Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Жмурик Ірини Миколаївни

на здобуття ступеня вищої освіти Бакалавра

Система захисту доказів для відділу цифрової криміналістики

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.220239.22.02.26 ПЗ

Виконала студентка 4 курсу група КБ-22-2 Ірина ЖМУРИК
Керівник канд. техн. наук, доцент Віктор ЧЕШУН
Нормоконтролер д-р філософії Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

4 06 2026 р.

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій
Кафедра Кібербезпеки
Рівень вищої освіти Бакалавр
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

9 січня 2026 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Жмурик Ірині Миколаївні

1 Тема роботи Система захисту доказів для відділу цифрової криміналістики.

Керівник роботи _канд. техн. наук, доцент, Чешун Віктор Миколайович
Затверджено наказом ректора університету від 8 січня 2026 р. № 7
2 Строк подання студентом кваліфікаційної роботи на кафедру 27 травня 2026р.
3 Вихідні дані до роботи Проаналізувати предметну область та існуючі рішення в галузі захисту та зберігання цифрових доказів. Сформулювати постановку задачі, визначити категорію оброблюваної інформації та клас автоматизованої системи для відділу цифрової криміналістики. Розробити модель загроз та модель порушника інформаційної безпеки. Забезпечити цілісність даних, контроль доступу та безпечне зберігання доказів.
4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз предметної області та нормативно-правової бази у сфері захисту інформації. Огляд існуючих підходів до захисту цифрових доказів у криміналістиці. Постановка задачі. Характеристика об'єкта захисту, розробка моделі загроз та моделі порушника. Проєктування системи захисту інформації та політики безпеки. Вибір та обґрунтування інженерно-технічних і програмно-апаратних засобів захисту. Розробка організаційних заходів захисту. Оцінка ефективності.
5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Генеральний план. Ситуаційний план. План-схема технічних засобів

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 12 січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Травень	
Захист КР	Червень	

Студент _____ Ірина ЖМУРИК

Керівник кваліфікаційної роботи _____ Віктор ЧЕШУН

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система захисту доказів для відділу цифрової криміналістики.

Автор роботи: Жмурик Ірина Миколаївна.

Керівник роботи: канд. техн. наук, доц. Чешун Віктор Миколайович.

Пояснювальна записка: 84 сторінки, 12 додатків, 23 рисунка, 3 таблиці, 50 джерел.

Графічна частина: 3 плакати.

Ключові слова: автентичність, захист інформації, інформаційна безпека, комплексна система захисту інформації, контроль доступу, криптографічний захист, ланцюг зберігання доказів, несанкціонований доступ, цифрова криміналістика, цифровий доказ.

Метою кваліфікаційної роботи є розроблення системи захисту цифрових доказів для відділу цифрової криміналістики. У роботі проведено аналіз особливостей роботи з цифровими доказами, досліджено нормативно-правові вимоги у сфері технічного захисту інформації та побудовано модель загроз і модель порушника.

Обґрунтовано вибір організаційних, програмних і технічних заходів захисту, спрямованих на забезпечення цілісності, автентичності та конфіденційності доказової інформації. Особливу увагу приділено контролю доступу, журналюванню подій та використанню криптографічних механізмів контролю цілісності цифрових доказів.

Результати роботи можуть бути використані під час створення або модернізації комплексних систем захисту інформації у підрозділах цифрової криміналістики.

25.05.2026 _____

ANNOTATION

Theme of qualification work: Evidence Protection System for the Digital Forensics Department

Author of the work: Zhmuryk Iryna Mykolaivna

Mentor: Ph.D. Cheshun Viktor Mykolaiovych

Explanatory note: 84 pages, 12 appendices, 23 figures, 3 tables, 50 references.

Graphic part: 3 posters.

Keywords: authenticity, information protection, information security, comprehensive information protection system, access control, cryptographic protection, chain of custody, unauthorized access, digital forensics, digital evidence.

The purpose of the qualification work is to develop a digital evidence protection system for the digital forensics department. The work analyzes the specifics of handling digital evidence, studies regulatory requirements in the field of information security, and develops a threat model and an intruder model.

Organizational, software, and technical protection measures aimed at ensuring the integrity, authenticity, and confidentiality of evidentiary information are substantiated. Particular attention is paid to access control, audit logging, and cryptographic integrity control mechanisms.

The obtained results can be used in the development and modernization of integrated information security systems in digital forensics departments.

25.05.2026

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АС – автоматизована система;

ДСК – для службового користування;

ІКС – інформаційно-комунікаційна система;

КЗЗ – комплекс засобів захисту;

КМУ – Кабінет Міністрів України;

КПК – Кримінальний процесуальний кодекс;

КСЗІ – комплексна система захисту інформації;

МВС – Міністерство внутрішніх справ України;

НДЕКЦ – науково-дослідний експертно-криміналістичний центр;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС – операційна система;

ПЗ – програмне забезпечення;

СЗІ – служба захисту інформації

ТЗ – технічне завдання;

ТЗІ – технічний захист інформації;

ЦД – цифровий доказ;

DLP – Data Loss Prevention;

ISO/IEC – International Organization for Standardization / International Electrotechnical Commission;

RBAC – Role-Based Access Control;

SIEM – Security Information and Event Management;

SWGDE – Scientific Working Group on Digital Evidence.

ВСТУП

Сучасні цифрові середовища інформації дедалі частіше виступають не лише засобом комунікації чи ресурсом, а й повноцінним доказом у кримінальному провадженні. Використання комп'ютерних систем, мобільних пристроїв, хмарних сервісів та мережевих технологій призвело до стрімкого зростання обсягів цифрових даних, які можуть містити відомості про обставини правопорушення. Листування у месенджерах, журнали подій операційних систем, мережевий трафік, файли користувачів та метадані сьогодні є важливими джерелами доказової інформації, що активно використовуються у діяльності правоохоронних органів.

Разом із розвитком інформаційних технологій змінюються і способи вчинення злочинів. Значна частина сучасних правопорушень прямо або опосередковано пов'язана з використанням цифрового середовища, тому цифрова криміналістика стала одним із ключових напрямів сучасної системи розслідування. Її основним завданням є виявлення, фіксація, аналіз та збереження цифрових доказів із дотриманням вимог їх автентичності та процесуальної допустимості.

Особливість цифрових доказів полягає у високій чутливості до будь-яких змін. Навіть незначне втручання в структуру файлу або зміна службових атрибутів можуть поставити під сумнів достовірність отриманих результатів. На відміну від традиційних речових доказів, цифрові дані можуть бути змінені без очевидних зовнішніх ознак, тому питання забезпечення їх цілісності та контролю доступу є критично важливими. Порушення ланцюга зберігання цифрових доказів може призвести до втрати їх доказового значення у судовому процесі.

У зв'язку з цим особливої актуальності набуває створення комплексних систем захисту інформації для підрозділів цифрової криміналістики. Такі системи повинні забезпечувати не лише конфіденційність, цілісність і доступність інформації, а й відповідати вимогам кримінального процесуального

законодавства щодо збереження автентичності доказів. Важливими складовими такого захисту є контроль доступу, журналювання дій користувачів, криптографічний захист даних та підтримання безперервного ланцюга володіння доказами.

Актуальність теми кваліфікаційної роботи зумовлена необхідністю забезпечення надійного захисту цифрових доказів у діяльності експертно-криміналістичних підрозділів. Сучасні інформаційні системи відділів цифрової криміналістики обробляють значні обсяги конфіденційної інформації, включаючи персональні дані, матеріали кримінальних проваджень та результати судових експертиз. За відсутності належних механізмів захисту існує ризик несанкціонованого доступу, модифікації або витоку інформації, що може негативно вплинути на результати розслідування.

Об’єктом проєктування у кваліфікаційній роботі є інформаційна система відділу цифрової криміналістики Хмельницького НДЕКЦ МВС України.

Для виконання умов завдання в роботі вирішуються такі задачі:

– аналіз особливостей функціонування відділу цифрової криміналістики та специфіки роботи з цифровими доказами;

– дослідження нормативно-правових вимог щодо забезпечення автентичності, цілісності та допустимості цифрових доказів;

– визначення категорій інформації та аналіз аналіз процесів зберігання, обробки й передачі доказових даних;

– побудова моделі загроз та моделі порушника;

– обґрунтування вибору заходів захисту цифрових доказів;

– оцінювання ефективності запропонованої системи захисту.

Практичне значення роботи полягає у можливості використання запропонованих рішень під час створення або вдосконалення систем захисту інформації у підрозділах цифрової криміналістики, діяльність яких пов’язана з обробкою цифрових доказів та іншої інформації з обмеженим доступом.

1 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА НОРМАТИВНОЇ БАЗИ

1.1 Характеристика відділу цифрової криміналістики як об'єкта інформаційної діяльності та поняття цифрового доказу

Відділ цифрової криміналістики є спеціалізованим підрозділом, діяльність якого спрямована на забезпечення повного циклу роботи з цифровими доказами від моменту їх виявлення та вилучення до формування експертного висновку та передачі матеріалів у процесуальні органи. Його функціонування відбувається на стику інформаційних технологій, кримінального процесуального права та систем забезпечення інформаційної безпеки, що зумовлює комплексний характер організації роботи [1].

На відміну від традиційних криміналістичних підрозділів, які мають справу з фізичними речовими доказами, цифрова криміналістика оперує даними, що існують у віртуальному середовищі та можуть бути представлені у вигляді файлів, системних журналів, мережевого трафіку, образів накопичувачів, хмарних сховищ або мобільних додатків. Така специфіка визначає принципово інший підхід до збереження та обробки доказової інформації. Цифровий доказ не має сталих фізичних характеристик і може бути змінений без видимих ознак втручання, що суттєво підвищує вимоги до процедур його фіксації та контролю цілісності [2].

Функціонування підрозділу передбачає суворе дотримання принципу збереження автентичності доказів. Будь-яке втручання в цифрове середовище потенційно може призвести до модифікації метаданих, зміни часових міток або перезапису інформації. Саме тому процес вилучення та дослідження повинен здійснюватися із застосуванням спеціалізованих програмно-апаратних засобів, що забезпечують створення точних бітових копій носіїв без впливу на оригінал. Уся подальша робота здійснюється виключно з копіями, а контроль незмінності даних реалізується через використання криптографічних механізмів перевірки цілісності [3].

Особливістю діяльності відділу є також необхідність забезпечення

безперервного контролю над доказом протягом усього періоду його зберігання та використання. Кожна операція з доказом повинна бути зафіксована, а відповідальна особа зобов'язана бути ідентифікованою. Таким чином формується ланцюг зберігання доказів, який має процесуальне значення та впливає на допустимість матеріалів у судовому провадженні. Порушення цього ланцюга, навіть формальне, може стати підставою для визнання доказів недопустимими [4]. Крім того, відсутність належного контролю за процесами отримання, передачі та зберігання цифрових доказів створює ризик втрати їх цілісності та автентичності, що може негативно вплинути на результати експертного дослідження та об’єктивність судового розгляду.

Ще однією характерною рисою функціонування підрозділу є підвищений рівень конфіденційності інформації. У цифрових доказах можуть міститися персональні дані, службова інформація, комерційна таємниця або відомості, що становлять державну таємницю. У зв'язку з цим відділ цифрової криміналістики фактично виконує функції об'єкта інформаційної діяльності з обробкою інформації з обмеженим доступом. Це означає, що організація його роботи повинна відповідати вимогам нормативно-правових актів у сфері технічного та криптографічного захисту інформації [5].

Інфраструктура підрозділу має багаторівневу структуру і охоплює фізичний, прикладний та організаційно-керуючий рівні. На фізичному рівні розміщуються ізольовані робочі місця експертів та засоби зберігання доказів, відокремлені від загальної мережі установи. Прикладний рівень представлений спеціалізованим програмним забезпеченням для цифрової криміналістики та засобами криптографічного захисту. Організаційно-керуючий рівень визначає систему розмежування повноважень, аудиту дій та реагування на інциденти на основі принципу мінімізації привілеїв [6].

Важливим аспектом є наявність внутрішніх ризиків, працівники підрозділу мають легітимний доступ до значного обсягу чутливої інформації, що формує потенційну загрозу внутрішнього порушника. Відповідно до Закону України «Про Національну поліцію», підрозділи кіберполіції та криміналістики

зобов'язані забезпечувати захист оброблюваної інформації з урахуванням актуального стану загроз, а відповідно до Закону України «Про судову експертизу», судово-експертна діяльність здійснюється на принципах законності, незалежності та повноти дослідження [7,8].

Аналіз існуючих рішень щодо побудови систем захисту цифрових доказів дозволяє виділити кілька домінуючих підходів, які різняться за рівнем ізоляції, централізації та методами контролю доступу. Основним архітектурним рішенням для об’єктів класу «1» (окреме автоматизоване робоче місце) є концепція повної фізичної ізоляції. На таких робочих станціях розгортаються спеціалізовані комерційні комплекси для криміналістичного аналізу, такі як EnCase Forensic або FTK Forensic Toolkit, а також інструментарій з відкритим вихідним кодом [9–11]. Такий підхід мінімізує ризик віддаленого втручання, проте вимагає суворого дотримання міжнародних стандартів обробки цифрових доказів [12].

Іншим поширеним рішенням є впровадження логічної сегментації мережі на базі технології VLAN у поєднанні з апаратними міжмережевими екранами та системами запобігання вторгненням (IPS). Це дозволяє інтегрувати робочі станції експертів у загальну інфраструктуру установи при збереженні високого рівня захищеності. У частині зберігання інформації рішення поділяються на децентралізовані, де кожен експерт використовує локальні захищені сховища з апаратним шифруванням, та централізовані (рішення класу «Захищений диск»), що забезпечують колективну роботу над великими масивами даних, але потребують впровадження складних механізмів автентифікації [13].

Сучасні комплексні рішення також базуються на використанні засобів суворого контролю доступу, таких як двофакторна автентифікація з використанням апаратних токенів, та систем безперервного аудиту подій (SIEM), що гарантують невідворотність реєстрації будь-яких дій із доказовою базою. Вибір конкретного рішення залежить від обсягу завдань підрозділу та необхідного рівня атестації комплексної системи захисту інформації. Порівняльна характеристика найбільш розповсюджених інструментальних засобів, що реалізують дані рішення, наведена в таблиці 1.1.

Таблиця 1.1 – Порівняльний аналіз засобів захисту цифрових доказів

Засіб	Тип	Призначення та ключові функції	Ліцензія / Сертифікат UA	Придатність для держорганів України
1	2	3	4	5
EnCase Forensic	Комерційний	Побітове копіювання, аналіз ФС, відновлення даних, формат E01/Ex01 з контролем CRC32+MD5	Комерційна; сертифікату Держспецзв'язку немає	Обмежено (без атестації КСЗІ)
FTK (Forensic Toolkit)	Комерційний	Централізована архітектура, паралельний аналіз, підтримка E01/DD, автоматичний збір артефактів	Комерційна; потребує мережевого сервера ліцензій	Не придатний для АС кл. «1»
Autopsy / Sleuth Kit	Відкритий	Аналіз NTFS/FAT/EXT, відновлення файлів, пошук за хешами, відкритий код для верифікації	Безкоштовна (Apache 2.0); сертифікату немає	Допускається як допоміжний засіб
Tableau T8u (Guidance)	Апаратний	Апаратний write-blocker: SATA/SAS/USB 3.0/IDE; журнал підключень; індикатор захисту	Рекомендований SWGDE та NIST 800-86	Так (рекомендований стандарт)
Програмний write-blocker	Програмний	Блокування запису через параметр Start	Немає (штатний засіб ОС)	Допоміжний (не основний)

Кінець таблиці 1.1

1	2	3	4	5
ІІТ Захищений диск-4	КЗІ (UA)	Прозоре шифрування за ДСТУ 7624 (AES-256), двофакторна автентифікація, розмежування дисків	Позитивний висновок Держспецзв'язку України	Так (єдиний варіант для атест. КСЗІ)
BitLocker (Microsoft)	Комерційний (вбудований)	Шифрування системного / логічного розділу; відсутнє розмежування ключів за ролями	Без сертифікату Держспецзв'язку України	Заборонений в атестованих КСЗІ
VeraCrypt	Відкритий	Шифрування контейнерів і розділів; відкритий код; без підтримки апаратних токенів UA	Без сертифікату Держспецзв'язку України	Заборонений в атестованих КСЗІ

Цифровізація суспільства спричинила кардинальні зміни у способах вчинення правопорушень та методах їх розслідування. Сучасні злочини все частіше пов'язані з використанням комп'ютерних систем, мобільних пристроїв, хмарних сервісів і комунікаційних мереж. У зв'язку з цим у межах криміналістики сформувався окремий напрям, а саме цифрова криміналістика, що спеціалізується на роботі з електронними слідами. Дані про способи вчинення кіберзлочинів та методи їх розслідування систематизуються у Будапештській конвенції про кіберзлочинність [14].

Поняття цифрового доказу охоплює будь-які відомості, зафіксовані у цифровій формі, які можуть підтверджувати або спростовувати факти, що мають значення для кримінального провадження. На відміну від традиційних доказів, цифрові дані не мають фізично стабільної форми, а лише існують у вигляді електронних сигналів, записів у пам'яті пристроїв або передаються мережею. До

таких доказів належать не лише окремі файли, а й системні журнали, метадані, історія мережевої активності, резервні копії та навіть інформація, що тимчасово зберігається в оперативній пам'яті [15, 16].

Суттєвою особливістю цифрових доказів є їхня залежність від середовища існування. Один і той самий файл може мати різне значення залежно від контексту: часу створення, місця зберігання, пов'язаних процесів або користувача, який з ним працював. Саме тому цифрова криміналістика передбачає не лише вилучення інформації, а й відновлення повної картини її функціонування у відповідному середовищі. Інструменти класу EnCase Forensic дозволяють відтворювати таке цифрове середовище для дослідження [17].

Цифрові докази характеризуються рядом специфічних властивостей, які ускладнюють роботу з ними. Насамперед це їхня висока чутливість до змін: навіть звичайне відкриття файлу або підключення носія до системи може призвести до зміни службових атрибутів, таких як час останнього доступу. Настанови SWGDE зазначають, що будь-яке необережне втручання може знищити або спотворити важливу інформацію [18].

Ще однією важливою рисою є можливість точного копіювання без втрати змісту. На відміну від фізичних об'єктів, цифрові дані можуть бути відтворені ідентично без жодної деградації. З одного боку, це полегшує створення резервних копій, а з іншого це ускладнює встановлення оригіналу та перевірку автентичності доказу. Настанови NIST щодо інтеграції криміналістичних технік описують механізми забезпечення ідентичності копії оригіналу через верифікацію контрольних значень [19].

Не менш важливим є забезпечення ланцюга зберігання доказів. Це документований процес, який фіксує кожну дію з доказом: хто, коли і з якою метою здійснював доступ до нього. НД ТЗІ 1.1-003-99 визначає термінологічну базу у сфері захисту інформації, яка використовується при документуванні таких процедур. Порушення ланцюга зберігання може призвести до втрати доказової сили навіть за наявності технічно коректних даних [20]. Використання смарт-контрактів та блокчейну дозволяє створити децентралізоване, криптографічно

захищене середовище для незмінної фіксації кожного кроку взаємодії з цифровим доказом, гарантуючи його процесуальну цілісність без ризику внутрішніх маніпуляцій [21].

Складність роботи з цифровими доказами також зумовлена їх розподіленістю. Дані можуть зберігатися одночасно на кількох пристроях або в хмарних середовищах, які фізично знаходяться в різних юрисдикціях. Експерти стикаються з проблемою децентралізації та ізоляції даних, а також із залежністю від постачальників хмарних послуг при отриманні доступу до віртуальних машин, що вимагає застосування новітніх методів віддаленого збору доказів [22]. Закон України «Про електронні документи та електронний документообіг» встановлює правовий статус електронних документів, що є підставою для їх визнання як доказів [23].

Крім технічних аспектів, важливе значення мають правові вимоги. Цифровий доказ повинен відповідати загальним принципам доказування: бути належним, допустимим, достовірним і достатнім. Закон України «Про електронні довірчі послуги» визначає механізми забезпечення автентичності електронних документів через кваліфікований електронний підпис та часові мітки, що безпосередньо впливає на допустимість цифрових доказів у судовому провадженні [24]. Цифрові докази є особливим видом доказової інформації, який поєднує технічну складність із високими вимогами до процесуального оформлення. Їх ефективне використання можливе лише за умови дотримання комплексного підходу, що включає правильне вилучення, надійне збереження, точний аналіз і юридично коректне представлення результатів.

1.2 Аналіз законодавчої та нормативної бази захисту цифрових доказів

Функціонування відділу цифрової криміналістики нерозривно пов'язане з обробкою інформації з обмеженим доступом, до якої належать таємниця слідства, комерційна таємниця, службова інформація, а також персональні дані

фізичних осіб. Особливістю діяльності підрозділу є те, що така інформація не лише підлягає захисту відповідно до законодавства у сфері інформаційної безпеки, але й має процесуальне значення як доказ у кримінальному провадженні. Це зумовлює необхідність одночасного виконання вимог інформаційного та кримінального процесуального законодавства [25].

Формування ефективної системи роботи з цифровими доказами неможливе без належного нормативно-правового регулювання. В Україні законодавча база у цій сфері перебуває на етапі активного розвитку, що зумовлено зростанням кількості правопорушень, пов'язаних із використанням інформаційних технологій. Водночас чинне законодавство вже містить низку положень, які прямо або опосередковано регламентують порядок обігу, обробки та захисту цифрових доказів [26].

Ключовим нормативним актом, що визначає загальні засади доказування у кримінальному провадженні, є Кримінальний процесуальний кодекс України. У ньому встановлено поняття доказів, їх допустимість, належність та порядок отримання. Хоча термін «цифровий доказ» безпосередньо не завжди використовується, положення кодексу поширюються і на інформацію, що зберігається в електронній формі. Зокрема, електронні документи, дані з інформаційних систем та інші цифрові відомості визнаються джерелами доказів за умови дотримання процесуальних вимог.

Нормативну основу організації захисту інформації в ІКС відділу цифрової криміналістики становлять Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-комунікаційних системах», Закон України «Про захист персональних даних», а також, у разі обробки відповідних категорій відомостей, Закон України «Про державну таємницю». Вказані нормативні акти визначають правові засади обробки інформації, встановлюють вимоги до забезпечення її конфіденційності, цілісності та доступності, а також регламентують права та обов'язки володільців і розпорядників інформаційних ресурсів.

Відповідно до Закону України «Про захист інформації в інформаційно-

телекомунікаційних системах», інформація, яка є власністю держави або підлягає захисту згідно із законом, повинна оброблятися в системі з побудованою КСЗІ. Порядок створення та впровадження КСЗІ визначається нормативними документами системи ТЗІ: НД ТЗІ 2.5-005-99 встановлює класифікацію АС та профілі захищеності; НД ТЗІ 2.5-004-99 визначає критерії оцінки захищеності; НД ТЗІ 3.7-003-2005 регламентує порядок проведення робіт зі створення КСЗІ [27 – 29]. Нові нормативні документи НД ТЗІ 3.6-004-21, НД ТЗІ 3.6-005-21 та НД ТЗІ 3.6-006-24 встановлюють сучасні підходи до категоріювання ІС та вибору заходів захисту [30–32].

НД ТЗІ 3.6-007-21 визначає порядок впровадження відібраних заходів захисту, а НД ТЗІ 2.3-025-21 встановлює методику оцінювання їх ефективності після реалізації [33, 34]. Ці документи утворюють нормативне підґрунтя для атестаційних випробувань КСЗІ. Управління ризиками інформаційної безпеки регламентується ISO/IEC 27005:2022, що визначає процес ідентифікації, аналізу та оцінювання ризиків [35].

Особливе місце в аналізі нормативних вимог займають положення КПК України щодо електронних доказів. Електронні докази визнаються процесуальними джерелами доказів, однак їх допустимість визначається з урахуванням загальних критеріїв доказування. Типове положення про службу захисту інформації в автоматизованій системі НД ТЗІ 1.4-001-2000 встановлює організаційну основу для функціонування СЗІ у підрозділах, що обробляють ІзОД [36].

Ключовою вимогою до ІКС є забезпечення безперервності ланцюга зберігання доказів. На практиці це означає, що система повинна фіксувати всі дії з цифровим доказом: створення образу носія, обчислення контрольних хеш-значень, доступ експертів, копіювання, передачу результатів дослідження. Відповідні журнали реєстрації мають зберігатися в захищеному вигляді та бути недоступними для несанкціонованого редагування.

Під час дослідження вилучених комп'ютерів, мобільних пристроїв або серверного обладнання експерти неминуче обробляють персональні дані

підозрюваних, свідків, потерпілих та інших осіб. Відповідно до Закону України «Про захист персональних даних», відділ цифрової криміналістики може виступати володільцем або розпорядником баз персональних даних, що накладає обов'язок забезпечити їх захист від незаконної обробки, втрати або розголошення. Правовою підставою для обробки персональних даних у кримінальному провадженні є норми закону та процесуальні рішення, зокрема ухвали слідчого судді.

Передавання матеріалів слідчому, прокурору або суду має здійснюватися з використанням захищених каналів зв'язку або криптографічних засобів захисту інформації. Закон України «Про електронні документи та електронний документообіг» та Закон України «Про електронні довірчі послуги» визначають механізми використання електронного підпису та часових міток, що забезпечують автентичність і цілісність цифрових даних при їх передаванні.

Окрім національного законодавства, важливе значення мають міжнародні стандарти. Україна є учасницею Конвенції про кіберзлочинність, яка регламентує порядок збирання електронних доказів. ISO/IEC 27037:2012 визначає настанови щодо ідентифікації, збору, отримання та збереження цифрових доказів, а SWGDE формують кращі практики роботи з електронними даними у правоохоронній діяльності. Окрім цього, Європейське агентство з кібербезпеки публікує власні рекомендації щодо поводження з електронними доказами, адаптовані до потреб транскордонної співпраці. Настанови ENISA спрямовані на гармонізацію технічних процедур фіксації даних для полегшення їх взаємного визнання правоохоронними органами різних європейських юрисдикцій [37]. Логічним доповненням цього процесу є стандарт ISO/IEC 27042:2015, який надає керівні принципи безпосередньо щодо аналізу та інтерпретації цифрових доказів. Він регламентує методи забезпечення наукової обґрунтованості, повторюваності та відтворюваності результатів експертного дослідження, що є критично важливим критерієм для їх оцінки в суді [38].

Аналіз нормативних вимог свідчить про те, що ІКС відділу цифрової криміналістики повинна відповідати одночасно двом групам вимог: вимогам

інформаційної безпеки та вимогам кримінального процесуального законодавства. З одного боку, система має забезпечувати конфіденційність, цілісність і доступність інформації відповідно до законодавства у сфері ТЗІ. З іншого боку, вона повинна гарантувати автентичність, відтворюваність та процесуальну допустимість цифрових доказів. Така подвійна нормативна природа діяльності зумовлює необхідність створення атестованої КСЗІ.

Чинна законодавча база, попри її розвиненість, має і певні прогалини: відсутнє чітке та уніфіковане визначення поняття «цифровий доказ» у процесуальному праві, а механізм міжвідомчої взаємодії між правоохоронними органами та судовими експертними установами потребує стандартизації. Крім того, нові технологічні середовища, зокрема хмарні сервіси та розподілені мережі, не завжди охоплені чинними нормативними актами.

1.3 Категорії інформації та аналіз інформаційних потоків у відділі цифрової криміналістики

Об'єктом інформаційної діяльності у цій роботі є відділ цифрової криміналістики Хмельницького науково-дослідного експертно-криміналістичного центру МВС (НДЕКЦ МВС), розташований за адресою: м. Хмельницький, вул. Молодіжна, 12, кабінет № 101 (другий поверх). Хмельницький науково-дослідний експертно-криміналістичний центр Міністерства внутрішніх справ України є державною спеціалізованою установою, що входить до складу Експертної служби МВС та здійснює судово-експертне забезпечення досудового розслідування і судового розгляду кримінальних проваджень. Головним завданням установи є проведення незалежних, об'єктивних та науково обґрунтованих судових експертиз, серед яких комп'ютерно-технічні, комунікаційні, трасологічні, балістичні та інші види досліджень. Як об’єкт інформаційної діяльності, центр характеризується безперервним циклом обробки значних масивів даних, отриманих під час огляду

місць подій та вилучення речових доказів. Специфіка роботи установи вимагає використання сучасних апаратно-програмних комплексів, що дозволяють не лише отримувати цифрові сліди, а й гарантувати їхню цілісність, автентичність та юридичну значимість для подальшого використання у суді.

Увесь масив даних, що обробляється у відділі, доцільно класифікувати за функціональним та правовим критеріями. Найвищий рівень критичності мають цифрові докази, які включають побайтові образи накопичувачів, дампи оперативної пам'яті, мережеві логи та інші результати фіксації цифрового середовища. Для цієї категорії пріоритетною властивістю є цілісність, оскільки навіть мінімальна модифікація даних призводить до втрати їх доказового значення. Вимоги до доступності для цієї категорії мають контрольований характер: дані повинні бути доступними лише уповноваженим експертам у визначений період часу [39].

Окрему категорію становлять процесуальні та службові документи: постанови про призначення експертизи, внутрішні акти та фінальні висновки експертів. Для цієї групи однаково важливими є конфіденційність і цілісність [40].

Третьою категорією є персональні дані фізичних осіб, вилучені під час дослідження технічних пристроїв, для яких домінуючою властивістю безпеки є конфіденційність відповідно до вимог Закону України «Про захист персональних даних».

Окремо виділяють технологічну інформацію КСЗІ, а саме журнали аудиту, параметри конфігурації, криптографічні ключі, для якої критичними є всі три властивості безпеки [41].

Загальна класифікація засобів захисту цифрових доказів за функціональним призначенням наведена на рисунку 1.1.

Після визначення категорій інформації необхідним є аналіз інформаційних потоків, що відображають її рух у межах ІКС відділу. Дослідники у сфері цифрової криміналістики виділяють три стадії руху доказової інформації [42].

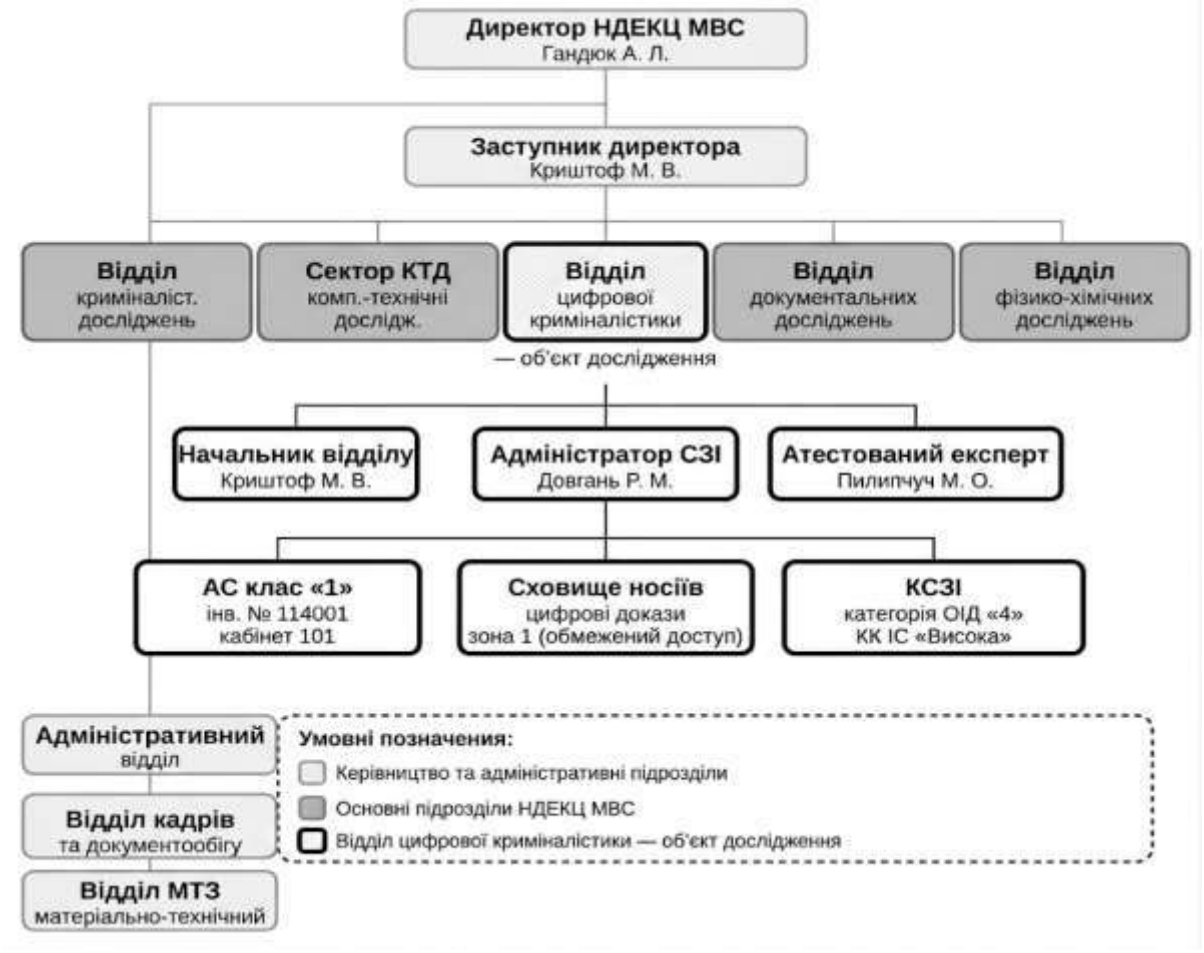


Рисунок 1.1 – Організаційна структура Хмельницького НДЕКЦ МВС

Перша стадія охоплює приймання та первинну обробку даних, під час якої носії або електронні дані копіюються у цифрові образи з обчисленням хеш-значень для фіксації їхнього стану. Основні ризики пов'язані з підключенням носіїв і передачею даних до захищеного сховища.

Друга стадія передбачає внутрішнє дослідження цифрових образів експертами без можливості їх зміни. На цьому етапі головними загрозами є несанкціоноване копіювання, витік інформації та перевищення службових повноважень, тому необхідні механізми контролю доступу й журналювання дій.

Третя стадія включає формування та передачу експертного висновку через захищені канали зв'язку або криптографічно захищені носії. Основними ризиками є перехоплення, підміна чи несанкціоноване поширення матеріалів.

Схема інформаційних потоків відділу цифрової криміналістики наведена на рисунку 1.2.

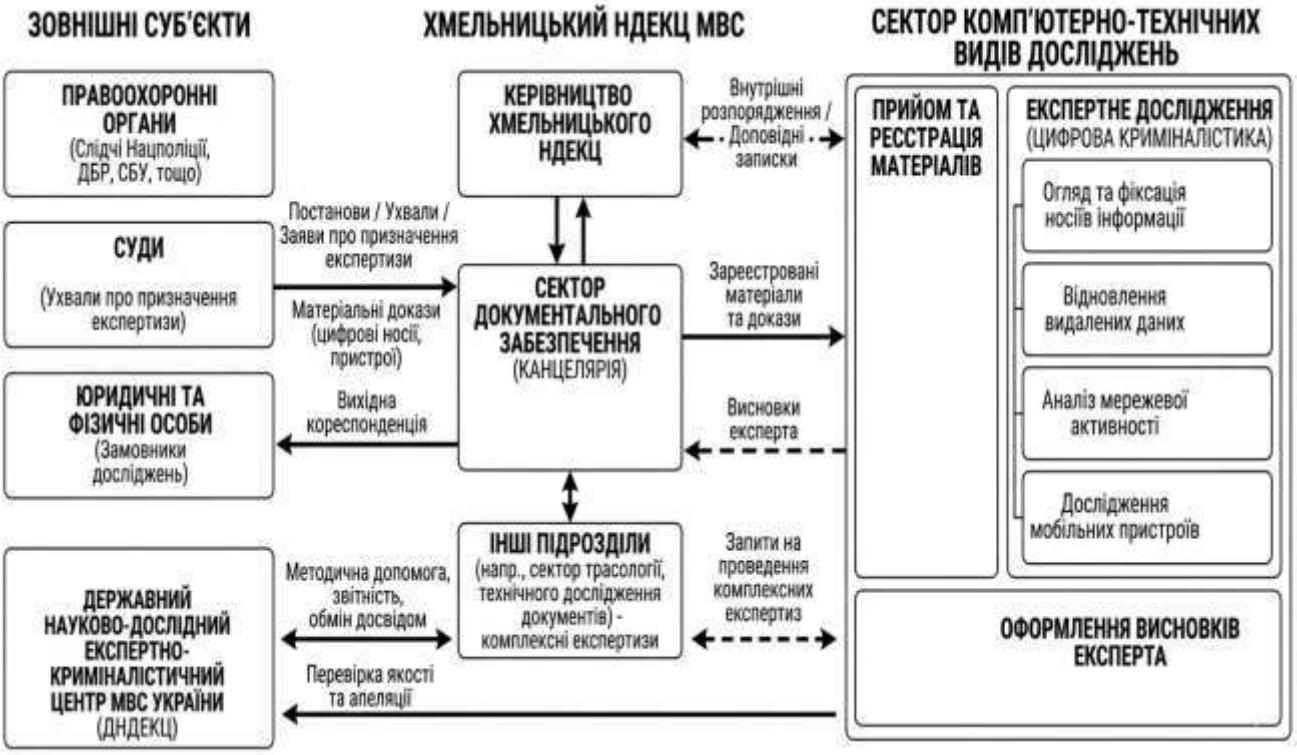


Рисунок 1.2 – Схема інформаційних потоків відділу цифрової криміналістики Хмельницького НДЕКЦ МВС

Таким чином, проведений аналіз демонструє, що інформаційні потоки у відділі цифрової криміналістики мають чітко виражену багатоступеневу структуру, а кожна категорія даних характеризується власним рівнем критичності за показниками конфіденційності, цілісності та доступності. Особливої уваги при цьому вимагають дані, отримані з пристроїв Інтернету речей (IoT), специфіка яких, від нестандартних протоколів шифрування до обмежених ресурсів збереження, потребує розширення підходів до криміналістичного аналізу та спеціалізованих заходів безпеки [43]. Важливо розуміти, що ступінь надійності КСЗІ прямо впливає на доказовість інформації: чим глибше інтегровані механізми захисту, тим меншою є вірогідність успішного оспорювання отриманих результатів під час судового розгляду. Отримані результати є вихідною основою для визначення вимог до архітектури КСЗІ, формування моделі загроз та розроблення профілю захищеності ІКС [44].

1.4 Постановка задачі захисту інформації

Проведений аналіз особливостей функціонування відділу цифрової криміналістики Хмельницького НДЕКЦ МВС, його інформаційно-телекомунікаційної структури, нормативно-правових вимог, а також категорій оброблюваної інформації та інформаційних потоків дозволяє зробити висновок про підвищений рівень вимог до забезпечення інформаційної безпеки в межах даного підрозділу.

Встановлено, що діяльність відділу пов'язана з обробкою критично важливих інформаційних ресурсів, зокрема цифрових доказів, персональних даних та процесуальних документів, для яких визначальними є вимоги до забезпечення цілісності, конфіденційності та контрольованого доступу. Особливу роль відіграє необхідність збереження доказових властивостей інформації, що передбачає гарантування її автентичності, незмінності та можливості відтворення результатів дослідження. Порушення зазначених вимог може призвести до втрати доказової сили та негативно вплинути на результати кримінального провадження [45].

Аналіз інформаційних потоків показав, що обробка даних у відділі здійснюється в межах складного багатостадійного процесу, який включає етапи приймання, дослідження та передачі результатів. На кожному з цих етапів існують потенційні вразливості, пов'язані з несанкціонованим доступом, модифікацією або витоком інформації. Стандарт ISO/IEC 27035 щодо управління інцидентами встановлює, що особливу небезпеку становлять як зовнішні, так і внутрішні загрози від користувачів, що мають легітимний доступ до ресурсів [46]. Враховуючи високу критичність внутрішніх загроз, передові підходи до проєктування безпеки в експертних середовищах поступово переходять до моделі нульової довіри. Її впровадження передбачає відмову від концепції захищеного внутрішнього периметра, а отже кожна транзакція або спроба доступу до доказової бази вимагає безперервної криптографічної верифікації та суворого моніторингу контексту запиту [47].

Нормативний аналіз показав, що ІКС відділу повинна функціонувати відповідно до вимог законодавства України у сфері захисту інформації та обробки персональних даних, а також відповідати положенням нормативних документів ТЗІ. NIST SP 800-53 визначає комплексні вимоги до засобів контролю безпеки та конфіденційності для інформаційних систем, що є орієнтиром при визначенні заходів захисту [48].

Разом з тим, існуючі підходи до організації захисту інформації у подібних підрозділах часто не враховують специфіку роботи з цифровими доказами, зокрема необхідність забезпечення безперервності ланцюга їх зберігання, гарантування цілісності на рівні бітових образів та забезпечення повного аудиту доступу до інформації. Оперативно-розшукова діяльність та криміналістична практика свідчать про необхідність розроблення спеціалізованих підходів до захисту доказової бази [49].

У зв'язку з цим метою цієї роботи є розроблення КСЗІ для відділу цифрової криміналістики Хмельницького НДЕКЦ МВС, яка забезпечує захист цифрових доказів та супутньої інформації від несанкціонованого доступу, модифікації та витоку, а також відповідає вимогам чинного законодавства та нормативних документів. Для досягнення зазначеної мети вирішуються такі задачі: провести аналіз структури та умов функціонування відділу; визначити категорії інформаційних ресурсів та інформаційних потоків; побудувати модель загроз і модель порушника; обґрунтувати вибір профілю безпеки та заходів захисту; розробити технічне завдання на створення КСЗІ та провести оцінювання її ефективності [50].

2 ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ ЦИФРОВИХ ДОКАЗІВ

2.1 Методологія створення середовища для роботи з цифровими доказами та забезпечення їх цілісності

Створення комплексної системи захисту інформації є нормативно регламентованим процесом, який виконується у чіткій послідовності етапів відповідно до НД ТЗІ 3.7-003-2005 та НД ТЗІ 3.6-004-21. Першим етапом є передпроєктне обстеження, яке передбачає категоріювання об'єкта інформаційної діяльності, обстеження інформаційно-комунікаційної системи та розроблення технічного завдання. Другим етапом можна виділити проєктування, яке охоплює формування цільового профілю безпеки та вибір конкретних заходів захисту. Третім етапом є впровадження та атестація, яке включає практичну реалізацію заходів і підтвердження відповідності системи вимогам ТЗ.

Ключовою особливістю проєктування КСЗІ для відділу цифрової криміналістики є подвійна нормативна природа вимог: з одного боку це технічні вимоги системи ТЗІ щодо захисту інформації з обмеженим доступом, з іншого ж процесуальні вимоги КПК України до автентичності та допустимості цифрових доказів. Це означає, що при виборі заходів захисту недостатньо задовольнити лише стандартний базовий профіль безпеки, а також необхідно додатково врахувати специфічні вимоги криміналістичного середовища, зокрема обов'язковість апаратного захисту від запису при роботі з носіями доказів та криптографічну верифікацію цілісності образів на кожному етапі їх обробки.

Фундаментальною основою забезпечення цілісності цифрових доказів у процесі їх зберігання в межах АС є технологія хешування. На відміну від типових інформаційних систем, де контроль цілісності є допоміжним сервісом безпеки, у цифровій криміналістиці застосування криптографічних алгоритмів хешування виступає базовим інструментом підтвердження автентичності даних. Кожен цифровий об’єкт при потраплянні до системи отримує унікальний "цифровий відбиток", який залишається незмінним протягом усього життєвого циклу дослідження. Процедура зберігання передбачає обов'язкову верифікацію

контрольних сум перед початком та після завершення будь-яких маніпуляцій із даними, що дозволяє математично довести відсутність навіть мінімальних (побітових) змін у структурі доказу. Таким чином, проєктована система зберігання розглядається не просто як сховище файлів, а як цілісне доказове середовище, де будь-яка спроба несанкціонованого доступу або випадкового спотворення даних буде негайно виявлена шляхом розбіжності значень хеш-функцій. Це забезпечує виконання процесуальної вимоги щодо незмінності доказової бази від моменту її фіксації до представлення результатів у суді.

Важливою особливістю об’єктів зберігання у межах проєктованої системи є те, що робота ведеться не з окремими файлами, а з повними криміналістичними образами носіїв інформації (Forensic Images). Використання спеціалізованих форматів, таких як .E01 (EnCase Evidence File) або .raw (DD-образ), дозволяє створити ідентичну копію фізичного накопичувача на бітовому рівні. На відміну від звичайного копіювання файлової системи, криміналістичний образ включає не лише видимі дані, а й нерозмічені області (unallocated space), зарезервовані сектори та залишки видалених файлів (slack space), що мають критичне значення для проведення експертного дослідження. Такий підхід до зберігання гарантує, що експерт працює у безпечному віртуальному середовищі, яке повністю дублює стан оригінального носія на момент його вилучення. Це дозволяє багаторазово проводити аналіз без ризику пошкодження первинного речового доказу та забезпечує можливість перевірки результатів іншими експертами або сторонами процесу, що є невід’ємною умовою забезпечення прозорості та об’єктивності цифрової криміналістики.

Процес зберігання цифрових доказів у межах проєктованого середовища має дворівневу структуру, що поєднує методи фізичного та логічного захисту. Фізичне зберігання стосується безпосередньо первинних носіїв інформації (речових доказів), таких як накопичувачі, мобільні пристрої або карти пам’яті. Після процедури клонування та фіксації ці носії повинні зберігатися у спеціалізованих сейфах або шафах із контрольованим рівнем доступу, що захищає їх від механічних пошкоджень, впливу електромагнітних полів та

несанкціонованого вилучення.

Паралельно з цим реалізується логічне зберігання, яке охоплює роботу з цифровими копіями на базі захищеної експертної станції або спеціалізованого сервера. На цьому рівні захист забезпечується технічними засобами: криптографічним шифруванням контейнерів із даними, суворим розмежуванням прав доступу (RBAC) та безперервним логуванням усіх маніпуляцій. Такий розподіл функцій дозволяє реалізувати ключовий принцип цифрової криміналістики, а саме мінімізацію прямої взаємодії з оригінальним носієм. Використання верифікованих логічних копій для аналізу гарантує збереження первинного речового доказу в незмінному стані, що є критично важливим для підтримання ланцюжка довіри до результатів експертизи.

На першому етапі розроблено комплект організаційно-розпорядчих документів, що є нормативною передумовою для будь-яких подальших робіт зі створення КСЗІ. Перелік та призначення цих документів визначаються НД ТЗІ 1.6-005-13 і НД ТЗІ 3.7-003-2005. Без їх наявності неможливо ані сформувати цільовий профіль безпеки, ані провести атестаційні випробування КСЗІ.

Наказ про створення СЗІ (Додаток Б) та Положення про СЗІ (Додаток В) встановлюють організаційну структуру захисту, а саме визначають трьох суб'єктів КСЗІ і розмежовують їхні повноваження. Керівник СЗІ (начальник відділу Криштоф М. В.) несе повну юридичну відповідальність за організацію захисту інформації, а саме затверджує політику безпеки та план захисту, приймає рішення про початок або зупинку експлуатації АС-1 у разі критичних порушень, організовує службові розслідування інцидентів. Адміністратор безпеки (головний судовий експерт Довгань Р. М.) відповідає за технічне управління засобами захисту, а саме керує обліковими записами, щотижнево переглядає журнали аудиту, веде журнал обліку носіїв та журнал інцидентів, виконує резервне копіювання. Принципово важливим є те, що адміністратор безпеки не має права самостійно вносити зміни до доказових матеріалів, а користувач не може змінювати параметри захисту системи. Користувач (старший судовий експерт Пилипчук М. О.) отримує доступ лише до тих баз даних, які необхідні

для призначеної йому експертизи, і не може самостійно змінювати конфігурацію безпеки системи. Такий розподіл унеможливлює реалізацію загрози від внутрішнього порушника, який є найбільш небезпечним суб'єктом для відділу ЦК.

Наказ про створення КСЗІ (Додаток Г) та наказ про утворення комісії з категоріювання (Додаток Д) запускають формальний процес проєктування. Наказ № 3 від 15.02.2026 визначає строки, виконавців і нормативну підставу для розроблення КСЗІ. Наказ № 4 від 18.02.2026 формує склад комісії, яка уповноважена встановити категорію ОІД та задокументувати стан ІКС.

Акт категоріювання ОІД (Додаток Е), затверджений директором, встановив четверту категорію ОІД. На об'єкті здійснюється обробка інформації з грифом «Для службового користування» та конфіденційної інформації (матеріали судових експертиз, цифрові докази та персональні дані суб'єктів кримінальних проваджень). Категорія ОІД є правовою підставою для обов'язкового створення атестованої КСЗІ та визначає мінімальний рівень захищеності системи. Первинне категоріювання означає, що КСЗІ створюється вперше, а усі проєктні рішення є новими, а не оновленням існуючої системи.

Акт обстеження ОІД та ІКС (Додаток Ж) фіксує фактичний стан об'єкта на момент проєктування: фізичне середовище (кабінет №101, площа 24,75 м², периметр КЗ), апаратний склад АРМ (Fujitsu Esprimo E710, ІІТ Захищений диск-4), програмне середовище (Windows 10 Pro, EnCase Forensic) та наявні засоби захисту. Акт обстеження є єдиним документом де допустимо детально описувати фізичне середовище. Ситуаційний і генеральний плани ОІД та схема розташування основних технічних засобів наведені на рисунках 2.1–2.3.

Технічне завдання на створення КСЗІ (Додаток З), затверджене директором, є центральним документом першого етапу. На відміну від актів, які фіксують існуючий стан, ТЗ визначає вимоги до майбутньої системи, що саме і від чого повинна захищати КСЗІ, які властивості безпеки мають бути забезпечені, якому профілю захищеності система повинна відповідати і за якими критеріями буде оцінюватись її ефективність.

Рисунок 2.1 – Ситуаційний план об'єкта інформаційної діяльності

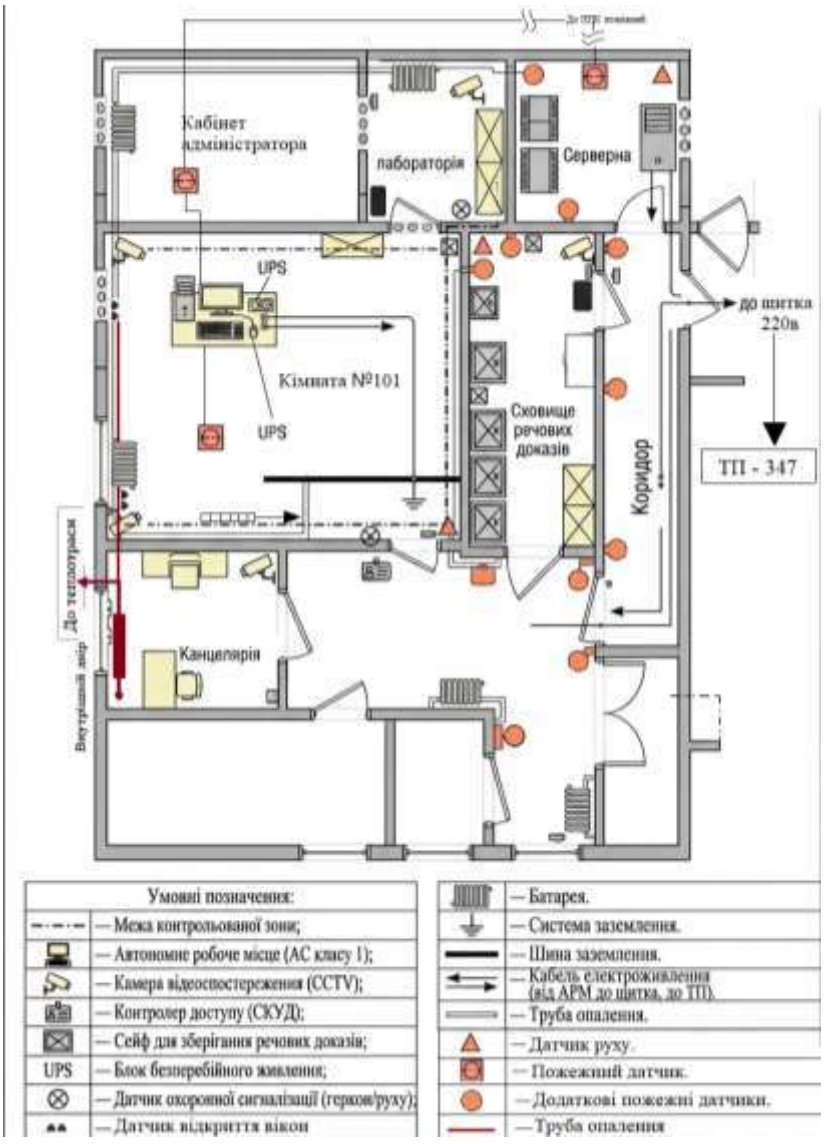


Рисунок 2.2 – Генеральний план приміщення

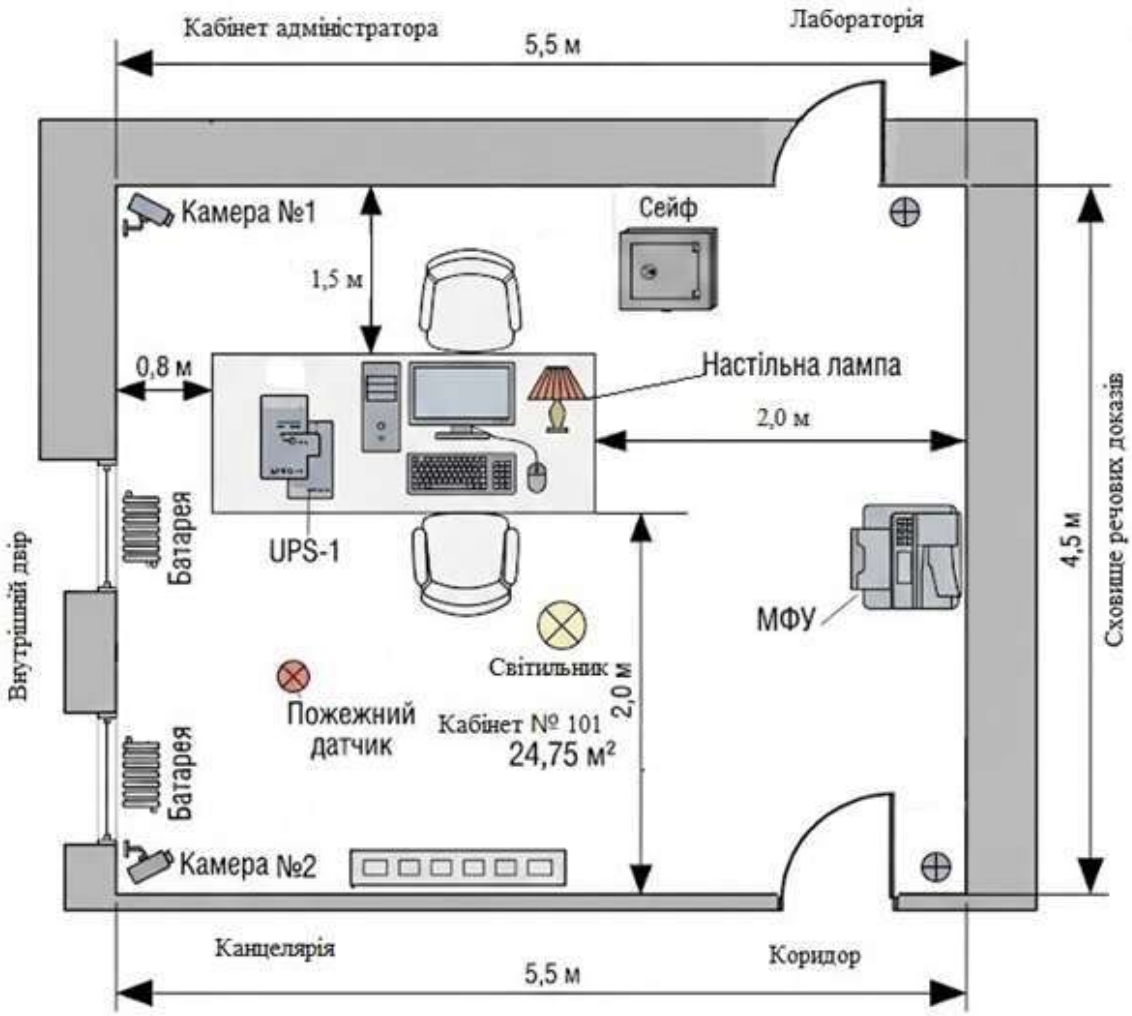


Рисунок 2.3 – Схема розташування основних технічних засобів

ТЗ є нормативно обов'язковим документом, без якого неможливо провести атестаційні випробування КСЗІ відповідно до НД ТЗІ 3.6-007-21.

У ТЗ визначено чотири групи вимог до АС-1 відділу ЦК. Вимоги до конфіденційності містять недопущення розголошення відомостей досудового розслідування та персональних даних, суворе розмежування доступу та фізична ізоляція від мереж. Вимоги до цілісності охоплюють повну ідентичність цифрових доказів від моменту отримання до формування висновку, обов'язкове хешування (SHA-256 / MD5) та використання апаратного write-blocker при кожному підключенні носія. Вимоги до доступності включають постійну готовність АРМ до проведення досліджень у законодавчо встановлені строки, забезпечення ДБЖ та регламента технічного обслуговування.

Реєстраційна картка АС (Додаток Н) та план захисту інформації (Додаток

П) завершують пакет документів першого етапу. Реєстраційна картка є офіційним обліковим документом АС-1 в Адміністрації Держспецзв'язку та є передумовою для проведення атестаційних випробувань. План захисту інформації трансформує вимоги ТЗ на конкретну програму дій. Він визначає шість послідовних етапів реалізації КСЗІ, до них відносять організаційну підготовку, обстеження ІС, розроблення документації, реалізацію заходів, випробування та введення в дію. Ключовою особливістю плану впровадження є те, що він структурований за заходами цільового профілю безпеки. Для кожного коду заходу визначено конкретний засіб реалізації, відповідальну особу та строк виконання.

Кінцевою метою усього комплекту документів першого етапу є формування цільового профілю безпеки (ЦПБ), а саме документа, який визначає вичерпний перелік заходів захисту, адаптованих до конкретних умов функціонування АС-1 відділу ЦК. ЦПБ є проміжною ланкою між загальними вимогами ТЗ і конкретними технічними налаштуваннями. Якщо ТЗ відповідає на питання «що захищати і від чого», то ЦПБ відповідає на питання «якими саме заходами». Відповідно до НД ТЗІ 3.6-006-24, ЦПБ формується на основі базового профілю безпеки рівня «Високий» з доповненням специфічних параметрів, що враховують особливості криміналістичного середовища, модель загроз та категорію оброблюваної інформації.

2.2 Аналіз загроз автентичності цифрових доказів та модель порушника в експертній лабораторії

Окремим критично важливим аспектом функціонування проєктованої системи є автоматизована підтримка ланцюжка збереження цифрових доказів (Chain of Custody). У межах розробленого середовища традиційний журнал аудиту безпеки трансформується у спеціалізований процесуальний лог роботи з об’єктами дослідження. Система в автоматичному режимі забезпечує безумовну фіксацію трьох ключових параметрів для кожної операції: ідентифікацію особи

(експерта), яка отримала доступ до захищеного контейнера з доказом; точну часову мітку кожної дії, синхронізовану з сервером точного часу; а також деталізований перелік проведених маніпуляцій (створення образу, хешування, запуск засобів аналізу тощо).

Такий рівень деталізації аудиту дозволяє відстежити повну історію поводження з цифровим доказом від моменту його імпорту до системи до формування фінального звіту. Це перетворює технічний контроль цілісності на юридичний інструмент підтвердження автентичності: будь-яка спроба анонімного або несанкціонованого доступу до матеріалів справи буде негайно зафіксована, що гарантує допустимість результатів експертизи у судовому процесі та виключає сумніви щодо можливого стороннього втручання у доказову базу.

Формування моделі загроз є обов'язковим етапом проєктування КСЗІ, що передує вибору заходів захисту. Відповідно до НД ТЗІ 1.6-005-13 та НД ТЗІ 3.6-004-21, модель загроз визначає перелік актуальних загроз для конкретної ІКС з урахуванням особливостей об'єкта та середовища функціонування. Для АС-1 відділу цифрової криміналістики актуальність загроз оцінювалась з урахуванням двох ключових чинників. По-перше, система є ізольованою (АС клас «1»), що виключає цілий клас мережевих загроз. По-друге, специфіка роботи з цифровими доказами породжує унікальні загрози цілісності, не характерні для звичайних адміністративних систем. Повна модель загроз із детальним описом наслідків та заходами протидії наведена в Додатку З.

Для кількісної оцінки загроз застосовано метод матриці ризиків, тобто кожній загрозі призначається значення ймовірності реалізації (P, від 1 до 5) та значення впливу (C, від 1 до 5), а рівень ризику (R) обчислюється як їх добуток. Загрози класифікуються за критерієм, що $R \geq 15$ відповідає рівню «Критичний», значення $10 \leq R < 15$ відповідає рівню «Високий», значення $5 \leq R < 10$ відповідає рівню «Середній». Для кожної загрози окремо визначено вплив на властивості безпеки, а саме конфіденційність (К), цілісність (Ц) та доступність (Д), що позначені символом у відповідній колонці таблиці.

Для АС класу «1» виключені як неактуальні такі загрози: несанкціоноване

підключення до мережі, перехоплення мережевого трафіку, атаки типу DDoS, а також будь-які загрози, що реалізуються виключно через мережеві канали зв'язку. Водночас з'являється специфічна загроза, що є унікальною для криміналістичного середовища, зокрема зараження АРМ шкідливим ПЗ з дисків та флеш-накопичувачів, що є безпосередніми об'єктами дослідження. Саме цей вектор є особливо небезпечним, оскільки перевірені зловмисниками диски-докази можуть містити спеціально підготовлені шкідливі програми.

Модель порушника визначає категорії осіб, що потенційно можуть здійснити несанкціоновані дії щодо ІКС, та їхні можливості. Для відділу цифрової криміналістики виділено п'ять категорій порушників, що відрізняються рівнем доступу, мотивами та характером потенційних дій.

Перша категорія являє собою авторизованого користувача (атестований експерт Пилипчук М. О.), який має легальний доступ до АРМ і доказових матеріалів у межах призначених справ. Є найнебезпечнішим з погляду цілісності тому, що може ненавмисно або умисно змінити образи носіїв при роботі без write-blocker, несанкціоновано скопіювати матеріали на особистий носій або навмисно видалити критичні докази. Мотивами можуть бути корупційна вигода (продаж інформації сторонам провадження), недбалість або зовнішній тиск з боку учасників справи. Кваліфікація цього порушника є середня.

Друга категорія – адміністратор безпеки (Довгань Р. М.), який має найширші технічні права в системі, як-от управління обліковими записами, доступ до журналів та налаштування засобів захисту. Згідно з Положенням про СЗІ (Додаток В), адміністратор безпеки не має логічного доступу до матеріалів кримінальних проваджень, лише до системних налаштувань ОС. Небезпека полягає у можливості вимкнення антивірусного захисту, модифікації журналів аудиту для приховування слідів інцидентів або несанкціонованого розширення власних привілеїв. Мотивом може бути приховане сприяння злочинним угрупованням або зловживання посадовими повноваженнями. Кваліфікація цього порушника є висока.

Третя категорія – адміністративний персонал (керівники установи,

співробітники суміжних підрозділів), який може мати тимчасовий доступ до приміщення в службових цілях. Потенційна загроза полягає у використанні адміністративних привілеїв для несанкціонованого перегляду або вилучення матеріалів без фіксації в журналі відвідувань. Кваліфікація цього порушника є змінна.

Четверта категорія – технічний персонал (електрики, прибиральники, фахівці з обслуговування будівлі), який має фізичний доступ до приміщення в супроводі уповноважених осіб, але без права роботи з АРМ. Основна загроза полягає у фізичному встановленні закладних пристроїв (апаратних кейлогерів для перехоплення паролів) або викраденні змінних носіїв у момент, коли приміщення тимчасово залишене без нагляду. Кваліфікація цього порушника є низька або середня.

П'ята категорія – стороння особа без права доступу до КЗ, який не має легального права перебувати в приміщенні (відвідувач установи або зловмисник). Реалізує переважно загрози фізичного проникнення з метою крадіжки обладнання або носіїв. Для відділу ЦК особлива небезпека полягає у вилученні SSD-накопичувача з усією доказовою базою до застосування шифрування. Мотивом є перешкоджання правосуддю або знищення доказів. Кваліфікація цього порушника є змінна.

Принциповим висновком аналізу моделі порушника є те, що найнебезпечніші загрози для відділу ЦК походять від внутрішніх суб'єктів перших двох категорій, які мають легальний доступ до системи. Саме тому організаційні заходи контролю, зокрема чітке розмежування повноважень, обов'язковий аудит дій, двопідписний порядок роботи з носіями доказів є рівнозначними за важливістю з технічними засобами захисту. В таблиці 2.1 реалізовано модель загроз для відділу цифрової криміналістики (Р – ймовірність реалізації загрози (1 – низька ... 5 – висока); С – рівень впливу (1 – незначний ... 5 – критичний); R – рівень ризику; К, Ц, Д – вплив на конфіденційність, цілісність та доступність; «×» – наявність впливу).

Таблиця 2.1 – Модель загроз АС-1 відділу цифрової криміналістики Хмельницького НДЕКЦ МВС

№	Загроза	P	C	R	Класифікація	К	Ц	Д
1	2	3	4	5	6	7	8	9
1	Несанкціонований доступ до матеріалів експертизи	4	4	16	Критичний	+	+	
2	Порушення цілісності цифрових доказів	3	5	15	Високий		+	
3	Викрадення апаратних ліцензійних ключів	2	5	10	Середній	+		+
4	Зараження АС-1 шкідливим програмним забезпеченням	4	3	12	Високий		+	+
5	Візуальний перехват інформації	2	3	6	Середній	+		
6	Інсайдерське копіювання образів дисків	2	4	8	Середній	+		
7	Втрата даних через технічну відмову	2	4	8	Середній		+	+
8	Порушення доступності через збій електроживлення	3	4	12	Високий			+
9	Несвоєчасне виявлення інцидентів	3	3	9	Середній	+	+	
10	Фізична крадіжка носіїв інформації	2	5	10	Середній	+	+	+

Аналіз моделі загроз показує, що найбільш критичною є загроза несанкціонованого доступу до матеріалів експертизи (R = 16). Її реалізація відбувається через використання слабких паролів або доступ до АРМ, залишеного без нагляду в активному стані. Загроза впливає одночасно на

конфіденційність і цілісність, оскільки зловмисник може як переглянути, так і змінити матеріали провадження. До категорії «Високий» відносяться ще три загрози, як-от порушення цілісності цифрових доказів (R = 15) через підключення носія без write-blocker, зараження шкідливим ПЗ (R = 12) через диски-докази та збій електроживлення (R = 12) під час критичного процесу копіювання.

Оцінка залишкового ризику після застосування заходів цільового профілю безпеки показує суттєве його зниження. Для загрози НСД після впровадження заходів AC-3, IA-2 та AC-11 ймовірність знижується з 4 до 1, що дає залишковий R = 4 (рівень «Низький»). Для загрози цілісності доказів після впровадження SI-7 та SC-28 залишковий R = 5. Для загрози № 4 (шкідливе ПЗ) після впровадження SI-3 та MP-7 залишковий R = 3. Таким чином, усі загрози категорій «Критичний» та «Високий» після реалізації заходів ЦПБ переходять до рівня «Низький» або «Середній», що підтверджує достатність обраних заходів захисту.

Загрози середнього рівня охоплюють широкий спектр векторів від фізичної крадіжки (R = 10) до несвоєчасного виявлення інцидентів (R = 9). Показово, що загроза несвоєчасного виявлення інцидентів впливає одночасно на конфіденційність і цілісність і є організаційною за природою. Вона усувається регулярним аналізом журналів подій, а не технічними засобами. Результати оцінки ризиків є вихідними даними для вибору пріоритетних заходів цільового профілю безпеки.

2.3 Категоріювання інформаційної системи та формування цільового профілю безпеки

Категоріювання інформаційної системи є нормативно обов'язковим кроком, що передує вибору заходів захисту. Відповідно до НД ТЗІ 3.6-005-21, категорія безпеки визначається на підставі максимального рівня критичності інформації, що обробляється в системі, за трьома властивостями, а саме конфіденційністю, цілісністю та доступністю. Результати категоріювання задокументовано в Акті

категоріювання ОІД (Додаток Е).

За результатами аналізу інформаційних ресурсів відділу цифрової криміналістики встановлено такі рівні критичності. Конфіденційність оцінено як «Висока», тобто система обробляє матеріали кримінальних проваджень, персональні дані учасників справ та відомості з грифом «Для службового користування», несанкціоноване розкриття яких може завдати суттєвої шкоди слідству. Цілісність оцінено як «Критична», тобто будь-яка несанкціонована модифікація цифрових доказів призводить до їх процесуальної недопустимості та може унеможливити судове переслідування. Доступність оцінено як «Висока», тобто система повинна бути готовою до проведення досліджень у законодавчо встановлені строки (30 днів з моменту призначення), порушення яких тягне процесуальні наслідки.

На підставі максимального рівня критичності встановлено категорію безпеки ІС, як «Висока». Ця категорія зобов'язує застосовувати базовий профіль безпеки рівня «Високий» за НД ТЗІ 3.6-006-24. Категорія ОІД «четверта» та клас АС «1» підтверджені актами (Додатки Д та Е) і є юридичною підставою для побудови атестованої КСЗІ.

Цільовий профіль безпеки (ЦПБ) є проєктним документом, що визначає вичерпний перелік заходів захисту, адаптованих до конкретних умов функціонування АС-1. Відповідно до НД ТЗІ 3.6-006-24, ЦПБ формується на основі базового профілю безпеки рівня «Високий» з урахуванням специфіки системи.

При формуванні ЦПБ для АС-1 відділу ЦК враховано три особливості, які відрізняють його від стандартного базового профілю. По-перше, ізольованість системи (АС клас «1») дозволяє виключити з профілю всі заходи, пов'язані із захистом мережевих з'єднань, фільтрацією трафіку та захистом від мережевих атак. Вони є неактуальними для автономного АРМ. По-друге, специфіка криміналістичної діяльності вимагає посиленого контролю над носіями інформації, кожне підключення досліджуваного носія потенційно вносить загрозу, тому заходи класу МР набувають особливого пріоритету. По-третє,

процесуальні вимоги до цілісності доказів встановлюють для заходів класу SI вимоги, що виходять за межі стандартного профілю, наприклад, обов'язкове обчислення та верифікація хеш-значень SHA-256 для кожного образу носія на кожному етапі його обробки.

Структура ЦПБ охоплює дванадцять функціональних груп заходів захисту таких, як: ідентифікацію та автентифікацію (IA), управління доступом (AC), реєстрацію та аудит (AU), захист носіїв (MP), фізичний захист (PE), захист цілісності та обслуговування (SI, MA), криптографічний захист (SC), планування та реагування на інциденти (IR, CP), керування безпекою (SM), захист від НСД (NSD), кадрову безпеку (PS) та навчання (AT). Для кожного заходу визначено функціональний рівень відповідно до НД ТЗІ 2.5-004-99 та конкретний спосіб реалізації в умовах АС-1. Такий системний розподіл дозволяє побудувати ешелоновану модель безпеки, де взаємодоповнюваність контрольних механізмів мінімізує критичні ризики та забезпечує безперервність захисту на всіх етапах життєвого циклу інформаційних активів. У таблиці 2.2 наведено ключові заходи ЦПБ, що є специфічними або першочерговими для відділу цифрової криміналістики.

Таблиця 2.2 – Ключові заходи цільового профілю безпеки АС-1 відділу цифрової криміналістики

Група заходів	Код	Рівень	Реалізація в АС-1 Хмельницького НДЕКЦ МВС
1	2	3	4
Ідентифікація та автентифікація (IA)	IA-2	Рівень 1	Кожному суб'єкту доступу присвоєно унікальний ідентифікатор. Доступ до АРМ дозволено лише після успішної автентифікації за логіном та паролем.
	IA-5(1)	Рівень 2	Парольна політика: мінімум 12 символів, великий та малий регістри, цифри та спецсимволи, обов'язкова зміна кожні 60 днів. Вхід до BIOS також захищено паролем.
	IA-8	Рівень 1	Доступ до АС-1 заборонено особам, що не є штатними співробітниками підрозділу. Список допуску затверджується наказом керівника СЗІ.

Продовження таблиці 2.2

1	2	3	4
	IA-8	Рівень 1	Доступ до АС-1 заборонено особам, що не є штатними співробітниками підрозділу. Список допуску затверджується наказом керівника СЗІ.
Управління доступом (AC)	AC-2	Рівень 2	Рольова модель: в системі існують виключно два облікові записи «Адміністратор» та «Експерт». Гостьовий доступ заблоковано. Автоматична деактивація облікового запису через 30 днів неактивності.
	AC-5	Рівень 2	Розмежування обов'язків: адміністратор безпеки не має логічного доступу до матеріалів кримінальних проваджень (лише до налаштувань ОС).
	AC-11	Рівень 1	Автоматичне блокування сеансу через 10 хвилин бездіяльності. Блокування термінала на 30 хвилин після 5 невдалих спроб входу (AC-7).
Реєстрація та аудит (AU)	AU-2	Рівень 1	У журналі «Безпека» Windows реєструються: вхід/вихід з системи, спроби доступу до файлів, зміна політик безпеки, події принтера. Зберігання журналів не менше 1 року.
	AU-6	Рівень 1	Адміністратор безпеки щотижнево переглядає журнали подій на предмет аномальної активності та фіксує результати перевірки.
	AU-9	Рівень 1	Журнали подій доступні лише для читання адміністратору безпеки. Захист журналів від перезапису налаштовано.
Захист носіїв (MP)	MP-4	Рівень 1	Усі змінні носії інформації (флеш-накопичувачі, зовнішні HDD) обліковані в журналі та зберігаються в металевому сейфі в КЗ у неробочий час.
	MP-7	Рівень 1	USB-порти, що не використовуються, програмно вимкнено через реєстр Windows. Дозволено підключення лише облікованих службових носіїв.
Криптографічний захист (SC)	SC-28	Рівень 2	Шифрування системного розділу диска та каталогів з образами доказів засобами «ІІТ Захищений диск-4». Забезпечує захист конфіденційності.

Кінець таблиці 2.2

1	2	3	4
Цілісність системи (SI)	SI-3	Рівень 1	Антивірусний захист Avast Business Antivirus в автономному режимі. Оновлення сигнатурних баз вручну адміністратором не рідше 1 разу на тиждень. Обов'язкове сканування кожного підключеного носія до надання доступу до його вмісту.
	SI-7	Рівень 1	Контроль цілісності системних файлів ОС засобами утиліти SFC. Щоденний контроль цілісності образів доказів через обчислення контрольних сум.
Фізичний захист (PE)	PE-3	Рівень 1	Двері з замком та пристосуванням для опечатування, грати та жалюзі на вікнах, охоронна сигналізація з виведенням на пульт охорони, журнал обліку відвідувачів.
	PE-11	Рівень 1	АС-1 підключена до ДБЖ APC Back-UPS BX700U-GR (700 ВА), що забезпечує щонайменше 20 хвилин автономної роботи для коректного завершення процесів копіювання та збереження даних.
Резервування та відновлення (CP)	CP-9	Рівень 1	Щотижневе повне резервне копіювання образів дисків та баз даних проєктів на зовнішній носій. Носій із резервними копіями зберігається в металевому сейфі в КЗ. Щоквартальне тестове відновлення.

Особливої уваги заслуговує захід MP-7 (контроль носіїв). Для звичайної адміністративної системи блокування USB є стандартним заходом, тоді як для криміналістичного підрозділу він набуває процесуального значення. Підключення несанкціонованого носія є не лише порушенням правил безпеки, а й потенційним порушенням ланцюга зберігання доказів, що може призвести до недопустимості всіх результатів конкретної експертизи в суді. Саме тому для цього заходу встановлено не лише програмне обмеження, а й організаційну процедуру. Кожне підключення носія фіксується в журналі із зазначенням ідентифікатора пристрою, дати та відповідальної особи.

Захід SC-28 (шифрування носіїв) також є специфічним для умов відділу ЦК. Фізичне вилучення накопичувача SSD Kingston є реалістичним сценарієм.

Зловмисник може отримати доступ до всієї доказової бази за одну дію. Шифрування засобами «ІІТ Захищений диск-4» унеможливлює читання даних без ключа шифрування навіть при підключенні накопичувача до стороннього комп'ютера, що нейтралізує загрозу № 8 з таблиці 2.1 до прийнятного рівня залишкового ризику.

Заходи групи AU (аудит) набувають у криміналістичному середовищі правового значення. Журнали подій Windows є частиною доказової документації. Вони підтверджують, що доступ до образів носіїв здійснювався лише авторизованими особами у визначений час. Цілісність журналів захищено заходом AU-9. Адміністратор безпеки має право лише читати їх, але не змінювати. Таким чином, засоби аудиту одночасно виконують функцію технічного захисту та процесуального підтвердження автентичності дій у системі.

Відповідність реалізованих заходів вимогам ТЗ підтверджується шляхом зіставлення кодів заходів ЦПБ із загрозами з таблиці 2.1. Кожна загроза класу «Критичний» та «Високий» охоплена не менш ніж двома заходами захисту. Повний перелік всіх 37 заходів ЦПБ з детальним описом реалізації та строками впровадження наведено в Додатку Л.

2.4 Обґрунтування вибору засобів захисту та порівняльний аналіз рішень

Вибір конкретних засобів захисту є практичним кроком, що трансформує вимоги цільового профілю безпеки у конкретне технічне рішення. Для кожного заходу ЦПБ існують альтернативні засоби реалізації, і обґрунтований вибір серед них визначає не лише рівень захищеності, а й відповідність системи вимогам нормативно-правового регулювання України. Принциповою вимогою НД ТЗІ 3.6-004-21 є застосування засобів захисту, які мають позитивний експертний висновок Державної служби спеціального зв'язку та захисту інформації України або включені до відповідних переліків дозволених засобів. Ця вимога суттєво

звужує вибір і водночас гарантує відповідність засобів вимогам державної атестації КСЗІ.

Центральним засобом криптографічного захисту в складі КСЗІ відділу цифрової криміналістики є комплекс «ІІТ Захищений диск-4» виробництва ПрАТ «Інститут Інформаційних Технологій» (Україна).

При обґрунтуванні вибору програмного комплексу «ІІТ Захищений диск-4» ключовим фактором стала можливість його використання не просто як інструменту шифрування дисків, а як технологічної основи для створення ізольованих захищених контейнерів для зберігання доказової бази. У контексті цифрової криміналістики це дозволяє реалізувати модель суворого розмежування доступу між різними фахівцями підрозділу. Завдяки створенню індивідуальних віртуальних шифрованих дисків для кожного експерта, система забезпечує технічну неможливість доступу одного співробітника до матеріалів дослідження іншого. Такий підхід є критично важливим для дотримання принципу процесуальної незалежності експерта. Він гарантує, що робота з цифровими доказами у межах конкретного провадження залишається повністю конфіденційною та захищеною від будь-якого внутрішнього впливу. Таким чином, використання «Захищеного диска» перетворює робочу станцію на багатокористувацьке експертне середовище, де цілісність ланцюжка володіння кожним окремим доказом підтримується на рівні криптографічно захищених контейнерів.

Першим і визначальним чинником є наявність позитивного експертного висновку Держспецзв'язку на комплекс «ІІТ Захищений диск-4». Це означає, що засіб пройшов державну експертизу відповідно до вимог НД ТЗІ та визнаний придатним для захисту інформації в системах органів державної влади і правоохоронних органів. Без наявності такого висновку застосування будь-якого криптографічного засобу в КСЗІ, що підлягає державній атестації, є неприпустимим незалежно від його технічних характеристик. Саме ця вимога виключає з розгляду популярні комерційні засоби шифрування, зокрема BitLocker (Microsoft, США) та VeraCrypt (відкрите ПЗ), що не мають відповідних

вітчизняних висновків.

Другим чинником є функціональна відповідність специфіці криміналістичного середовища. Комплекс «ІІТ Захищений диск-4» реалізує прозоре шифрування розділів диска та логічних дисків з використанням алгоритму ДСТУ 7624, що забезпечує захист даних у стані спокою без впливу на процедури роботи з файлами. Для відділу ЦК це означає, що образи носіїв доказів, які зберігаються на зашифрованому розділі SSD Kingston, залишаються повністю захищеними від несанкціонованого читання при фізичному вилученні накопичувача. Криміналістичне ПЗ (EnCase Forensic) при цьому працює з зашифрованим розділом у штатному режимі після успішної автентифікації, що не вносить жодних змін у процедуру дослідження.

Третім чинником є підтримка апаратних носіїв ключів та двофакторної автентифікації. «ІІТ Захищений диск-4» підтримує роботу з апаратними ключами-носіями (токенами) серії ІІТ Token, що дозволяє реалізувати двофакторну автентифікацію для доступу до зашифрованих розділів: PIN-код плюс апаратний токен. У стандартній адміністративній АС-1 така вимога, як правило, відсутня; для криміналістичного підрозділу вона критична, оскільки зашифровані образи доказів не повинні бути доступними навіть для адміністратора безпеки без фізичної наявності токена відповідального експерта.

Четвертим чинником є можливість розмежованого шифрування на рівні логічних дисків. Комплекс дозволяє створювати окремо зашифровані логічні диски з різними ключами доступу: системний розділ (C:) захищається ключем адміністратора, а робочий розділ з образами доказів (D:) захищається ключем конкретного експерта. Це технічно реалізує принцип розмежування доступу (захід АС-5 ЦПБ) на рівні криптографії: адміністратор безпеки, навіть маючи повний доступ до ОС, фізично не може прочитати вміст розділу з доказами без ключа експерта. Жоден з розглянутих альтернативних засобів (BitLocker, VeraCrypt) не надає такого гнучкого розмежування в умовах єдиного АРМ.

П'ятим чинником є прозорість роботи для криміналістичного ПЗ. Ряд комерційних засобів шифрування може конфліктувати зі спеціалізованим ПЗ

(зокрема з низькорівневими інструментами роботи з диском EnCase Forensic) через перехоплення системних викликів введення-виведення. «ІІТ Захищений диск-4» реалізований як драйвер файлової системи Windows і забезпечує прозоре шифрування на рівні блоків, що унеможливлює конфлікт з будь-яким легітимним ПЗ, включаючи криміналістичні інструменти.

Шостим чинником є відповідність вимогам щодо захисту від несанкціонованого читання при транспортуванні носіїв. Порядок роботи відділу передбачає переміщення зашифрованих зовнішніх носіїв між сховищем (сейф у КЗ) та АРМ. «ІІТ Захищений диск-4» підтримує шифрування зовнішніх носіїв (USB-дисків) з тими самими алгоритмами та рівнем захисту, що й внутрішніх, забезпечуючи наскрізний криптографічний захист у всьому ланцюгу зберігання доказів.

Вибір апаратного блокатора запису Tableau Forensic Bridge T8u обумовлений тим, що він є одним із найбільш поширених засобів у практиці цифрової криміналістики та входить до переліку засобів, рекомендованих SWGDE і NIST. На відміну від програмних блокаторів запису (наприклад, реалізованих через реєстр Windows або групові політики), апаратний write-blocker є фізичним пристроєм, що перехоплює сигнали запису на шині між носієм і контролером. Це унеможливлює обхід захисту засобами ОС або шкідливим ПЗ, що є критичною властивістю для криміналістичного середовища: якщо носій містить шкідливий код, що намагається приховати сліди модифікації через системні виклики, апаратний write-blocker нейтралізує цю загрозу незалежно від стану ОС.

Tableau T8u підтримує інтерфейси підключення носіїв SATA, SAS, USB 3.0 та IDE, що охоплює весь спектр носіїв, що можуть надходити на дослідження. Пристрій має індикатор активного захисту від запису (світлодіод), що дозволяє адміністратору безпеки та судовому експерту візуально підтвердити коректну роботу перед початком копіювання. Вбудований журнал пристрою фіксує серійні номери підключених носіїв і часові мітки операцій, що є частиною технічного підтвердження.

Порівняльний аналіз з типовими рішеннями для стандартної адміністративної АС класу «1» дозволяє виявити ключові відмінності КСЗІ відділу цифрової криміналістики. Стандартна адміністративна АС-1 (наприклад, бухгалтерська або канцелярська) передбачає такий типовий набір заходів: парольна автентифікація з політикою складності, розмежування прав доступу до файлів, антивірусний захист та шифрування системного диска. Цей набір відповідає заходам IA-2, AC-2, SI-3, SC-28 і є достатнім для захисту фінансових або кадрових документів.

КСЗІ відділу цифрової криміналістики відрізняється від стандартного рішення за чотирма суттєвими параметрами. По-перше, наявність апаратного write-blocker є унікальною для криміналістичного середовища і відсутня у будь-якій іншій типовій АС-1 тому, що жоден адміністративний підрозділ не потребує апаратного захисту від запису при роботі з виробничими носіями. По-друге, розмежоване шифрування на рівні логічних дисків з різними ключами для адміністратора і користувача є більш складним рішенням ніж стандартне шифрування системного диска без розмежування ролей. По-третє, вимога до контролю цілісності через хешування є більш жорсткою. Стандартна АС-1 перевіряє цілісність системних файлів ОС засобом SFC раз на місяць, тоді як для відділу ЦК контроль хешів образів доказів є обов'язковим при кожному доступі до них. По-четверте, аудит подій у стандартній АС-1 ведеться для виявлення інцидентів безпеки, тоді як в АС-1 відділу ЦК журнали аудиту мають також процесуальне значення. Вони є частиною доказової документації, що підтверджує законність процедури дослідження.

Зіставлення з міжнародними практиками свідчить про відповідність обраного рішення стандарту ISO/IEC 27037:2012 та рекомендаціям SWGDE. Стандарт ISO/IEC 27037 вимагає верифікації цілісності доказів через хешування, застосування write-blocker при роботі з оригінальними носіями та документування кожного кроку роботи з доказом. Усі ці вимоги реалізовані в КСЗІ відповідними заходами ЦПБ. Відмінністю від міжнародних практик є необхідність застосування вітчизняних сертифікованих засобів криптографічного

захисту замість міжнародно визнаних рішень (BitLocker, FileVault), що обумовлено вимогами законодавства України щодо захисту інформації з обмеженим доступом.

Таким чином, обрані засоби захисту є оптимальними для умов функціонування відділу цифрової криміналістики Хмельницького НДЕКЦ МВС. Кожен засіб обрано на підставі нормативної відповідності (наявність позитивного висновку Держспецзв'язку), функціональної сумісності зі спеціалізованим криміналістичним ПЗ та здатності реалізувати специфічні вимоги, що виходять за межі стандартного базового профілю безпеки для АС класу «1».

2.5 Висновок

У другому розділі виконано повний цикл аналітичних і проєктних робіт з розроблення комплексної системи захисту інформації для відділу цифрової криміналістики Хмельницького НДЕКЦ МВС.

У підрозділі 2.1 визначено методологічну основу проєктування КСЗІ відповідно до вимог НД ТЗІ 3.7-003-2005 та НД ТЗІ 3.6-004-21. Розроблено повний комплект організаційно-розпорядчих документів першого етапу (Додатки Б–З, Н, П), що є нормативною передумовою для будь-яких подальших робіт зі створення КСЗІ. Встановлено організаційну структуру СЗІ з трьома чітко розмежованими ролями. Такий розподіл реалізує принцип мінімальних привілеїв і унеможливлює реалізацію загроз від внутрішнього порушника. Визначено, що ЦПБ є кінцевою метою першого етапу і трансформує вимоги ТЗ у конкретні заходи захисту.

У підрозділі 2.2 побудовано модель загроз та модель порушника для АС класу «1». Виявлено десять актуальних загроз. Визначено п'ять категорій порушників, як-от авторизований експерт, адміністратор безпеки, адміністративний персонал, технічний персонал та стороння особа без права

доступу до КЗ. Встановлено, що найбільш небезпечними є внутрішні порушники перших двох категорій, які мають легальний доступ до системи, що обумовлює першочергову важливість організаційних заходів контролю поряд із технічними засобами захисту.

У підрозділі 2.3 проведено категоріювання інформаційної системи та сформовано цільовий профіль безпеки. Встановлено категорію безпеки ІС «Висока» на підставі критичного рівня цілісності оброблюваної інформації, що зобов'язує застосовувати базовий профіль безпеки рівня «Високий» за НД ТЗІ 3.6-006-24. ЦПБ охоплює дванадцять функціональних груп заходів захисту; ключові з них наведено в таблиці 2.2. Визначено три специфічні особливості профілю відносно стандартного БПБ. Повний ЦПБ наведено в Додатку Л.

У підрозділі 2.4 обґрунтовано вибір конкретних засобів захисту та виконано порівняльний аналіз прийнятих рішень.

Результатом другого розділу є повний комплект проєктних рішень, що включає модель загроз, модель порушника, категоріювання ІС, цільовий профіль безпеки з обґрунтуванням вибору засобів захисту.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ЦИФРОВИХ ДОКАЗІВ

3.1 Реалізація заходів захисту в операційній системі Windows

Практична реалізація заходів цільового профілю безпеки на АРМ відділу цифрової криміналістики здійснюється штатними засобами операційної системи Windows 11 та спеціалізованим програмним забезпеченням. Відповідно до плану впровадження КСЗІ (Додаток П), заходи реалізуються у визначеній послідовності: спочатку налаштовуються засоби управління доступом та автентифікації (заходи IA та AC), потім реєстрація та аудит (AU), контроль носіїв (MP), антивірусний захист (SI) та криптографічний захист даних (SC). Кожне налаштування безпосередньо відповідає конкретному коду заходу ЦПБ та усуває відповідні загрози з реєстру (таблиця 2.1).

Рольова модель доступу реалізована через налаштування локальних облікових записів у консолі управління комп'ютером (lusrmgr.msc). На АРМ створено три облікові записи. Вбудований системний обліковий запис з повними правами адміністрування ОС, обліковий запис атестованого судового експерта-криміналіста, який є авторизованим користувачем АС-1, та вбудований обліковий запис з вимкненим доступом. Розподіл на облікові записи «Admin» та «Expert» реалізує не лише захист від НСД, а й вимогу процесуальної незалежності. Експерт працює у середовищі з обмеженими правами, що гарантує, будь-які встановлені програми для аналізу (FTK, EnCase) не зможуть змінити системні налаштування або втрутитися в роботу блокаторів запису. Своєю чергою, заблокований запис "Guest" та сувора парольна політика відсікають можливість доступу до доказової бази сторонніх осіб, що забезпечує неперервність ланцюжка володіння (Chain of Custody). Перелік облікових записів з їх статусами наведено на рисунку 3.1.

Принцип розмежування обов'язків (захід АС-5) реалізовано через членство в групах. Це технічно унеможливлює виконання експертом будь-яких адміністративних дій у системі, таких як встановлення або видалення програм,

зміну налаштувань безпеки, управління іншими обліковими записами. Водночас адміністратор не має доступу до розділу диска із зашифрованими доказовими матеріалами, захищеного особистим ключем «ІІТ Захищений диск-4» облікового запису «Expert».

Рисунок 3.1 – Перелік локальних облікових записів АРМ

Парольна політика налаштована через редактор локальної політики безпеки. Встановлено такі параметри: мінімальна довжина пароля – 12 символів (забезпечує стійкість до підбору методом грубої сили); вимога складності – увімкнено (пароль повинен містити символи щонайменше трьох з чотирьох категорій); максимальний термін дії пароля – 60 днів (примусова ротація); мінімальний термін дії – 1 день (унеможливлює негайну заміну на попередній пароль); журнал паролів – 5 паролів (заборона повторення останніх паролів). Налаштування парольної політики наведено на рисунку 3.2.

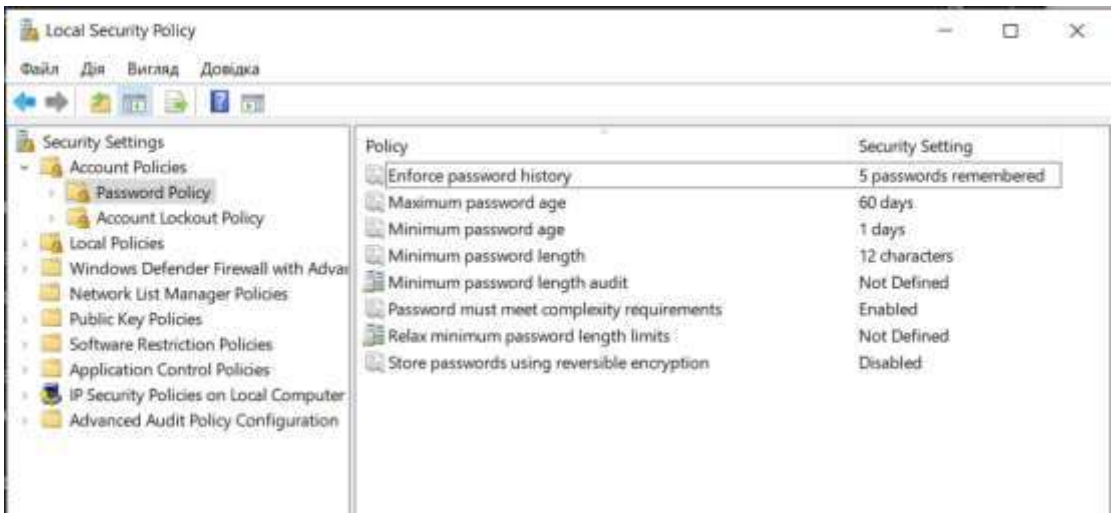


Рисунок 3.2 – Параметри парольної політики у редакторі локальної політики

Політика блокування облікових записів налаштована в розділі «Account Lockout Policy» того самого редактора. Встановлено такі параметри: порогове значення блокування – 5 невдалих спроб входу (захист від атак підбору пароля); тривалість блокування – 30 хвилин (обліковий запис автоматично розблоковується через 30 хвилин без участі адміністратора); скидання лічильника блокування – через 30 хвилин після останньої невдалої спроби. Системний обліковий запис адміністратора не підлягає автоматичному блокуванню, що запобігає ситуації повної втрати доступу до системи у разі атаки. Налаштування політики блокування наведено на рисунку 3.3.

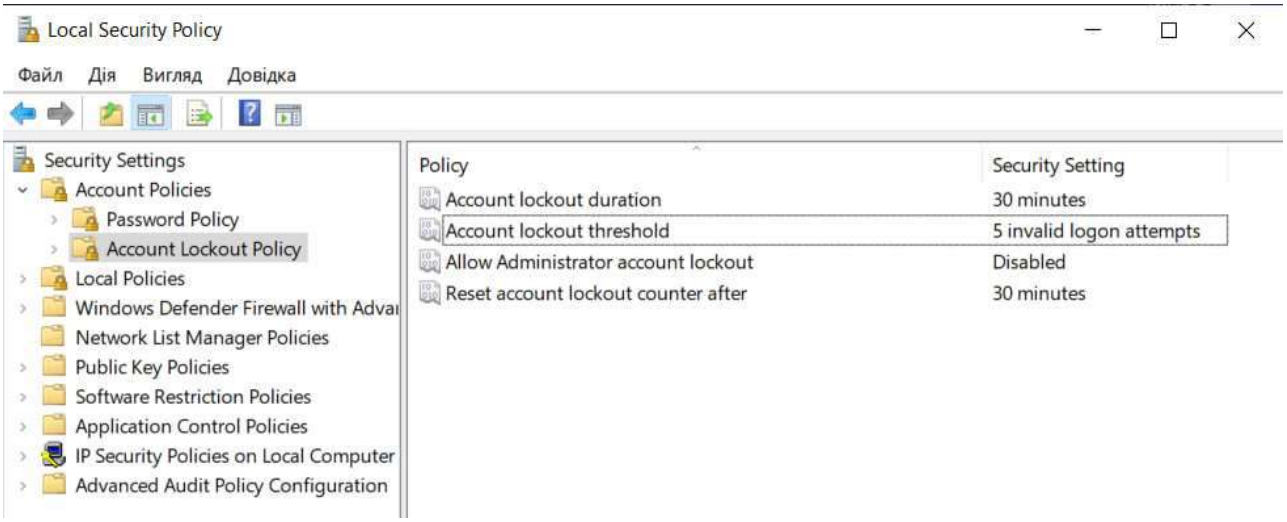


Рисунок 3.3 – Параметри політики блокування облікових записів

Автоматичне блокування робочого сеансу після визначеного часу бездіяльності є критично важливим заходом для відділу цифрової криміналістики: АРМ, залишений без нагляду в активному стані, є одним з основних векторів несанкціонованого доступу до матеріалів кримінальних проваджень. Захід реалізовано через редактор групових політик. Активовано три параметри: «Enable screen saver» (увімкнути заставку), «Password protect the screen saver» (блокувати екран при увімкненні заставки), «Screen saver timeout» (час очікування перед блокуванням). Активований список параметрів у розділі «Personalization» наведено на рисунку 3.4.

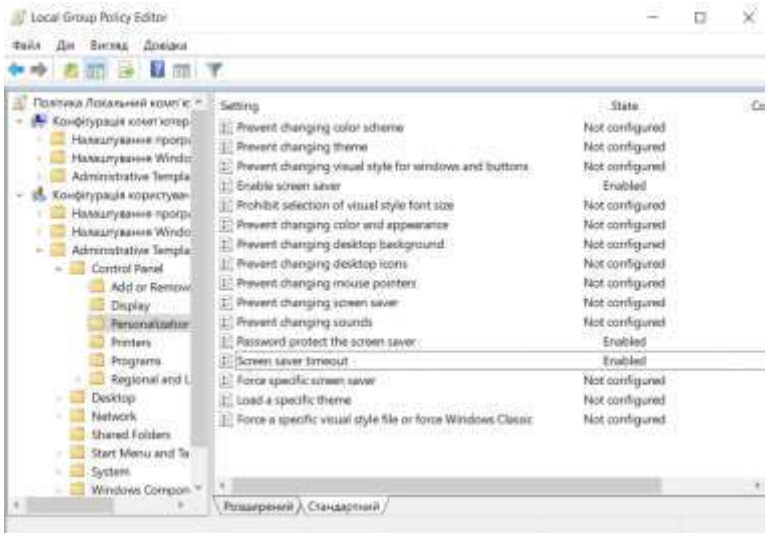


Рисунок 3.4 – Налаштування параметрів персоналізації у редакторі групових політик

Параметр «Screen saver timeout» встановлено у значення 600 секунд (10 хвилин). Це означає, що після 10 хвилин відсутності дій з клавіатурою або мишею АРМ автоматично переходить до заблокованого стану з вимогою введення пароля для розблокування. Вікно налаштування параметра з введеним значенням 600 секунд наведено на рисунку 3.5. У поєднанні з вимогою автентифікації при блокуванні екрана.

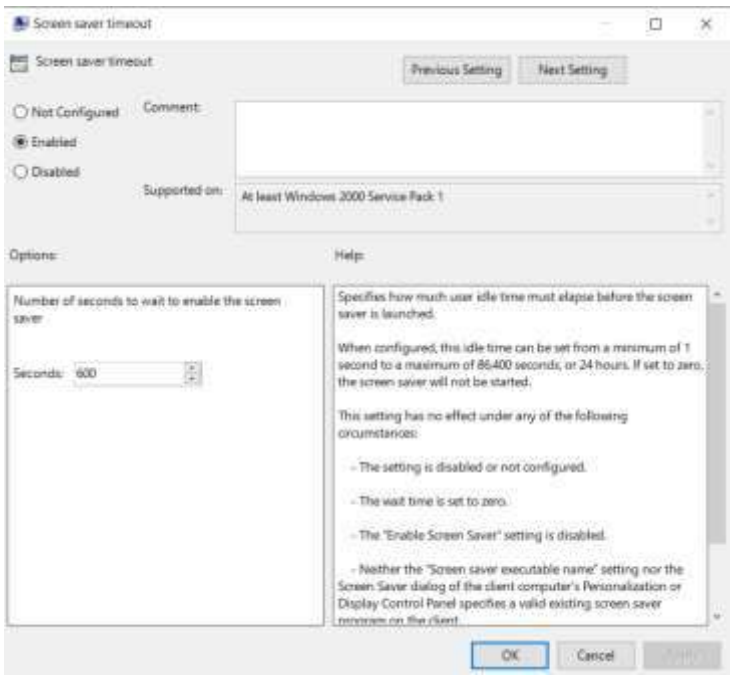


Рисунок 3.5 – Налаштування часу очікування заставки

Аудит подій безпеки налаштований у розділі редактора локальної політики безпеки. Для відділу цифрової криміналістики всі дев'ять категорій аудиту увімкнено на рівні «Success, Failure» (успіх і відмова). Це забезпечує фіксацію не лише успішних дій, а й усіх невдалих спроб, що є критичним для виявлення спроб несанкціонованого доступу. Зокрема, «Audit account logon events» та «Audit logon events» фіксують усі входи в систему та спроби автентифікації; «Audit object access» фіксує звернення до файлів та папок у сховищі доказів; «Audit account management» реєструє будь-які зміни в обліковими записами; «Audit policy change» виявляє спроби зміни самих налаштувань аудиту. Перелік усіх налаштованих категорій аудиту наведено на рисунку 3.6.

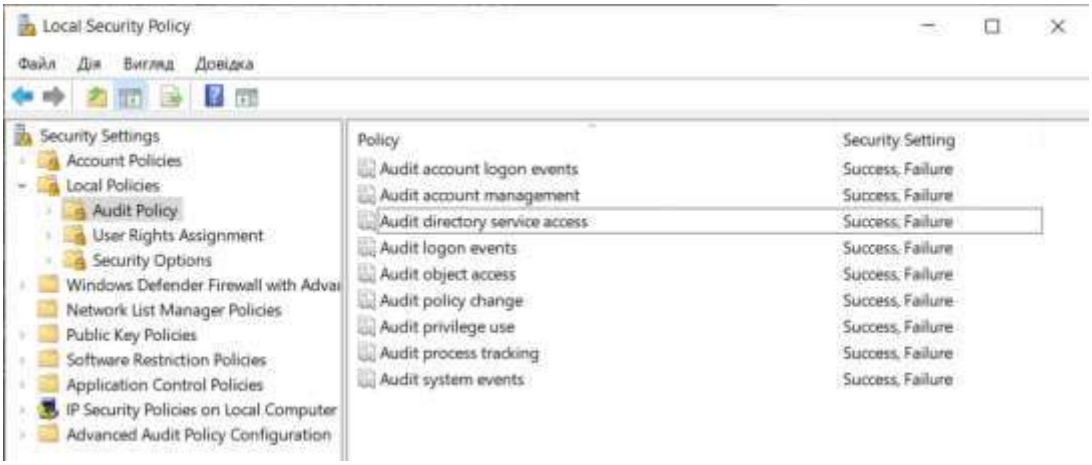


Рисунок 3.6 – Налаштування категорій аудиту у редакторі локальної політики безпеки

Захист журналів аудиту від перезапису налаштований через властивості журналу «Security» у переглядачі подій. Встановлено максимальний розмір журналу 102 400 КБ (100 МБ) та режим «Archive the log when full, do not overwrite events», тобто при досягненні максимального розміру журнал автоматично архівується під унікальним іменем, а записи не перезаписуються. Це гарантує збереження повної хронології подій за весь термін роботи АРМ, що є важливим як для розслідування інцидентів інформаційної безпеки, так і для підтвердження законності процедур у судовому провадженні. Налаштування властивостей журналу безпеки наведено на рисунку 3.7.

Рисунок 3.7 – Властивості журналу безпеки Windows

Контроль підключення знімних носіїв реалізовано через редактор реєстру Windows. У гілці змінено значення параметра Start з 3 (автоматичний запуск служби) на 4 (служба вимкнена). Встановлення значення 4 означає, що Windows не завантажує цей драйвер навіть при підключенні USB-пристрою, і операційна система не розпізнає жоден USB-накопичувач. Вікно редагування параметра з введеним значенням 4 наведено на рисунку 3.8.

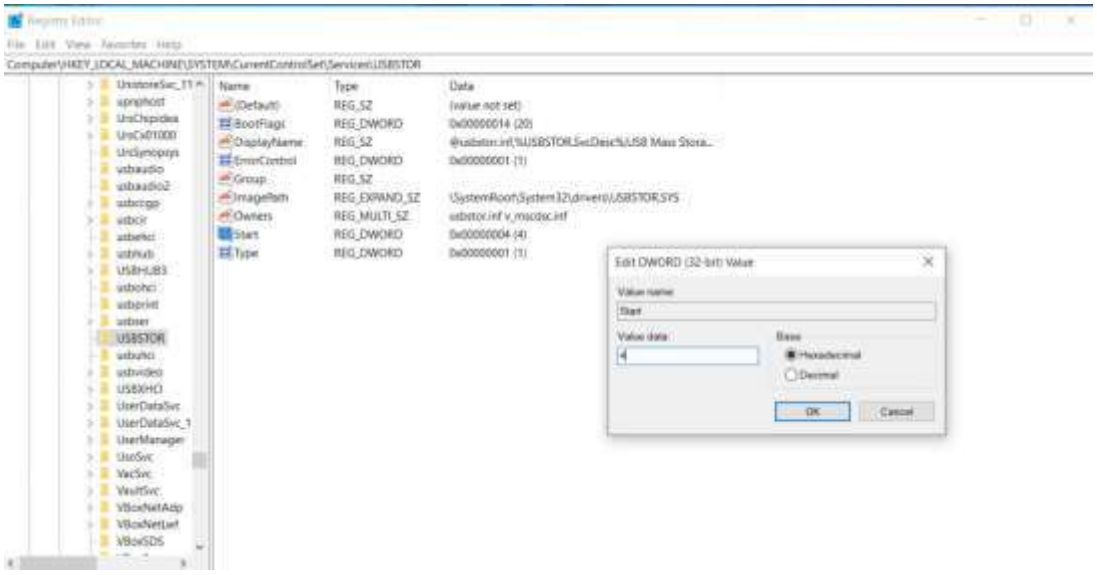


Рисунок 3.8 – Встановлення значення для вимкнення служби

Важливо, що апаратний write-blocker Tableau T8u підключається через стандартний USB-порт і використовує окремий драйвер, що не залежить від служби USBSTOR. Тому блокування USBSTOR не впливає на роботу write-blocker і не перешкоджає основній діяльності відділу. Будь-який же звичайний USB-накопичувач при спробі підключення залишається невидимим для системи.

Антивірусний захист реалізовано за допомогою Avast Business Antivirus, що функціонує в повністю автономному режимі без підключення до мережі. Специфіка криміналістичного середовища полягає в тому, що АРМ не має доступу до мережі Інтернет, тому оновлення антивірусних баз виконується вручну адміністратором безпеки з використанням атестованого знімного носія. Відповідно до плану впровадження КСЗІ (Додаток П), оновлення виконується не рідше одного разу на тиждень. Остання дата оновлення баз фіксується в журналі адміністратора разом із підписом відповідальної особи. Автоматичне повне сканування системи один раз на тиждень. Окрім планового сканування, будь-який носій інформації перед наданням доступу до його вмісту проходить обов'язкове антивірусне сканування у режимі вибіркової перевірки. Захист у реальному часі увімкнено постійно. Статус захисту Avast Business Antivirus після ручного оновлення баз та налаштування розкладу сканування наведено на рисунку 3.9.

Рисунок 3.9 – Статус антивірусного захисту

Криптографічний захист даних у стані спокою реалізовано за допомогою комплексу «ІІТ Захищений диск-4. Користувач», що має позитивний експертний висновок Держспецзв'язку. Алгоритм шифрування – ДСТУ 7624 (стандарт симетричного шифрування «Калина», що є аналогом AES-256 за рівнем стійкості). Комплекс реалізує прозоре шифрування захищених логічних дисків, що відображаються в операційній системі як звичайні логічні диски і є повністю прозорими для будь-якого легітимного програмного забезпечення, включаючи спеціалізовані криміналістичні інструменти.

На АРМ створено захищений диск типу «Постійний диск», що зберігається у вигляді зашифрованого файлу-образу на SSD Kingston. Після успішної автентифікації за допомогою особистого ключа (зчитування ключа та введення PIN-коду) захищений диск підключається до системи як логічний диск з літерою J: та відображається у головному вікні програми у розділі «Підключені диски». Статус підключеного захищеного диска в програмі «ІІТ Захищений диск-4. Користувач» наведено на рисунку 3.10. Використання алгоритму ДСТУ 7624 "Калина" в комплексі «ІІТ Захищений диск-4» дозволяє створити захищене сховище, яке фізично та логічно відокремлює матеріали одного кримінального провадження від іншого.

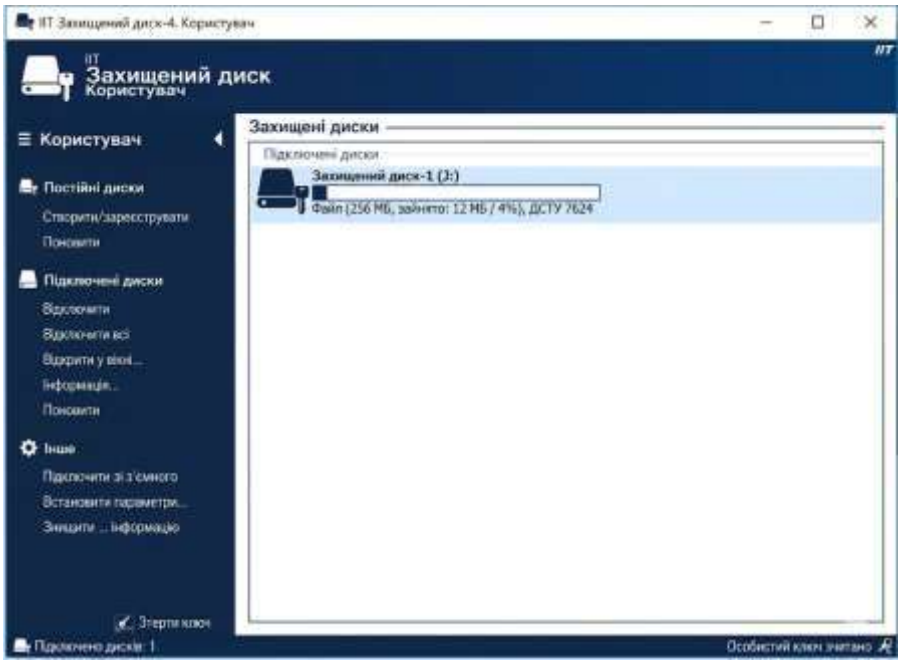


Рисунок 3.10 – Головне вікно програми «ІІТ Захищений диск-4»

Доступ до захищеного диска вимагає наявності особистого ключа на носії ключової інформації та знання PIN-коду. Після завершення роботи з матеріалами справи захищений диск відключається командою «Відключити» або «Відключити всі», після чого всі дані на ньому стають недоступними без повторної автентифікації. У разі спроби читання зашифрованого файлу-образу стороннім комп'ютером без програмного комплексу і відповідного ключа дані є абсолютно нечитабельними, що повністю нейтралізує загрозу фізичної крадіжки накопичувача.

3.2 Перевірка ефективності впроваджених заходів та верифікація цілісності

Після практичного впровадження всіх заходів цільового профілю безпеки, необхідним кроком є перевірка їх фактичної ефективності. Перевірка вирішує два завдання. Перше полягає в підтвердженні того, що кожне технічне налаштування дійсно працює й унеможливлює реалізацію відповідної загрози, а не лише формально виконане. Друге полягає в верифікації цілісності доказової бази, тобто підтвердження того, що цифрові докази, які зберігаються в АС-1 відділу цифрової криміналістики, залишились незміненими від моменту їх первинного надходження. Саме ця двостороння перевірка є необхідною умовою підготовки до атестаційних випробувань КСЗІ.

Принципова відмінність перевірки ефективності від первинного налаштування полягає в зміні точки зору. Необхідно фіксуватися що реально відбувається при спробі здійснити дію, яку захід повинен унеможливлювати. Для засобів контролю доступу це означає проведення провокаційних тестів, зокрема спроб входу з невірним паролем, спроба підключення несанкціонованого носія, спроба доступу до чужого розділу. Для засобів криптографічного захисту це означає перевірку хеш-значень образів доказів, а для засобів аудиту це означає перевірку того, що всі тестові дії були зафіксовані в журналі.

Перевірка заходу IA-5 (парольна політика) здійснюється через спробу встановити пароль, що не відповідає вимогам складності. При спробі задати пароль коротший за 12 символів або такий, що не містить символів різних категорій, система відхиляє зміну з відповідним повідомленням про невідповідність вимогам складності. Тест підтверджує, що параметр є діючим.

Перевірка заходу AC-7 (блокування після невдалих спроб) виконується шляхом п'яти послідовних спроб входу до облікового запису експерта з навмисно невірним паролем. Після п'ятої невдалої спроби система відображає повідомлення про блокування облікового запису. Спроба увійти протягом 30 хвилин після блокування залишається безуспішною. Система відмовляє у вході навіть при введенні правильного пароля. Це підтверджує, що захід AC-7 функціонує коректно і унеможливлює автоматизований підбір пароля. Скріншот заблокованого облікового запису у консолі lusrmgr.msc наведено на рисунку 3.11.

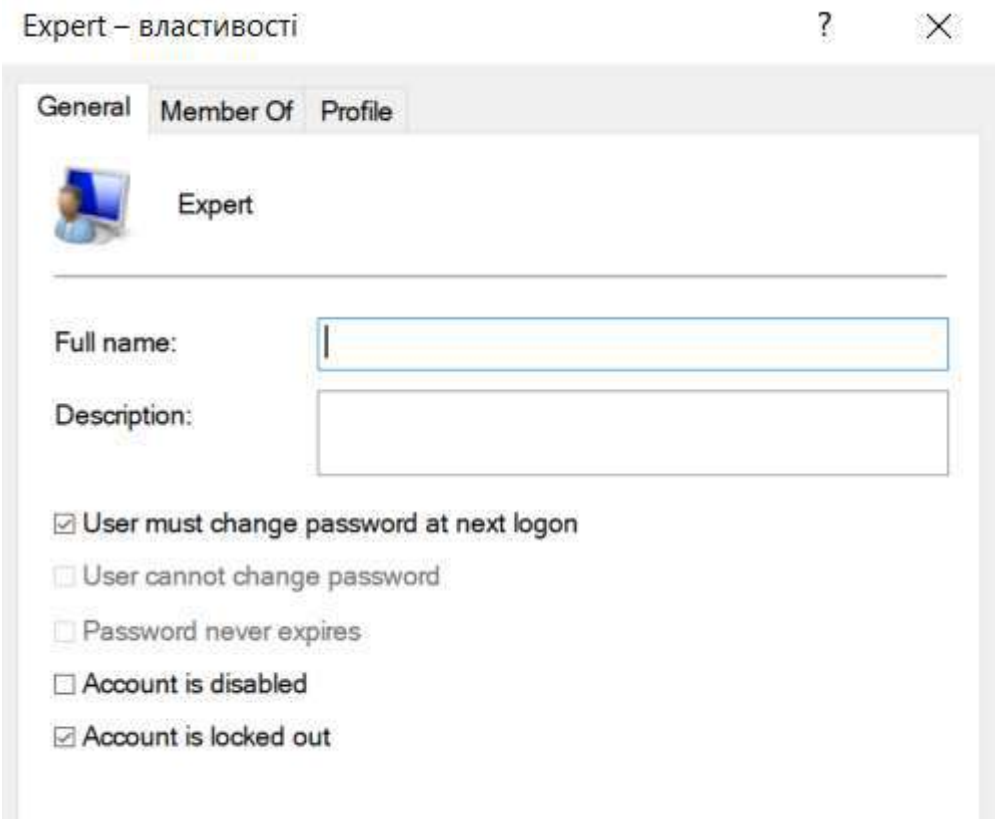


Рисунок 3.11 – Статус блокування облікового запису

Перевірка заходу АС-5 (розмежування обов'язків) здійснюється через спробу виконати адміністративну дію від імені облікового запису експерта. При спробі відкрити редактор локальної політики безпеки або консоль управління комп'ютером система відображає запит на введення облікових даних адміністратора (UAC-запит). Це підтверджує, що обліковий запис експерта справді обмежений правами звичайного користувача і не може самостійно змінювати налаштування безпеки системи.

Перевірка заходу АС-11 (автоблокування сеансу) виконується очікуванням 10 хвилин бездіяльності в активному сеансі облікового запису експерта. Після закінчення встановленого часу система автоматично активує захищену заставку з вимогою введення пароля для розблокування. Спроба закрити заставку без введення пароля залишається безуспішною. Доступ до робочого столу і матеріалів справи заблоковано. Для відділу цифрової криміналістики цей захід є особливо важливим. Незаблокований АРМ навіть за короткочасної відсутності експерта є потенційним вектором доступу до матеріалів кримінального провадження сторонніх осіб.

Перевірка заходу МР-7 є критично важливою саме для криміналістичного середовища, оскільки USB-носії є єдиним каналом зовнішнього інформаційного обміну ізольованої АС-1. Тест виконується шляхом підключення звичайного USB-флеш-накопичувача до вільного порту системного блоку. Попри фізичне підключення, операційна система не реєструє появу нового накопичувача у провіднику Windows і не призначає йому букву диска. У диспетчері пристроїв пристрій відображається з позначкою помилки, що свідчить про відмову у завантаженні драйвера служби USBSTOR. Скріншот диспетчера пристроїв з заблокованим USB-пристроєм наведено на рисунку 3.12.

Паралельно проводиться тест на підтвердження того, що апаратний write-blocker продовжує функціонувати після блокування USBSTOR. При підключенні write-blocker до того самого USB-порту операційна система успішно розпізнає пристрій і дозволяє доступ до носія доказів у режимі лише читання. Це підтверджує, що блокування USBSTOR вибірково діє лише на звичайні USB

Mass Storage накопичувачі і не впливає на роботу спеціалізованого криміналістичного обладнання, яке використовує власний драйвер.

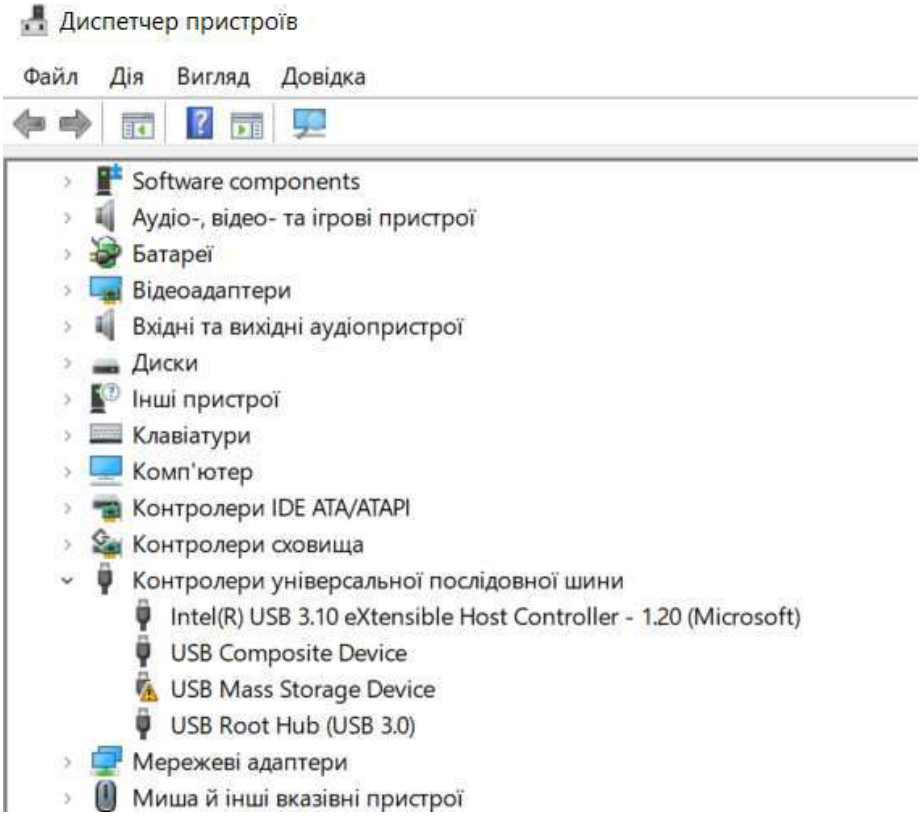


Рисунок 3.12 – Відображення несанкціонованого USB-накопичувача

Важливим аспектом перевірки є підтвердження процесуальної цілісності. У разі успішного обходу технічного блокування кожна дія в системі фіксується журналом аудиту. Спроба несанкціонованого підключення носія залишає запис у журналі системи та безпеки, що дозволяє виявити інцидент при наступному аудиті. Для судового провадження це означає, що навіть потенційна компрометація носія може бути виявлена та задокументована.

Верифікація цілісності цифрових доказів є центральним елементом, оскільки саме вона безпосередньо забезпечує процесуальну допустимість доказів у судовому провадженні. Відповідно до вимог, кожен цифровий доказ повинен супроводжуватись контрольними хеш-значеннями, обчисленими в момент первинного надходження носія, і ці значення повинні збігатися з хеш-значеннями, обчисленими на будь-якому наступному етапі обробки. Розбіжність

хеш-значень є доказом того, що дані були змінені, незалежно від того, сталось це навмисно чи внаслідок технічного збою.

Процедура верифікації цілісності в АС-1 відділу цифрової криміналістики виконується в три кроки. На першому кроці під час первинного надходження носія з доказами адміністратор безпеки підключає його до АРМ виключно через апаратний write-blocker і за допомогою вбудованих засобів криміналістичного ПЗ обчислює хеш-значення MD5 та SHA-256 оригінального носія. Обидва значення фіксуються у реєстрі ланцюга зберігання та у внутрішньому журналі АРМ із підписом відповідальної особи, датою та часом. На другому кроці після завершення аналізу обчислюються хеш-значення збереженого образу носія і порівнюються з первинно зафіксованими. На третьому кроці перед передачею матеріалів ініціатору експертизи виконується фінальна верифікація образу.

Перевірка коректності роботи засобу верифікації цілісності виконується шляхом тестового сценарію. Спочатку обчислюється хеш-значення тестового файлу образу, потім у файл вноситься навмисна зміна, і обчислення повторюється. Результат демонструє, що навіть мінімальна зміна даних (1 байт) повністю змінює хеш-значення SHA-256, що унеможливлює непомітну модифікацію образу. Порівняння хеш-значень оригінального та модифікованого образу наведено на рисунку 3.13.

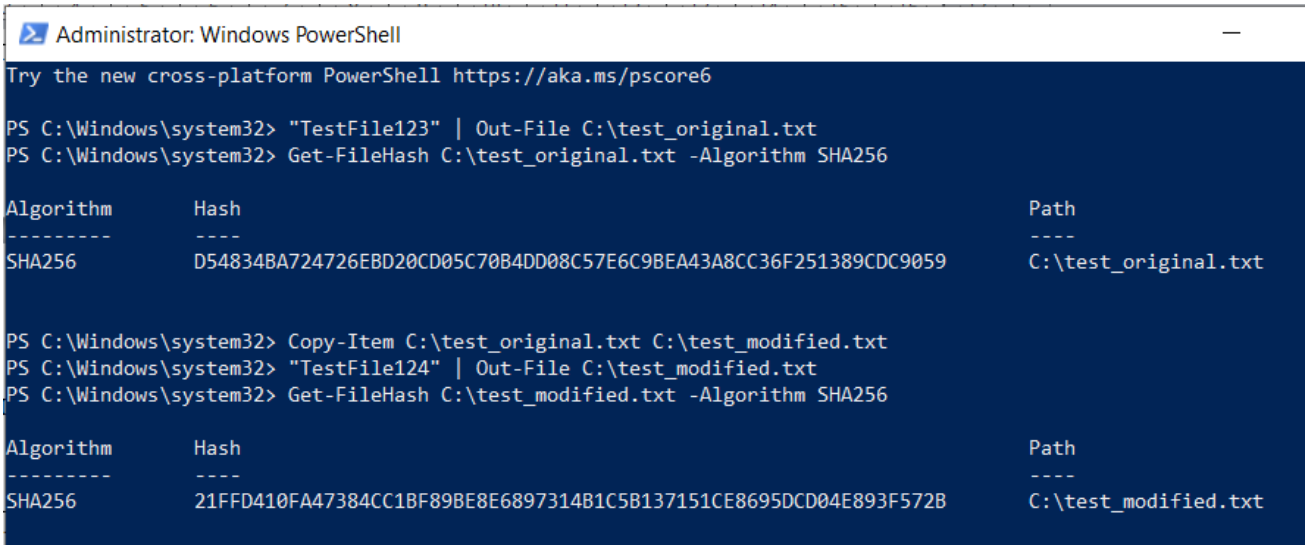


Рисунок 3.13 – Результат зміни одного байту

Для обчислення контрольних сум у штатному режимі роботи відділу використовується вбудована утиліта Windows CertUtil або команда в PowerShell Get-FileHash. Обидва інструменти підтримують алгоритми MD5 та SHA-256 і не потребують встановлення додаткового ПЗ. Перша утиліта повертає 64-символьний рядок хеш-значення, який фіксується в реєстрі ланцюга зберігання. Використання двох алгоритмів одночасно (MD5 для швидкої перевірки сумісності зі старими системами та SHA-256 як основний) відповідає рекомендаціям щодо криміналістичних процедур.

Верифікація цілісності виконується не лише щодо образів носіїв, а й щодо власних системних файлів АС-1. Вбудована утиліта Windows System File Checker перевіряє цілісність системних файлів ОС і відновлює їх у разі виявлення відмінностей від еталонних значень. Ця перевірка виконується адміністратором безпеки щомісячно відповідно до плану впровадження КСЗІ (Додаток П). За результатами виконання команди система виявила пошкоджені системні файли та успішно відновила їх з еталонних копій. Це підтверджує не лише коректність роботи заходу SI-7, а й практичну цінність регулярної перевірки цілісності. Без систематичного контролю пошкоджені файли могли б залишитись непоміченими і потенційно вплинути на коректність роботи криміналістичного ПЗ або засобів захисту. Скріншот результату виконання команди на рисунку 3.14.

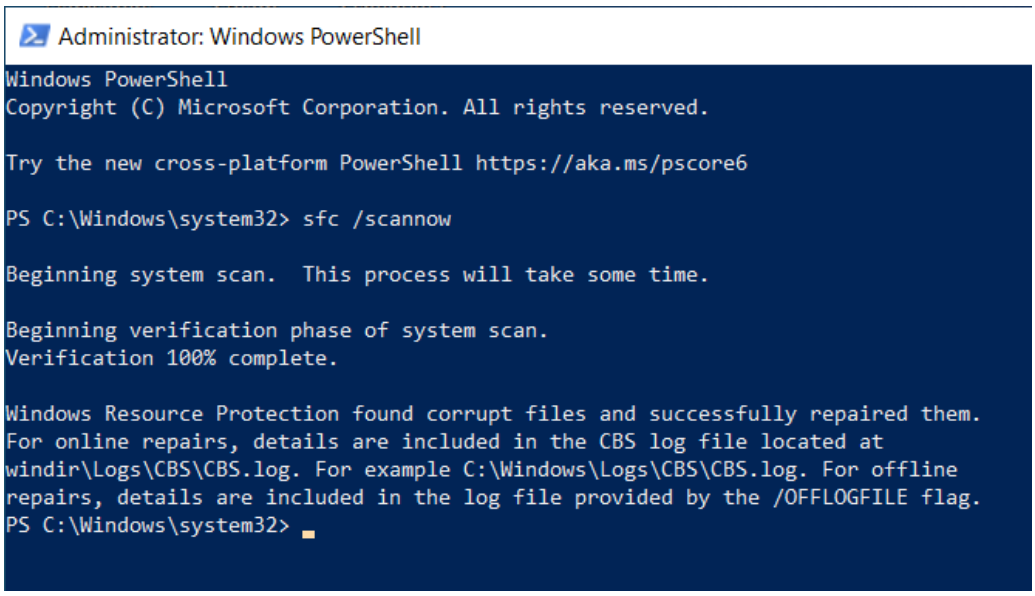


Рисунок 3.14 – Результат перевірки цілісності системних файлів Windows

Журнали аудиту виконують у відділі цифрової криміналістики подвійну функцію, а саме технічну (виявлення інцидентів безпеки) та процесуальну (підтвердження законності дій з доказами). Перевірка повноти журналювання здійснюється шляхом аналізу журналу безпеки після виконання серії тестових дій. Наприклад, входу в систему від імені експерта, відкриття папки з тестовими образами доказів, спроби входу з невірним паролем та підключення несанкціонованого USB-носія.

Перевірка повноти журналювання здійснюється через аналіз журналу безпеки у переглядачі подій Windows (Event Viewer). Серед зафіксованих подій присутні записи кількох категорій, а саме 4673 (використання чутливих привілеїв), 4656 та 4658 (відкриття та закриття дескрипторів об'єктів файлової системи), 4688 та 4689 (створення та завершення процесів), 4703 (зміна прав маркера доступу), 4611 (реєстрація довіреного процесу входу). Сукупність цих подій підтверджує, що аудит охоплює ключові категорії заходу AU-2, наприклад доступ до об'єктів файлової системи (що є критичним для фіксації будь-яких звернень до сховища доказів), управління привілеями та активність процесів. Для верифікації конкретних категорій подій застосовується фільтрація журналу через вбудований засіб (Filter Current Log). Журнал безпеки з записами тестових дій наведено на рисунку 3.15.

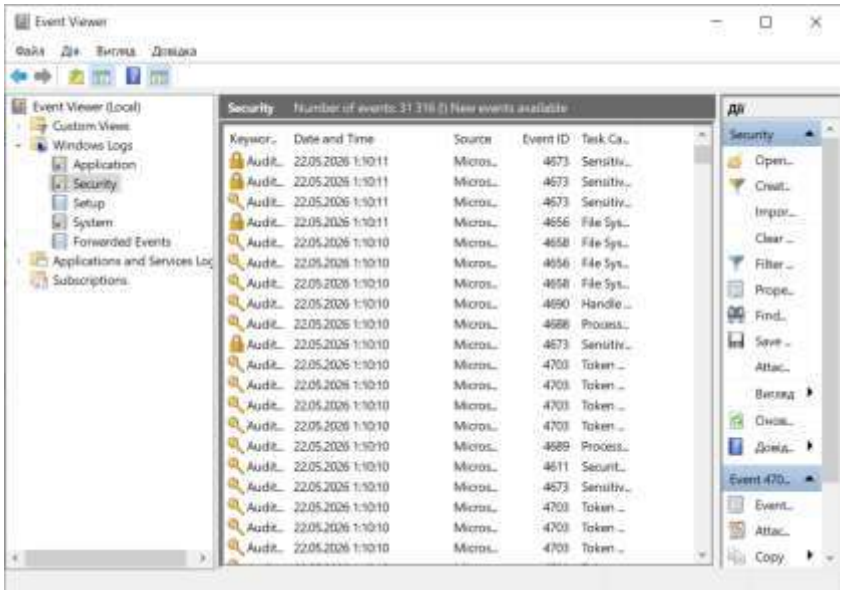


Рисунок 3.15 – Записи журналу безпеки Windows

Перевірка захисту журналів від несанкціонованої модифікації (захід AU-9) виконується спробою очистити журнал від імені облікового запису експерта. При спробі виконати команду очистити журнал у переглядачі подій система відображає повідомлення про відмову у доступі. Це підтверджує, що обліковий запис не має права модифікувати журнали аудиту. Навіть доказовий матеріал може бути лише прочитаний, але не знищений. Захист журналів від модифікації є критичним для запобіганню несанкціонованим діям з доказовою базою.

Перевірка заходу SI-3 (антивірусний захист) у криміналістичному контексті відрізняється від стандартної. Метою є не лише підтвердження що антивірус увімкнений, а й перевірка процедури обов'язкового сканування носіїв перед наданням доступу до їх вмісту. Тестовий носій зі спеціально розміщеним тестовим файлом EICAR підключається до АРМ через write-blocker.

При виконанні вибіркового антивірусного сканування підключеного носія Avast Business Antivirus виявляє тест-файл EICAR і виводить попередження. Сканування блокується до усунення загрози. Доступ до решти файлів носія не надається до завершення перевірки. Цей тест підтверджує, що процедура обов'язкового сканування носія функціонує коректно і унеможливлює автоматичне поширення шкідливого ПЗ з досліджуваних носіїв на АРМ. Виявлення загрози антивірусом фіксується у журналі аудиту як подія та підлягає занесенню до журналу інцидентів із підписом адміністратора безпеки.

Верифікація криптографічного захисту «ІІТ Захищений диск-4» виконується двома тестами. Перший тест перевіряє недоступність зашифрованих даних без автентифікації. Здійснюється спроба знайти та відкрити файл-образ захищеного диска безпосередньо на файловій системі без використання програмного комплексу. Файл-образ фізично присутній на диску, однак відкрити його як звичайний файл неможливо, бо він відображається як набір нечитабельних байтів. Будь-яка спроба інтерпретувати його зміст без ключа шифрування є безрезультатною, що підтверджує ефективний захист даних у стані спокою.

Другий тест перевіряє цілісність образів доказів, збережених на захищеному диску. Після підключення диска виконується повторне обчислення SHA-256 хешів усіх образів та порівняння з хеш-значеннями, зафіксованими в реєстрі на момент первинного надходження. Збіг хеш-значень підтверджує, що за весь час зберігання в зашифрованому середовищі жоден образ доказів не зазнав жодних змін, навіть мінімальних. Саме цей документально підтверджений збіг хеш-значень є технічним підґрунтям для заяви у судовому засіданні про те, що цифрові докази досліджувались у незміненому вигляді.

Порівняння хеш-значень образів доказів при первинному надходженні та після зберігання наведено на рисунку 3.16. Для зручності документування результати верифікації оформлюються у вигляді акту верифікації цілісності, що підписується судовим експертом та адміністратором безпеки і долучається до матеріалів кримінального провадження.

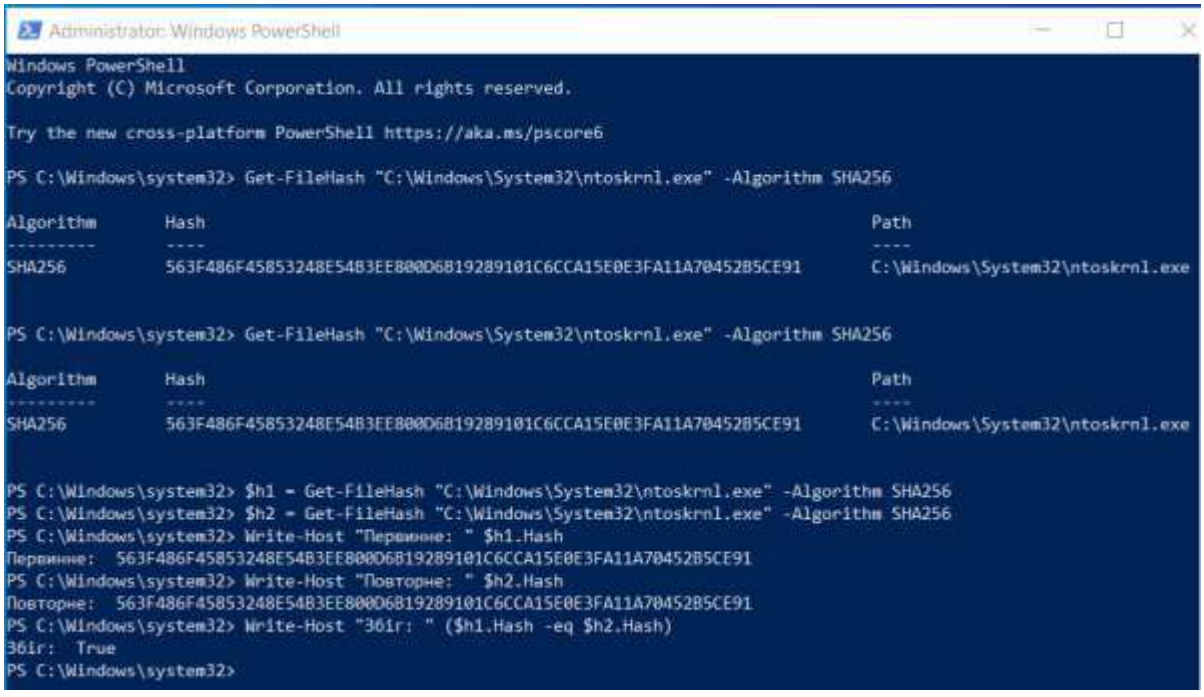


Рисунок 3.16 – Верифікація цілісності образів доказів

Атестація КСЗІ є завершальним нормативно обов'язковим кроком, що підтверджує відповідність реалізованої системи захисту вимогам технічного завдання та нормативних документів. Атестація проводиться організацією, що

має ліцензію на здійснення робіт у сфері технічного захисту інформації, і завершується видачею атестату відповідності. Без атестату КСЗІ вважається такою, що функціонує в тестовому режимі, а обробка ІзОД в неатестованій системі є порушенням законодавства.

Першим етапом органу з атестації надається пакет документів, що містить технічне завдання, цільовий профіль безпеки, акт обстеження, акт категоріювання та реєстраційна картка АС. Повнота і коректність документального пакету є необхідною умовою початку випробувань.

На другому етапі орган з атестації проводить перевірку відповідності фактичного стану системи задокументованому. Перевіряється склад обладнання, версії ПЗ, відсутність мережевого підключення, стан фізичного захисту приміщення. На третьому етапі виконуються технічні випробування. Незалежно від власних тестів підрозділу орган з атестації повторює ключові перевірки заходів захисту, включаючи автентифікацію, контроль носіїв, аудит, шифрування.

На четвертому етапі перевіряється повнота організаційного забезпечення. Наявність підписаних інструкцій для всіх суб'єктів КСЗІ, заповнених журналів, наказів. На п'ятому етапі орган з атестації перевіряє результати верифікації цілісності. Хеш-значення образів доказів, зафіксовані в актах, мають відповідати фактичному стану файлів. На шостому етапі за умови успішного проходження всіх перевірок видається атестат відповідності КСЗІ, що підтверджує право на обробку інформації з обмеженим доступом в АС-1.

Результати перевірки ефективності впроваджених заходів є безпосередньою підготовкою до атестаційних випробувань. Кожен тестовий сценарій і кожен скріншот є попереднім підтвердженням того, що відповідна вимога ТЗ і ЦПБ виконана. Технічна документація з результатами тестів разом із актами верифікації цілісності надається органу з атестації як доказова база при проведенні випробувань.

3.3 Організаційне забезпечення процесу дослідження та ланцюжка володіння

Технічні засоби захисту, забезпечують захист від зовнішніх і технічних загроз. Однак захист цифрових доказів у криміналістичному середовищі має принципово важливий організаційний вимір. Одна помилка в процедурі роботи з носієм і доказ може бути визнаний недопустимим у суді незалежно від досконалості технічних засобів. Організаційне забезпечення функціонування КСЗІ відділу цифрової криміналістики охоплює три взаємопов'язані компоненти: інструкцію атестованого судового експерта з акцентом на роботі з доказами, порядок реагування на інциденти виявлення розбіжності хеш-значень та ведення реєстру ланцюжка володіння.

Інструкція атестованого судового експерта регламентує порядок дій при кожному зверненні до цифрових доказів, від моменту отримання носія від ініціатора експертизи до передачі результатів. Дотримання інструкції є обов'язковою процедурною умовою допустимості доказів у судовому провадженні. Відхилення від встановленого порядку фіксується в журналі аудиту і може бути використане захистом для оскарження результатів експертизи. Інструкція ґрунтується на вимогах та процедурних положеннях КПК України щодо залучення спеціалістів.

Інструкція охоплює шість послідовних етапів роботи з носієм доказів, кожен з яких є обов'язковим і не може бути пропущений.

Перший етап передбачає отримання носія та проведення його початкового огляду. Судовий експерт отримує носій доказів від ініціатора (слідчого або прокурора) виключно за наявності постанови про призначення експертизи та супровідного листа. Носій повинен бути у пломбованому пакеті або опечатаній упаковці. Факт отримання фіксується підписом у реєстрі ланцюжка володіння. Якщо упаковка порушена або носій має механічні пошкодження, що не відповідають описаному стану в супровідних документах, складається акт розбіжностей і роботу не починають до отримання роз'яснень від ініціатора.

На другому етапі здійснюється реєстрація та зберігання оригінального носія. Отриманий носій передається адміністратору безпеки, який поміщає його до металевого сейфа в межах контрольованої зони кабінету. Носій зберігається у сейфі протягом усього часу проведення експертизи, за винятком безпосереднього підключення для копіювання. Факт поміщення до сейфа та кожного вилучення з нього фіксується у реєстрі chain of custody з підписами двох осіб, а саме судового експерта та адміністратора безпеки. Зберігання оригінального носія за межами сейфа або на робочому столі під час перерви є порушенням інструкції.

Третій етап передбачає виконання побітового копіювання із застосуванням write-blocker. Підключення оригінального носія до АРМ здійснюється виключно через апаратний write-blocker. Порядок дій: спочатку до АРМ підключається write-blocker, потім до write-blocker підключається носій і лише після появи індикатора на корпусі пристрою починається робота. Під час копіювання на екрані криміналістичного ПЗ відображається інформація про носій, як-от модель, серійний номер, об'єм, стан. Усі ці відомості вносяться до реєстру chain of custody. Після завершення копіювання носій відключається у зворотному порядку. Спочатку від write-blocker, потім write-blocker від АРМ. Підключення носія доказів безпосередньо до USB-порту АРМ в обхід write-blocker є грубим порушенням інструкції і підставою для службового розслідування.

На четвертому етапі здійснюється обчислення та документування контрольних хеш-значень. Одразу після завершення побітового копіювання судовий експерт обчислює хеш-значення MD5 та SHA-256 як оригінального носія, так і створеного образу. Обчислення виконується за допомогою вбудованих засобів або засобами криміналістичного ПЗ. Обидва хеш-значення (оригінал і образ) вносяться до реєстру chain of custody. Збіг хеш-значень образу і оригіналу є обов'язковою умовою для початку аналізу. Якщо значення не збігаються, тоді фіксується інцидент і застосовується порядок реагування. Загальний покроковий алгоритм проведення дослідження та логіку активації порядку реагування на інциденти відображено на рисунку 3.17.

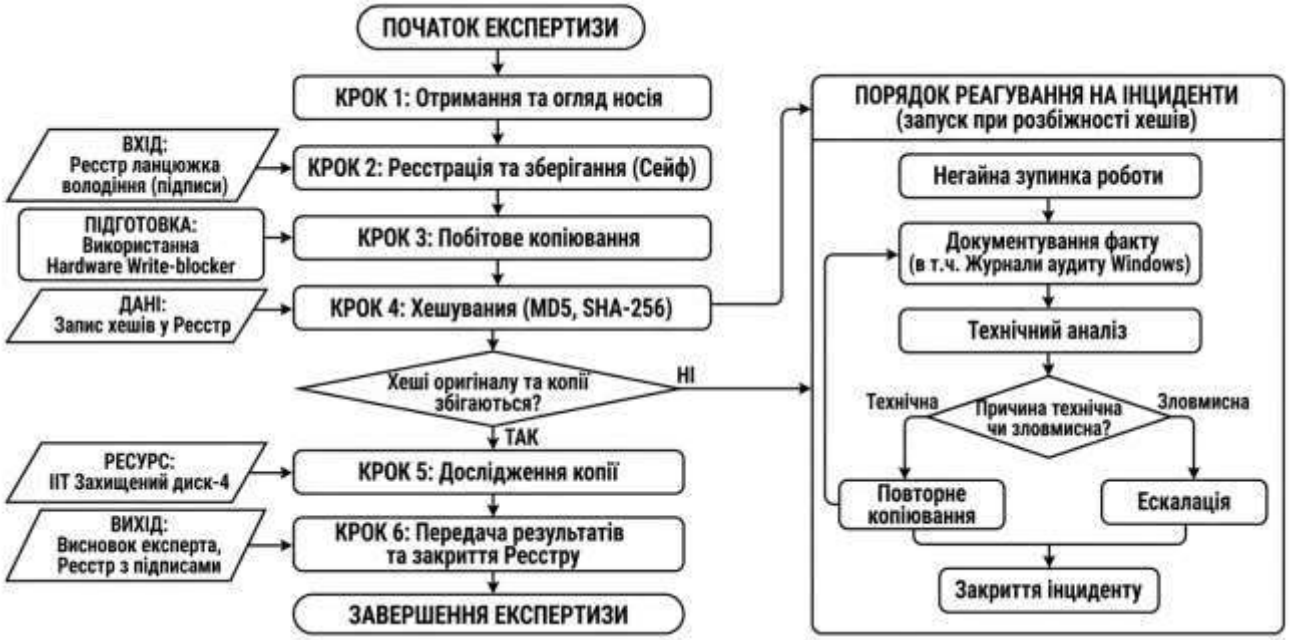


Рисунок 3.17 – Система захисту цифрових доказів

На п’ятому етапі дослідження проводиться виключно з використанням копії. Уся аналітична робота судового експерта виконується виключно з образом носія (копією), збереженим на захищеному диску, комплексу «ІІТ Захищений диск-4». Оригінальний носій після копіювання повертається до сейфа і залишається там до завершення всіх стадій провадження. Доступ до захищеного диска надається лише після автентифікації за допомогою особистого ключа та PIN-коду облікового запису експерта. Завершення кожного сеансу роботи з образами супроводжується від'єднанням захищеного диска в інтерфейсі «ІІТ Захищений диск-4». Залишати диск підключеним у неробочий час або при покиданні приміщення забороняється.

На шостому етапі здійснюється передача результатів та закриття ланцюга. Сформований висновок судового експерта передається ініціатору з обов'язковою верифікацією цілісності. До матеріалів додається роздруківка хеш-значень образів, які досліджувались, із зазначенням дати первинного надходження та дати завершення дослідження. Реєстр chain of custody закривається підписами судового експерта, адміністратора безпеки та керівника СЗІ. Оригінальний носій передається разом з матеріалами справи або залишається на зберіганні відповідно до рішення слідчого.

Окрім основного регламенту, інструкція містить перелік заборонених дій, що є типовими помилками у практиці, як-от підключення особистих носіїв до АРМ; вхід до системи з чужим обліковим записом; відкриття електронної пошти або будь-яких файлів, не пов'язаних з поточною справою; встановлення будь-якого ПЗ без дозволу адміністратора безпеки; виконання операцій запису на оригінальний носій; залишення АРМ без блокування при покиданні приміщення навіть на короткий час; розголошення відомостей про матеріали поточної справи. Кожне порушення будь-якого пункту інструкції підлягає фіксації у журналі інцидентів і розгляду керівником СЗІ.

Розбіжність хеш-значень є найсерйознішим інцидентом інформаційної безпеки у відділі цифрової криміналістики, оскільки свідчить про можливу модифікацію цифрового доказу. Такий інцидент може мати як технічне пояснення (збій при копіюванні, пошкодження носія, помилка ПЗ), так і правове значення, якщо модифікація була навмисною, мають місце ознаки злочину проти правосуддя. Саме тому порядок реагування є суворо регламентованим і не допускає самостійних дій судового експерта без участі адміністратора безпеки та керівника СЗІ.

Розбіжність хеш-значень може бути виявлена у трьох ситуаціях: при первинному порівнянні хешів оригіналу та образу одразу після копіювання; при контрольній перевірці хешів образу перед початком аналізу (якщо образ зберігався певний час після копіювання); при фінальній верифікації перед передачею результатів ініціатору. Незалежно від моменту виявлення порядок дій є однаковим.

Першою дією є негайна зупинка роботи. При виявленні розбіжності хеш-значень судовий експерт негайно припиняє будь-яку роботу з матеріалами справи, зберігає поточний стан та повідомляє адміністратора безпеки. Самостійно продовжувати роботу, виправляти ситуацію або повторно копіювати носій без дозволу заборонено, будь-яка додаткова дія може знищити сліди інциденту.

Другою дією передбачається документування факту розбіжності. Адміністратор безпеки документує інцидент у журналі інцидентів із зазначенням про дати та часу виявлення; ідентифікатора носія та справи; очікуваного хеш-значення (з реєстру chain of custody); фактично отриманого хеш-значення; імені особи, яка виявила розбіжність; переліку дій, що передували виявленню. Журнал аудиту Windows блокується від подальшого перезапису через примусове архівування поточного журналу безпеки, це зберігає хронологію всіх подій, що передували інциденту.

Третьою дією є технічний аналіз причини. Адміністратор безпеки аналізує журнал аудиту на наявність записів, які могли б пояснити розбіжність, наприклад, несанкціонований доступ до файлу образу (події 4663), зміна прав доступу (4670), операції запису в каталог зберігання, підключення несанкціонованих пристроїв (6416). Якщо журнал містить аномальні події, то це є ознакою навмисної модифікації. Якщо аномалій немає, то розбіжність, вірогідно, має технічну причину (збій запису, пошкодження ділянки диска).

Четвертою дією передбачається повторне копіювання з оригіналу за наявності технічної причини. Якщо технічний аналіз встановив, що причиною є збій запису, а оригінальний носій не зазнав змін (хеш оригіналу збігається із зафіксованим при первинному надходженні), адміністратор безпеки має право санкціонувати повторне копіювання. Повторне копіювання виконується з обов'язковим записом до реєстру, де вказується дата, причина повторного копіювання, хеш нового образу, підписи двох осіб. Новий образ отримує порядковий номер версії.

П’ятою дією передбачається ескалація за наявності ознак навмисної модифікації. Якщо журнал аудиту містить ознаки несанкціонованого доступу або якщо розбіжність не отримала технічного пояснення, адміністратор безпеки негайно доповідає керівнику СЗІ. Керівник СЗІ приймає рішення про призупинення обробки матеріалів справи, повідомлення ініціатора про неможливість завершення експертизи у встановлений строк та, за наявності ознак умисного злочину, ініціювання службового розслідування. Матеріали по

інциденту (журнали аудиту, роздруківки хеш-значень, записи chain of custody) зберігаються окремо як потенційні докази.

Шостою дією є закриття інциденту. Після встановлення причини інциденту та усунення її наслідків складається акт закриття інциденту, підписаний усіма задіяними особами. Акт зберігається разом з матеріалами справи та надається ініціатору разом з результатами експертизи. Навіть якщо інцидент мав технічну природу і не вплинув на доказову базу. Ця прозорість є необхідною умовою довіри до результатів. Суд або сторони провадження мають право знати про будь-які нестандартні ситуації, що виникали при обробці доказів.

Ключовим принципом реагування на інцидент розбіжності хеш-значень є незворотність документування. Жоден запис не видаляється, жоден журнал не очищається, жодна дія не виконується без фіксації. Цей принцип відповідає вимозі неспростовності. Кожна подія прив'язана до конкретної особи, часу та контексту, що унеможливлює подальше заперечення факту або обставин інциденту.

Реєстр ланцюжка володіння є центральним документом організаційного забезпечення роботи з цифровими доказами. Його призначенням є нерозривна документальна фіксація кожної дії з носієм або образом доказу від моменту першого контакту до завершення провадження. Реєстр виконує одночасно три функції: технічну (фіксує хеш-значення на кожному етапі), організаційну (ідентифікує відповідальних осіб) та правову (є документальним підтвердженням законності процедури дослідження у суді).

Структура реєстру відділу цифрової криміналістики охоплює декілька обов’язкових полів. Ідентифікаційний блок включає унікальний номер справи, реквізити постанови про призначення експертизи, дату надходження, а також найменування та реквізити ініціатора. Блок опису носія містить тип носія (HDD/SSD/флеш/SD), виробника, модель, серійний номер, ємність, стан упаковки при отриманні, а також наявність пломб. Блок хеш-значень охоплює MD5 та SHA-256 оригінального носія, MD5 та SHA-256 образу після копіювання, дату та час обчислення, а також версію програмного забезпечення, що використовувалось. Блок доступу фіксує кожну операцію в окремому рядку,

включаючи дату, час, виконавця, зміст дії (отримано зі сховища, повернуто до сховища, досліджувався образ, передано ініціатору), а також підписи двох осіб.

Правило двох підписів є фундаментальним принципом ведення реєстру. Жоден рядок не вважається дійсним, якщо під ним стоїть лише один підпис. Для операцій з оригінальним носієм обов'язкова наявність підписів судового експерта та адміністратора безпеки. Для операцій передачі використовується підпис передавача та підпис отримувача. Це виключає можливість оспорювання факту будь-якої операції в суді, навіть якщо одна зі сторін заперечуватиме свою участь, другий підпис є незалежним підтвердженням.

Реєстр ведеться у двох форматах. Паперовий примірник зберігається у металевому сейфі разом з оригінальним носієм і заповнюється власноручно від руки, що забезпечує захист від цифрового підроблення. Електронна копія реєстру зберігається на захищеному диску у зашифрованому середовищі «ІІТ Захищений диск-4» і є оперативним інструментом для швидкого пошуку та перевірки. У разі розбіжності між паперовим і електронним примірниками пріоритет має паперовий.

Часова безперервність реєстру означає відсутність будь-яких прогалин у хронології. Якщо між двома записами пройшло більше ніж стандартний робочий день без операцій з носієм, робиться окремий запис з підписом адміністратора безпеки. Ця вимога унеможливлює заперечення сторони захисту про те, що між двома зафіксованими операціями носій міг перебувати у неконтрольованому середовищі. Узагальнений функціональний потік управління реєстром ланцюжка володіння та виконання обов'язкових вимог щодо його ведення наведено на рисунку 3.18.

Після завершення провадження та передачі всіх матеріалів ініціатору реєстр не знищується і не повертається слідчому. Він зберігається в архіві відділу протягом строку, встановленого для зберігання матеріалів судових експертиз. У разі повторного залучення матеріалів справи до провадження реєстр є головним документом, що підтверджує незмінність доказів протягом усього часу зберігання.

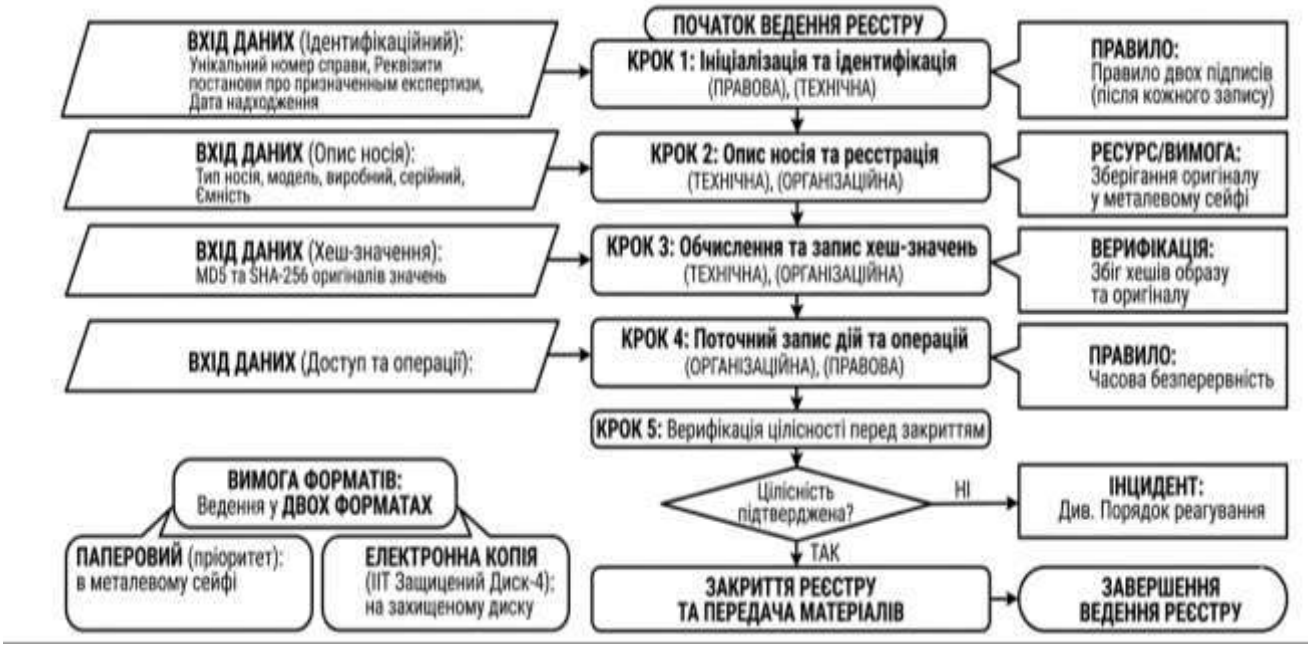


Рисунок 3.18 – Процес володіння реєстром ланцюжка володіння

Організаційне забезпечення КСЗІ відділу цифрової криміналістики утворює захист доказів. Інструкція атестованого експерта визначає правильні дії в штатному режимі, порядок реагування на інциденти регламентує дії в позаштатних ситуаціях, а реєстр забезпечує документальну неперервність ланцюга зберігання незалежно від будь-яких технічних чи організаційних обставин. Разом з технічними заходами ці три компоненти складають повноцінну систему захисту цифрових доказів.

3.4 Висновок

У третьому розділі здійснено практичну реалізацію комплексної системи захисту інформації відділу цифрової криміналістики Хмельницького НДЕКЦ МВС, що охопила три взаємопов'язані складові: технічне налаштування засобів захисту, перевірку їх ефективності та організаційне забезпечення процесу дослідження.

Практично реалізовано сім груп заходів цільового профілю безпеки засобами операційної системи Windows та спеціалізованого програмного

забезпечення. Налаштовано рольову модель доступу з двома обліковими записами і заблокованим гостьовим входом. Встановлено парольну політику, а також блокування облікового запису після невдалих спроб. Реалізовано автоматичне блокування сеансу через 10 хвилин бездіяльності, повний аудит усіх дев'яти категорій подій безпеки з архівуванням журналу, блокування несанкціонованих USB-носіїв, антивірусний захист в автономному режимі з щотижневим оновленням баз та криптографічний захист засобами «ІІТ Захищений диск-4» за алгоритмом ДСТУ 7624. Проведено перевірку фактичної ефективності впроваджених заходів та верифікацію цілісності цифрових доказів.

Розроблено організаційне забезпечення, що утворює захист цифрових доказів. Інструкція атестованого судового експерта визначає обов'язкові етапи роботи з носієм доказів від отримання до передачі результатів та перелік заборонених дій. Також визначено порядок реагування на інцидент розбіжності хеш-значень. Система ведення реєстру ведеться одночасно у паперовому та електронному форматах з вимогою часової безперервності.

Сукупність технічних заходів, підтверджених перевіркою ефективності, та організаційних процедур, що регламентують роботу персоналу, утворює КСЗІ, яка одночасно відповідає технічним вимогам та процесуальним стандартам. Система готова до проведення атестаційних випробувань.

ВИСНОВКИ

За результатами проведено комплексне дослідження питань захисту цифрових доказів у діяльності відділу цифрової криміналістики та розроблено підхід до побудови комплексної системи захисту інформації для середовища їх обробки і зберігання. У процесі виконання роботи було встановлено, що цифрові докази є особливо чутливим видом інформації, для якого критично важливими є забезпечення цілісності, автентичності та безперервного контролю доступу на всіх етапах роботи з даними.

У ході дослідження проаналізовано специфіку функціонування відділу цифрової криміналістики як об’єкта інформаційної діяльності, визначено основні категорії інформації та особливості інформаційних потоків, пов’язаних із прийманням, дослідженням, зберіганням і передаванням цифрових доказів. Встановлено, що навіть незначне порушення процедур роботи з доказовими даними може призвести до втрати їх процесуальної допустимості та негативно вплинути на результати кримінального провадження.

Під час виконання роботи було досліджено нормативно-правову базу України у сфері технічного захисту інформації, обробки персональних даних та використання електронних доказів у кримінальному процесі. Проведений аналіз підтвердив необхідність створення комплексної системи захисту інформації, яка повинна враховувати не лише вимоги інформаційної безпеки, а й специфіку цифрової криміналістики та процесуального законодавства.

У роботі побудовано модель загроз та модель порушника для середовища роботи з цифровими доказами, визначено основні джерела внутрішніх і зовнішніх загроз, а також ризики, пов’язані з несанкціонованим доступом, модифікацією, копіюванням або витоком доказової інформації. На основі проведеного аналізу обґрунтовано вибір організаційних, програмних та технічних заходів захисту, спрямованих на забезпечення безпечного функціонування системи.

Особливу увагу приділено забезпеченню контролю цілісності цифрових

доказів шляхом використання криптографічних механізмів хешування, розмежування доступу користувачів, ведення журналів аудиту та підтримання ланцюга зберігання доказів. Запропоновані рішення дозволяють мінімізувати ризик несанкціонованого втручання у доказову базу та забезпечують можливість підтвердження незмінності цифрових даних протягом усього періоду їх використання.

Практична частина роботи включала реалізацію окремих заходів захисту в операційному середовищі та оцінювання їх ефективності. Отримані результати підтвердили доцільність використання комплексного підходу до захисту цифрових доказів, який поєднує організаційні процедури, технічні засоби контролю доступу та механізми криптографічного захисту інформації.

Перспективами подальшого розвитку роботи є вдосконалення системи захисту цифрових доказів шляхом інтеграції централізованих систем моніторингу та аналізу подій безпеки (SIEM), автоматизації контролю ланцюга зберігання доказів, а також впровадження сучасних механізмів виявлення аномальної активності. Окремим напрямом розвитку є забезпечення безпечної роботи з цифровими доказами, отриманими з хмарних сервісів, мобільних платформ та розподілених мережевих середовищ.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Academic Press, 2011. 840 p.
2. Carrier B. File System Forensic Analysis. Addison-Wesley, 2005. 600 p.
3. Lyle J. R. NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics. NIST, 2014. 85 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf (дата звернення: 19.03.2026).
4. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva : ISO, 2012. 36 p. URL: https://www.iso.org/standard/44381.html (дата звернення: 19.03.2026).
5. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 20.04.2025 № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 20.03.2026).
6. Pollitt M. Digital Forensics: An Analytic Course of Study / Advances in Digital Forensics. Springer, 2005. P. 129–140.
7. Про Національну поліцію : Закон України від 13.03.2026 № 580-VIII. Відомості Верховної Ради України. 2015. № 40–41. Ст. 379. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 20.03.2026).
8. Про судову експертизу : Закон України від 01.01.2026 № 4038-XII. Відомості Верховної Ради України. 1994. № 28. Ст. 232. URL: https://zakon.rada.gov.ua/laws/show/4038-12 (дата звернення: 21.03.2026).
9. EnCase Forensic: The Industry Standard in Digital Investigations. Guidance Software (OpenText), 2020. URL: https://www.opentext.com/products/forensic (дата звернення: 21.03.2026).
10. FTK Forensic Toolkit: Product Overview and Technical Specifications. Exterro Inc., 2023. URL: https://www.exterro.com/ftk-forensic-toolkit (дата

звернення: 22.03.2026).

11. Carrier B. Open Source Digital Forensics. URL: https://www.sleuthkit.org (дата звернення: 22.03.2026).

12. SWGDE Best Practices for Computer Forensics. Scientific Working Group on Digital Evidence, 2023. URL: https://www.swgde.org/documents/ (дата звернення: 22.03.2026).

13. ІІТ Захищений диск-4. Інструкція користувача. Версія 4.0. ТОВ «Інститут Інформаційних Технологій», 2024. URL: https://iit.com.ua/itemdetails?p=3&gtype=1&type=1&id=44 (дата звернення: 22.03.2026).

14. Конвенція про кіберзлочинність (Будапештська конвенція) від 23.11.2001 : Міжнародний документ ETS № 185. URL: https://rm.coe.int/1680081561 (дата звернення: 22.03.2026).

15. Кримінальний процесуальний кодекс України : Закон України від 01.08.2025 № 4651-VI. Відомості Верховної Ради України. 2013. № 9–10. Ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 24.03.2026).

16. Про інформацію : Закон України від 20.01.2026 № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 25.03.2026).

17. Beebe N. L., Clark J. G. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation. 2005. Vol. 2. No. 2. P. 147–167. URL: https://surl.li/chwguw (дата звернення: 25.03.2026).

18. Cichonski P., Millar T., Grance T., Scarfone K. Computer Security Incident Handling Guide : NIST Special Publication 800-61 Revision 2. NIST, 2012. 160 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (дата звернення: 25.03.2026).

19. Kent K. et al. NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response. NIST, 2006. 121 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (дата звернення: 26.03.2026).

20. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ : ДСТСЗІ СБ України, 1999. URL: https://tzi.com.ua/downloads/1.1-003-99.pdf (дата звернення: 26.03.2025).

21. Management of the Chain of Custody of Digital Evidence Using Blockchain and Self-Sovereign Identities: A Systematic Literature Review / Loffi L. et al. IEEE Access. 2025. Vol. 13. P. 15420–15445.

22. Про електронні документи та електронний документообіг : Закон України від 31.12.2023 № 851-IV. Відомості Верховної Ради України. 2003. № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 27.03.2026).

23. Ruan K., Carthy J., Kechadi T., Baggili I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. Digital Investigation. 2013. Vol. 10, No. 1. P. 34–43.

24. Про електронні довірчі послуги : Закон України від 18.12.2024 № 2155-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 400. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення: 27.03.2026).

25. Про захист персональних даних : Закон України від 14.06.2025 № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 28.03.2026).

26. Про державну таємницю : Закон України від 27.08.2025 № 3855-XII. Відомості Верховної Ради України. 1994. № 16. Ст. 93. URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення: 28.03.2026).

27. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності. Київ : ДСТСЗІ СБ України, 1999. URL: https://tzi.ua/assets/files/НД-ТЗІ-2.5-005--99.pdf (дата звернення: 29.03.2026).

28. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ : ДСТСЗІ СБ України, 1999. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення: 30.03.2026).

29. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення КСЗІ в ІТС. Київ : ДСТСЗІ СБ України, 2005. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення: 30.03.2026).

30. НД ТЗІ 3.6-004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, в організаціях в ІКС яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. Київ : Адміністрація Держспецзв'язку, 2021. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66072 (дата звернення: 30.03.2026).

31. НД ТЗІ 3.6-005-21. Порядок категоріювання безпеки інформаційної системи та інформації. Київ : Адміністрація Держспецзв'язку, 2021. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66073 (дата звернення: 01.04.2026).

32. НД ТЗІ 3.6-006-24. Порядок вибору заходів захисту інформації для інформаційних систем. Київ : Адміністрація Держспецзв'язку, 2024. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66109 (дата звернення: 01.04.2026).

33. 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. Київ : Адміністрація Держспецзв'язку, 2021. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66075 (дата звернення: 01.04.2026).

34. НД ТЗІ 2.3-025-21. Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. Київ : Адміністрація Держспецзв'язку, 2021. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66108 (дата звернення: 02.04.2026).

35. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva : ISO, 2022. URL: https://www.iso.org/standard/80585.html (дата звернення: 02.04.2026).

36. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Київ : ДСТСЗІ СБ України, 2000. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення: 03.04.2026).

37. Безпека інформаційно-комунікаційних систем : підручник / Ю. Костюк, П. Складний, Б. Бебешко та ін. Київ : КСУ ім. Б. Грінченка, 2025. 1016 с.

38. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. Київ : BHV, 2009. 608 с.

39. Electronic Evidence – A Basic Guide for First Responders. European Union Agency for Cybersecurity (ENISA), 2015. URL: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders (дата звернення: 04.04.2026).

40. Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки : навч. посіб. Вінниця : ВНТУ, 2018. 316 с.

41. ISO/IEC 27042:2015. Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. Geneva : ISO, 2015. URL: https://www.iso.org/standard/44406.html (дата звернення: 04.04.2026).

42. Криміналістика : підручник : у 2 т. / за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової. Харків : ХНУВС, 2018. Т. 2. 312 с.

43. Марущак А. І. Правові основи захисту інформації з обмеженим доступом в Україні. Київ : КНТ, 2007. 208 с.

44. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva : ISO, 2022. URL: https://www.iso.org/standard/75652.html (дата звернення: 05.04.2026).

45. ISO/IEC 27035-1:2023. Information security, cybersecurity and privacy protection – Incident management – Part 1. Geneva : ISO, 2023. URL: https://www.iso.org/standard/78973.html (дата звернення: 06.04.2026).

46. NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. NIST, 2020. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/final (дата звернення: 06.04.2026).

47. Rose S., Borchert O., Mitchell S., Connelly S. NIST Special Publication 800-207: Zero Trust Architecture. NIST, 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (дата звернення: 07.04.2026).

48. Stoyanova M., Nikoloudakis Y., Panagiotakis S., Pallis E., Markakis E. K. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials. 2020. Vol. 22, No. 2. P. 1191–1221.

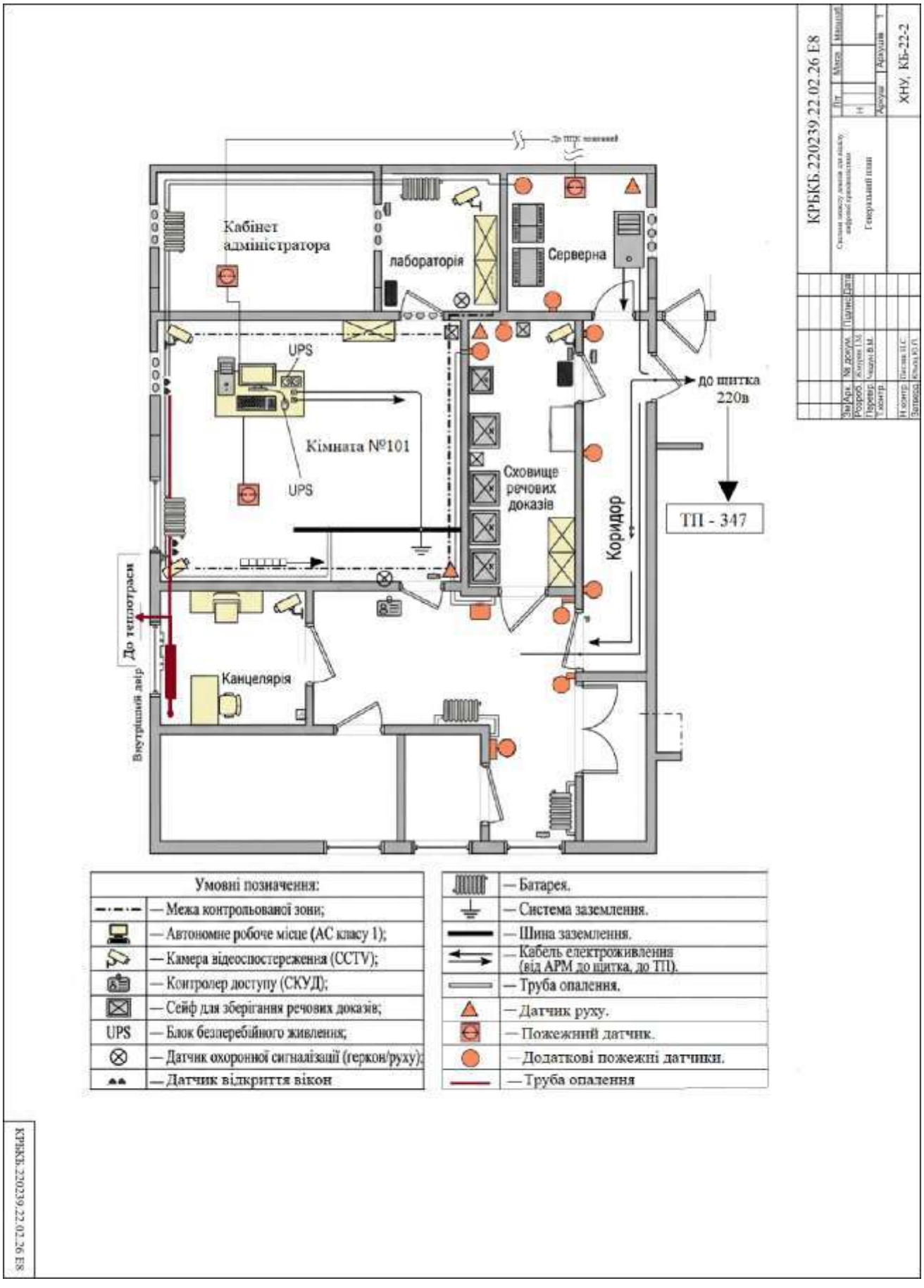
49. Про оперативно-розшукову діяльність : Закон України від 09.08.2024 № 2135-XII. Відомості Верховної Ради України. 1992. № 22. Ст. 303. URL: https://zakon.rada.gov.ua/laws/show/2135-12 (дата звернення: 07.04.2026).

50. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа ; за ред. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.

ДОДАТОК А

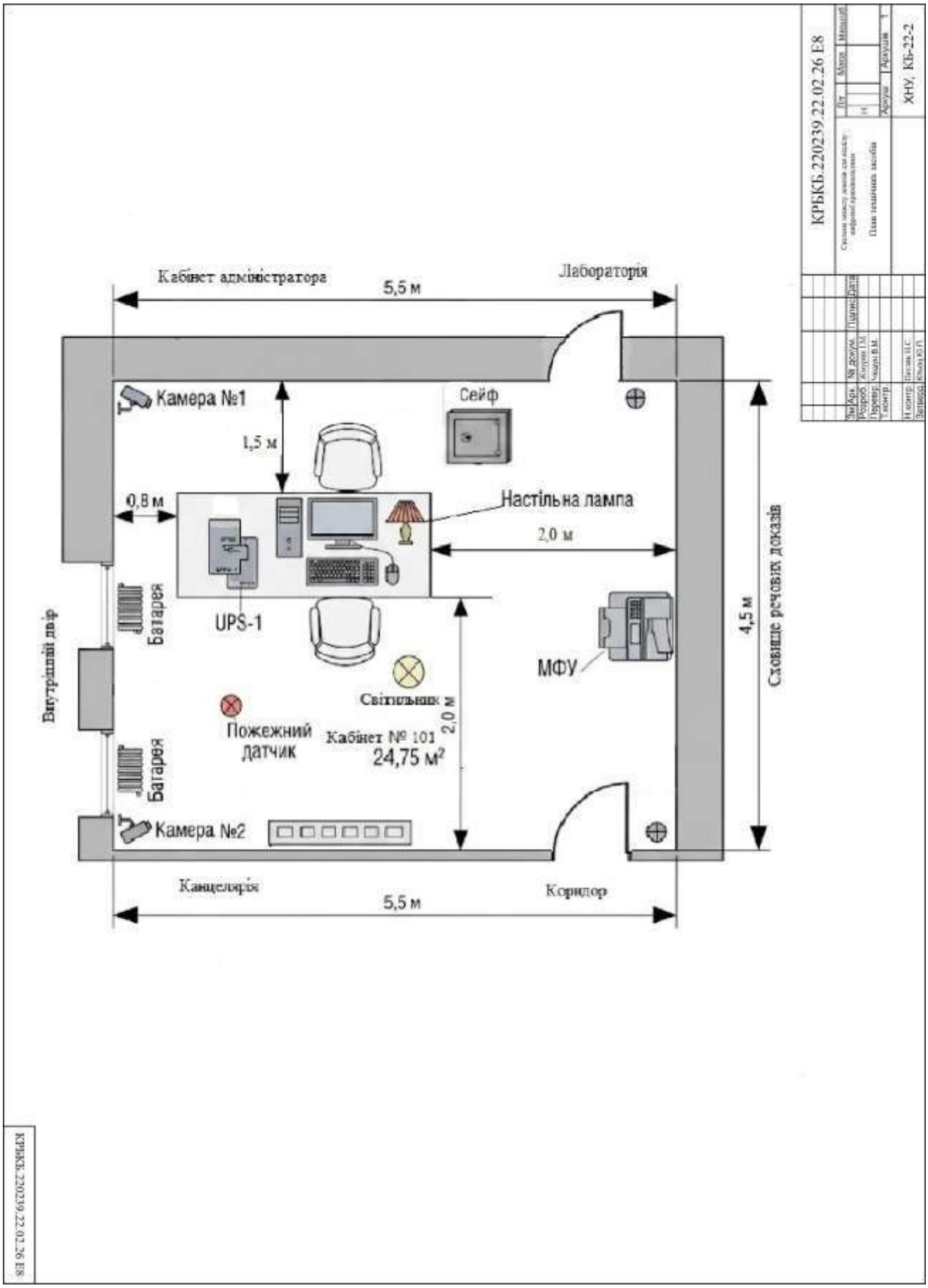
(обов’язковий)

Копії графічної частини



КРБКБ.220239.22.02.26 ЕВ

					КРБКБ.220239.22.02.26 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту даних для відділу цифрової криміналістики	Літ	Маса	Масшт.
Розроб.		Жмурин І.М.			Ситуаційний план			
Перевір.		Чищин В.М.				Аркуш	Аркушів	1
Т.контр.								
Н.контр.		Писяк В.С.				ХНУ, КБ-22-2		
Затверд.		Юльц Ю.П.						


Кабінет адміністратора
5,5 м
Лабораторія
Камера №1
Сейф
1,5 м
0,8 м
Настільна лампа
2,0 м
Батарея
UPS-1
МФУ
4,5 м
Сховище речових доказів
Внутрішній двір
Світильник
Пожежний датчик
Кабінет № 101
24,75 м²
2,0 м
Батарея
Камера №2
Канцелярія
5,5 м
Коридор
КРБКБ.220239.22.02.26 Е8
Пит.
Маса
Масштаб
Змін.
Арк.
№ докум.
Підпис
Дата
Розроб.
Перевір.
Т.контр.
Н.контр.
Затверд.
Арк.
Аркушів
ХНУ, КБ-22-2
КРБКБ.220239.22.02.26 Е8

ДОДАТОК Б

Наказ про створення служби захисту інформації

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАУКОВО-ДОСЛІДНИЙ ЕКСПЕРТНО-КРИМІНАЛІСТИЧНИЙ ЦЕНТР
НАКАЗ

14.02.2026 м. Хмельницький № 15

Про створення служби захисту інформації
в автоматизованій системі класу «1»

Відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах» (із змінами), Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 р. № 373 (із змінами), та Типового положення про службу захисту інформації в автоматизованій системі (НД ТЗІ 1.4-001-2000), затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, а також з метою впровадження заходів із створення та підтримки функціонування комплексної системи захисту інформації (КСЗІ) в автоматизованій системі, яка призначена для обробки інформації з грифом обмеження доступу «Для службового користування», конфіденційної інформації (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень).

НАКАЗУЮ:

1. Створити у Хмельницькому НДЕКЦ МВС службу захисту інформації (СЗІ) для автоматизованої системи класу «1» відділу цифрової криміналістики, що призначена для обробки інформації з грифом обмеження доступу «Для службового користування», конфіденційної інформації (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень).

2. Затвердити Положення про службу захисту інформації в автоматизованій системі класу «1», які призначені для обробки інформації з грифом обмеження доступу «Для службового користування», конфіденційної інформації (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень).

3. Затвердити склад служби захисту інформації в автоматизованій системі класу «1», яка призначена для обробки інформації з грифом обмеження доступу «Для службового користування», конфіденційної інформації (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень).

4. Призначити:

головного судового експерта сектору комп'ютерно-технічних видів досліджень Хмельницького НДЕКЦ МВС ДОВГАНЯ Романа Віталійовича адміністратором безпеки та системним адміністратором автоматизованої системи класу «1»;

старшого судового експерта відділу цифрової криміналістики Хмельницького НДЕКЦ МВС ПИЛИПЧУК Марину Олександрівну адміністратором засобів захисту автоматизованої системи класу «1»;

заступника директора Хмельницького НДЕКЦ МВС КРИШТОФА Миколу Віталійовича начальником служби захисту інформації автоматизованої системи класу «1» та відповідальним за загальну координацію робіт із захисту інформації.

5. Контроль за виконанням цього наказу залишаю за собою.

Директор Хмельницького НДЕКЦ МВС **Андрій ГАНЗЮК**

ДОДАТОК В

Наказ про створення комплексної системи захисту інформації

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАУКОВО-ДОСЛІДНИЙ ЕКСПЕРТНО-КРИМІНАЛІСТИЧНИЙ ЦЕНТР
Н А К А З

15.02.2026 Хмельницький № 3

Про створення комплексної
системи захисту інформації

Відповідно до Закону України «Про захист інформації в інформаційно- комунікаційних системах» №80/94-ВР від 05.07.1994 (зі змінами), Положення про технічний захист інформації в Україні №1229/99 від 27.09.1999 та Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах №373 від 29.03.2006

НАКАЗУЮ:

1. Створити комплексну систему захисту інформації (далі КСЗІ) в автоматизованій системі класу «1», інв. № 114001, у відділі цифрової криміналістики Хмельницького НДЕКЦ МВС, де обробляється інформації з грифом обмеження доступу «Для службового користування», конфіденційної інформації (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень).
2. Відповідальним за створення КСЗІ та впровадження заходів із захисту інформації призначити головного судового експерта сектору комп'ютерно-технічних видів досліджень Довганя Романа Миколайовича.
3. Контроль за виконанням цього наказу залишаю за собою.

Директор Хмельницького НДЕКЦ МВС Ганзюк А.Л.

ДОДАТОК Г

Наказ про створення комісії з категоріювання та обстеження об’єктів інформаційної діяльності

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАУКОВО-ДОСЛІДНИЙ ЕКСПЕРТНО-КРИМІНАЛІСТИЧНИЙ ЦЕНТР
Н А К А З

18.02.2026 Хмельницький № 4

Про утворення комісії з категоріювання та обстеження
об’єктів інформаційної діяльності

Відповідно до законів України «Про інформацію» №2657-XII від 02.10.1992, «Про захист інформації в інформаційно-комунікаційних системах» №80/94-ВР від 05.07.1994 (зі змінами), Тимчасового положення по категоріювання об’єктів №35 від 10.07.95, Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці №215 від 15.04.2013, НД ТЗІ 3.1-001-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Переддипломні роботи»»

НАКАЗУЮ:

1. Утворити комісію з категоріювання та обстеження автоматизованої системи класу 1 у складі:

ГОЛОВА:

Криштоф Микола Віталійович – заступник директора Хмельницького НДЕКЦ МВС

ЧЛЕНИ КОМІСІЇ:

Довгань Роман Миколайович – головний судовий експерт сектору комп'ютерно-технічних видів досліджень

Пилипчук Марина Олександрівна – старший судовий експерт відділу цифрової криміналістики

2. Контроль за виконання цього наказу залишаю за собою.

Директор Хмельницького НДЕКЦ МВС Ганзюк А.Л.

ДОДАТОК Д
Акт категоріювання ОІД (приміщення № 101 відділу цифрової криміналістики)

«ЗАТВЕРДЖУЮ»
Директор Хмельницького НДЕКЦ МВС
_____ Ганзюк А.Л.
«19» лютого 2026 р.
М. П.

АКТ
категоріювання автоматизованої системи класу «1» інв. № 114001 розташованої в приміщенні №101 відділу цифрової криміналістики
(найменування об'єкта категоріювання)

1. Підстава для категоріювання наказ № 3 від 15.02.2026 про створення КСЗІ
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
_____
зміна ознаки, за якою була встановлена категорія об'єкта тощо;
наказ № 4 від 18.02.2026 про утворення комісії з категоріювання та обстеження об’єктів інформаційної діяльності
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання первинне
(первинне, чергове, позачергове)
_____
(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється обробка інформації технічними засобами
(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті
інформація з грифом обмеження доступу «Для службового користування», конфіденційна інформація (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень)
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія IV (четверта)

Голова комісії _____ Криштоф М.В.
(підпис) (ініціали, прізвище)
Члени комісії: _____ Довгань Р.В.
(підпис) (ініціали, прізвище)
_____ Пилипчук М.О.
(підпис) (ініціали, прізвище)

ДОДАТОК Е

Положення про службу захисту інформації в автоматизованій системі класу «1» відділу цифрової криміналістики

ЗАТВЕРДЖЕНО
Наказ Хмельницького НДЕКЦ МВС
14 лютого 2026 року №15

ПОЛОЖЕННЯ

про службу захисту інформації в автоматизованій системі класу «1» відділу цифрової криміналістики

Е.1 Мета створення служби захисту інформації

Метою створення служби захисту інформації (СЗІ) у у Хмельницькому НДЕКЦ МВС є організація та забезпечення комплексного захисту інформації в АС класу «1», де обробляється інформація з грифом обмеження доступу «Для службового користування», конфіденційна інформація (матеріали судових експертиз, цифрові докази та персональні дані суб'єктів кримінальних проваджень).

Створення служби захисту інформації має забезпечити:

1. Організацію системної роботи із захисту інформації, включаючи планування, координацію та контроль заходів ТЗІ.
2. Гарантування цілісності та автентичності цифрових доказів, образів дисків (forensic images) та матеріалів судових експертиз на всіх етапах їх обробки.
3. Недопущення несанкціонованого копіювання, розголошення або передачі відомостей про хід та результати кримінальних проваджень, що обробляються в АС.
4. Підтримання КСЗІ у працездатному стані та впровадження оновлень згідно з сучасними вимогами.
5. Встановлення чіткого порядку доступу судових експертів до ресурсів АС, виключаючи можливість несанкціонованих дій або випадкового знищення даних.
6. Створення та ведення нормативної документації щодо інформаційної безпеки й технічного захисту інформації.
7. Впровадження заходів відповідно до НД ТЗІ 3.6-006-24, зокрема організаційних, технічних, інженерних, режимних заходів.
8. Забезпечення постійної працездатності комплексної системи захисту інформації, контроль за станом антивірусного захисту та засобів блокування несанкціонованого запису.
9. Реагування на інциденти інформаційної безпеки, проведення розслідувань, недопущення повторення порушень.

Таким чином, мета створення СЗІ – забезпечити гарантований рівень захисту інформації в АС-1 підприємства та виконати встановлені державою вимоги у сфері технічного захисту інформації.

Е.2 Місце служби захисту інформації у структурі

Служба захисту інформації є функціонально незалежним підрозділом у складі Хмельницького НДЕКЦ МВС. Вона створюється з метою забезпечення об'єктивного контролю за станом безпеки інформації та є незалежною від персоналу, який безпосередньо використовує АС для проведення судових експертиз.

У структурі відділу цифрової криміналістики служба захисту інформації створена як окремий підрозділ, що включає таких відповідальних осіб:

Керівником СЗІ є заступник директора Центру – Криштоф Микола Віталійович.

Адміністратором безпеки та системним адміністратором є головний судовий експерт – Довгань Роман Миколайович.

Адміністратором засобів захисту є старший судовий експерт – Пилипчук Марина Олександрівна.

Підпорядкованість:

Служба захисту інформації у своїй діяльності керується розпорядженнями директора центру та вимогами нормативних документів системи ТЗІ України.

Адміністратор безпеки та адміністратор засобів захисту підпорядковуються безпосередньо керівнику СЗІ.

Експерти відділу, які мають доступ до роботи в АС, у питаннях забезпечення безпеки інформації зобов'язані виконувати всі вимоги та вказівки СЗІ.

СЗІ виконує функції: розмежування прав користувачів; розробки політики безпеки; організації режимних заходів; ведення журналів обліку; проведення інструктажів; реагування на інциденти; забезпечення вимог НД ТЗІ 1.4-001-2000.

СЗІ діє як самостійна контролююча одиниця, що гарантує відсутність конфлікту інтересів між тими, хто обслуговує техніку, і тими, хто контролює її безпеку.

Е.3 Наказ про створення служби захисту інформації

Додаток Б.

Е.4 Структури служби захисту інформації

Структура служби захисту інформації визначається організаційними та технічними особливостями підприємства, кількістю працівників, обсягами оброблюваної інформації та класом автоматизованої системи. Оскільки в Хмельницькому НДЕКЦ МВС експлуатується одна автоматизована система класу "1", служба формується за спрощеною моделлю, яка допускається нормативними документами ТЗІ.

Е.4.1 Повноваження служби захисту інформації

У процесі функціонування СЗІ співробітники Хмельницького НДЕКЦ МВС, які входять до її складу, мають право:

здійснювати поточний контроль за станом захисту інформації в АС відділу цифрової криміналістики та діяльністю експертів щодо виконання ними вимог нормативно-правових актів у сфері ТЗІ;

подавати пропозиції начальнику СЗІ щодо призупинення процесу проведення експертних досліджень в АС у випадку виявлення порушень політики безпеки або виникнення реальної загроз цілісності чи конфіденційності цифрових доказів;

складати і подавати начальнику СЗІ акти щодо виявлених порушень режиму доступу та правил роботи з інформацією «Для службового користування»;

проводити службові перевірки або брати участь у розслідуванні інцидентів безпеки (спроб несанкціонованого копіювання образів дисків);

готувати пропозиції щодо оснащення АС класу «1» спеціалізованими технічними та програмними засобами захисту (засоби блокування запису, антивірусні пакети тощо), які мають експертний висновок;

виходити до керівництва Центру з пропозиціями щодо проведення державної експертизи КСЗІ;

отримувати безперешкодний доступ до журналів реєстрації подій, носіїв резервного копіювання доказової бази та конфігурацій системного ПЗ для виконання контрольних функцій;

надавати рекомендації щодо включення нових компонентів до складу АС-1 або подавати пропозиції щодо заборони їх використання, якщо вони порушують політику безпеки;

ініціювати зміну паролів та перегляд прав доступу користувачів у разі кадрових змін або виникнення підозр щодо компрометації облікових даних.

Е.4.2 Обов'язки служби захисту інформації

У процесі функціонування СЗІ співробітники Хмельницького НДЕКЦ МВС зобов'язані:

організовувати та забезпечувати повноту і якість виконання організаційно-технічних заходів із захисту інформації в АС-1;

вчасно та у повному обсязі доводити до користувачів інформацію про зміни у сфері захисту інформації, які стосуються їх роботи;

контролювати відповідність правил, інструкцій та режимних вимог, прийнятих у АС-1, чинному законодавству України та НД ТЗІ;

здійснювати контрольні перевірки стану захищеності інформації в АС відділу цифрової криміналістики;

забезпечувати конфіденційність робіт з монтажу, обслуговування та тестування засобів захисту інформації;

брати участь у проведенні оцінок ризиків, аналізу загроз та перевірок відповідності режиму захисту інформації;

забезпечувати ведення та належне заповнення журналів:

– журнал обліку носіїв;

– журнал обліку інцидентів;

– журнал обліку доступу;

– журнал обслуговування засобів захисту інформації;

сприяти створенню та дотриманню безпечних умов для збереження інформації, отриманої за договорами, контрактами та від приватних осіб;

здійснювати моніторинг стану програмних і апаратних засобів, що впливають на безпеку АС-1;

негайно повідомляти начальника СЗІ про виявлені порушення, інциденти або спроби несанкціонованого доступу.

Е.4.3 Відповідальність

Е.4.3.1 Загальна відповідальність

Керівництво та співробітники СЗІ за невиконання або неналежне виконання службових обов'язків несуть дисциплінарну, адміністративну або кримінальну відповідальність згідно з законодавством України.

Е.4.3.2 Відповідальність начальника СЗІ

Керівник СЗІ (заступник директора – Криштоф М.В.) відповідає за:

організацію робіт із захисту інформації в АС;

ефективність функціонування КСЗІ та виконання вимог НД ТЗІ;

своєчасне розроблення та виконання «Плану захисту інформації в АС»;

якість виконання завдань співробітниками СЗІ;

координацію взаємодії підрозділів щодо питань інформаційної безпеки;

організацію навчання персоналу з питань ТЗІ та КСЗІ;

виконання внутрішніх розпоряджень, режимних вимог та правил охорони праці.

Е.4.3.3 Відповідальність співробітників СЗІ

Співробітники СЗІ відповідають за:

дотримання вимог нормативних документів і внутрішніх положень підприємства;

повноту та якість реалізації організаційних і технічних заходів захисту;

точність і достовірність результатів контрольних перевірок та оцінювання ризиків;

дотримання строків проведення перевірок стану КСЗІ;

правильність документального оформлення результатів робіт;

забезпечення режиму захисту інформації та збереження носіїв.

Е.5 Організація робіт служби захисту інформації Хмельницького НДЕКЦ МВС

Е.5.1 Структура та організація СЗІ

Служба захисту інформації (СЗІ) Хмельницького НДЕКЦ МВС здійснює свою діяльність відповідно до Положення про СЗІ Центру, Плану захисту інформації в АС класу «1», технічної документації на комплексну систему захисту інформації (КСЗІ), експлуатаційних та організаційно-розпорядчих документів установи та вимог нормативного документа НД ТЗІ 1.4-001-2000.

СЗІ створена на підставі наказу директора Хмельницького НДЕКЦ МВС. У наказі визначено особовий склад служби та призначено начальника СЗІ.

Структура СЗІ підприємства включає три основні посади начальник СЗІ, адміністратор безпеки та системний адміністратор АС-1, адміністратор засобів захисту.

Функціональні обов'язки та відповідальність усіх членів СЗІ визначено у відповідних розділах цього Положення.

СЗІ взаємодіє з керівництвом Центру, сектором фінансового забезпечення та за потреби залучення сертифікованих фахівців для аудиту або експертизи КСЗІ.

Матеріально-технічну базу СЗІ складають автономна робоча станція експерта (інв. № 114001), програмні та апаратні засоби захисту, система резервного копіювання образів доказів, журнали реєстрації подій та носіїв, документація з ТЗІ та інструкції користувачів. Матеріально-технічне забезпечення діяльності СЗІ здійснюється за рахунок бюджету Центру.

Е.5.2 Обов'язки начальника СЗІ

Е.5.2.1 Основні завдання начальника СЗІ

Начальник служби захисту інформації:

бере участь у розробленні плану захисту інформації в АС-1;

затверджує інструкції користувача, посадові обов'язки членів СЗІ та режимні вимоги;

організовує встановлення і налаштування програмного забезпечення, необхідного для роботи АС-1;

організовує категоріювання АС-1 та проводить роботи з оцінки ризиків і загроз;

контролює виконання вимог плану захисту інформації;

контролює дотримання користувачами правил безпеки та режимних вимог;

керує створенням, впровадженням і підтримкою КСЗІ;

проводить інструктажі для користувачів АС-1 та забезпечує підвищення кваліфікації членів СЗІ;

організовує службові перевірки та розслідування інцидентів інформаційної безпеки.

Е.5.2.2 Начальник СЗІ зобов'язаний:

забезпечувати виконання встановлених правил доступу до конфіденційної інформації;

розробляти та впроваджувати процедури захисту інформації від НСД, витоку або втрати;

проводити аналіз загроз та ризиків інформаційній безпеці;

забезпечити навчання персоналу правилам інформаційної безпеки;

здійснювати моніторинг стану захищеності інформації;

вживати заходів реагування у випадку інцидентів інформаційної безпеки;

підтримувати належний стан технічних засобів захисту та контролю.

Е.5.2.3. Права начальника СЗІ

Начальник СЗІ має право:

визначати вимоги щодо захисту інформації в АС-1;

приймати рішення про модернізацію, оновлення або внесення змін до КСЗІ;

контролювати стан захищеності інформації в АС-1;

ініціювати проведення перевірок, аудитів та службових розслідувань;

вимагати виконання правил безпеки від працівників підприємства.

Е.5.3 Обов'язки адміністратора безпеки

Е.5.3.1 Адміністратор безпеки зобов'язаний:

розробляти та впроваджувати політики безпеки АС-1;

контролювати облікові записи користувачів, розмежування доступу та права доступу;

вести журнали реєстрації подій, носіїв, інцидентів;

контролювати виконання політик доступу;

проводити аудит АС-1 для виявлення потенційних загроз;

забезпечувати резервне копіювання та контроль цілісності копій;

повідомляти начальника СЗІ про всі випадки НСД, порушення режиму та інциденти;

реагувати на інциденти та брати участь у їх розслідуванні.

Е.5.3.2 Права адміністратора безпеки:

контролювати та налаштовувати засоби захисту інформації;

здійснювати аудит доступів користувачів;

вимагати зміни паролів та параметрів безпеки у разі загроз;

пропонувати нові технічні рішення для покращення безпеки АС-1.

Е.5.4 Обов'язки системного адміністратора

Е.5.4.1 Системний адміністратор зобов'язаний:

налаштовувати ПЗ АС-1 і підтримувати його працездатність;

виконувати оновлення ПЗ відповідно до вимог захисту інформації;

реєструвати користувачів та налаштовувати параметри доступу;

проводити резервне копіювання;
моніторити стан технічних ресурсів;
забезпечувати цілісність та доступність інформації.
Е.5.4.2 Права системного адміністратора:
доступ до всіх технічних ресурсів АС-1 для обслуговування;
змінювати налаштування ПЗ для забезпечення безпеки.
Е.5.5 Обов’язки адміністратора ЗЗ
Е.5.5.1 Адміністратор ЗЗ зобов’язаний:
впроваджувати та налаштовувати технічні засоби захисту;
контролювати технічні канали витоку інформації;
проводити перевірки стану апаратних засобів захисту;
брати участь у модернізації технічних аспектів КСЗІ;
забезпечувати фізичний захист приміщення АС-1.
Е.5.5.2 Права адміністратора ЗЗ:
проводити оцінку технічних вразливостей;
вимагати усунення технічних загроз;
надавати пропозиції щодо модернізації засобів ТЗІ.

ДОДАТОК Ж

Акт обстеження на об’єкті інформаційної діяльності автоматизованої системи класу «1» інв. №114001, приміщення № 101 відділу цифрової криміналістики

ЗАТВЕРДЖУЮ
Директор Хмельницького
НДЕКЦ МВС
_____ Ганзюк А.Л.
(підпис, ініціали, прізвище)
21.02.2026

АКТ

обстеження на об’єкті інформаційної діяльності

автоматизована система класу «1» інв. №114001, приміщення № 101 відділу цифрової криміналістики

(назва, належність об'єкта інформаційної діяльності)

Обстеження ОІД проведено комісією у складі: голови комісії: заступника директора Центру Криштофа Миколи Віталійовича та членів комісії: головний судовий експерт Довганя Романа Миколайовича та старший судовий експерт Пилипчук Марини Олександрівни, призначеною наказом Хмельницького НДЕКЦ МВС від 18.02.2026 №4.

Ж.1 Ситуаційний план ОІД

Ж.1.1 Схема ситуаційного плану ОІД

Схему ситуаційного плану ОІД наведено на рис. Ж.1.

Рисунок Ж.1 – Схема ситуаційного плану ОІД

Ж.1.2 Опис ситуаційного плану ОІД

Об’єкт інформаційної діяльності (ОІД) – це частина інженерно-технічної споруди, а саме службове приміщення відділу цифрової криміналістики (кабінет № 101), у якому здійснюється експертне дослідження цифрових доказів та обробка інформації з обмеженим доступом у складі автоматизованої системи класу “1”.

ОІД розташований на 2-му поверсі адміністративно-виробничої будівлі Хмельницького НДЕКЦ МВС за адресою: 29018, Хмельницька область, м. Хмельницький, вул. Молодіжна, 12.

Будівля – капітальна, цегляна, 4-поверхова. Приміщення має звичайне розташування, без особливих архітектурних ризиків щодо захисту інформації. Приміщення кабінету № 101 розташоване у внутрішній частині будівлі, що мінімізує ризики дистанційного технічного спостереження з боку громадських місць.

Категорія приміщення за функціональним призначенням – четверта.

Категорія інформаційної системи – перша (АС-1 без виходу в Інтернет, один користувач, один ПК).

Пропускний та внутрішньооб'єктовий режим на території установи здійснюється згідно з відомчими наказами та інструкціями МВС щодо порядку доступу осіб, режимних вимог та охорони майна. Територія є суворо контрольованою. Доступ сторонніх осіб у приміщення ОІД заборонений; вхід здійснюється виключно за службовою необхідністю персоналом, що має відповідний допуск. У позаробочий час приміщення перебуває під охороною технічних засобів сигналізації.

Підприємство не примикає до будівель, де знаходяться офіси іноземних компаній або проживають іноземні громадяни. У радіусі 200 метрів таких об'єктів немає.

Схематично на ситуаційному плані (рис. 1) відображені: межі контрольованої зони; пропускний пункт; розміщення будівлі, де знаходиться ОІД; відстані від ймовірних місць розташування технічних засобів розвідки (ТЗР) до ОІД (20 м, 30 м, 58 м, 148 м); напрямки та сторони горизонту; можливі точки встановлення мобільних або стаціонарних засобів технічної розвідки.

Основні характеристики вулиць, що проходять поруч з будинком в якому знаходиться ОІД наведено в таблиці Ж.1.

Таблиця Ж.1 – Характеристики вулиць

№ з/п	Назва вулиці	Розташування відносно ОІД	Ширина частини для про-їзду, м	Ширина пішохідної частини, м	Інтенсивність руху автотранспорту	Наявність місць неконтрольованого перебування автотранспорту
1	вул. Молодіжна	Південь	9,0	2,5	Середня	Так
2	вул. Тернопільська	Схід	12,0	3,0	Висока	Так

Об'єкти, що оточують будинок, в якому знаходиться ОІД наведено в таблиці Ж.2.

Таблиця Ж.2

№ з/п	Розташування відносно ОІД	Кількість поверхів	Адреса	Характер діяльності	Відстань від ОІД, (м)
1	2	3	4	5	6
1	Схід	9	вул. Молодіжна, 15	Житлова забудова	35
2	Південний схід	2	вул. Тернопільська, 15/2	Електротранс	72
3	Північний схід	5	вул. Тернопільська, 15	Житловий будинок, стоматологія	100
4	Південь	1	вул. Молодіжна, 14/1а	Автоплощадка	40
5	Північ	2	вул. Молодіжна, 14а	Ваш автосервіс	140

6	Захід	2	вул. Молодіжна, 16/1	ООО "СВ-Текстиль"	75

Ж.2 Вказують такі відомості:

Ж.2.1 Характеристика ОІД

Об’єктом інформаційної діяльності (ОІД) є службове приміщення відділу цифрової криміналістики (кабінет № 101), розташоване на 2-му поверсі адміністративної будівлі за адресою: м. Хмельницький, вул. Молодіжна, 12. Кабінет призначений для проведення комп’ютерно-технічних досліджень, роботи з цифровими доказами та обробки конфіденційної інформації. Приміщення належить до звичайного типу розміщення, характеризується стандартними умовами експлуатації та звичайним рівнем проникності огороджувальних конструкцій.

Ж.2.2 Характеристика складових ОІД

Приміщення має площу 24,75 м², висота стелі становить 2,8 м. Будівля цегляна, за функціональним призначенням – адміністративна. Приміщення забезпечене природним освітленням через два вікна, що виходять на західну сторону (у внутрішній двір установи).

Стіни та перегородки виконані з паленої цегли. Зовнішні стіни мають товщину 510 мм, внутрішні міжкімнатні стіни – 380 мм. Стан огороджувальних конструкцій задовільний: візуальне обстеження не виявило наскрізних тріщин, незаповнених порожнин або технологічних отворів до суміжних приміщень, крім місць проходження інженерних комунікацій, які належним чином ущільнені.

Підлога – залізобетонна плита перекриття з покриттям лінолеумом на бетонній стяжці. Стеля – залізобетонна, підвісні декоративні конструкції відсутні. Світлопрозорі конструкції (вікна) представлені двома металопластиковими блоками з двокамерними склопакетами. Обидва вікна обладнані щільними жалюзі, що унеможливлюють візуальний перегляд екранів моніторів ззовні. Двері – дерев’яні, посилені, обладнані внутрішнім замком та пристосуванням для опечатування в неробочий час.

Суміжні приміщення розташовані таким чином: північ – кабінет адміністратора та лабораторія; південь – канцелярія, коридор; знизу – складські приміщення на 1-му поверсі; зверху – службові кабінети адміністрації; захід – зовнішня стіна будівлі, схід – сховище речових доказів. Найбільший потенційний вплив на рівень захищеності становить коридор через періодичний рух працівників та можливість доступу сторонніх осіб.

У приміщенні проходять такі інженерні комунікації: електромережа 220 В, виконана прихованою проводкою, освітлювальна мережа. Телефонна лінія відсутня. Встановлено димові сповіщувачі пожежної сигналізації та датчик відкриття дверей (геркон), підключені до пульта охорони установи. Опалення – центральне водяне. Сталеві труби проходять вертикально крізь міжповерхові перекриття. Встановлено два чавунних радіатори (під кожним вікном). Вентиляція – природна, механічна відсутня. Водопостачання та каналізація у приміщенні відсутні.

Серед обладнання, що розташоване в ОІД, наявні: персональний комп’ютер (АС-1), монітор, принтер локальний, сейф для зберігання документів, офісні меблі (робочий стіл), паперознищувальна машинка. Бездротові інтерфейси (Wi-Fi, Bluetooth) відсутні.

Потенційні канали витоку інформації з приміщення включають: несанкціонований доступ до ПК, використання зовнішніх носіїв, підключення сторонніх пристроїв, оптичні через вікна.

За результатами обстеження встановлено, що приміщення кабінету № 101 відповідає типовим вимогам до ОІД у складі АС класу "1" та може бути використане для оброблення інформація з грифом обмеження доступу «Для службового користування», конфіденційна інформація (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень) за умови впровадження додаткових організаційних та технічних заходів, які усунуть наявні фактори ризику.

Ж.2.3 Схеми розміщення комунікацій, обладнання систем електроживлення, у т.ч. трансформаторної підстанції.

У приміщенні кабінету № 101 відділу цифрової криміналістики, що є складовою об’єкта інформаційної діяльності (ОІД), проходить низка інженерних комунікацій та мереж. Аналіз розміщення цих комунікацій проводився згідно з технічною документацією на будівлю та ситуаційним планом (рис. 1).

Приміщення підключене до основної електромережі будівлі напругою 220 В. Живлення надходить від розподільчого щита, розташованого на поверсі. Електропроводка прокладена приховано (у штробах стін), що мінімізує можливість несанкціонованого підключення до ліній живлення АС. У кабінеті встановлено 6 розеткових груп для підключення оргтехніки та спеціалізованого обладнання, а також окрема розетка для електронно-обчислювальної техніки (складової АС класу «1»). Система освітлення представлена стельовими світильниками, що утворюють єдину зону освітлення.

Трансформаторна підстанція, що забезпечує живлення об'єкта, розташована поза межами контрольованої зони (КЗ) на відстані близько 115 м від будівлі. Кабельні лінії живлення від ТП до будівлі прокладені підземним способом у кабельних каналах.

У приміщенні наявні такі системи: пожежний датчик системи протипожежної безпеки (представлена димовим сповіщувачем, підключеним до загальнооб’єктного пульта пожежної охорони); опалювальний радіатор, підключений до центральної системи опалення (у приміщенні встановлено два опалювальні радіатори (чавунні)); вентиляційні канали (природна вентиляція через решітку проходять у товщі стіни й виходять на дах будівлі); освітлювальна система (одна зона освітлення).

Телевізійні, радіотрансляційні та інші широкомовні системи в приміщенні відсутні. Системи кондиціонування, водопостачання та каналізації у приміщенні відсутні.

Під час обстеження встановлено такі елементи, що виходять за межі КЗ:

Електрична лінія живлення, що частково проходить через суміжну стіну:

– є частиною загальної мережі будівлі;

– вимагає контролю цілісності та перевірки відсутності несанкціонованих підключень.

Вентиляційний канал, що виходить за межі КЗ:

– необхідний для природної вентиляції.

Трубопроводи системи опалювання:

– проходять через суміжні приміщення зверху та знизу.

За результатами обстеження елементів, які: не мають виробничої необхідності, можуть створювати технічні канали витоку, підлягають демонтажу – не виявлено.

Усі комунікації, що проходять через приміщення, відповідають функціональному призначенню ОІД та експлуатації АС класу «1».

Ж.2.4 Технічні засоби, що розташовані в приміщенні ОІД

У приміщенні кабінету № 101 відділу цифрової криміналістики, яке є об’єктом інформаційної діяльності (ОІД), встановлені технічні засоби, що використовуються для проведення комп’ютерно-технічних досліджень та оброблення інформація з грифом обмеження доступу «Для службового користування», конфіденційна інформація (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень). Під час обстеження визначено такі категорії технічних засобів: обчислювальна техніка, спеціалізоване експертне обладнання, офісна техніка та засоби технічного захисту інформації.

У приміщенні розміщено:

Персональний комп’ютер (ПК) бухгалтерії, який входить до складу АС класу «1».

Призначення: оброблення конфіденційної інформації, проведення експертних досліджень цифрових носіїв, формування висновків експерта.

Монітор 24 дюйми

Призначення: відображення інформації, у тому числі ІзОД.

Клавіатура та маніпулятор “миша”

Призначення: керування ПК та введення даних.

Комп’ютерне обладнання розташоване на робочому столі, підключене до електроживлення.

Програмне забезпечення включає: ОС Windows 11 (без доступу до зовнішніх ресурсів), бухгалтерське ПЗ, антивірусний захист («ІІТ Захищений диск-4»), засоби контролю доступу.

У приміщенні знаходяться такі офісні засоби:

Лазерний принтер. Призначення: друк документів, включно з документами ІзОД. Підключення: USB до ПК. Не має бездротових інтерфейсів. Ризики: можливе залишкове зображення на термобарабані (потребує контрольного очищення).

Металевий сейф. Призначення: тимчасове зберігання речових доказів (жорстких дисків, флеш-накопичувачів) та робочих документів.

Засоби відображення та аудіотехніка. Телевізори, радіоприймачі, аудіосистеми та інші засоби широкомовного прийому – відсутні.

Веб-камера та мікрофон у ПК – вимкнені та заблоковані.

У приміщенні встановлені засоби технічного захисту інформації:

Пожежний датчик (оптичний) – підключений до централізованої сигналізації.

Металеві двері з замком – забезпечують контроль доступу до приміщення.

На обох вікнах встановлені щільні жалюзі для захисту від зорового спостереження та металеві решітки (з огляду на розташування на 2-му поверсі та режимність об'єкта).

Пломбувальні наклейки на корпусі ПК.

Під час обстеження встановлено можливі джерела ризику: електропроводка, що проходить через інші приміщення, наявність двох віконних прорізів, що потребують постійного контролю положення жалюзі під час роботи.

Усі перелічені канали підлягають подальшому врахуванню під час розроблення моделі загроз та технічного завдання на КСЗІ.

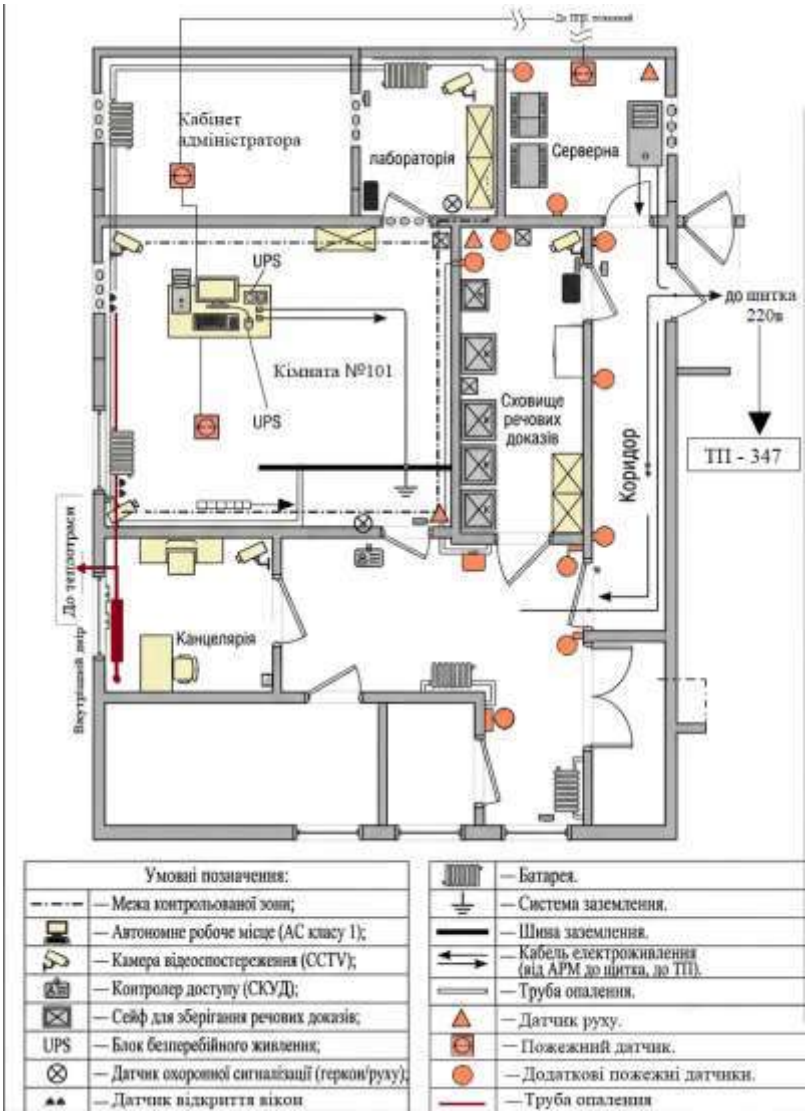


Рисунок Ж.2 – Генеральний план ОІД

Ж.2.5 Результати аналізу наявності документів та засобів ТЗІ в установі

У ході обстеження перевірено наявність нормативних, організаційних і технічних документів, що регламентують захист інформації в установі, а також засобів ТЗІ, впроваджених та функціонуючих у межах об’єкта. Результати наведено нижче.

Схема контрольованої зони (КЗ), у межах якої розташований ОІД – наявна (рисунок 2)

Модель загроз для інформації з обмеженим доступом (ІзОД) – наявна

Дані про проведення випробувань та спеціальних досліджень технічних засобів – рекомендується провести випробування

Дані про виконавців робіт з ТЗІ на інших ОІД установи – у підприємстві немає інших ОІД, які підлягають ТЗІ.

Дані про проєктні та монтажні організації, що виконували роботи на інших ОІД – зовнішніх спеціалізованих організацій до робіт з ТЗІ не залучали.

Системи безпеки, до яких може бути інтегрований комплекс ТЗІ – ТЗІ може бути інтегрований з пожежною системою та загальною електромережею.

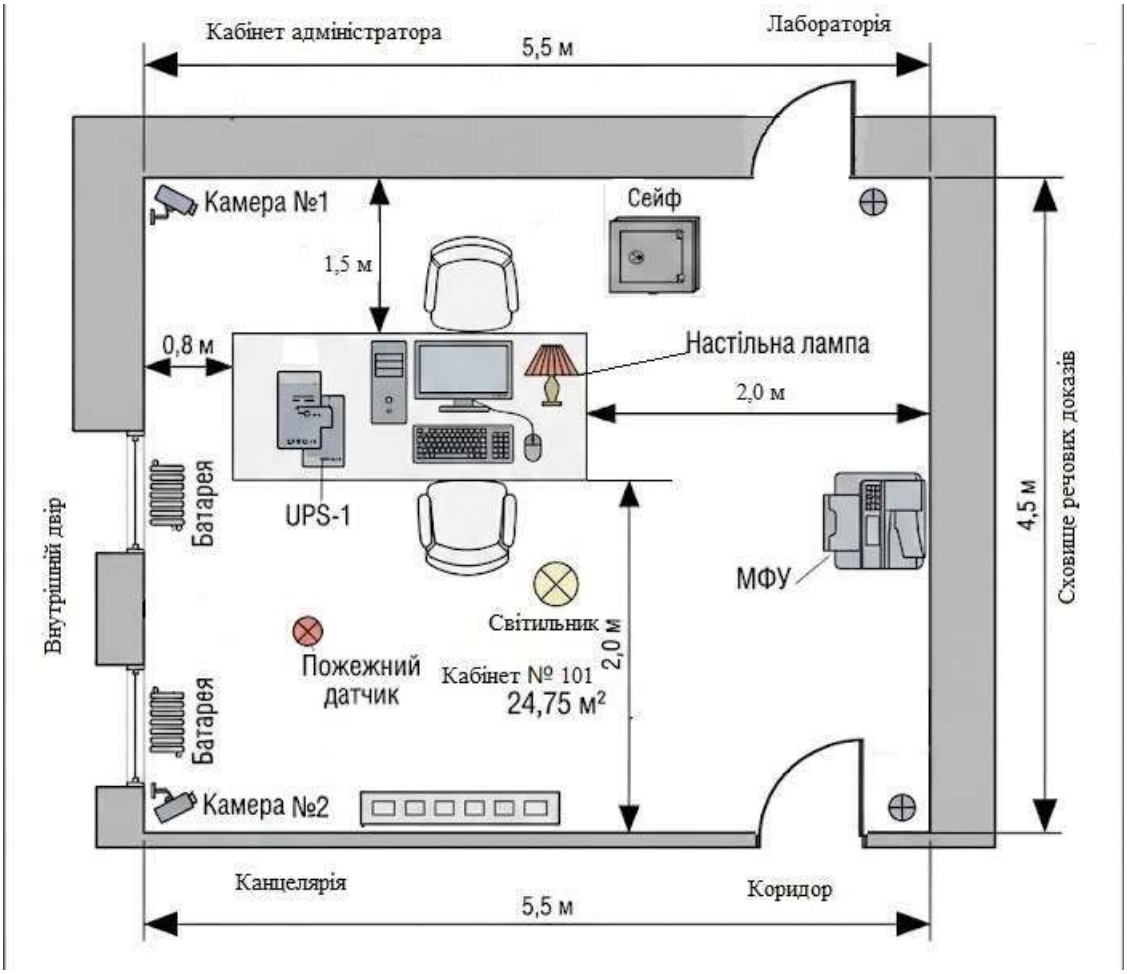


Рисунок Ж.3 – Схема розташування основних технічних засобів

Ж.3 Основні технічні засоби

Ж.3.1 Схему розташування ОТЗ наведено на рис. Ж.3.

Ж.3.2 Опис ОТЗ.

У приміщенні кабінету № 101 розміщені основні технічні засоби (ОТЗ), що входять до складу автоматизованої системи класу «1» та використовуються експертами відділу цифрової криміналістики для виконання функціональних обов’язків (дослідження цифрових доказів).

Загалом у приміщенні функціонує один робочий комплекс, що містить персональний комп’ютер (Fujitsu) із відповідними периферійними пристроями та багатофункціональним пристроєм (HP). Усі технічні засоби знаходяться в працездатному стані та експлуатуються відповідно до технічних інструкцій та вимог безпеки.

Перелік ОТЗ, розміщених у приміщенні кабінету № 101, наведено в таблиці Ж.3.

Таблиця Ж.3.

№ з\п	Найменування технічного засобу	Тип	Серійний №
1	Системний блок у складі:	Fujitsu Esprimo E710 SFF	14950803
	Материнська плата	Fujitsu D3161-A1 (Intel Q75)	C6-SN334455
	Центральний процесор	Intel Core i3-3220	621156
	НЖМД	Samsunq HD080HJ	S08EJ1GYB32110
	ОЗП	DDR3 16GB (2x8GB) Kingston	MIU25664DS88C36-5T
	Накопичувач системний	Kingston SSD Now A400 2 Tb	MIU25664DS88C36
	Накопичувач архівний	Samsung HD080HJ (80 GB)	S08EJ1GYB32110
	Корпус	Open Gray	4000388
	Дисковод	Sony	22960954
	CD-ROM	DVD-RW SH-224DB	TS34AO2388BB
	Блок живлення	Fujitsu 280W 80+ Gold	BX700U-SN556677
2	Клавіатура	Logitech K120	K120-UK112233
3	Апаратний блокатор запису	Tableau Forensic Bridge T8u	T8U-2024-0912
4	Маніпулятор "миша"	Logitech M100	M100-SN445566
5	Монітор	Dell 22″ P224W	SN-DP224W7890
6	МФУ (принтер, сканер, копір)	HP LaserJet Pro MFP M281fdw	LJMFP-M281-778899
7	Джерело безперебійного живлення	APC Back-UPS BX700U-GR	BX700U-SN556677

Ж.4 Допоміжні технічні засоби та системи

Ж.4.1 Схему розташування ДТЗС наведено на рис. Ж.3.

Ж.4.2 Опис ДТЗС. Перелік ДТЗС, які встановлено у приміщені, наведено в таблиці Ж.4.

Таблиця Ж.4.

№ з/п	Найменування, тип ТЗПІ та ДТЗС	Серійний номер	Кількість	Призначення
1	Система водяного опалення (радіатори + труби)	б/н	2	Обігрів приміщення
2	Знищувач паперу "Inteimus"	777381.12067	1	Фізичне знищення документів бухгалтерії
3	Датчик охоронної сигналізації дверний ДМК-П2	б/н	2	Контроль відкриття дверей
4	Датчик охоронної сигналізації на відкриття вікна ДМК-П2	б/н	2	Контроль відкриття вікна
5	Датчик охоронної сигналізації на рух	85705	1	Виявлення руху всередині приміщення
6	Датчики пожежної сигналізації СПД3.2	б/н	2	Реагування на появу диму

№ з/п	Найменування, тип ТЗПІ та ДТЗС	Серійний номер	Кількість	Призначення
7	Канал природної вентиляції	б/н	1	Забезпечення циркуляції повітря
8	Жалюзі металопластикові (вертикальні)	б/н	2	Захист від зорового спостереження через вікна

Електроживлення приміщення кабінету № 101 (відділ цифрової криміналістики) здійснюється від внутрішньої електромережі адміністративного будинку за адресою вул. Молодіжна, 12. Живлення будівлі надходить від трансформаторної підстанції, розташованої поза межами КЗ на відстані близько 115 м. Слід враховувати, що дана трансформаторна підстанція також забезпечує електроенергією сторонніх споживачів (житлові будинки та приватні заклади по вул. Молодіжній та вул. Тернопільській), що враховано при аналізі загроз.

Схеми електроживлення, освітлення та заземлення приміщення № 101 наведені на план-схемі (рис. 2). Заземлення виконано відповідно до діючих будівельних норм та підключено до загального контуру заземлення будівлі.

У приміщенні кабінету № 101 прокладено систему охоронної сигналізації, що складається з датчика відкриття дверей, двох датчиків відкриття вікон та одного об'ємного датчика руху. Лінії охоронної сигналізації виведені на пульт чергового воєнізованої охорони, який розташований на першому поверсі будівлі. Сигналізація є частиною загальнобудинкової системи охорони та працює в цілодобовому режимі.

Приміщення кабінету № 101 обладнане також системою пожежної сигналізації. Два димових пожежних датчики СПД 3.2 під'єднані до загальної пожежної системи будівлі. Кінцеві ланцюги пожежної сигналізації виведено на пожежний пульт, що розташований на першому поверсі адміністративної будівлі.

Система водяного опалення приміщення складається з двох чавунних радіаторів (розміщених під вікнами) та з’єднувальних сталевих труб. Трубопроводи опалення проходять транзитом через суміжні приміщення (службові кабінети) на даному поверсі, а також через перекриття на верхній та нижній поверхи.

До ОІД не заходять лінії радіофікації, системи оповіщення, годинофікації або системи холодного чи гарячого водопостачання.

Ж.5. Телекомунікації ОТЗ і ДТЗС, а також будівельні та інженерні конструкції та комунікації, що виходять за межі КЗ

У результаті обстеження встановлено, що з приміщення № 35 частина інженерних комунікацій виходить за межі контрольованої зони.

До таких складових належать:

1. Труби системи водяного опалення

– У приміщенні кабінету № 101 розміщено два опалювальних радіатори (відповідно до кількості віконних прорізів), які підключені до загальнобудинкової мережі опалення.

– Сталеві трубопроводи проходять вертикально через міжповерхові перекриття до суміжних приміщень та виходять за межі контрольованої зони для підключення до міської тепломережі.

2. Система заземлення

– Використовується загальнобудинкова заземлювальна шина.

– Провідники заземлення під’єднані до спільного заземлювального контуру будівлі та виходять за межі КЗ. Стан контактів заземлення задовільний.

3. Електромережа

– Електроживлення подається від внутрішньої мережі будівлі, яка живиться від ТП і має сторонніх споживачів.

4. Вентиляційний канал

– Природна вентиляція здійснюється через вертикальний вентиляційний канал, який виходить на дах будівлі.

5. Будівельні конструкції (вікна)

– Оскільки об'єкт розташований на 2-му поверсі, два вікна приміщення виходять на відкриту територію внутрішнього двору. Незважаючи на наявність решіток та жалюзі, склопакети є елементами, що межують із зовнішнім середовищем за межами КЗ, і можуть бути використані для дистанційного зняття інформації (оптичний канал).

Пропозиції щодо необхідності.

За результатами обстеження рекомендується виконати наступні заходи, які забезпечать відповідність ОІД вимогам із захисту інформації з грифом обмеження доступу «Для службового користування», конфіденційної інформації (матеріали судових експертиз, цифрові докази та персональні дані суб'єктів кримінальних проваджень).

1. Провести випробування та дослідження технічних засобів.

2. Провести огляд та випробування охоронної та пожежної сигналізації,

зокрема працездатність датчиків, стан каналів сповіщення, наявність резервного живлення та відповідність встановленому регламенту експлуатації.

3. Перевірити цілісність заземлення та стійкість електромережі,

включно з оцінкою опору заземлення, стану кабельних ліній, відповідності електромережі вимогам стійкості та безпечної експлуатації.

4. Застосування організаційних і інженерно-технічних заходів захисту:

обмежити доступ сторонніх працівників до приміщення № 101;

встановити пломби або охоронні наклейки на точки підключення ОТЗ;

запровадити журнал реєстрації відвідувачів;

проводити інструктажі працівників щодо правил обробки інформації;

розглянути встановлення додаткових засобів захисту.

Ж.6. Висновки

У процесі обстеження приміщення № 101 відділу цифрової криміналістики встановлено такі потенційні загрози для інформації з грифом обмеження доступу «Для службового користування», конфіденційної інформації (матеріали судових експертиз, цифрові докази та персональні дані суб'єктів кримінальних проваджень): існує ризик несанкціонованого доступу до автоматизованої системи або до приміщення за умов порушення встановленого режиму. Можливі програмно-технічні загрози – шкідливе ПЗ, порушення цілісності даних, недоліки конфігурації засобів захисту. Серед фізичних загроз – крадіжка або пошкодження обладнання, несправності електромережі та пожежні ризики. Виявлені загрози підлягають урахуванню під час формування моделі загроз та створення КСЗІ.

Голова комісії _____ Криштоф М.В.
(підпис) (ініціали, прізвище)

Члени комісії: _____ Довгань Р.В.
(підпис) (ініціали, прізвище)

_____ Пилипчук М.О.
(підпис) (ініціали, прізвище)

ДОДАТОК К
Формування матриці ризиків та вибір заходів захисту інформації для АС-1 відділу цифрової криміналістики Хмельницького НДЕКЦ МВС

К.1 Вихідні дані

Хмельницький науково-дослідний експертно-криміналістичний центр МВС України забезпечує проведення судових експертиз та експертних досліджень. Ключовим підрозділом, що розглядається, є відділ цифрової криміналістики, який здійснює пошук, фіксацію та аналіз цифрових слідів у межах кримінальних проваджень.

Інформаційна система відділу реалізована у вигляді автономного автоматизованого робочого місця (АРМ) експерта класу АС-1, яке не має підключення до мережі Інтернет.

Типи даних. Конфіденційна інформація та інформації з грифом обмеження доступу «Для службового користування»:

– образи дисків (forensic images), дампи пам'яті, вилучені файли, що є частиною кримінальних проваджень;

– проєкти та оригінали документів за результатами комп'ютерно-технічних експертиз;

– закриті методики проведення досліджень та внутрішні інструкції МВС;

– відомості про учасників кримінальних проваджень.

Користувачі: судовий експерт, завідувач відділу (адміністратор безпеки).

Наявні засоби захисту: антивірусне програмне забезпечення, апаратні блокатори запису, парольний захист, фізичне обмеження доступу до приміщення (решітки, жалюзі, дверний замок, охоронна сигналізація).

Вразливості:

– можливість фізичного доступу сторонніх осіб;

– використання змінних носіїв інформації;

– відсутність централізованого контролю доступу до USB-портів;

– ризик компрометації цілісності цифрових доказів при їх копіюванні;

– ризик візуального перехоплення інформації через наявність двох вікон;

– ризики, пов’язані з людським фактором.

К.2 Активи ІКС

Таблиця К.1

№	Актив	Значимість	Тип даних	Примітка
1	Електронні докази та дампи	Критична	Конфіденційна інформація	Об’єкти дослідження. Втрата або зміна веде до недійсності експертизи.
2	Висновки експерта (проєкти)	Висока	Службова інформація	Містять результати аналізу слідства.
3	Системні логи та журнали	Середня	Службова інформація	Записи про дії експерта та підключення пристроїв.
4	Резервні копії	Висока	Конфіденційна інформація	Копії завершених експертиз, що зберігаються в сейфі на зовнішніх носіях.
5	ОС та прикладне ПЗ	Середня	Службова інформація	Windows, спеціалізовані програми.
6	Апаратні засоби	Середня	Технічні дані	Системний блок, SSD-накопичувач

К.3 Потенційні зловмисники

Таблиця К.2

Категорія	Приклад дій	Мотив
Зовнішній порушник	Несанкціоноване проникнення до кабінету, крадіжка носіїв з доказами.	Перешкоджання правосуддю, знищення доказів.
Внутрішній працівник	Несанкціоноване копіювання матеріалів експертизи для передачі третім особам.	Особиста вигода, шантаж
Адміністративний персонал	Використання привілеїв доступу для перегляду або зміни даних	Зловживання повноваженнями
Технічний фактор	Випадкове пошкодження обладнання або збій системи під час обслуговування.	Технічна несправність, недбалість
Колишній працівник	Спроба використання залишкових знань про систему або паролі	Помста, особиста зацікавленість

К.4 Основні загрози

Таблиця К.3

№	Загроза	Причина / вектор реалізації
1	Несанкціонований доступ до матеріалів експертизи	Використання слабких паролів, підбір пароля або доступ до АРМ, залишеного без нагляду в активному стані.
2	Порушення цілісності цифрових доказів	Ненавмисна зміна метаданих або вмісту оригінального носія через підключення без апаратного блокатора запису.
3	Викрадення апаратних ліцензійних ключів	Фізичне вилучення USB-токенів захисту, без яких неможливе функціонування криміналістичних засобів.
4	Зараження АС-1 шкідливим програмним забезпеченням	Проникнення вірусів-шифрувальників або троянів з дисків та флешок, що є об'єктами дослідження.
5	Візуальне перехоплення конфіденційної інформації	Спостереження за екраном сторонніми особами
6	Інсайдерське копіювання образів дисків	Несанкціоноване перенесення конфіденційних копій доказів на особисті USB-носії працівниками з доступом до кабінету.
7	Втрата даних через технічну відмову накопичувача	Вихід з ладу SSD-диска АС-1 або пошкодження архівних копій на зовнішніх дисках через механічні пошкодження чи знос.
8	Порушення доступності через збій електроживлення	Аварійне вимкнення світла під час критичного процесу клонування диска, що може призвести до пошкодження файлової системи доказу.
9	Несвоєчасне виявлення інцидентів безпеки	Відсутність регулярного аналізу журналів подій
10	Фізична крадіжка носіїв інформації	Доступ сторонніх осіб до приміщення

К.5 Оцінка ризиків

Таблиця К.4

№	Загроза	P	C	R	Класифікація
1	Несанкціонований доступ до матеріалів експертизи	4	4	16	Критичний
2	Порушення цілісності цифрових доказів	3	5	15	Високий
3	Викрадення апаратних ліцензійних ключів	2	5	10	Середній
4	Зараження АС-1 шкідливим програмним забезпеченням	4	3	12	Високий
5	Візуальний перехват інформації	2	3	6	Середній
6	Інсайдерське копіювання образів дисків	2	4	8	Середній
7	Втрата даних через технічну відмову накопичувача	2	4	8	Середній
8	Порушення доступності через збій електроживлення	3	4	12	Високий
9	Несвоєчасне виявлення інцидентів	3	3	9	Середній
10	Фізична крадіжка носіїв інформації	2	5	10	Середній

К.6 Заходи захисту (з Каталогу НД ТЗІ 3.6-006-24)

Таблиця К.5

№	Загроза	Потен-ційний ризик (R)	Заходи з каталогу	Очікуваний ефект	Новий R
1	Несанкціонований доступ до матеріалів експертизи	16	AC-3 (Управління доступом), IA-2 (Ідентифікація та автентифікація), AC-11 (Блокування сеансу)	Зменшення ймовірності НСД через сувору автентифікацію (4→1)	4
2	Порушення цілісності цифрових доказів	15	SI-7 (Цілісність системи та інформації), SC-28 (Захист інформації в стані спокою)	Використання хешування та write-blocker-ів знижує ризик модифікації (3→1)	5
3	Викрадення апаратних ліцензійних ключів	10	MP-2 (Доступ до носіїв), PE-3 (Фізичний контроль доступу)	Зберігання токенів у сейфах унеможливлює вільний доступ (2→1)	5
4	Зараження АС-1 шкідливим ПЗ	12	SI-3 (Захист від шкідливого коду), MP-7 (Використання носіїв інформації)	Обов'язкова перевірка флешок-доказів на ізольованому вузлі (4→1)	3
5	Візуальний перехват інформації	6	PE-2 (Дозволи на фізичний доступ), AC-11 (Блокування сеансу)	Зменшення ймовірності спостереження (2→1)	3
6	Інсайдерське копіювання образів дисків	8	AC-6 (Принцип мінімальних повноважень), MP-7 (Контроль використання портів), AU-2 (Реєстрація подій)	Технічне блокування USB-портів на запис для персоналу (2→1)	4
7	Втрата даних через технічну відмову накопичувача	8	SI-13 (Передбачуване запобігання збоям), CP-9 (Резервне копіювання)	Регулярний моніторинг SMART-параметрів дисків (2→1)	4
8	Порушення доступності через збій електроживлення	12	PE-11 (Аварійне живлення), CP-10 (План відновлення системи)	Встановлення ДБЖ для завершення процесу клонування дисків (3→1)	4
9	Несвоєчасне виявлення інцидентів безпеки	9	AU-6 (Аналіз записів аудиту), IR-4 (Обробка інцидентів)	Перехід від реактивного до проактивного моніторингу подій (3→1)	3
10	Фізична крадіжка носіїв інформації	10	PE-3 (Фізичний контроль доступу), MP-5 (Транспортування носіїв)	Обмеження винесення дисків за межі режимної зони (2→1)	5

К.7 Можливі фінансові наслідки витоку

Таблиця К.6

Тип даних	Опис можливих наслідків	Потенційний збиток, санкції
Електронні докази (образи дисків, дампи)	Втрата цілісності або конфіденційності доказів призводить до їх недопустимості у суді. Це спричиняє розвал кримінальних проваджень.	Репутаційні втрати МВС, ризик службових розслідувань, від 500 000 грн (вартість процесуальних дій)
Висновки експерта (проєкти документів)	Передчасне розголошення результатів експертизи (таємниця слідства) може попередити фігурантів справи про хід розслідування.	Кримінальна відповідальність за ст. 387 ККУ, дисциплінарні стягнення
Апаратні ліцензійні ключі захисту	Фізична крадіжка або пошкодження USB-токенів (EnCase, Belkasoft тощо) зупиняє роботу відділу на тривалий термін.	Вартість відновлення ліцензій: 150 000 – 350 000 грн за одиницю
Персональні дані учасників проваджень	Витік даних потерпілих або свідків створює загрозу їхній безпеці та порушує вимоги Закону України «Про захист персональних даних».	Штрафні санкції, судові позови проти установи: 100 000 – 200 000 грн
Закриті методики та інструкції МВС	Попадання методичних рекомендацій до третіх осіб дозволяє зловмисникам розробляти методи протидії криміналістичному аналізу.	Зниження ефективності розкриття злочинів (нематеріальний збиток)
Службова інформація	Компрометація ланцюжка зберігання доказів (Chain of Custody), що ставить під сумнів об'єктивність експерта.	Репутаційні втрати НДЕКЦ: 50 000 – 100 000 грн

К.8 Висновки

У результаті виконання роботи для інформаційної системи відділу цифрової криміналістики Хмельницького НДЕКЦ МВС було ідентифіковано шість основних груп інформаційних активів, що мають критичне значення для проведення судових експертиз, а також десять актуальних загроз, притаманних автономній системі класу АС-1.

Аналіз показав, що найбільш небезпечними для установи є ризики, пов’язані з порушенням цілісності цифрових доказів, несанкціонованим доступом до матеріалів справ, викраденням апаратних ліцензійних ключів та специфічними каналами витоку інформації (візуальний та віброакустичний) через архітектурні особливості приміщення кабінету № 101. Реалізація цих загроз може призвести не лише до фінансових збитків через втрату ліцензійного ПЗ, а й до юридичної відповідальності персоналу та втрати доказової бази у кримінальних справах.

Оцінка ризиків до впровадження заходів захисту виявила наявність критичних та високих рівнів (R = 12–16). Завдяки застосуванню комплексу організаційних та технічних заходів, обраних згідно з вимогами НД ТЗІ 3.6-006-24, рівень ризиків було знижено до прийнятного (R = 3–5).

ДОДАТОК Л

Формування цільового профілю безпеки в автоматизованій системі класу «1» об’єкту інформаційної діяльності № 101 відділу цифрової криміналістики

Форма профілю безпеки (ПБ)

Л.1 Загальні відомості

Назва профілю безпеки: Цільовий профіль безпеки інформації (ЦПБ) для автоматизованої системи криміналістичного аналізу (АС-1) Хмельницького НДЕКЦ МВС.

Версія: 1.0

Дата розроблення: 17.03.2026 р.

Організація-розробник: Хмельницький науково-дослідний експертно-криміналістичний центр МВС України.

Підрозділ / відповідальна особа: Відділ цифрової криміналістики / головний судовий експерт Довгань Роман Миколайович

Контактна інформація: м. Хмельницький, вул. Молодіжна 12, відділ цифрової криміналістики, кабінет № 101 (2-й поверх)

тел. (0382) 78-46-62

email: ndekckm@gmail.com

Л.2 Призначення профілю безпеки

Опис системи: АС-1 є автономним автоматизованим робочим місцем (АРМ) на базі персонального комп'ютера, що не підключений до глобальної мережі Інтернет. Система призначена для обробки інформації з грифом обмеження доступу «Для службового користування» та конфіденційної інформації (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень).

Короткий опис функцій системи: створення побітових копій (образів) накопичувачів інформації з використанням апаратних блокаторів запису; пошук, та відновлення видалених файлів, аналіз артефактів операційних систем, дослідження мобільних пристроїв; формування висновків судового експерта на основі виявлених цифрових доказів; обчислення та верифікація хеш-функцій для підтвердження автентичності даних.

Умови експлуатації / середовище: система розміщена в межах контрольованої зони (КЗ) підприємства, в окремому кабінеті № 101 (2-й поверх). Доступ до приміщення обмежений (наявна охоронна сигналізація, грати на вікнах). Система функціонує в автономному режимі.

Л.3 Об’єкт захисту

Перелік інформації, що підлягає захисту: цифрові образи та дампи пам’яті носіїв інформації, що є речовими доказами; проєкти та фінальні версії висновків судового експерта; персональні дані фігурантів та учасників кримінальних проваджень; відомості про методики криміналістичного аналізу та спеціалізоване програмне забезпечення; апаратні ліцензійні ключі захисту.

Класифікація інформації: інформація з грифом обмеження доступу «Для службового користування», конфіденційна інформація (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень).

Носії інформації: друковані висновки експертизи (принтер HP LaserJet Pro); жорсткий диск (Kingston SSD Now A400 2 Tb), зовнішні жорсткі диски та флеш-накопичувачі для зберігання контрольних копій та резервного копіювання результатів (зберігаються в сейфі).

Користувачі та ролі:

Основний користувач: судовий експерт (повний доступ до криміналістичного ПЗ, право створення та видалення робочих проєктів, доступ до обробки конфіденційної інформації, обмежені права налаштування ОС).

Адміністратор системи: інженер з ТЗІ (налаштування підсистеми захисту, контроль цілісності ПЗ, керування обліковими записами та аудит подій безпеки).

Л.4 Загрози та вимоги до безпеки

Перелік загроз інформації:

НСД (несанкціонований доступ) до матеріалів експертизи сторонніми особами;

Вірусні атаки та шкідливе ПЗ;

Знищення або пошкодження інформації;

Порушення цілісності доказів (випадкова або навмисна модифікація цифрових образів під час аналізу);

Витік даних;

Збій обладнання / відмова системи;

Несанкціоноване копіювання документів.

Оцінка ризиків: високий рівень ризику фізичного проникнення, а також загрози цілісності даних, мережеві загрози відсутні, бо АС не підключена до мережі.

Безпекові припущення: вважається, що співробітники є довіреними особами, але можуть припуститися ненавмисних помилок. Всі співробітники мають необхідну кваліфікацію та проходили інструктаж з ТЗІ. Приміщення перебуває під цілодобовою охороною.

Політика безпеки: заборона обробки інформації без використання засобів захисту; принцип мінімальних необхідних прав доступу; використання парольної політики; робота зі змінними носіями дозволена лише для зареєстрованих пристроїв; обов’язкове блокування екрана при відсутності користувача; обов'язкове ведення та регулярний перегляд журналів реєстрації подій; обов'язкове використання сейфів для зберігання об'єктів досліджень у неробочий час.

Л.5 Функціональні вимоги безпеки

Ідентифікація та автентифікація: вхід в BIOS захищено паролем. Вхід в ОС Windows здійснюється за унікальним логіном та паролем (мінімум 12 символів, включає малий та великий регістри та спеціальні символи, зміна кожні 60 днів, кількість невдалих спроб входу 5).

Управління доступом: здійснюється розмежування прав доступу на рівні файлової системи (NTFS); заборона гостьового доступу та автозапуску зі змінних носіїв; блокування USB-портів для неавторизованих пристроїв.

Реєстрація та аудит: автоматична реєстрація подій, вхід/вихід із системи, спроби доступу до файлів, зміна політик безпеки, події принтера. Зберігання журналів аудиту не менше 1 року.

Захист даних: захист цілісності завантажувальних секторів (Secure Boot), перевірка антивірусним сканером, шифрування системного диску та каталогів.

Захист комунікацій: блокування невикористовуваних фізичних портів (USB, COM) фізично (пломби), всі мережеві кабелі відключенні.

Криптографічний захист: шифрування розділів диска та робочих каталогів з образами доказів (комплекс захисту інформації на носіях "ІІТ Захищений диск-4") для забезпечення конфіденційності інформації.

Фізичний захист: наявні датчики відкриття вікон та дверей, грати та жалюзі на вікнах, металеві двері, контроль цілісності системного блоку за допомогою номерних одноразових пломб.

Резервування та відновлення: щотижневе повне резервне копіювання образів дисків та проєктів висновків на зовнішній носій, зберігання резервних копій у вогнетривкому сейфі.

Л.6 Нефункціональні вимоги безпеки

Надійність: використання джерела безперебійного живлення (APC Back-UPS) потужністю 1500 ВА для забезпечення щонайменше 20 хвилин автономної роботи, що необхідно для коректного припинення процесів аналізу даних.

Цілісність: контроль цілісності системних файлів ОС та спеціалізованого криміналістичного ПЗ за допомогою обчислення контрольних сум.

Доступність: час відновлення після збою повинен бути не більше 4 годин.

Стійкість до помилок: автоматичне перезавантаження служб захисту у разі їх зупинки, а також здатність системи відновлюватись після некоректних дій користувача.

Вимоги до продуктивності: засоби захисту (антивірус, аудит) не повинні знижувати швидкодію системи більше ніж на 15%.

Вимоги до експлуатаційного середовища: захищене приміщення, температура від +18 до +25°С, вологість 40-60%, заземлення (опір < 4 Ом).

Л.7 Конфігурація та склад системи

Апаратні компоненти:

Системний блок: Fujitsu Esprimo E710 SFF (S/N: 14950803).

Процесор: Intel Core i3-3220.

Накопичувач: Kingston SSD Now A400 2 Tb.

Монітор: Dell 22″ P224W.

МФУ: HP LaserJet Pro MFP M281fdw.

ДБЖ: APC Back-UPS BX700U-GR.

Програмні компоненти:

ОС: Microsoft Windows 11 Pro (ліцензійна, наявна позитивна експертиза).

Антивірус: Avast Business Antivirus 19.X.Y (актуальна версія включена до переліку технічних засобів, дозволених до застосування).

Офісне ПЗ: Microsoft Office 2019 (ліцензійна).

Спеціалізоване ПЗ: Комплекси для пошуку та аналізу цифрових доказів (EnCase Forensic).

Мережева архітектура: відсутня. Фізичне відключення від мережі (Ethernet).

Інтеграції з іншими системами: відсутні (обмін даними тільки через контрольовані змінні носії).

Л.8 Організаційні заходи безпеки

Ролі та відповідальність:

1. Керівник служби захисту інформації. Основна функція: Загальне керівництво, планування та контроль діяльності системи захисту. Обов’язки: затверджує політику безпеки, план захисту інформації та інші дозвільні документи (списки допуску до приміщення); приймає рішення про початок експлуатації АС-1 або її зупинку у разі виявлення критичних порушень; забезпечує виділення ресурсів (фінансування закупівлі ліцензійного криміналістичного ПЗ, засобів ТЗІ, ремонт приміщення); організовує службові розслідування у випадках інцидентів безпеки та приймає рішення про притягнення винних до відповідальності. Відповідальність: Несе повну юридичну відповідальність за організацію захисту інформації на підприємстві.

2. Адміністратор безпеки. Основна функція: Управління правами доступу, контроль за дотриманням правил роботи в АС, реєстрація подій. Обов’язки: керує обліковими записами користувачів в ОС та спеціалізованому криміналістичному ПЗ (створення, блокування, зміна паролів); щотижнево переглядає журнал реєстрації подій (аудит) операційної системи для виявлення підозрілої активності; веде журнал обліку інцидентів та журнал обліку носіїв інформації (реєструє флеш-накопичувачі, жорсткі диски); виконує резервне копіювання результатів експертиз та забезпечує їх зберігання у сейфі; негайно повідомляє керівника СЗІ про спроби несанкціонованого доступу. Має право блокувати роботу АС-1 у разі виявлення загрози вірусного зараження або злому.

3. Інженер з технічного захисту інформації. Основна функція: Захист від витоку інформації технічними каналами, контроль фізичного середовища та апаратних засобів. Обов’язки: контролює цілісність фізичних засобів захисту: замків, грат на вікнах, пломб на корпусі системного блоку; перевіряє відсутність сторонніх підключень до інженерних комунікацій; відповідає за технічне обслуговування засобів охоронної та пожежної сигналізації в кабінеті; забезпечення безперебійної роботи програмного та апаратного забезпечення. Має право проводити інструментальний контроль та перевірку робочого місця на наявність сторонніх пристроїв.

4. Користувач (головний судовий експерт). Обов’язки: зберігати у таємниці свій особистий пароль доступу; не залишати ідентифікатори без нагляду; суворо дотримуватися регламенту роботи з речовими доказами; блокувати екран комп'ютера при кожному виході з

кабінету; не підключати особисті мобільні телефони та неперевірені флеш-носії до службового ПК; негайно звітувати про будь-які аномалії в роботі криміналістичного ПЗ.

Політики та інструкції: інструкція користувача АС-1; інструкція з антивірусного захисту; інструкція про порядок поводження з ключовими документами (паролями).

Регламент обслуговування: технічне обслуговування тільки в присутності адміністратора безпеки; перевірка журналів подій проводиться щотижня; перевірка цілісності пломб проводиться щомісяця.

Порядок реагування на інциденти: підготовка до реагування на інциденти; виявлення, аналіз та інформування про інциденти начальника СЗІ, стримування, усунення наслідків та відновлення після інцидентів, а також аналіз ефективності заходів реагування на інциденти.

Порядок контролю доступу: вхід у приміщення тільки дозволеним особам, запис у журнал відвідувачів.

Л.9 Вимоги до сертифікації / атестації

Критерії: Оскільки система класифікована як АС класу «1» (однокористувацька система, що не підключена до зовнішніх мереж) і обробляє інформацію з грифом обмеження доступу «Для службового користування» та конфіденційну інформацію обрано профіль, який визначає мінімальний набір організаційних та технічних заходів захисту, які адаптовані до умов експлутації в АС-1 Хмельницького НДЕКЦ МВС та спрямовані на запобігання витоку інформації та порушенню цілісності доказової бази.

Рівні довіри: рівень довіри до засобів захисту відповідає вимогам до систем, що обробляють конфіденційну інформацію та персональні дані суб’єктів кримінальних проваджень. Забезпечення належного рівня довіри реалізується через використання ліцензійного спеціалізованого криміналістичного ПЗ та засобів захисту інформації, що мають позитивний експертний висновок ДССЗЗІ; коректність налаштування параметрів безпеки операційної системи та підсистеми захисту приміщення; наявність повного комплекту організаційно-розпорядчої документації, що регламентує порядок експлуатації АС-1 у режимі обробки обмежених даних.

Нормативні документи:

НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

НД ТЗІ 3.6-006-24 «Технічний захист інформації. Загальні вимоги до захисту інформації від витоку технічними каналами».

Л.10 Додатки

Таблиця Л.1 – Загрози та вразливості

№	Джерело загрози	Опис загрози (Вразливість)	Рівень ризику	Наслідки	Код заходу (з профілю UB)
1	Несанкціонований доступ до приміщення	Незаконне проникнення сторонніх осіб до каб. №101 через вхідні двері або вікно (2-й поверх) для фізичного контакту з АС-1	Високий	Втрата конфіденційності (копіювання доказів), цілісності (спотворення експертних даних).	PE-3, PE-6
2	Змінні носії (USB), шкідливе ПЗ	Зараження системи вірусами/шифруваль никами через	Високий	Порушення цілісності та доступності	SI-3, MP-4, MP-7

		неконтрольовані змінні носії		(блокування криміналістичних проєктів, пошкодження образів)	
3	Людський фактор, НСД до системи	Використання слабких паролів, залишення комп'ютера розблокованим, ненавмисне видалення результатів аналізу.	Середній	НСД до системи під обліковим записом судового експерта, витік таємниці слідства.	IA-5, AC-7, AC-11
4	Збій обладнання, втрата доступності	Втрата даних через критичну поломку SSD Kingston 2 Tb або збій живлення під час тривалого копіювання доказів.	Середній	Тимчасова або повна втрата результатів поточної експертизи, пошкодження файлової системи.	CP-9, PE-11
5	Несанкціоноване копіювання	Неконтрольоване винесення копій експертних висновків на особистих цифрових носіях.	Середній	Розголошення матеріалів кримінального провадження, порушення регламенту роботи з ДСК.	AC-3, MP-5

Таблиця Л.2 – Матриця відповідності

№	Група вимог безпеки	Код заходу	Функціональний рівень (НД ТЗІ 2.5-004-99)	Реалізація в АС-1 Хмельницького НДЕКЦ МВС
1.	Ідентифікація та Автентифікація (IA)	IA-2	Рівень 1 (Базова ідентифікація)	Кожному експерту присвоєно унікальний ідентифікатор. Доступ дозволено лише після успішної автентифікації.
		IA-5 (1)	Рівень 2 (Парольна автентифікація)	Використання складних паролів (від 12 символів) з вимогою зміни кожні 60 днів.
		IA-8	Рівень 1 (Зовнішні системи)	Заборона доступу для осіб, що не є співробітниками підрозділу.
2.	Управління доступом (AC)	AC-2	Рівень 2 (Рольовий доступ)	В системі створено лише 2 записи: "Адміністратор" та "Експерт". Доступ "Гість" – заборонено.
		AC-2 (3)	Рівень 1 (Автоматичні дії)	Автоматична деактивація облікових записів після 30 днів неактивності.

		AC-5	Рівень 2 (Рольовий доступ)	Адміністратор безпеки не має логічного доступу до матеріалів експертиз (лише до налаштувань ОС), а судовий експерт не має прав змінювати конфігурацію безпеки системи.
		AC-6	Рівень 1 (Керування доступом)	Експерт має доступ лише до тих баз, які необхідні для його експертизи.
		AC-7	Рівень 1 (Невдалі спроби)	Блокування термінала на 30 хв після 5 невдалих спроб входу.
		AC-11	Рівень 1 (Блокування пристрою)	Налаштовано автоблокування екрана через 10 хвилин бездіяльності.
		AC-20	Рівень 1 (Обмеження використання)	Заборонено підключення особистих ноутбуків/телефонів до AC-1.
3.	Реєстрація та Аудит (AU)	AU-2	Рівень 1 (Локальні журнали)	В ОС Windows налаштовано аудит: вхід/вихід, доступ до файлів, зміна політик безпеки.
		AU-6	Рівень 1 (Аналіз аудиту)	Адміністратор безпеки щотижня переглядає журнал подій.
		AU-9	Рівень 1 (Аналіз аудиту)	Журнали подій доступні лише для читання адміністратору безпеки; налаштовано захист від перезапису.
4.	Захист носіїв (MP)	MP-4	Рівень 1 (Фізичний контроль)	Резервні копії (флеш-носії) зберігаються у металевому сейфі.
		MP-6	Рівень 2 (Очищення пам'яті)	Застосування спеціалізованих утиліт для гарантованого затирання залишкових даних експертиз.
		MP-7	Рівень 1 (Обмеження використання)	USB-порти, що не використовуються, програмно вимкнено. Використання особистих носіїв суворо заборонено. Всі службові носії обліковані в журналі.
5.	Фізичний захист (PE)	PE-3	Рівень 1 (Керування доступом)	Двері з замком, грати на вікнах, охоронна сигналізація, журнал відвідувачів.

		PE-6	Рівень 1 (Моніторинг)	Встановлено охоронну сигналізацію з виведенням на пульт охорони. Ведеться журнал обліку відвідувачів.
		PE-11	Рівень 1 (Електроживлення)	АС-1 підключена до ДБЖ (APC Back-UPS BX700U-GR) для коректного вимкнення.
6.	Цілісність та Обслуговування (SI, MA)	SI-3	Рівень 1 (Захист від коду)	Встановлено антивірус Avast Business Antivirus.
		SI-4	Рівень 1 (Контроль цілісності)	Постійний моніторинг АРМ за допомогою засобів ОС на предмет несанкціонованого підключення сторонніх пристроїв.
		SI-7	Рівень 1 (Захист від коду)	Використання інструментів контролю цілісності для перевірки системних файлів ОС Windows.
		SI-12	Рівень 1 (Захист від коду)	Налаштовано автоматичне очищення кеш-пам'яті та тимчасових файлів при завершенні сеансу.
		MA-2	Рівень 1 (Обслуговування)	Заведено журнал технічного обслуговування АРМ та перевірки стану ДБЖ.
		MA-4	Рівень 1 (Обслуговування)	Технічне обслуговування проводиться тільки в присутності адміністратора безпеки.
7.	Криптографія (SC)	SC-28	Рівень 2 (Захист інформації на носіях)	Використання ПЗ «ІІТ Захищений диск-4» для шифрування системного розділу.
8.	Планування та Реагування (IR, CP)	IR-4	Рівень 1 (Обробка інциденту)	Розроблено порядок реагування на інциденти, ведеться журнал обліку інцидентів.
		CP-2	Рівень 1 (Обслуговування)	Наявність затвердженого регламенту дій експерта та адміністратора у разі апаратного збою АРМ.
		CP-9	Рівень 1 (Резервне копіювання)	Щотижневе повне резервне копіювання на зовнішній носій,

				що зберігається в сейфі.
9.	Керування безпекою (SM)	SM-1	Рівень 1 (Ручне керування)	Затверджено внутрішні інструкції з експлуатації КСЗІ та правила парольного захисту.
		SM-3	Рівень 1 (Ручне керування)	Процедура блокування доступу при звільненні працівника протягом 1 робочої години.
10.	Захист від НСД (NSD)	NSD-1	Рівень 2 (Технічні засоби)	Активовано режим самозахисту антивірусного ПЗ та локальний міжмережевий екран.
11.	Кадрова безпека (PS)	PS-3	Рівень 1 (Перевірка персоналу)	Надання доступу до АС-1 виключно після проходження внутрішньої перевірки.
		PS-4	Рівень 1 (Обробка інциденту)	Блокування доступу протягом години при звільненні працівника.
12.	Обізнаність і навчання (AT)	AT-2	Рівень 1 (Керування персоналом)	Проведення щорічного інструктажу судових експертів щодо правил кібергігієни та обробки інформації з обмеженим доступом в АС-1. Фіксація проходження інструктажу в спеціальному журналі.
		AT-3	Рівень 1 (Керування персоналом)	Окреме спеціалізоване навчання для ролі "Адміністратор безпеки" щодо процедур аудиту та моніторингу АРМ експертів.
13.	Управління конфігурацією (CM)	CM-8	Рівень 1 (Керування конфігурацією)	Ведення актуального апаратного та програмного паспорта АРМ експерта.
		CM-10	Рівень 1 (Обмеження використання)	Заборона встановлення будь-якого стороннього ПЗ на АРМ. Дозволено лише використання сертифікованого криміналістичного ПЗ.

ДОДАТОК М

Технічне завдання на створення комплексної системи захисту інформації в автоматизованій системі класу «1» об’єкту інформаційної діяльності № 101 відділу цифрової криміналістики

ЗАТВЕРДЖУЮ
Директор Хмельницького
НДЕКЦ МВС
_____ Ганзюк А.Л.
20.03.2026 р.

ТЕХНІЧНЕ ЗАВДАННЯ НА СТВОРЕННЯ КСЗІ
для обробки інформації з обмеженим доступом (ІзОД)

М.1 Загальна частина

М.1.1 Підстава для розроблення ТЗ

Наказ № 3 від 15.02.2026 «Про створення комплексної системи захисту інформації».

Акт категоріювання ОІД (категорія IV).

Закон «Про захист інформації в ІКС».

НД ТЗІ 3.6-006-2024, 3.7-003-2024, 3.6-001-2024.

М.1.2 Найменування АС

Повне найменування: автоматизована система класу 1 відділу цифрової криміналістики Хмельницького НДЕКЦ МВС.

Умовне позначення: АС-1

Функціональне призначення: Система призначена для проведення комп'ютерно-технічних експертиз, аналізу цифрових доказів, ведення реєстрів експертних досліджень та обробки конфіденційної інформації (персональних даних фігурантів справ).

М.1.3 Власник АС

Повна назва організації: Хмельницький науково-дослідний експертно-криміналістичний центр МВС України

Адреса: 29018, м. Хмельницький, вул. Молодіжна, 12

Підрозділ: відділ цифрової криміналістики, кабінет № 101 (2-й поверх)

Відповідальна особа: директор Хмельницького НДЕКЦ МВС Ганзюк Олександр Леонідович.

М.1.4 Мета створення КСЗІ

Забезпечення конфіденційності, цілісності та доступності інформації під час проведення експертних досліджень.

Створення захищеного середовища, що виключає можливість витоку доказової бази або несанкціонований доступ (НСД).

Захист від навмисного або випадкового порушення цілісності цифрових доказів.

М.1.5 Тип АС і клас системи

АС класу “1” – автономна автоматизована система, не підключена до мереж, призначена для обробки інформацію з грифом обмеження доступу «Для службового користування» та конфіденційну інформацію (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень).

М.1.6 Межі КСЗІ

Опис приміщення: КСЗІ охоплює приміщення кабінету № 101 відділу цифрової криміналістики (2-й поверх). Фізичні межі захисту визначаються зовнішніми стінами, підлогою, стелею, вхідними дверима та вікнами кабінету.

М.2 Інформація, що підлягає захисту

М.2.1 Види ІзОД:

В АС-1 відділу цифрової криміналістики Хмельницького НДЕКЦ МВС обробляється інформацію з грифом обмеження доступу «Для службового користування» та конфіденційну інформацію (матеріали судових експертиз, цифрові докази та персональні дані суб'єктів кримінальних проваджень), вимоги до захисту якої встановлені законом. Персональні дані учасників кримінальних проваджень (підозрюваних, потерпілих, свідків), що включають ПІБ, адреси, контакти, відомості про приватне життя, виявлені під час криміналістичного аналізу пристроїв. Внутрішні реєстри призначених експертиз, плани роботи відділу, акти прийому-передачі речових доказів, а також методики проведення досліджень.

М.2.2 Форми обробки

Електронна: основна форма обробки. Включає роботу з бінарними образами дисків (файли форматів .E01, .raw), базами даних криміналістичного ПЗ, реєстрами та текстовими звітами. Обробка здійснюється за допомогою спеціалізованого програмного забезпечення (EnCase). Включає створення копій, хешування, пошук, відновлення видалених даних та резервне копіювання.

Паперова: використовується при оформленні офіційних висновків експерта, журналів реєстрації речових доказів та супровідної документації. Друк здійснюється на принтері, що знаходиться в межах контрольованої зони (КЗ) (кабінет № 101). Поводження з паперовими носіями (зберігання, знищення) регулюється.

М.2.3 Обсяги та періодичність обробки

Обсяг інформації, що зберігається та обробляється є значним, що зумовлено специфікою цифрових доказів (від 2 ТБ до 10 ТБ накопичуваної інформації на робочих дисках). Очікується динамічне зростання обсягів залежно від кількості та складності призначених експертиз, що враховано при плануванні обсягів резервного копіювання. Обробка інформації відбувається з понеділка по четверг протягом робочого часу (з 09:00 до 18:00), а також в п'ятницю з 9:00 до 16:45. Резервне копіювання журналів та баз даних щотижня; контроль цілісності ПЗ та антивірусна перевірка щомісяця або перед початком кожного нового дослідження.

М.2.4 Вимоги до КЦД

Конфіденційність: високий рівень захисту. Недопущення розголошення відомостей досудового розслідування та персональних даних. Забезпечується суворим розмежуванням доступу, автентифікацією за паролями та фізичною ізоляцією АС-1 від мережі.

Цілісність: високий рівень контролю. Забезпечення повної ідентичності цифрових доказів з моменту їх отримання до моменту винесення висновку. Забезпечується обов'язковим розрахунком та контролем хеш-функцій, використанням засобів захисту від запису та аудитом дій користувача, антивірусним контролем та регулярним резервним копіюванням.

Доступність: локальна доступність, високий рівень. Забезпечення оперативного доступу авторизованих користувачів до інформації. Постійна готовність АС-1 до проведення досліджень у встановлені законодавством терміни. Забезпечується використанням джерел безперебійного живлення (ДБЖ) та регулярним технічним обслуговуванням обладнання.

М.3 Опис середовища функціонування АС класу "1"

М.3.1 Апаратне забезпечення

Центральне обладнання (АРМ)

Основний об'єкт обробки інформації – системний блок з інвентарним номером №114001 (модель Fujitsu Esprimo E710 SFF). Корпус цього ПК має бути опломбований для контролю несанкціонованого доступу та унеможливлення вилучення внутрішніх носіїв чи встановлення сторонніх пристроїв.

Основний носій інформації – внутрішній SSD-накопичувач Kingston SSD Now A400 2 Тб. Для запобігання несанкціонованому доступу до даних у разі викрадення обладнання, носій має бути захищений на рівні операційної системи за допомогою засобів шифрування.

Периферійні пристрої та підключення

Периферійні порти (АС-20, МР-7): усі невикористовувані комунікаційні порти (COM, LPT, невикористовувані USB-порти, мережевий адаптер) мають бути фізично заблоковані/опломбовані. Мережевий порт RJ-45 опломбований.

Спеціалізоване обладнання: апаратні блокуватори запису для підключення речових доказів. Підключення здійснюється через виведені порти, марковані для криміналістичних цілей.

Монітор: РК-монітор Dell 22″ P224W. Його розміщення виконано згідно з ситуаційним планом ОІД, щоб унеможливити візуальне зчитування інформації через вікна або двері приміщення.

Принтер: лазерний принтер HP LaserJet Pro MFP M281fdw. Принтер розташований у КЗ, а його використання (друк ІзОД) суворо контролюється користувачем АС та реєструється у журналі друку.

Засоби живлення: для забезпечення коректного завершення роботи системи у разі зникнення живлення використовується джерело безперебійного живлення (ДБЖ) APC Back-UPS, яке гарантує 20 хвилин автономної роботи. Лінії електроживлення та заземлення підлягають контролю.

Змінні носії інформації

До складу апаратного забезпечення входять обліковані службові USB-накопичувачі та зовнішній HDD, призначені для резервного копіювання. Всі носії повинні бути зареєстровані в журналі обліку змінних носіїв інформації із присвоєнням облікового номера. Зберігання носіїв, включно із зовнішнім HDD для резервного копіювання, здійснюється у металевому вогнетривкому сейфі. Всі службові змінні носії повинні мати встановлене програмне шифрування для захисту даних у разі їхньої втрати чи крадіжки.

М.3.2 Програмне забезпечення

Програмне середовище АС-1 базується на ліцензійному програмному забезпеченні (ПЗ), яке має необхідні сертифікати відповідності або позитивні експертні висновки для використання.

В АС-1 використовується ліцензійна операційна система, наявна позитивна експертиза, налаштована відповідно до вимог безпеки для автономних систем.

Найменування та версія: Microsoft Windows 11 Pro (64-bit).

Тип ліцензії: комерційна, активована легальним ключем.

Тип захисту та налаштування:

В ОС активовані вбудовані механізми захисту: контроль облікових записів (UAC), журнали аудиту безпеки (Security Logs) та політики блокування (Local Security Policy).

Криптографічний захист: використовується шифрування розділів диска (комплекс захисту інформації на носіях "ІІТ Захищений диск-4") для забезпечення конфіденційності інформації.

Статус оновлень: автоматичне оновлення ОС вимкнено (система автономна). Критичні оновлення безпеки встановлюються адміністратором вручну з перевірених носіїв.

До складу прикладного ПЗ, необхідного для виконання функціональних завдань судового експерта, входять:

Офісний пакет: Microsoft Office 2019 (Word, Excel) – для роботи з документами та підготовки висновків.

Спеціалізоване ПЗ: EnCase Forensic – для аналізу.

Адміністративне та службове ПЗ використовується виключно адміністратором безпеки для керування захистом та обслуговування системи.

Засоби адміністрування ОС: вбудовані консолі управління Microsoft Management Console (MMC), редактор локальних групових політик, перегляд подій для аналізу журналів аудиту.

Утиліти обслуговування: програми для створення резервних копій та роботи з архівами (вбудовані засоби Windows Backup).

В системі встановлено антивірусний комплекс, адаптований до роботи в автономному середовищі.

Найменування: Avast Business Antivirus 19.X.Y (актуальна версія включена до переліку технічних засобів, дозволених до застосування).

Автономність: Антивірус налаштований на роботу без підключення до Інтернету. Функції хмарного аналізу та автоматичного оновлення через мережу вимкнено.

Оновлення баз: оновлення сигнатурних баз здійснюється вручну (щотижня) адміністратором безпеки за допомогою завантаження файлів оновлень з довіреного носія.

Сканування: налаштовано автоматичне сканування всіх змінних носіїв при підключенні та регулярне повне сканування системи за розкладом.

М.3.3 Відсутність мереж

Немає підключення до Інтернету, фізично відсутній мережевий адаптер.

Немає LAN/VPN/Wi-Fi. Немає підключення до локальної мережі підприємства, VPN-з'єднань чи бездротових мереж.

Немає Bluetooth (вимкнений). Усі невикористовувані інтерфейси є вимкненими на рівні BIOS та програмно заблокованими.

Немає інших каналів передачі (ІЧ-порти, модеми).

М.3.4 Приміщення та доступ

Кабінет № 101 (2-й поверх) обладнаний металевими дверима та двома замками високої міцності, гратами на вікнах, охоронною сигналізацією з виведенням на пульт охорони. Вхід до приміщення здійснюється через звичайний замок. Доступ обмежений, ведеться журнал обліку відвідувачів. Система контролю та управління доступом відсутня, її функції виконують режимні та організаційні заходи (журнал, сигналізація, замок). В приміщенні встановлено металевий вогнетривкий сейф для зберігання резервних копій, облікованих змінних носіїв та паперових документів. Приміщення обладнане первинними засобами пожежогасіння (вогнегасником) та пожежними датчиками підключеними до загальної пожежної сигналізації будівлі.

М.4 Аналіз загроз та оцінка ризиків (для АС класу «1»)

М.4.1 Загрози виникають переважно від:

Людський фактор (Персонал):

Ненавмисні помилки користувачів (введення некоректних даних, випадкове пошкодження або видалення оригінальних образів цифрових доказів під час аналізу). Порушення політик захисту. Використання слабких паролів, які легко підібрати.

Навмисні дії співробітників:

Спроби несанкціонованої модифікації результатів експертизи в інтересах третіх осіб. Копіювання конфіденційних матеріалів досудового розслідування на особисті носії з метою подальшого розголошення.

Загрози, пов’язані з носіями інформації:

Підміна носіїв. Спроба завантаження ОС зі стороннього носія (LiveCD/USB) для обходу засобів захисту. Піднесення фальшивих носіїв. Підключення невідомих USB-пристроїв, що містять шкідливий код. Втрата або крадіжка службового носія (флешки з резервною копією). Зараження АС-1 шкідливим кодом, що міститься на речових доказах (флешках, дисках, смартфонах), які підключаються для аналізу.

Фізичні загрози:

Втрата або крадіжка обладнання. Фізичне вилучення системного блоку або SSD-диска з приміщення. Порушення правил фізичного доступу. Проникнення сторонніх осіб до приміщення через вікно або підбір ключа до дверей. Візуальне знімання інформації з монітора експерта через вікна або під час тимчасової відсутності спеціаліста на робочому місці.

Програмно-технічні загрози:

Шкідливе ПЗ (віруси, трояни, шифрувальники). Зараження системи через змінні носії інформації (оскільки мережа відсутня). Раптовий збій накопичувачів або блоку живлення під час виконання складних обчислювальних операцій (наприклад, дешифрування паролів), що може призвести до незворотної втрати результатів багатоденної роботи.

М.4.2 Рівень ризиків оцінюється для:

Конфіденційності (Рівень ризику – високий). Розголошення таємниці слідства, персональних даних підозрюваних або свідків, виявлених під час аналізу пристроїв, призведе до кримінальної відповідальності (ст. 387 ККУ), зриву оперативних заходів та дискредитації НДЕКЦ МВС.

Цілісності (Рівень ризику – високий). Несанкціонована зміна цифрових доказів, метаданих файлів або тексту експертного висновку є фатальною. Будь-яке порушення

цілісності робить доказову базу юридично нікчемною, що унеможливлює використання результатів експертизи в судовому процесі.

Доступності (Рівень ризику – середній). Тимчасова відмова обладнання або збій живлення перериває процес криміналістичного копіювання чи дешифрування даних. Хоча це затягує терміни слідства, ризик компенсується наявністю ДБЖ та можливістю повторного запуску процесів із «майстер-копій».

М.4.3 Модель порушника

Судовий експерт (авторизований користувач): має легальний логічний доступ до АС-1 та матеріалів конкретних експертиз. Мотив – корупційна вигода (продаж інформації сторонам процесу), недбалість або зовнішній тиск. Основні дії: несанкціоноване копіювання образів дисків на необліковані носії або навмисне видалення критичних доказів.

Адміністратор (привілейований користувач): має повні логічні права на керування ОС та засобами захисту. Мотив – приховане сприяння злочинним угрупованням або зловживання владою. Основні дії: вимкнення антивірусного захисту, модифікація журналів аудиту (log-файлів) для приховування дій користувачів, несанкціонована зміна паролів.

Технічний персонал: має фізичний доступ до приміщення для обслуговування. Співробітники, що здійснюють технічну підтримку будівлі (електрики, прибиральники). Мотив – викрадення дорогих компонентів АРМ або встановлення фізичних закладок («кейлогерів») для перехоплення паролів.

Стороння особа з фізичним доступом (зовнішній порушник): не має легального доступу до приміщення. Особа, що не має права перебування в КЗ (наприклад, відвідувач центру). Мотив – промислове шпигунство або перешкоджання правосуддю. Основні дії: фізичне проникнення до приміщення зі зламом замків, викрадення системного блоку або SSD-накопичувачів, що містять ключову доказову базу.

М.4.4 Визначення заходів протидії

1. Контроль доступу та автентифікація для протидії НСД та загрозам, пов'язаним із людським фактором, впроваджена сувора політика автентифікації. Це включає встановлення сильної парольної політики (мінімальна довжина, регулярна зміна, блокування після невдалих спроб). Розмежування доступу реалізується на рівні операційної системи: експерт має права лише на роботу з криміналістичним ПЗ та даними експертиз, тоді як повні права на зміну конфігурації безпеки має виключно адміністратор безпеки.

2. Захист носіїв інформації та цілісність протидія загрозам, пов'язаним із фальшивими або сторонніми носіями, забезпечується програмною забороною використання не облікованих USB-пристроїв. Дозволені до використання лише службові, зареєстровані носії, які підлягають обов'язковій перевірці. Підключення речових доказів (дисків, флеш-накопичувачів) дозволяється виключно через апаратні блокуватори запису, що гарантує неможливість випадкової зміни чи видалення оригінальних даних під час дослідження.

3. Захист від шкідливого програмного забезпечення для протидії шкідливому ПЗ, що може бути занесене вручну через носії, буде встановлено та налаштовано ліцензійне антивірусне програмне забезпечення. Воно функціонує в автономному режимі, а оновлення баз здійснюється адміністратором безпеки вручну.

4. Фізичний та технічний захист протидія несанкціонованому фізичному доступу реалізується за рахунок охоронної сигналізації та контролю доступу до кабінету. Додатково застосовуються сейфи для зберігання облікованих носіїв та речових доказів у позаробочий час.

5. Адміністрування, моніторинг та реагування для своєчасного виявлення та ліквідації наслідків інцидентів буде активовано журналювання всіх критичних подій. Адміністратор безпеки регулярно проводить аналіз цих журналів. У разі виникнення інциденту (збій, вірус, НСД) персонал керується планом реагування на інциденти, що включає порядок відновлення даних з резервних копій, які створюються щотижня.

М.5 Вимоги до КСЗІ для АС класу «1»

М.5.1 Функціональні вимоги

М.5.1.1 Управління доступом

Система повинна забезпечувати надійне розмежування доступу до ресурсів та функцій відповідно до принципу мінімальних необхідних повноважень.

Авторизація користувачів. Доступ до системи надається лише після успішної ідентифікації та автентифікації (логін/пароль). Кожен користувач має індивідуальний обліковий запис.

Розмежування прав. Повинно бути реалізовано чітке розмежування прав, користувач (доступ лише до прикладного та спеціалізованого ПЗ) та адміністратор (повний доступ до налаштувань ОС та ЗЗІ).

Контроль привілейованих користувачів. Дії адміністратора безпеки підлягають обов’язковому протоколюванню та моніторингу. При звільненні співробітника або зміні його службових обов'язків, адміністратор безпеки зобов'язаний у день підписання наказу заблокувати обліковий запис користувача та перенести його дані до архіву, після чого обліковий запис видаляється.

Захист паролів. Політика паролів має включає мінімальну довжину не менше 12 символів, вимоги до складності та примусову зміну пароля кожні 60 днів. Система повинна блокувати обліковий запис користувача після 5 невдалих спроб входу.

Заборона використання сторонніх носіїв USB. Програмно-апаратні засоби повинні забезпечувати блокування підключення будь-яких несанкціонованих USB-пристроїв.

М.5.1.2 Контроль фізичного доступу

Фізичний доступ до контрольованої зони та апаратного забезпечення АС-1 повинен бути обмежений та контрольований.

Доступ до КЗ лише дозволеним особам. Вхід сторонніх осіб контролюється засобами відеоспостереження, датчиками відкриття дверей та вікон.

Журнал відвідувань. Впровадження журналу обліку відвідувачів для фіксації входу/виходу осіб до АС-1.

Контроль цілісності. Усі критичні вузли (корпус ПК, порти) повинні бути опломбовані для контролю несанкціонованого втручання.

М.5.1.3 Криптографічний захист

Шифрування дисків. Для захисту конфіденційної інформації у стані спокою, у разі фізичної крадіжки обладнання, необхідно реалізувати шифрування системного диска (комплекс захисту інформації на носіях "ІІТ Захищений диск-4").

Захист носіїв у сейфі. Захищені носії резервних копій, а також паролі шифрування дисків, мають зберігатися в металевому сейфі в межах КЗ.

М.5.1.4 Захист від шкідливого ПЗ

Антивірус з локальними сигнатурами. Антивірусне програмне забезпечення повинно бути налаштоване на роботу без мережевого підключення. Оновлення сигнатурних баз здійснюється виключно адміністратором безпеки.

Перевірка кожного носія перед використанням. Антивірусний комплекс повинен автоматично проводити повне сканування будь-якого підключеного змінного носія до моменту надання доступу до його вмісту.

Заборона автозапуску. Функція автозапуску (Autorun) для всіх типів носіїв має бути програмно вимкнена в ОС.

М.5.1.5 Захист носіїв інформації

Реєстрація всіх носіїв. Всі службові змінні носії (флешки, зовнішні HDD) повинні бути облікові у журналі обліку носіїв інформації.

Сейфи для зберігання. Облікові носії (з резервними копіями) зберігаються у металевому сейфі на території КЗ.

М.5.1.6 Логування та протоколювання

Журнали дій користувачів. Система повинна фіксувати всі події, пов'язані з безпекою, включаючи вхід/вихід користувачів, спроби НСД, дії адміністратора.

Журнали адміністрування. Потрібна детальна фіксація змін у конфігурації безпеки (зміна паролів, налаштування антивірусу).

Зберігання логів. Журнали безпеки повинні зберігатися на системі протягом терміну не менше 1 року, що дозволяє проводити розслідування інцидентів.

М.5.1.7 Резервне копіювання

Політика доступу. До резервних копій має бути забезпечений виключно обмежений доступ (адміністратора безпеки). Копії повинні бути захищені паролем.

Копіювання на окремий захищений носій. Резервне копіювання критичних баз даних проводиться щотижня на окремий зовнішній носій.

Захист копій у сейфі. Носій із резервними копіями має бути зашифрований та зберігатися у сейфі в КЗ.

М.6 Вимоги до документації та організаційних заходів

Формати документів наявні накази інструкції та інше є актуальними і відповідають дійсним нормативним документам.

М.6.1 Накази

Про створення КСЗІ. Наказ № 3 від 15.02.2026 «Про створення комплексної системи захисту інформації».

Про призначення відповідальних осіб (СЗІ). Наказ № 15 від 14.02.2026 «Про створення служби захисту інформації в автоматизованих системах класу «1»». (призначено адміністратором безпеки та системним адміністратором – Довганя Ростислава Віталійовича, адміністратором засобів захисту – Пилипчук Марину Олександрівну, начальником СЗІ – Криштофа Миколу Віталійовича).

М.6.2 Інструкції

Для забезпечення єдиних правил функціонування системи розроблені та чинні такі інструкції.

Інструкція користувача регламентує правила роботи з інформацією, правила автентифікації та дій при виявленні порушень або інцидентів. Як підключати речові докази через блокуватори запису, як зберігати результати та що категорично заборонено робити (наприклад, встановлювати стороннє ПЗ).

Інструкція адміністратора описує порядок налаштування ЗЗІ, управління обліковими записами, адміністрування ОС, проведення моніторингу та технічного обслуговування, перегляд журналу аудиту, оновлення антивірусних баз, резервне копіювання.

Інструкція щодо резервного копіювання встановлює порядок, періодичність (щотижня), методи створення, маркування та безпечного зберігання резервних копій.

М.6.3 Реагування на інциденти

Для ефективної протидії загрозам та мінімізації наслідків порушень впроваджені чіткі процедури реагування.

План реагування на інциденти детально описує алгоритм дій персоналу та адміністратора безпеки у разі виникнення інциденту (виявлення, первинна локалізація, оповіщення, технічний аналіз, локалізація та ліквідація, відновлення, повідомлення зацікавлених сторін/звітність, постінцидентний аналіз).

Фіксація інцидентів. Впроваджений журнал обліку інцидентів, де реєструється кожен випадок порушення політики безпеки, проведена локалізація та ліквідація. У журналі фіксується дата, час, тип порушення (НСД, збій, вірусна атака), вжиті заходи з ліквідації та дані про особу, яка виявила інцидент.

Повідомлення керівництва. Встановлений порядок негайного інформування керівництва організації та, за необхідності, Держспецзв'язку про інциденти, що впливають на конфіденційність або цілісність даних.

М.6.4 Навчання персоналу

Для забезпечення належного рівня обізнаності та культури безпеки здійснюється навчання персоналу.

Інструктаж проводиться первинний (при прийнятті на роботу) та періодичний (не рідше 1 разу на рік) інструктаж користувачів щодо правил роботи з інформацією з грифом обмеження доступу «Для службового користування», конфіденційною інформацією та вимог КСЗІ.

Журнал перевірки знань, де результати проведених інструктажів та перевірки знань фіксуються у журналі перевірки знань та допуску до роботи в АС-1.

М.7 Вимоги до документації, що має бути створена

Модель загроз і порушника. Документ, що формалізує результати аналізу ризиків. Повинен містити детальний перелік актуальних загроз для АС-1 (з виключенням неактуальних мережевих загроз), класифікацію потенційних порушників та оцінку рівня ризиків для КЦД.

Опис середовища функціонування. Документ, що детально описує апаратні, програмні та фізичні компоненти системи. Повинен включати інвентарні номери обладнання, повний перелік ліцензійного програмного забезпечення, опис контрольованої зони та ситуаційний план ОІД.

Політика безпеки. Основний організаційно-розпорядчий документ, що встановлює загальні принципи та правила захисту ІзОД в АС-1. Політика безпеки повинна охоплювати: визначення всіх видів інформації з обмеженим доступом, вимоги до управління персоналом (права, обов'язки, навчання), правила використання засобів захисту (парольна політика, КЕП, антивірус), порядок поводження зі змінними носіями інформації (облік, зберігання, використання), порядок реагування на інциденти та відновлення даних.

М.8 Вимоги до сумісності

Незважаючи на автономний режим роботи АС, для забезпечення надійності функціонування встановлюються вимоги.

Повинна бути забезпечена повна сумісність прикладного, системного та адміністративного програмного забезпечення між собою. Операційна система (Windows 11 Pro) повинна бути офіційно підтримана розробниками всього прикладного ПЗ (Microsoft Office). Це гарантує стабільну роботу та цілісність оброблюваних даних. Встановлений антивірусний комплекс (Avast Business Antivirus 19.X.Y має експертний висновок) не повинен конфліктувати з спеціалізованими криміналістичними програмами, не викликати їхнього зависання та не блокувати легітимні операції.

Всі внутрішні інструкції, накази та звіти повинні використовувати узгоджені формати (DOCX, XLSX, PDF, XML) для забезпечення їхнього коректного перегляду, друку, копіювання та відновлення на АС-1. Криміналістичне ПЗ повинно підтримувати роботу з образами дисків, що мають різні файлові системи (NTFS, FAT32, exFAT, EXT4, APFS, HFS+) для забезпечення можливості всебічного аналізу цифрових доказів.

Враховуючи високу ресурсомісткість процесів індексації та дешифрування даних, антивірусне ПЗ та засоби шифрування диска повинні мати налаштовані виключення для робочих директорій криміналістичного ПЗ, щоб уникнути конфліктів за доступ до оперативної пам'яті та процесорного часу.

Криптографічні модулі, що використовуються в АС-1, повинні забезпечувати єдиний стандарт захисту. Засіб шифрування системного диска (комплекс захисту інформації на носіях "ІІТ Захищений диск-4") повинен коректно функціонувати в середовищі встановленої операційної системи та не конфліктувати з BIOS/UEFI та апаратним забезпеченням ПК.

М.9 Вимоги до випробувань КСЗІ

Створення комплексної системи захисту інформації в АС-1 завершується проведенням випробувань та офіційним введенням системи в експлуатацію. Побудова КСЗІ базується на дотриманні вимог цього технічного завдання та реалізації цільового профілю безпеки. Захист інформації в АС-1 реалізується шляхом впровадження заходів, що відповідають затвердженому профілю безпеки для автономних систем класу «1». Визначено та зафіксовано мінімальний набір функціональних профілів, реалізація яких є обов'язковою для забезпечення необхідного рівня захищеності. Підсистема ідентифікації та автентифікації (IA-5). В системі реалізовано механізм перевірки користувачів за допомогою паролів, що мають довжину не менше 12 символів, з обов'язковою періодичною зміною. Підсистема управління доступом (AC-2, AC-7). Для кожного користувача створено персональний обліковий запис. Для захисту від підбору паролів налаштовано автоматичне блокування сеансу або облікового запису після певної кількості невдалих спроб входу. Підсистема аудиту та звітності (AU-2, AU-6). Забезпечено реєстрацію критичних подій безпеки (вхід/вихід із системи, доступ до файлів) та налагоджено процедуру періодичного (щотижневого) перегляду журналів аудиту адміністратором безпеки. Підсистема захисту носіїв інформації (MP-4, MP-7). Всі змінні носії підлягають суворому обліку та зберіганню у сейфі. Реалізовано програмну заборону використання будь-яких сторонніх (не облікованих) USB-пристроїв. Підсистема забезпечення

цілісності (SI-3). Впроваджено антивірусний захист з функцією локального оновлення баз та обов'язковим попереднім скануванням змінних носіїв. Фізичний захист (PE-3, PE-6). Забезпечено контроль доступу до приміщення, ведення журналу відвідувань та використання охоронної сигналізації.

Після завершення налаштування технічних засобів захисту та затвердження організаційної документації проводяться попередні випробування КСЗІ. Випробування здійснюються власною службою захисту інформації. Метою є перевірка працездатності КСЗІ та відповідності реалізованих заходів вимогам цього технічного завдання. Перевіряється коректність налаштувань парольної політики, надійність блокування сторонніх змінних носіїв, реакція антивірусного програмного забезпечення на тестові загрози, а також правильність ведення журналів аудиту. Результати фіксуються у протоколі попередніх випробувань. Позитивний висновок протоколу є підставою для переходу до етапу введення в експлуатацію.

На підставі позитивних результатів попередніх випробувань та за умови наявності повного комплекту організаційно-розпорядчої документації (наказів, інструкцій, моделі загроз) складається акт приймання КСЗІ в експлуатацію.

Акт підписується членами комісії та затверджується директором Хмельницького НДЕКЦ МВС. Затверджений Акт є офіційним документальним підтвердженням того, що в АС-1 створена комплексна система захисту інформації. З моменту затвердження акта система вважається введеною в експлуатацію та отримує право на обробку інформації з обмеженим доступом.

М.10 Вимоги до супроводу

Регламент оновлень ПЗ. Оновлення сигнатур антивірусного ПЗ та встановлення критичних патчів ОС Windows та прикладного ПЗ здійснюється в ручному режимі (офлайн) адміністратором безпеки. Оновлення сигнатурних баз антивірусного комплексу повинно проводитися не рідше одного разу на тиждень. Перед встановленням будь-якого оновлення створюється контрольна точка відновлення системи для забезпечення можливості відкату у разі конфлікту сумісності або збою.

Регламент перевірки цілісності. Щоденна візуальна перевірка цілісності пломб та охоронних наклейок на корпусі системного блоку, моніторі та невикористовуваних портах. Регулярна (щотижнева) перевірка наявності всіх ключових файлів КСЗІ, включаючи конфігураційні файли ОС та засобів захисту. Щоденний контроль цілісності криміналістичних баз даних та архівів із результатами експертиз за допомогою вбудованих функцій спеціалізованого ПЗ та розрахунку контрольних сум.

План технічного обслуговування. Регулярна діагностика стану апаратного забезпечення, перевірка роботи ДБЖ та стану заземлення. Перевірка стану (доступності та цілісності) облікованих змінних носіїв, які використовуються для резервного копіювання. Щомісячне архівування та перенесення журналів аудиту безпеки на архівний носій для довгострокового зберігання (не менше 1 року).

Періодичний перегляд КСЗІ. Повний перегляд (аудит) КСЗІ та її документації (зокрема, моделі загроз та політики безпеки) проводиться не рідше одного разу на 2 роки (або позапланово у разі суттєвих змін в архітектурі системи чи умовах експлуатації).

Директор Хмельницького НДЕКЦ МВС Андрій ГАНЗЮК

ДОДАТОК Н

Реєстраційна інформація для доступу до ресурсів веб-серверу Центру антивірусного захисту інформації

РЕЄСТРАЦІЙНА ІНФОРМАЦІЯ

для доступу до ресурсів веб-серверу Центру антивірусного захисту інформації

Призначення поля	Значення
Повна назва установи	Хмельницький Науково-дослідний експертно-криміналістичний центр МВС України
Прізвище, ім'я, по батькові користувача	Пилипчук Марина Олександрівна
Посада користувача	Адміністратор безпеки
Назва та версія антивірусного програмного засобу	Avast Business Antivirus 19.X.Y
Перелік IP-адрес для доступу до ресурсів веб-серверу Центру антивірусного захисту інформації	78.152.14.56
Телефон користувача	+380680364599
Адреса електронної пошти користувача	ndekckm@gmail.com
Ім'я користувача*	pulupchykmo

_____

* Ім'я користувача - коротка назва користувача (англійськими буквами) для доступу до ресурсів веб-серверу Центру антивірусного захисту інформації.

ДОДАТОК П

План впровадження комплексної системи захисту інформації в автоматизованій системі класу «1» об’єкту інформаційної діяльності № 101 відділу цифрової криміналістики

ЗАТВЕРДЖУЮ
Директор Хмельницького
НДЕКЦ МВС
_____ Ганзюк А.Л.
20.03.2026 р.

ПЛАН ВПРОВАДЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

П.1 Загальні відомості

Об’єкт захисту: Автоматизована система класу «1» відділу цифрової криміналістики Хмельницького НДЕКЦ МВС.

Підстава для впровадження КСЗІ:

- Закон України «Про захист інформації в інформаційно-комунікаційних системах»
- Затверджений цільовий профіль безпеки
- Наказ Директора Хмельницького НДЕКЦ МВС № 3 від 15.02.2026 р. «Про створення комплексної системи захисту інформації»

Мета впровадження:

Забезпечення конфіденційності, цілісності та доступності інформації з грифом обмеження доступу «Для службового користування», конфіденційної інформації (матеріали судових експертиз, цифрові докази та персональні дані суб’єктів кримінальних проваджень) відповідно до вимог нормативно-правових актів у сфері ТЗІ.

П.2 Основні етапи впровадження КСЗІ

№	Етап	Зміст робіт	Результат
1	Організаційна підготовка	Призначення відповідальних (адміністратора безпеки, адміністратора ЗЗІ, інженера ТЗІ), формування служби захисту інформації	Накази про призначення
2	Обстеження ІС	Аналіз архітектури, ресурсів, потоків інформації, перевірка захищеності	Акт категоріювання, Акт обстеження
3	Розробка документації	Розробка ТЗ, профілю безпеки, моделі загроз, політики безпеки, інструкцій (користувача, адміністратора).	Комплект документів
4	Реалізація заходів	Встановлення та налаштування засобів захисту, політик аудиту та блокування USB-портів	Реалізовані механізми захисту
5	Випробування	Перевірка ефективності впроваджених заходів захисту (проведення попередніх випробувань, перевірка блокувань та журналювання)	Протоколи випробувань
6	Введення в дію	Оформлення Акта приймання в експлуатацію та допуск користувачів до роботи.	Акт введення в експлутацію

П.3 План реалізації заходів безпеки

№	Вимога профілю безпеки	Захід	Засіб / Метод	Відповідальний	Термін
1	IA-2 (Ідентифікація, Рівень 1)	Впровадження системи унікальної ідентифікації користувачів АС-1.	Локальні користувачі та групи	Адміністратор безпеки	1 день
2	IA-5 (1) (Автентифікація, Рівень 2)	Реалізація політики суворої парольної автентифікації.	GPO: Політики облікових записів Політика паролів	Адміністратор безпеки	1 день
3	IA-8 Рівень 1 (Ідентифікація, Рівень 1)	Заборона доступу до АС-1 для осіб, що не є співробітниками підрозділу.	Організаційні заходи / Журнал відвідувачів	Керівник СЗІ	Постійно
4	AC-2 (Доступ, Рівень 2)	Організація рольового управління доступом до системних ресурсів.	Властивості папок (NTFS Permissions)	Адміністратор безпеки	2 дні
5	AC-2 (3) (Управління доступом, Рівень 1)	Автоматична деактивація облікових записів після 30 днів неактивності.	Скрипт PowerShell / GPO	Адміністратор безпеки	1 день
6	AC-5 (Управління доступом, Рівень 2)	Обмеження логічного доступу (Адміністратор не бачить файли експертиз, експерт не змінює безпеку).	Властивості безпеки (NTFS Permissions)	Адміністратор безпеки	2 дні
7	AC-6 (Управління доступом, Рівень 1)	Надання експерту доступу лише до тих баз, які необхідні для експертизи.	Розмежування прав на робочі каталоги (NTFS)	Адміністратор безпеки	Постійно
8	AC-7 (Управління доступом, Рівень 1)	Блокування термінала на 30 хв після 5 невдалих спроб входу.	GPO: Політика блокування облікового запису	Адміністратор безпеки	2 дні

9	AC-11 (Блокування пристрою, Рівень 1)	Впровадження механізму автоматичного блокування сеансу користувача.	Персоналізація Windows / GPO	Адміністратор безпеки	1 день
10	AC-20 (Зовнішні системи, Рівень 1)	Заборона підключення особистих ноутбуків/телефонів до АС-1.	Інструкція користувача / Адміністративні заходи	Керівник СЗІ	1 день
11	AU-2 (Аудит, Рівень 1)	Налаштування реєстрації подій, що впливають на стан безпеки системи.	Політика аудиту (Audit Policy)	Адміністратор безпеки	1 день
12	AU-6 (Аналіз, Рівень 1)	Організація регулярного моніторингу та аналізу журналів аудиту.	Журнал "Перегляд подій" (Event Viewer)	Адміністратор безпеки	Щотижня
13	AU-9 Рівень 1 (Аналіз аудиту)	Доступ до журналів подій лише для читання; налаштування захисту від перезапису.	Властивості журналу безпеки / NTFS	Адміністратор безпеки	1 день
14	MP-4 (Зберігання носіїв, Рівень 1)	Забезпечення фізичної цілісності та безпечного зберігання носіїв ІзОД.	Металевий сейф у КЗ	Інженер ТЗІ	1 день
15	MP-6 Рівень 2 (Очищення пам'яті)	Застосування спеціалізованих утиліт для гарантованого затирання залишкових даних.	Утиліти гарантованого знищення (напр., SDelete)	Адміністратор безпеки	За потреби
16	MP-7 (Використання носіїв, Рівень 1)	Програмно-технічне обмеження використання сторонніх змінних носіїв.	Редактор реєстру / Device Control	Адміністратор безпеки	3 дні
17	PE-3 / PE-6 (Фізичний захист, Рівень 1)	Організація фізичного захисту та моніторингу доступу до приміщення КЗ.	Охоронна сигналізація, Журнал відвідувачів	Інженер з ТЗІ	7 днів

18	PE-11 (Живлення, Рівень 1)	Забезпечення стабільного електроживлення для запобігання втраті даних.	ДБЖ APC Back-UPS	Інженер ТЗІ	2 дні
19	SI-3 (Антивірус, Рівень 1)	Впровадження антивірусного захисту та регламенту оновлення баз.	Avast Business Antivirus	Адміністратор безпеки	1 день
20	SI-4 Рівень 1 (Контроль цілісності)	Постійний моніторинг АРМ на предмет підключення сторонніх пристроїв.	Журнали ОС Windows / Засоби аудиту PnP	Адміністратор безпеки	Постійно
21	SI-7 Рівень 1 (Захист від коду)	Перевірка цілісності системних файлів ОС Windows інструментами системи.	Утиліта перевірки файлів системи (SFC)	Адміністратор безпеки	Щомісяця
22	SI-12 Рівень 1 (Захист від коду)	Налаштування автоматичного очищення кеш-пам'яті та тимчасових файлів при завершенні сеансу.	GPO / Локальні скрипти (Logoff script)	Адміністратор безпеки	1 день
23	MA-2 Рівень 1 (Обслуговування)	Ведення журналу технічного обслуговування АРМ та перевірки стану ДБЖ.	Паперовий журнал ТО	Інженер ТЗІ	Постійно
24	MA-4 (Обслуговування, Рівень 1)	Встановлення регламенту контрольованого технічного обслуговування.	Номерні пломби / стікери	Інженер ТЗІ	2 дні
25	SC-28 Рівень 2 (Захист інформації на носіях)	Використання шифрування системного розділу для захисту інформації на носіях.	ПЗ «ІІТ Захищений диск-4»	Адміністратор безпеки	2 дні
26	IR-4 Рівень 1 (Обробка інциденту)	Розроблення порядку реагування на інциденти, ведення журналу інцидентів.	Інструкція з реагування / Журнал інцидентів	Адміністратор безпеки	5 днів

27	CP-2 Рівень 1 (Обслуговування)	Наявність затвердженого регламенту дій експерта та адміністратора у разі апаратного збою АРМ.	Інструкція з експлуатації КСЗІ	Керівник СЗІ	5 днів
28	CP-9 Рівень 1 (Резервне копіювання)	Щотижневе повне резервне копіювання на зовнішній носій (зберігання в сейфі).	Засоби Windows Backup / Зовнішній HDD	Адміністратор безпеки	Щотижня
29	SM-1 Рівень 1 (Ручне керування)	Затвердження внутрішніх інструкцій з експлуатації КСЗІ та правил парольного захисту.	Накази та інструкції по НДЕКЦ	Керівник СЗІ	7 днів
30	SM-3 Рівень 1 (Ручне керування)	Блокування доступу до системи протягом 1 робочої години при звільненні працівника.	Організаційний регламент взаємодії з ОК	Адміністратор безпеки	За потреби
31	NSD-1 Рівень 2 (Технічні засоби)	Активація режиму самозахисту антивірусного ПЗ та локального міжмережевого екрана.	Налаштування Avast / Windows Defender Firewall	Адміністратор безпеки	1 день
32	PS-3 Рівень 1 (Перевірка персоналу)	Надання доступу до АС-1 виключно після проходження внутрішньої перевірки.	Наказ / Кадрова процедура	Керівник СЗІ	Постійно
33	PS-4 Рівень 1 (Обробка інциденту)	Блокування доступу протягом години при звільненні працівника (технічна реалізація).	Адміністративні процедури в ОС Windows	Адміністратор безпеки	За потреби
34	AT-2 Рівень 1 (Керування персоналом)	Проведення щорічного інструктажу експертів щодо кібергігієни (запис у журналі).	Журнал інструктажів / Програма навчання	Керівник СЗІ	Щороку

35	АТ-3 Рівень 1 (Керування персоналом)	Спеціалізоване навчання ролі "Адміністратор безпеки" щодо процедур аудиту.	Програми підвищення кваліфікації / Курси	Керівник СЗІ	Щорок у
36	СМ-8 Рівень 1 (Керування конфігураціє ю)	Ведення актуального апаратного та програмного паспорта АРМ експерта.	Формуляр (Паспорт) АС-1	Адміністратор безпеки	Постій но
37	СМ-10 Рівень 1 (Обмеження використання)	Заборона встановлення стороннього ПЗ на АРМ. Дозволено лише криміналістичне ПЗ.	AppLocker / Software Restriction Policies	Адміністратор безпеки	2 дні

П.4 Технічні заходи

1. Розмежування доступу до ресурсів. На об'єкті впроваджується рольова модель доступу на базі локальних облікових записів ОС Windows. Створюється обліковий запис «Експерт» із правами «Користувач», що обмежує доступ до системних каталогів та забороняє самостійне встановлення ПЗ. Доступ до робочих каталогів із матеріалами кримінальних проваджень, образами цифрових доказів та результатами експертиз налаштовується через дозволи безпеки файлової системи NTFS (доступ надається виключно авторизованому експерту). Фізично розмежування доступу забезпечується опломбуванням корпусу системного блоку та забороною підключення сторонніх пристроїв (особистих ноутбуків) у межах кабінету № 101.

2. Контроль автентифікації користувачів. Вхід до системи можливий лише після успішної парольної автентифікації. Через локальну політику безпеки встановлюється мінімальна довжина пароля 12 символів із вимогою використання цифр та спецсимволів. Пароль підлягає обов’язковій зміні кожні 60 днів. Після 5 невдалих спроб введення пароля обліковий запис автоматично блокується на 30 хвилин. Ініціюється автоматичне блокування екрана (Lock Screen) після 10 хвилин бездіяльності користувача.

3. Антивірусний захист. Захист від шкідливого коду реалізується за допомогою антивірусного комплексу Avast Business Antivirus 19.X.Y (актуальна версія включена до переліку технічних засобів, дозволених до застосування, має експертний висновок) . Оскільки АС-1 є автономною, оновлення вірусних сигнатур здійснюється адміністратором безпеки вручну (офлайн) за допомогою перевіреного службового носія не рідше одного разу на тиждень. Налаштовано автоматичне сканування будь-яких підключених змінних носіїв інформації. Щоденно проводиться швидке сканування оперативної пам'яті та завантажувальних секторів.

4. Журналювання подій безпеки. Система реєстрації подій налаштовується в ОС Windows для фіксації критичних дій. У журналі «Безпека» (Security) реєструються всі факти входу/виходу, спроби доступу до захищених файлів, зміни прав доступу та зміна системного часу. Адміністратор безпеки щотижня проводить аналіз журналів на

предмет аномальної активності. Журнали зберігаються в електронному вигляді протягом 1 року.

5. Резервне копіювання та відновлення. Для забезпечення доступності даних впроваджується регламент резервування. Кожної п'ятниці адміністратор виконує повне резервне копіювання баз даних та конфігураційних файлів на зовнішній жорсткий диск (HDD). Зовнішній диск маркується обліковим номером і зберігається у вогнетривкому металевому сейфі в кабінеті № 101. Раз на квартал проводиться тестове відновлення даних на контрольному обладнанні для перевірки цілісності копій.

6. Контроль цілісності інформації та обладнання здійснюється комплексно. Щоденна візуальна перевірка цілісності номерних пломб на корпусі ПК. Використання комплексу захисту інформації «ІІТ Захищений диск-4» для шифрування розділів диска, що запобігає несанкціонованій зміні даних у разі завантаження з іншого носія. Налаштування заборони автоматичного запуску (Autorun) зі змінних носіїв та використання контрольних сум для критичного ПЗ.

Директор Хмельницького НДЕКЦ МВС Андрій ГАНЗЮК