенням змін до налаштувань відповідних компонентів ІКС]* проводити резервне копіювання конфігураційних та технологічних налаштувань компонентів ІКС
16.1.3				*[при створенні, отриманні, оновленні системної документації]* проводити резервне копіювання системної документації, включно з документацією, пов'язаною із забезпеченням безпеки
16.1.4				забезпечити захист конфіденційності, цілісності та доступності резервних копій інформації в місцях їх зберігання
16.2	**Відновлення та відтворення системи**	**забезпечити відновлення та відтворення системи до відомого стану після збою, компрометації або помилок у межах *[призначення: визначеного організацією періоду часу, відповідного часу відновлення та встановлених цілей відновлення]***	**CP-10**	**забезпечити відновлення та відтворення ІКС до відомого стану після збою, компрометації або помилок протягом *[одного робочого дня]***