Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Александровської Дар'ї Максимівни

на здобуття ступеня вищої освіти Бакалавра

Комплексна система захисту інформації ТОВ "ПРАЩУР"

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

КРБКБ.220101.22.01.01 ПЗ

Виконала студентка 4 курсу група КБ-22-1 Дар'я АЛЕКСАНДРОВСЬКА

Керівник канд. техн. наук, доцент Віктор ЧЕШУН

Нормоконтролер д-р філософії Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

17 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
Александровській Дар'ї Максимівні

1 Тема роботи комплексна система захисту інформації ТОВ "ПРАЩУР"

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 особливості обробки конфіденційної інформації та інтелектуальної власності на АРМ директора ТОВ «ПРАЩУР». Забезпечити конфіденційність, цілісність та доступність управлінських даних шляхом впровадження технічних і організаційних заходів захисту.
4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз бізнес-процесів ТОВ «ПРАЩУР» та нормативно-правової бази у сфері захисту інформації. Сучасні підходи до захисту АРМ керівного складу в комерційному секторі. Формування архітектури системи захисту та розробка корпоративних політик безпеки. Вибір інженерно-технічних та програмно-апаратних засобів (зокрема, антивірусного захисту та шифрування).
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 _____ Дар'я АЛЕКСАНДРОВСЬКА

Керівник кваліфікаційної роботи _____ Віктор ЧЕШУН

АНОТАЦІЯ

Тема кваліфікаційної роботи: комплексна система захисту інформації ТОВ "ПРАЩУР"

Автор роботи: Александровська Дар'я Максимівна.

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

Загальний обсяг роботи: 72 сторінки, 14 рисунків, 4 таблиці, 7 додатків, 43 посилання.

Графічна частина: 3 плакати.

Ключові слова: захист інформації, комплексна система захисту інформації, система захисту, інформаційна безпека, політика безпеки.

Кваліфікаційна робота присвячена розробці проєктування комплексної системи захисту інформації для автоматизованого робочого місця керівника ТОВ «ПРАЩУР». У межах дослідження проаналізовано специфіку інформаційної діяльності підприємства, вивчено вимоги нормативно-правової бази у сфері технічного захисту інформації, а також сформовано детальну модель загроз і модель порушника для обраного об'єкта.

Обґрунтовано вибір та впровадження комплексу організаційних, програмних і технічних заходів, спрямованих на гарантування конфіденційності, цілісності та доступності критично важливих комерційних даних.

Отримані результати та розроблені інженерні рішення можуть бути використані як типовий взірець під час створення або модернізації систем безпеки для керівних ланок у комерційному секторі.

25.05.2026

ANNOTATION

Theme of qualification work: Comprehensive Information Security System of PRASCHUR LLC

Author of the work: Aleksandrovska Daria Maksymivna

Mentor: Ph.D. Cheshun Viktor Mykolaiovych

Total volume of the thesis: 72 pages, 14 figures, 4 tables, 7 appendices, 43 references.

Graphic section: 3 posters.

Keywords: information protection, comprehensive information protection system, protection system, information security, security policy.

This thesis is devoted to the development and design of a comprehensive information security system for the automated workstation of the director of PRASCHUR LLC. The study analyzes the specifics of the company's information activities, examines the requirements of the regulatory framework in the field of technical information security, and develops a detailed threat model and attacker model for the selected target.

The selection and implementation of a set of organizational, software, and technical measures aimed at ensuring the confidentiality, integrity, and availability of critically important commercial data are justified.

The results obtained and the engineering solutions developed can be used as a model when creating or modernizing security systems for management in the commercial sector.

25.05.2026

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце

ПЕМВН – побічні електромагнітні випромінювання

АС – автоматизовна система

ДТЗ – допоміжні технічні засоби

ДСТУ – Державний стандарт України

ЗЗІ – засоби захисту інформації

ЗУ – Закон України

ІзОД – інформація з обмеженим доступом

ІС – інформаційна система

ІКС – інформаційно - комунікаційна система

КСЗІ – комплексна система захисту інформації

НД ТЗІ – нормативний документ системи технічного захисту інформації

ОІД – об’єкт інформаційної діяльності

ОТЗ – основні технічні засоби

ПЗ – програмне забезпечення

ПІБ – політика інформаційної безпеки

ПП – приватне підприємство

ТЗІ – технічний захист інформації

ТОВ – товариство з обмеженою відповідальністю

ВСТУП

Глобальна цифровізація перетворила інформацію на ключовий стратегічний ресурс організації, від якого безпосередньо залежить її стабільність та ринкова репутація. Забезпечення безпеки даних сьогодні є не просто технічним завданням ІТ-відділу, а базовою умовою виживання бізнесу. Поява нових векторів кібератак та методів соціальної інженерії, створює постійні ризики для ІТ-інфраструктури підприємств, де вразливість автоматизованих робочих місць керівництва може призвести до миттєвої зупинки операційних процесів.

Для ТОВ «ПРАЩУР», що займається розробкою високотехнологічних вебдодатків та реалізацією складних інтеграційних рішень, захист інтелектуальної власності й конфіденційної інформації клієнтів є критично важливим. У період правового режиму воєнного стану, коли кібератаки стали невіддільною частиною гібридної агресії, будь-яке несанкціоноване втручання, модифікація чи витік даних тягнуть за собою значні фінансові втрати та руйнування довіри на ринку ІТ-послуг.

Локальні чи фрагментарні рішення вже не здатні протидіяти сучасним загрозам. Виникає потреба у переході до побудови комплексних систем захисту інформації (КСЗІ), які об'єднують організаційні регламенти, технічні та програмно-апаратні інструменти в єдину захищену архітектуру [1].

Метою даної кваліфікаційної роботи є проєктування та обґрунтування моделі КСЗІ для ТОВ «ПРАЩУР», що дозволить забезпечити надійний захист його інформаційно-комунікаційної системи, зокрема автоматизованого робочого місця керівника, та підготувати ІТ-інфраструктуру до подальшої державної атестації відповідно до чинних норм. Об’єктом дослідження є процеси забезпечення інформаційної безпеки в інформаційно-комунікаційній системі підприємства, а предметом - сукупність методів, технологій, програмно-апаратних засобів та організаційних регламентів, які формують захищене середовище ТОВ «ПРАЩУР».

Для реалізації визначеної мети необхідно вирішити низку взаємопов'язаних завдань. Спочатку потрібно проаналізувати вимоги законодавства України та положення міжнародних стандартів у сфері захисту інформації, після чого дослідити поточний стан ІТ-інфраструктури підприємства та ідентифікувати критичні активи. На основі отриманих даних необхідно побудувати моделі загроз та потенційного порушника для об'єкта дослідження, розробити безпосередню архітектуру КСЗІ та сформувати чіткі вимоги до підсистем моніторингу й розмежування доступу. Завершальним кроком є підготовка проєктів нормативно-розпорядчих документів, таких як положення та інструкції, що регулюватимуть діяльність служби інформаційної безпеки.

Методологічну основу дослідження становлять системний аналіз, теорія ризиків та нормативно-проєктувальний підхід. Практичне значення отриманих результатів полягає у створенні готової до розгортання моделі захисту. Її впровадження дозволить ТОВ «ПРАЩУР» мінімізувати ризики успішної реалізації кібератак, підвищити загальний рівень кіберстійкості та забезпечити повну відповідність чинній нормативній базі у сфері технічного захисту інформації.

1 АНАЛІЗ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТОВ «ПРАЩУР» ТА НОРМАТИВНО-МЕТОДОЛОГІЧНІ ЗАСАДИ ЇХ ЗАХИСТУ

1.1 Нормативно-правова база та стандарти у сфері технічного захисту інформації

Проєктування комплексної системи захисту інформації (КСЗІ) в ІТ-інфраструктурі ТОВ «ПРАЩУР» базується на суворому дотриманні вимог чинного законодавства України та чинних нормативних документів у сфері технічного захисту інформації. Базовий рівень правового регулювання забезпечують Закони України «Про інформацію» та «Про захист інформації в інформаційно-комунікаційних системах» [2,3].

Закон України «Про інформацію» визначає загальний правовий режим відомостей, регламентує процеси їх створення, збирання, використання та поширення. Згідно зі статтею 1 цього Закону, інформацією є будь-які відомості про події, явища або об'єкти незалежно від форми їхнього представлення. Цей нормативно-правовий акт класифікує види інформації за доступом і встановлює правові засади інформаційної діяльності, окреслюючи обов'язки суб'єктів щодо збереження конфіденційності чи обмеження доступу до певних категорій даних.

Своєю чергою, Закон України «Про захист інформації в інформаційно-електронних системах» безпосередньо регулює відносини у сфері захисту інформаційних ресурсів, які обробляються в автоматизованих системах. Цей документ є визначальним для ТОВ «ПРАЩУР», оскільки він чітко розмежовує поняття володільця інформації та володільця самої системи (організації, якій належить право власності або користування автоматизованим робочим місцем чи мережею). Закон покладає повну відповідальність за забезпечення захисту інформації на володільця системи, фіксуючи обов'язковість створення КСЗІ з підтвердженою відповідністю для систем, де обробляються державні ресурси або конфіденційні дані, захист яких гарантується державою.

З огляду на специфіку діяльності підприємства (зокрема, ведення

кадрового обліку, збереження клієнтських баз та фінансової звітності), критично важливим є дотримання Закону України «Про захист персональних даних» [4] Закон визначає персональні дані як відомості про фізичну особу, яку ідентифіковано або можна конкретно ідентифікувати (ім'я, контактні дані, реквізити рахунків тощо). Під час оформлення трудових відносин чи підписання контрактів із контрагентами ТОВ «ПРАЩУР» набуває статусу володільця бази персональних даних. Це накладає на підприємство юридичне зобов'язання забезпечити технічний та організаційний захист цих відомостей від незаконної обробки, випадкової втрати, знищення або несанкціонованого доступу на всіх етапах їхнього життєвого циклу.

Додатково, у разі взаємодії підприємства з державними замовниками чи виконання робіт у межах оборонного замовлення, правові відносини, пов’язані з віднесенням відомостей до державної таємниці, регулюються Законом України «Про державну таємницю» [5]. Цей акт чітко визначає категорії інформації у сферах оборони, економіки, науки та зовнішніх відносин, що підлягають засекречуванню, регламентує порядок надання допусків і доступів посадовим особам, а також встановлює сувору кримінальну та адміністративну відповідальність за розголошення такої інформації або її втрату.

Організаційно-методологічна модель нормативного регулювання побудови захищеного контуру підприємства має дворівневу структуру, де законодавчі акти вищого рівня визначають правове поле та обов'язки, а профільні стандарти НД ТЗІ регламентують конкретні інженерно-технічні вимоги. Взаємозв'язок елементів нормативно-правової бази технічного захисту інформації наведено на рисунку1.1.

Представлена на рисунку 1.1 модель чітко демонструє розподіл функцій між правовим та технічним інститутами регулювання. Верхній рівень (Рівень I) формує імперативний базис, який зобов'язує ТОВ «ПРАЩУР» як суб'єкта господарювання забезпечити недоторканність клієнтських та корпоративних даних. Нижній рівень (Рівень II) транслює ці загальні правові норми у площину конкретних інженерних рішень.

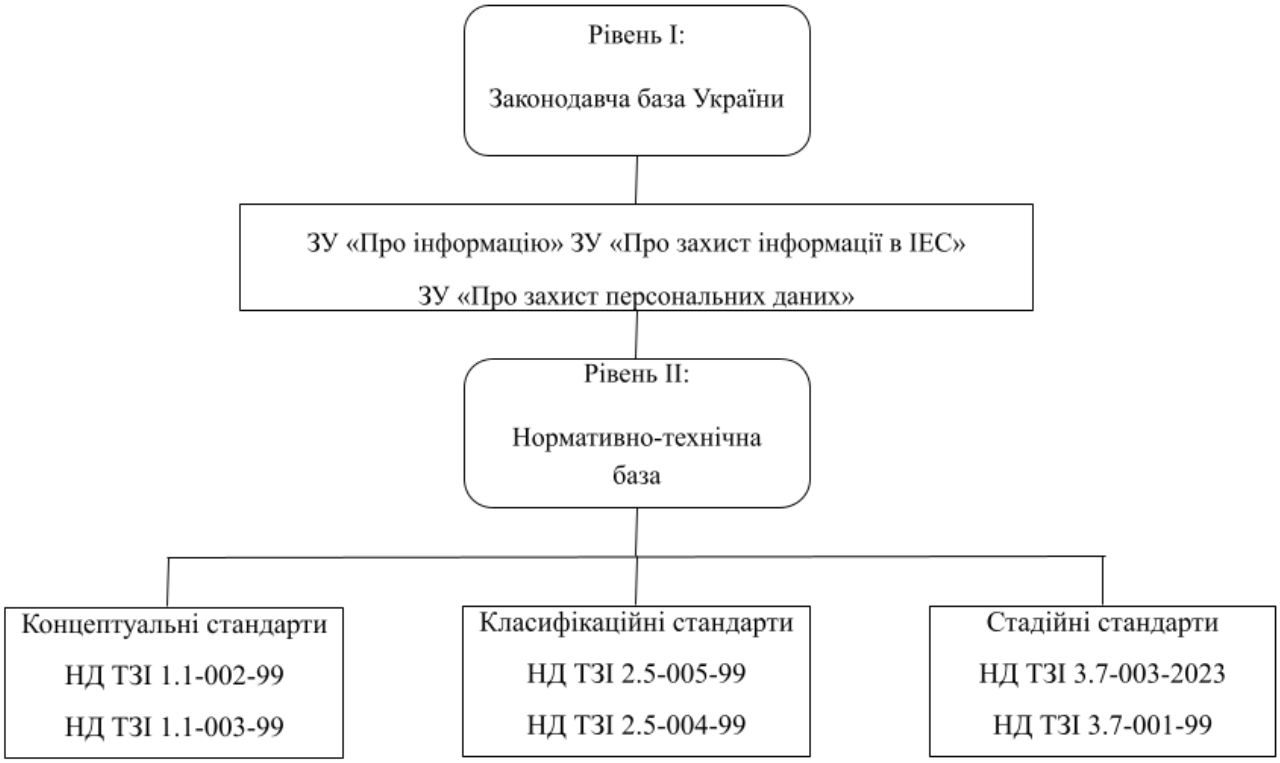


Рисунок 1.1 – Структура нормативно-правового та технічного регулювання ТЗІ в Україні

Концептуальні стандарти забезпечують єдину термінологічну мову для розробників, класифікаційні - дозволяють чітко позиціонувати АРМ керівника в структурі технічних вимог, а стадійні - визначають покроковий життєвий цикл проєктування від формування технічного завдання до проведення державної експертизи. Такий інтегрований підхід виключає суперечності при побудові архітектури безпеки та гарантує успішне отримання атестата відповідності.

Технічна та процедурна складові розробки системи безпеки регламентуються нормативними документами системи ТЗІ в Україні. Термінологічну основу та концептуальні принципи протидії несанкціонованому доступу закладено у документах НД ТЗІ 1.1-002-99 та НД ТЗІ 1.1-003-2000 [6-7]. Вони формують понятійний апарат, який використовується при аналізі архітектури системи. Для побудови коректної моделі безпеки ІТ-інфраструктури ТОВ «ПРАЩУР» першочергове значення має класифікація автоматизованих систем згідно з НД ТЗІ 2.5-005-99 [8]. Вона дозволяє визначити категорію

системи (наприклад, автономне робоче місце чи розподілена мережа) та обрати необхідний замовнику функціональний профіль захисту. Оцінка надійності та достатності впроваджених механізмів захисту здійснюється на основі критеріїв, викладених у НД ТЗІ 2.5-004-99 [9].

Практичний алгоритм розгортання захисних засобів регламентується стандартом НД ТЗІ 3.7-003-05 [10], який визначає стадії та етапи створення КСЗІ в інформаційно-комунікаційних системах. Процес розпочинається з розробки технічного завдання на створення системи захисту, вимоги до структури та змісту якого чітко прописані у методичних вказівках НД ТЗІ 3.7-001-99 [11].

1.2 Аналіз об'єкта захисту та класифікація інформаційних ресурсів автоматизованого робочого місця керівника ТОВ «ПРАЩУР»

Центральною ланкою в управлінській вертикалі ТОВ «ПРАЩУР» виступає директор компанії. Його повсякденна робота із ведення бізнесу, підписання угод та контролю підрозділів організована на базі індивідуального автоматизованого робочого місця [12]. У технічному розумінні це обчислювальна інфраструктура: комп'ютерне обладнання, системне й прикладне ПЗ, мережеві інтерфейси, яка дозволяє оперативно виконувати адміністративні завдання.

Оскільки керівник володіє максимальними повноваженнями в корпоративній мережі, його комп'ютер є головною мішенню для зовнішніх і внутрішніх загроз. Саме тут акумулюються та проходять обробку найбільш чутливі масиви даних підприємства:

– відомості про банківські рахунки, фінансові транзакції, кошториси та комерційні контракти;

– цифрові активи компанії, зокрема програмні коди вебплатформ, архітектурні схеми Hardware-рішень та технічна документація;

– конфіденційні картки кадрового обліку персоналу та реєстри замовників;

– криптографічні ключі, цифрові підписи та адміністративні паролі від хмарних серверів і внутрішніх баз даних.

Враховуючи профіль ТОВ «ПРАЩУР» як розробника програмно-апаратних комплексів, успішна кібератака на комп'ютер директора (через фішинг чи шкідливе ПЗ) матиме фатальні наслідки. Блокування роботи цього вузла, викрадення інтелектуальної власності або викривлення управлінської інформації здатні повністю дезорганізувати бізнес-процеси. З огляду на це, проєктування КСЗІ навколо комп'ютера керівника є першочерговою інженерною задачею, яка потребує впровадження суворих правил автентифікації та постійного аудиту подій безпеки.

Для підвищення ефективності адміністрування та запобігання несанкціонованому доступу до ПЗ, АРМ директора реалізує низку критичних функцій. Система забезпечує збір та обробку різнорідних первинних даних, що надходять із зовнішніх та внутрішніх джерел інформації, з можливістю подальшої генерації консолідованої звітності й аналітичних зрізів для оцінки ринкового стану компанії. Через програмні інтерфейси робочого місця здійснюється координація виробничих та бізнес-процесів розробки вебсофту, а також адміністрування персоналу, що включає моніторинг продуктивності інженерів, планування графіків та ведення обліку робочого часу. Завдяки високій структурованості інтерфейсів забезпечується експертна підтримка прийняття рішень, що мінімізує часові витрати керівництва на реагування у кризових ситуаціях [13].

Впровадження КСЗІ навколо АРМ директора спрямоване на збереження базових критеріїв безпеки, а саме конфіденційності, цілісності та доступності інформаційних ресурсів обмеженого доступу, а також підтримання доступності відкритої інформації, важливої для стабільного ведення бізнесу. Необхідність розробки такої інтегрованої системи захисту зумовлена постійним збільшенням кількості векторів кібератак, зумовлених кризовими економічними факторами, масовим переходом на хмарну архітектуру та доступністю інструментів

несанкціонованого втручання. Побудова всебічного контуру безпеки ТОВ «ПРАЩУР» охоплює три стратегічні напрямки:

– правовий (нагляд за виконанням вимог державної політики та профільного законодавства);

– організаційний (розробка внутрішніх регламентів, інструкцій, режимних заходів та контроль їх дотримання);

– програмно-апаратний (захист від витоку інформації технічними каналами, розмежування прав користувачів, антивірусні пакети, системи безперебійного електроживлення та аудит подій безпеки).

Важливим кроком у забезпеченні стійкості ІТ-інфраструктури є чітка класифікація інформаційних масивів за рівнем доступу. Наказом керівника затверджується Перелік відомостей, що становлять конфіденційну інформацію та дані ДСК підприємства [14]. Повна структурована класифікація електронних ресурсів АРМ керівника наведена у таблиці 1.1.

Таблиця 1.1 – Диференціація корпоративних даних ТОВ «ПРАЩУР» за грифами обмеження доступу

№ з/п	Найменування інформаційного масиву / категорія даних	Визначений гриф обмеження доступу
1	2	3
1	Фінансова звітність, баланси прибутків та збитків, бухгалтерія, інвестиційні плани	Для службового користування
2	Експлуатаційна та нормативна документація щодо технічних рішень у спеціальних проєктах	Для службового користування
3	Відомості про організаційну структуру, плани реагування в умовах надзвичайних ситуацій	Для службового користування
4	Опис технічних та організаційних заходів щодо захисту інформації на підприємстві	Для службового користування

Кінець таблиці 1.1

1	2	3
5	Технічні характеристики, специфікації послуг та розроблюваних товарів	Для службового користування
6	Реєстри клієнтів, бази контрагентів та відомості про замовників підприємства	Конфіденційно
7	Кадрові картки, анкети, персональні дані та посадові інструкції співробітників	Конфіденційно
8	Стратегічні плани розвитку ТОВ «ПРАЩУР», результати аналізу ринку та конкурентів	Конфіденційно
9	Дані про поточний стан, продуктивність та внутрішню ефективність роботи підрозділів	Конфіденційно
10	Відомості про конфігурацію корпоративної мережі, IP-адреси, схеми серверів та комутації	Конфіденційно
11	Загальнодоступна фінансова інформація та публічні звіти для податкових органів	Відкрита інформація
12	Публічні презентації завершених проєктів, новини та дані про загальнодоступні події	Відкрита інформація
13	Законодавство України, правила внутрішнього розпорядку, норми техніки безпеки	Відкрита інформація
14	Перелік підприємств-партнерів регіону, публічні контакти та імена їхніх керівників	Відкрита інформація

На основі диференціації корпоративних даних, наведеної у таблиці 1.1, доцільно провести структурно-кількісний аналіз інформаційних масивів АРМ директора ТОВ «ПРАЩУР». Зіставлення розподілу ресурсів за визначеними критеріями й грифами обмеження доступу відображено на рисунку 1.2.

Проведений статистичний аналіз дозволяє зробити висновки щодо

архітектури майбутньої КСЗІ. Левова частка інформаційних ресурсів, що циркулюють на робочому місці керівника (сумарно 72%, куди входять масиви ДСК та конфіденційні дані), належить до категорії інформації з обмеженим доступом.

Рисунок 1.2 – Структурний розподіл інформаційних масивів АРМ директора за рівнями конфіденційності

Паритетний розподіл між службовою та комерційною таємницею (по 36% відповідно) вказує на необхідність розгортання гнучких механізмів розмежування доступу. Наявність 28% відкритої інформації підтверджує, що АРМ директора не є повністю ізольованим сегментом, а активно взаємодіє із зовнішнім інформаційним простором. Отримане співвідношення строго обґрунтовує вибір політики безпеки, орієнтованої на захист конфіденційності без погіршення доступності публічних сервісів компанії.

Формування деталізованого класифікаційного переліку відомостей та комплексне документування технічних засобів, інтегрованих в автоматизоване робоче місце директора, є базовим підґрунтям для успішної побудови системи захисту і стабільного функціонування компанії. Інфраструктура АРМ розробляється з розрахунком на оперативне розв'язання низки інженерно-управлінських завдань, серед яких першочерговими є експрес-оцінка поточного

технічного стану комп'ютерного та програмного комплексів, а також раціональне адміністрування наявних цифрових ресурсів. Окрім цього, програмний контур системи має забезпечувати безперервний моніторинг і виявлення системних вразливостей, автоматичне формування планових чи позачергових звітів для керівництва та всебічне оцінювання стійкості впроваджених інструментів безпеки.

Усі захищувані масиви даних зберігають стабільну документовану форму, оскільки під електронним документом розуміють інформаційний об'єкт, зафіксований на матеріальному чи віртуальному носії та забезпечений реквізитами для його однозначної ідентифікації. Відповідно до цієї методології, захисту підлягають не лише текстові файли, а й графічні схеми, бази даних, системні логи, конфігураційні рядки та резервні копії, що зберігаються в пам'яті обчислювального комплексу [15].

Корпоративна інформація ТОВ «ПРАЩУР» чітко розмежовується за рівнями конфіденційності. До категорії загальнодоступних відомостей відносять тексти законодавчих актів, положення внутрішнього розпорядку компанії, вимоги охорони праці та техніки безпеки при роботі з обладнанням. До цього ж сегмента належать анкетні дані співробітників, їхні робочі контакти, графіки функціонування офісу, відкриті презентаційні матеріали для клієнтів та публічні реєстри контрагентів регіону. Натомість категорія даних з обмеженим доступом охоплює внутрішні посадові регламенти, персональні відомості штату, комерційні контракти на постачання техніки, фінансово-економічні показники компанії, а також детальній схеми мережевої архітектури, IP-адресацію та конфігураційні файли серверного обладнання. Наявність чіткої межі між відкритими та конфіденційними даними безпосередньо впливає на вибір архітектури майбутньої системи захисту. Здійснена класифікація інформаційних масивів АРМ директора ТОВ «ПРАЩУР» формує необхідний базис для оцінки кіберризиків.

1.3 Цільова спрямованість та призначення комплексної системи захисту інформації

Функціонування автоматизованого робочого місця керівника ТОВ «ПРАЩУР» організовується з урахуванням нормативно-правових вимог України щодо менеджменту та збереження даних. Головна функція директора полягає у забезпеченні стабільного оперування компанією та ухваленні управлінських рішень на основі актуальних відомостей. Оскільки цей вузол є найвищим в ієрархічній структурі підприємства, на ньому консолідуються абсолютно всі інформаційні потоки, що описують діяльність суб'єкта господарювання.

Головне призначення створення КСЗІ на об'єкті дослідження полягає у реалізації системи інженерно-технічних та організаційних методів, які гарантують постійне підтримання конфіденційності й цілісності інформаційних ресурсів, а також доступності даних для легітимних користувачів. Необхідність впровадження таких інтегрованих систем захисту викликана стрімким зростанням векторів компрометації даних, що обумовлено загальною нестабільністю економічного середовища, активним застосуванням хмарних обчислень і доступністю засобів несанкціонованого втручання.

Нормативно визначено, що КСЗІ є сукупністю програмно-апаратних засобів та організаційних рішень, які взаємодіють між собою задля безпечного оброблення електронних ресурсів в автоматизованій системі. Для побудови всебічного захисту спочатку здійснюється детальний аналіз каналів витоку відомостей та методів шкідливого впливу на софт, тому генеральне завдання системи – об'єднати наявні інструменти захисту в єдиний контур, що діятиме протягом усього періоду експлуатації обчислювальних засобів [16].

У межах проєктування КСЗІ для ТОВ «ПРАЩУР» розроблювана система має виконувати такі базові технічні завдання:

– регламентація та суворе розмежування прав доступу співробітників до мережевих і локальних файлів компанії;

– надійна фіксація, протоколювання та аудит усіх подій безпеки в операційній системі;

– збереження стабільності функціонування операційного середовища та прикладних програмних продуктів;

– постійний автоматизований пошук та усунення внутрішніх вразливостей конфігурації ОС;

– відбиття цілеспрямованих кібератак та нейтралізація шкідливого вірусного софту;

– криптографічне шифрування трафіку під час передачі інформації відкритими мережами зв'язку;

– забезпечення централізованого адміністрування всіма компонентами захисного контуру.

Практичний процес створення системи безпеки розпочинається з видання розпорядчої документації. Ключовим стартовим кроком є затвердження Наказу про створення КСЗІ, який юридично зобов'язує розгорнути систему захисту на підприємстві, фіксує перелік підстав для виконання робіт та визначає коло відповідальних посадових осіб. Для коректного проєктування архітектури захисту важливим етапом є оцінка ступеня чутливості інформації. З цією метою керівництво видає Наказ про призначення комісії з категоріювання та обстеження об’єктів інформаційної діяльності. Ця група фахівців проводить аудит робочих приміщень, виявляє критичні активи, фіксує результати в акті обстеження та встановлює категорію важливості даних, що циркулюють на АРМ директора.

Основним документом, який формалізує вимоги до безпеки середовища, виступає Акт категоріювання. Його складання відбувається відповідно до положень НД ТЗІ 1.6-005-2013 [17]. Згідно з чинними технічними стандартами, за рівнем важливості інформаційні ресурси диференціюють на чотири категорії. Перша, друга та третя категорії охоплюють відомості «особливої важливості», а також інформацію з грифами «цілком таємно» та «таємно», які містять державну

таємниць і вимагають особливого рівня захисту державних таємниць.

Четверта категорія включає інформаційні ресурси категорії «Для службового користування», конфіденційні дані підприємств, а також відкриті державні ресурси, що не відносяться до державних секретів, але потребують надійного технічного захисту. Оскільки перші три категорії охоплюють інформацію, що становить державну таємницю, для комерційної діяльності ТОВ «ПРАЩУР» та захисту АРМ його керівника базове значення має саме четверта категорія ОІД. Вона хоч і не містить державних секретів, проте вимагає побудови надійної системи технічного захисту конфіденційних даних та комерційної таємниці підприємства [18].

Для чіткого обґрунтування вибору нормативних вимог, диференціації критеріїв безпеки та подальшої оптимізації інженерно-технічних рішень доцільно систематизувати ключові критерії розподілу об'єктів інформаційної діяльності. Комплексний порівняльний аналіз організаційних та технічних вимог до різних категорій об'єктів згідно з чинною методологією НД ТЗІ наведено в таблиці 1.2.

Таблиця 1.2 – Техніко-організаційні вимоги до категорій об'єктів інформаційної діяльності

Категорія ОІД	Специфіка інформаційних ресурсів	Необхідність захисту від витоку ТКЗІ	Рівень гарантій проектованої КСЗІ
1 категорія	Особливої важливості, державна таємниця	Обов'язкова сертифікація засобів та захист від ПЕМВН	Найвищий (Г-3 / Г-4)
2 категорія	Цілком таємно, державна таємниця	Контроль фізичних полів, екранування приміщень	Високий (Г-3)
3 категорія	Таємно, державна таємниця	Спеціальні дослідження засобів ОВТ	Середній (Г-2)
4 категорія	Для службового користування, КТ підприємства	Організаційне розмежування, контроль локальних інтерфейсів	Базовий / Достатній (Г-1)

Зіставлення інженерно-технічних параметрів, структурованих у таблиці 1.2, наочно підтверджує, що для автоматизованого робочого місця директора ТОВ «ПРАЩУР» розгортання комплексу захисних засобів за критеріями саме 4-ї категорії є повністю виправданим та нормативно збалансованим. Оскільки на об'єкті дослідження обробляються ресурси ДСК та конфіденційна комерційна інформація, впровадження вимог перших трьох категорій призвело б до надлишкового навантаження на бюджет проєкту. Зокрема, це дозволяє компанії уникнути високовартісних процедур радіозондування суміжних просторів, екранування стін кабінету металевими сітками чи розгортання генераторів шуму для блокування витоку за рахунок побічних електромагнітних випромінювань та наведень (ПЕМВН). Натомість основний фокус інженерного проєктування переноситься на забезпечення програмно-апаратної стійкості операційної системи, тонке налаштування матриці доступу користувачів, захист від шкідливого ПЗ та впровадження надійних алгоритмів криптографічного шифрування мережевого трафіку [19].

Це дозволяє оптимізувати витрати на розробку системи захисту, зосередивши ресурси на нейтралізації реальних комерційних та репутаційних ризиків, з якими компанія може зіткнутися на ринку ІТ-послуг. Створення КСЗІ за цією категорією дозволить підприємству підготувати належне підґрунтя для подальшої сертифікації та атестації робочого місця керівника без необхідності впровадження надлишкових та високовартісних засобів захисту, що призначені виключно для військових або спеціальних державних об'єктів.

1.4 Постановка задачі

Проведений комплексний аналіз умов функціонування та організаційної структури ТОВ «ПРАЩУР», дослідження специфіки його локальної ІТ-інфраструктури, вивчення нормативно-правових вимог регулювання сфери ТЗІ, а

також детальна диференціація інформаційних потоків і категорій даних дозволяють зробити обґрунтований висновок про високу критичність забезпечення інформаційної безпеки на об'єкті дослідження. Встановлено, що повсякденна діяльність автоматизованого робочого місця (АРМ) керівника підприємства безпосередньо пов'язана з безперервною обробкою конфіденційних масивів, фінансової звітності, кадрових реєстрів та інтелектуальної власності у вигляді програмних кодів і технічних специфікацій продуктів. Для зазначених ресурсів визначальними та критично важливими є вимоги щодо суворого дотримання конфіденційності, гарантування цілісності та забезпечення контрольованого, легітимного доступу. Будь-яке порушення цих базових критеріїв (унаслідок кібератак чи внутрішніх збоїв) може призвести до значних фінансових збитків, комерційних втрат та тривалого блокування бізнес-процесів компанії на ринку IT-послуг [20].

Аналіз архітектури інформаційних потоків засвідчив, що циркуляція даних на АРМ директора є складним процесом, який включає стадії первинної агрегації, аналітичної обробки, генерації консолідованих звітів та координації циклів розробки вебсофту. На кожному з цих етапів існують потенційні технологічні вразливості, пов'язані з ризиками несанкціонованого доступу (НСД), модифікації або витоку відомостей через відкриті канали зв'язку. Сучасні стандарти управління інцидентами безпеки вказують на те, що особливу небезпеку для керівної ланки комерційних структур становлять як цілеспрямовані зовнішні кібератаки, так і внутрішні загрози від користувачів, які мають легітимні права в межах корпоративного периметра. З огляду на це, при проєктуванні системи безпеки для АРМ класу «1» виникає необхідність інтеграції передових концепцій захисту, зокрема елементів моделі нульової довіри (Zero Trust), де кожна операція, спроба доступу до бази контрагентів чи підключення матеріальних носіїв вимагають суворої автентифікації, шифрування та безперервного моніторингу подій безпеки [21-22].

Додатково, впровадження автоматизованих засобів превентивного аналізу

дозволить в режимі реального часу виявляти аномалії в поведінці системних процесів, що критично важливо для своєчасного запобігання складним APT-атакам. Таким чином, розбудова надійної КСЗІ передбачає не лише механічне обмеження прав користувачів, а й створення цілісного екосистемного підходу до захисту, що включає інструменти автоматизованого контролю цілісності кожного окремого сегмента мережі. Нормативно-методологічний аналіз показав, що проектована ІКС повинна функціонувати у строгому правовому полі України, відповідаючи положенням законів про інформацію та захист персональних даних, а також вимогам профільного стандарту НД ТЗІ 1.6-005-2013 для об'єктів четвертої категорії важливості. Водночас наявні типові підходи до організації безпеки в комерційному секторі часто мають узагальнений характер. Вони не враховують індивідуальну архітектуру робочого місця керівника, де одночасно акумулюються права максимального адміністрування та найбільш чутливі комерційні відомості, що потребує розробки спеціалізованих інженерних рішень та ведення суворого паперового й електронного аудиту. У зв'язку з цим, метою цієї роботи є розроблення комплексної системи захисту інформації (КСЗІ) для автоматизованого робочого місця директора ТОВ «ПРАЩУР», яка забезпечує надійний захист комерційної таємниці, службових даних та супутніх цифрових ресурсів від несанкціонованого доступу, шкідливого ПЗ і витоку, а також повністю відповідає вимогам чинного законодавства та нормативних документів системи ТЗІ в Україні.

2 ФОРМУВАННЯ АРХІТЕКТУРИ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ КОМПЛЕКСУ ЗАХИСТУ ДАНИХ

2.1 Методологія створення захищеного середовища обробки корпоративних ресурсів та забезпечення їх цілісності

Створення комплексної системи захисту інформації (КСЗІ) є чітко регламентованим інженерно-управлінським процесом, який реалізується у строгій послідовності етапів відповідно до вимог нормативних документів НД ТЗІ 3.7-003-05 та НД ТЗІ 2.5-005-99.

Першим (передпроєктним) етапом є всебічний аудит об'єкта інформаційної діяльності (ОІД), який передбачає визначення категорії важливості системи, детальне інженерне обстеження компонентів інформаційно-комунікаційної інфраструктури та розроблення технічного завдання (ТЗ) [24].

Другим етапом виступає безпосереднє проєктування, що охоплює формування цільового функціонального профілю безпеки, моделювання кіберризиків та обґрунтований вибір конкретних програмно-апаратних засобів захисту.

Третім етапом є практичне впровадження, розгортання та підготовка до державної атестації, що включає інсталяцію софту, налаштування політики доступу та проведення приймальних випробувань для підтвердження відповідності системи вимогам ТЗ.

Ключовою особливістю проєктування КСЗІ для ТОВ «ПРАЩУР» є необхідність врахування специфіки бізнес-процесів приватного підприємства, що спеціалізується на розробці програмно-апаратних комплексів. З одного боку, архітектура безпеки має суворо відповідати технічним стандартам ТЗІ щодо захисту інформації з обмеженим доступом четвертої категорії, з іншого – забезпечувати гнучкість та безперервність операційної діяльності керівника компанії при взаємодії з клієнтами та розробниками. Це означає, що при виборі засобів захисту недостатньо реалізувати стандартний базовий набір обмежень.

Необхідно додатково впровадити специфічні інструменти, які гарантують ізоляцію критичних цифрових активів (програмних кодів, схем Hardware-модулів) та унеможливлюють їх приховане копіювання чи викривлення [25].

Фундаментальною основою забезпечення цілісності комерційних та фінансових масивів даних у процесі їх збереження та обробки в межах автоматизованої системи є технологія криптографічного хешування. На відміну від типових офісних платформ, де контроль цілісності відіграє другорядну роль, у контурі безпеки АРМ директора ТОВ «ПРАЩУР» застосування стійких алгоритмів (наприклад, SHA-256) виступає базовим інструментом підтвердження автентичності інформації.

Кожен критичний корпоративний файл, база даних контрагентів чи фінансова відомість при реєстрації в системі отримують унікальний математичний "цифровий відбиток" [26]. Процедура оперування даними передбачає обов'язкову автоматизовану верифікацію контрольних сум перед початком та після завершення будь-яких сесій обробки файлів. Це дозволяє математично довести відсутність навіть мінімальних (побітових) санкціонованих чи деструктивних змін у структурі даних. Таким чином, проєктоване середовище АРМ розглядається як цілісний доказовий контур, де будь-яка спроба несанкціонованого втручання, модифікації або випадкового спотворення даних внутрішніми чи зовнішніми порушниками буде негайно зафіксована системою аудиту через розбіжність значень хеш-функцій [27].

Особливістю архітектури обробки даних на робочому місці керівника є чітке логічне та фізичне розділення інформаційних масивів. Для мінімізації ризиків компрометації інтелектуальної власності, технічна документація та вихідні коди програмного забезпечення зберігаються в ізольованих зашифрованих контейнерах. Використання спеціалізованих засобів захисту від несанкціонованого доступу (НСД) дозволяє створити захищене віртуальне середовище, яке повністю контролює життєвий цикл інформації. Такий підхід гарантує, що операційні процеси (наприклад, перегляд поточної звітності чи

підписання контрактів) відбуваються без ризику пошкодження або витоку суміжних критичних масивів даних. Це забезпечує прозорість внутрішнього моніторингу та повну аудиторію дій користувачів, що є невід'ємною умовою стабільного функціонування ІТ-компанії [28].

Процес захисту інформаційних ресурсів у межах ТОВ «ПРАЩУР» має дворівневу структуру:

– фізичний рівень захисту стосується безпосереднє розміщення обчислювальної техніки та матеріальних носіїв інформації. Комп'ютерне обладнання директора розташоване в кабінеті з контрольованим режимом доступу, що унеможливлює перебування сторонніх осіб без нагляду та захищає технічні засоби від механічних пошкоджень чи прямого викрадення;

– логічний рівень захисту охоплює роботу з електронними масивами на базі захищеного АРМ. На цьому рівні безпека забезпечується програмно-апаратними інструментами: надійним шифруванням дисків, суворим розмежуванням прав доступу на основі рольової моделі (RBAC) та безперервним веденням журналів подій безпеки (Syslog).

Стартовий етап розгортання комплексної системи захисту інформації в межах ТОВ «ПРАЩУР» базується на формуванні пакета організаційно-розпорядчих актів, які визначають правове поле для подальших технічних робіт. До цього первинного переліку належать наказ про початок створення системи захисту (додаток Б), а також наказ про призначення посадової особи, відповідальної за безпеку інформації на підприємстві. Якщо на об'єкті такий контур розгортається вперше, видається окреме розпорядження про створення служби захисту інформації, де фіксується її персональний склад (додаток В).

Адміністративні та функціональні межі діяльності цих суб'єктів чітко регламентуються Положенням про відповідальну особу та Положенням про службу захисту інформації, які деталізують обов'язки, права та процедури внутрішнього контролю. Паралельно розробляється Перелік відомостей, що підлягають обробленню в автоматизованій системі та вимагають технічного

захисту з боку підприємства. Наявність цих документів дозволяє юридично розпочати розробку інженерного проєкту, оскільки вони легалізують внутрішні процедури та встановлюють конкретні нормативні акти ДСТУ та НД ТЗІ, якими керуватиметься суб'єкт господарювання.

Для побудови коректної ієрархічної структури безпеки першочергово здійснюється чіткий розподіл адміністративних ролей між учасниками процесу. Володільцем автоматизованої системи та захищуваних інформаційних ресурсів за законом виступає безпосереднє директор ТОВ «ПРАЩУР». На нього покладається повна персональна юридична відповідальність за функціонування КСЗІ, легітимність обробки даних та своєчасність надання верифікованих відомостей органам державної експертизи.

Ослільки керівник здійснює загальне стратегічне управління, безпосереднє оперативне ведення технічних процесів захисту делегується призначеній відповідальній особі - начальнику ІТ-відділу або провідному інженеру з кібербезпеки. Ця особа здійснює безпосередній нагляд за діяльністю СЗІ, приймає регулярні звіти про стан захищеності об'єкта та координує процеси ліквідації наслідків можливих апаратних чи програмних збоїв [29].

Штатний склад СЗІ формується з адміністратора безпеки та системного адміністратора, причому для автономних АРМ класу «1» ці функції за рішенням керівництва може суміщати один фахівець. Співробітники служби безпосередньо реалізують затверджену корпоративну політику безпеки. До базового функціоналу СЗІ віднесено:

– безперервний аналіз кіберризиків та моніторинг локального трафіку;

– своєчасне виявлення спроб несанкціонованого доступу та розробку планів протидії комп'ютерним загрозам;

– регулярний інструктаж користувачів АРМ щодо правил безпечної експлуатації софту;

– нейтралізацію шкідливого програмного забезпечення;

– аудит системних журналів подій безпеки (Syslog);

– фіксацію внутрішніх інцидентів з метою відображення та запобігання компрометації даних з боку внутрішніх порушників.

Розробка КСЗІ має індивідуальний характер, оскільки не всі наявні на підприємстві конфіденційні масиви обробляються на конкретному робочому місці. Наприклад, технічна документація на Hardware-модулі не повинна зберігатися на комп'ютерах кадрового підрозділу, тому контур безпеки проєктується виключно під функціональні задачі конкретної АС. Затверджений директором перелік інформації накладає суворі технологічні обмеження: будь-яка обробка сторонніх файлів чи накопичення нерегламентованих персональних даних на АРМ суворо забороняється, що мінімізує зону потенційного ризику.

Після затвердження інформаційних меж наказом керівника призначається спеціальна комісія з категоріювання та обстеження об'єкта інформаційної діяльності (додаток Г), до складу якої залучаються виключно ті штатні працівники, які не є безпосередніми користувачами цього АРМ. На цій стадії комісія розробляє Акт категоріювання (додаток Д), який для ТОВ «ПРАЩУР» закріпив за об'єктом четверту категорію важливості, оскільки державна таємниця в системі не циркулює, а захисту підлягають ресурси ДСК та комерційна таємниця. Також формується Акт обстеження середовища ОІД (додаток Е) та заводиться технічний Формуляр системи [30-31].

Вся розпорядча документація та внутрішні положення ТОВ «ПРАЩУР» проходять багаторівневу процедуру внутрішнього погодження, що включає перевірку юридичним департаментом на відповідність трудовому та цивільному праву, а також верифікацію канцелярією. Тексти наказів, які стосуються обробки відомостей ДСК, у разі виконання державних замовлень можуть додатково узгоджуватися з профільними міністерствами та відомствами. Інформаційні переліки даних, що підлягають технічному захисту, за винятком конфіденційних комерційних параметрів, можуть частково оприлюднюватися на офіційному вебпорталі підприємства для ознайомлення контрагентів.

Детальний аудит та інженерне обстеження середовища ОІД є обов'язковою

передумовою для проєктування фізичного контуру безпеки і включає збір технічних характеристик за трьома основними напрямками:

– характеристика інфраструктури об'єкта – комісія фіксує поверх розташування кабінету керівника, суміжні приміщення (аудиторії, коридори, шахти ліфтів), наявність спільних стін із неконтрольованими зонами та загальний режим доступу сторонніх осіб до крила будівлі;

– архітектурні параметри приміщення – оцінюється товщина та матеріал капітальних стін і міжкімнатних перегородок (цегла, залізобетон, гіпсокартон), тип покриття підлоги, кількість та розміри віконних прорізів, конструкція стелі та клас стійкості вхідних дверей до зламу;

– інженерно-технічні системи безпеки – детально описується топологія пожежної та охоронної сигналізацій, розташування датчиків руху, траси проходження труб центрального опалення та вентиляційних отворів, зони покриття камер відеоспостереження, а також параметри системи електроживлення, включаючи точну схему розміщення розеток, вимикачів, світильників та контуру захисного заземлення.

Всі зібрані відомості про склад основного й допоміжного обчислювального обладнання, специфікацію інстальованого системного й прикладного ПЗ, а також матрицю доступу користувачів та їхні посадові повноваження заносяться до Акта обстеження, до якого додаються детальні ситуаційний та генеральний плани території підприємства представлені на рисунку 2.1. Графічні матеріали, представлені на рисунку 2.1, наочно демонструють межі контрольованої зони (КЗ) об'єкта інформаційної діяльності та дозволяють оцінити просторове розташування автоматизованого робочого місця відносно зовнішніх меж будівлі й бульвару Героїв АТО. Паралельно з цим ведеться заповнення технічного Формуляра, який є основним звітним документом на всіх етапах життєвого циклу КСЗІ. Цей документ містить детальні таблиці із зазначенням серійних та заводських номерів материнських плат, модулів оперативної пам'яті, центральних процесорів, жорстких дисків та знімних носіїв інформації.

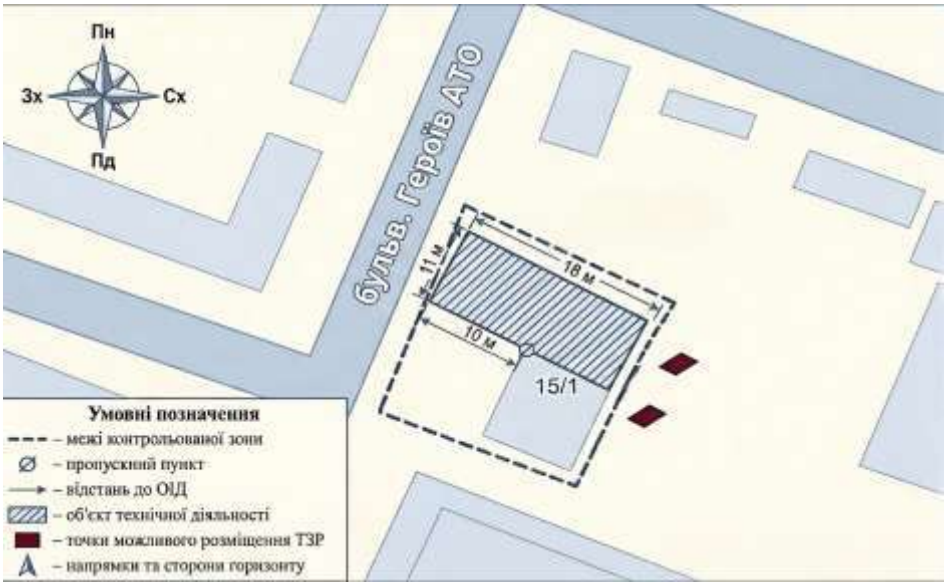


Рисунок 2.1 – Ситуаційний план об’єкта інформаційної діяльності

У формулярі окремо фіксуються назви всіх засобів захисту від НСД та антивірусних програм, номери їхніх діючих експертних висновків ДССЗЗІ України, терміни дії сертифікатів та реквізити компаній-розробників софту. Після завершення приймальних випробувань формуляр разом із результатами тестів передається до Служби спеціального зв’язку та захисту інформації України для проходження державної експертизи та отримання Атестата відповідності на АРМ [32].

Кінцевим результатом аналізу всієї сукупності зібраних даних є План захисту інформації ТОВ «ПРАЩУР». Цей стратегічний документ чітко визначає межі та цілі захисного контуру, містить актуальну модель кіберризиків та деталізує технічні процедури шифрування, резервного копіювання, автентифікації користувачів та мережевого екранування. План захисту додатково регламентує організаційні заходи (графіки навчання персоналу, розподіл адміністративних обов’язків, аудит подій безпеки) та містить алгоритми швидкого реагування на кіберінциденти з метою оперативного відновлення працездатності АРМ керівника. Окремо служба безпеки впроваджує та веде паперовий Журнал обліку та реєстрації матеріальних носіїв інформації, який унеможливлює неконтрольоване використання USB-накопичувачів на об’єкті та

фіксує час і мету підключення кожної «флешки» конкретною посадовою особою. Сформований таким чином організаційно-нормативний базис дозволяє перейти до безпосереднього аналізу моделей потенційних загроз та обґрунтування функціонального профілю безпеки.

2.2 Аналіз потенційних деструктивних впливів та обґрунтування вимог до безпеки

Результати комплексного обстеження середовища функціонування дозволили чітко визначити межі контрольованої зони (КЗ) та архітектурні особливості об’єкта інформаційної діяльності (ОІД) ТОВ «ПРАЩУР». Наступним обов’язковим етапом проєктування комплексної системи захисту інформації (КСЗІ) є аналіз потенційних деструктивних впливів та розробка нормативно-технічної документації, яка регламентує вимоги до безпеки. Відповідно до вимог нормативних документів системи технічного захисту інформації (НД ТЗІ 1.6-005-13 та НД ТЗІ 3.6-004-21), базовими документами на цьому етапі є «Модель порушника» та «Модель загроз» [33].

Аналіз безпеки інформації передбачає класифікацію загроз за їхнім походженням на дві основні категорії:

Випадкові (ненавмисні) загрози – деструктивні впливи, що реалізуються без чітко визначеної мети та злого наміру. Зазвичай вони є наслідком помилок або необережних дій персоналу ТОВ «ПРАЩУР» чи адміністраторів, апаратних збоїв обчислювальної техніки, відмов систем життєзабезпечення (енерго-, водо- або теплопостачання) або стихійних явищ. Наслідками таких подій є повна або часткова відмова автоматизованої системи (АС), збої в обробці даних або порушення штатного режиму функціонування компонентів.

Навмисні загрози – цілеспрямовані дії порушника, спрямовані на несанкціонований доступ до конфіденційних даних (комерційної таємниці,

фінансової звітності, баз даних 1С/BAS), модифікацію або знищення інформаційних масивів, а також на дезорганізацію роботи АС чи виведення з ладу її компонентів.

Основними джерелами загроз безпеці інформації виступають суб'єкти (внутрішні та зовнішні порушники), технічні засоби, а також середовище функціонування об'єкта. Залежно від просторового розташування джерела та наявності прав доступу, загрози поділяють на зовнішні (що реалізуються з-за меж КЗ) та внутрішні (джерелом яких є працівники компанії).

У контексті архітектурного планування приміщень особливу увагу приділено наявності віконних прорізів. Неправильне просторове розташування обладнання відносно вікон створює загрозу витоку інформації за рахунок візуального спостереження або дистанційного перехоплення побічних електромагнітних випромінювань та наведень (ПЕМВН). Під час моделювання природних чи техногенних загроз враховуються фізично можливі чинники. Зокрема, оскільки обладнання ТОВ «ПРАЩУР» розташоване на другому поверсі капітальної будівлі, загроза затоплення внаслідок повені оцінюється як неактуальна, тоді як загрози локальних аварій комунікаційних мереж залишаються в полі аналізу.

Реалізація загроз призводить до порушення базових властивостей інформації:

– конфіденційність порушується у разі несанкціонованого ознайомлення (читання, копіювання) з інформацією суб'єктами, які не мають на це законних повноважень;

– цілісність вважається порушеною, якщо відбулася несанкціонована модифікація структури файлів, заміна, викривлення чи повне знищення корпоративних даних;

– доступність порушується, якщо створюються умови, за яких авторизовані користувачі не можуть отримати своєчасний доступ до сервісів АС або необхідних комерційних документів;

– спостережність є властивістю системи, що дозволяє фіксувати та однозначно відстежувати всі події, пов’язані з безпекою. Порушення спостережності (наприклад, модифікація або очищення журналів аудиту) унеможливлює розслідування інцидентів.

Для кількісної та якісної оцінки деструктивних чинників використано метод матриці ризиків. Кожній ідентифікованій загрозі присвоюється показник ймовірності її реалізації (*P*, від 1 до 5) та показник можливого впливу на систему (*C*, від 1 до 5). Загальний рівень ризику обчислюється за формулою:

$$R = P \times C. \tag{2.1}$$

Класифікація здійснюється за чіткими критеріями: значення $R \geq 15$ відповідає критичному рівню ризику, $10 \leq R < 15$ – високому, а $5 \leq R < 10$ – середньому рівню [34]. Узагальнену модель актуальних загроз безпеці інформації для проектованого об’єкта наведено в таблиці 2.1.

Таблиця 2.1 – Модель актуальних загроз безпеці інформації

№	Види загрози	Рівень ризику	К	Ц	Д	С
1	2	3	4	5	6	7
1	Природні та техногенні загрози					
1.1	Виникнення пожежі, аварії опалювальної або водопровідної системи в будівлі	Середній		×	×	×
2	Зовнішні навмисні загрози					
2.1	Несанкціонований доступ сторонніх осіб до приміщення КЗ та технічних засобів	Високий	×	×	×	
2.2	Візуальне перехоплення інформації з екранів моніторів або залишених паперових носіїв	Низький	×			

Кінець таблиці 2.1

1	2	3	4	5	6	7
2.3	Викрадення змінних носіїв інформації або окремих апаратних компонентів АС	Високий	×	×		×
3	Загрози, пов'язані з порушенням режимів роботи					
3.1	Зараження операційного середовища шкідливим програмним забезпеченням (ШПЗ)	Середній		×	×	×
3.2	Втрата, компрометація або розголошення автентифікаційних даних (паролів)	Високий	×	×	×	×
3.3	Несанкціоноване внесення змін у конфігурацію ПЗ, ОС або бази даних	Середній		×		×
3.4	Використання несанкціонованого ПЗ або неконтрольована модифікація компонентів	Низький		×		×
3.5	Фізичне або логічне пошкодження внутрішніх чи зовнішніх носіїв інформації	Середній			×	
3.6	Спроби подолання логічних засобів захисту та вхід у систему під чужим обліковим записом	Середній	×	×	×	
4	Помилки та недбалість персоналу					
4.1	Помилки адміністрування (неправильне налаштування СКУД, Active Directory, засобів захисту)	Середній	×	×	×	
4.2	Порушення користувачами технологічного процесу введення, обробки та виведення даних	Середній	×	×	×	
4.3	Недбале зберігання, облік та утилізація паперових і магнітних носіїв інформації	Низький	×	×	×	
4.4	Навмисне або випадкове розголошення конфіденційних даних стороннім особам	Середній	×			

Оскільки спроєктована система за своїм архітектурним виконанням є повністю ізольованою автоматизованою системою класу «1» (АС-1), з моделі

загроз виключено як неактуальні такі чинники: несанкціоноване підключення до глобальних мереж, перехоплення мережевого трафіку на зовнішніх каналах зв'язку, атаки типу «відмова в обслуговуванні» (DDoS) та будь-які інші загрози, що реалізуються через інтернет [35].

Проте ізольованість системи породжує специфічну загрозу — зараження автоматизованих робочих місць шкідливим програмним забезпеченням зі змінних носіїв (наприклад, флеш-накопичувачів), які використовуються для обміну документацією. Цей вектор атаки потребує суворого інструментального контролю під час підключення будь-яких зовнішніх пристроїв.

Генеральний план приміщення ТОВ «ПРАЩУР» деталізує внутрішню структуру об'єкта. На ньому відображено планування кабінетів, розташування робочих місць, серверних зон, допоміжних технічних засобів та шляхи переміщення персоналу. Просторове розташування приміщень, робочих зон та інженерно-технічних засобів безпеки наведено на плані розміщення технічних засобів (рисунок 2.2).

Контрольованою зоною для ТОВ «ПРАЩУР» визначено виділене ізольоване приміщення (Кабінет № 7), доступ до якого суворо обмежений політиками безпеки й контролюється фізичними та технічними засобами. Фізичний захист забезпечується багаторівневою системою доступу, що включає пункти пропуску на входах до корпусу, ідентифікацію співробітників за перепустками та обмеження доступу сторонніх осіб (рисунок 2.3).

Паралельно з аналізом загроз розробляється «Модель порушника», яка формалізує потенційного зловмисника за його кваліфікацією, мотивацією та рівнем доступу до системи.

Порушники поділяються на зовнішніх (не мають легітимного доступу до КЗ) та внутрішніх (персонал, керівництво, які мають право перебувати в межах об'єкта). Мотиви дій порушників диференціюються від звичайної безвідповідальності або цікавості (людський фактор) до корисливого інтересу з метою компрометації корпоративних даних.

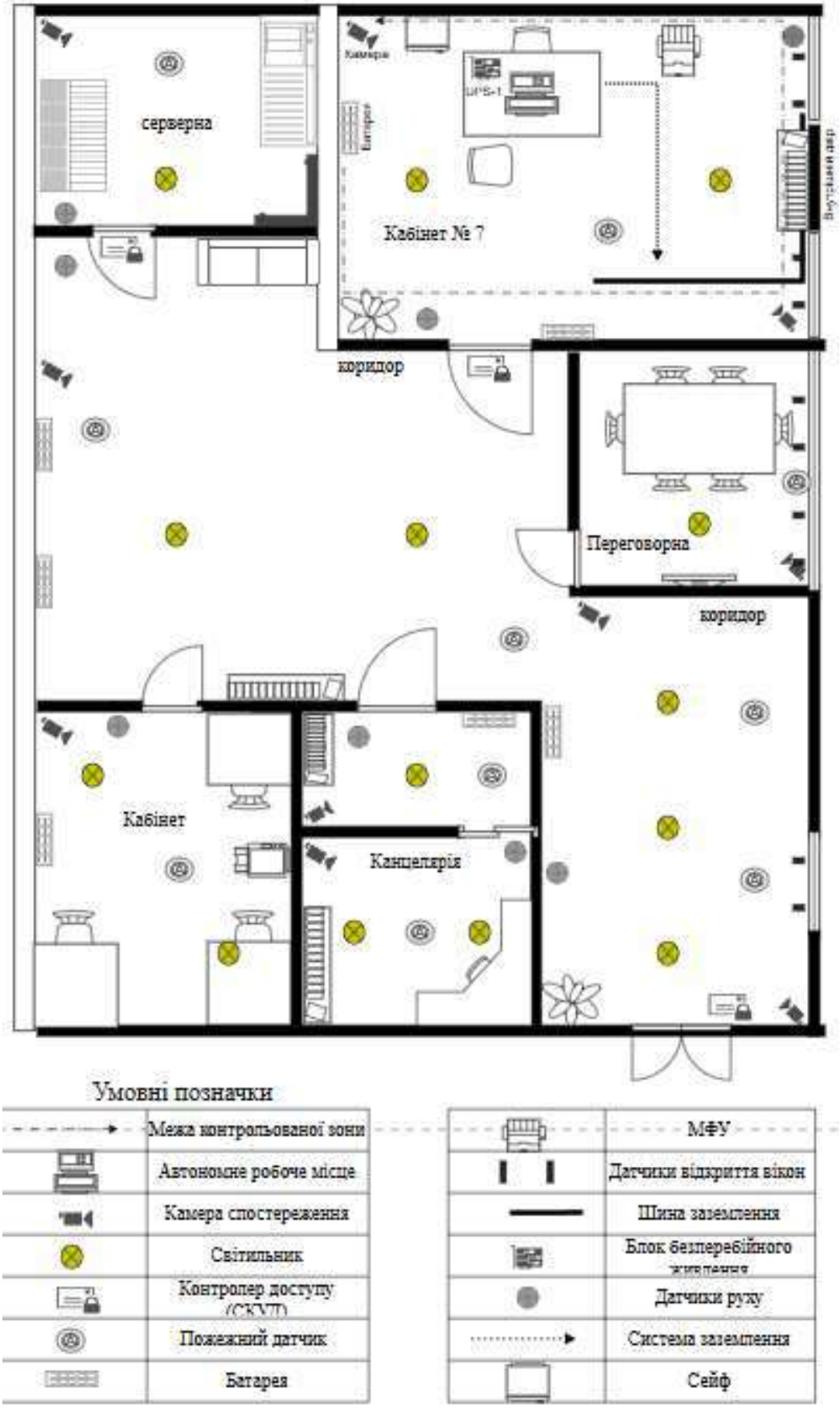


Рисунок 2.2 – План розміщення технічних засобів

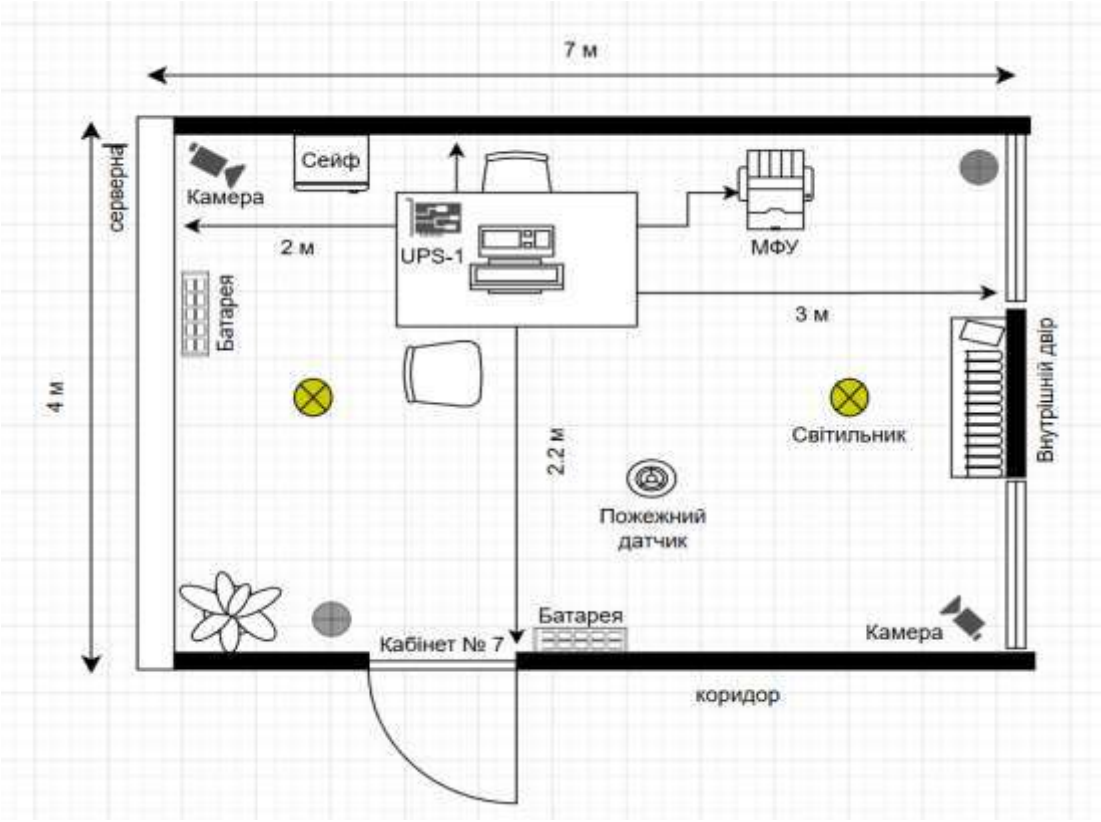


Рисунок 2.3 – План розміщення технічних засобів

За рівнем знань порушники поділяються на категорії: від мінімального рівня користувача до експертного фахівця, який досконало знає архітектуру та вразливості системи.

На основі розроблених моделей загроз та порушника формується правовий та організаційно-технічний фундамент КСЗІ – Технічне завдання (ТЗ) (додаток Ж). Документ визначає найменування системи, умови функціонування, вимоги до надійності, безпеки, а також часові рамки реалізації проєкту [36]. Основним інструментом формалізації технічних вимог до комплексу засобів захисту (КЗЗ) є функціональний профіль захищеності. Відповідно до НД ТЗІ 2.5-004-99, функціональні вимоги розподіляються за критеріями, де цифровий індекс вказує на рівень реалізації захисної функції. Для системи визначено обґрунтований функціональний профіль захищеності, наведений у таблиці 2.2.

Таблиця 2.2 – Критерії захищеності профілю безпеки та способи їх реалізації

Критерій захищеності	Опис технічних вимог згідно з НД ТЗІ 2.5-004-99	Конкретний спосіб реалізації в архітектурі системи
1	2	3
КД-2	Базова довірча конфіденційність. Забезпечення дискреційного принципу розмежування доступу користувачів до файлових об'єктів.	Налаштування списків доступу (ACL) файлової системи NTFS, впровадження рольових політик Active Directory.
КО-1	Повторне використання захищених об’єктів. Очищення областей оперативної пам'яті та дискового простору перед повторним виділенням.	Активація вбудованих локальних політик безпеки ОС Windows (очищення файлу підказки, заборона залишкових даних).
ЦД-1	Мінімальна довірча цілісність. Логічний контроль цілісності програмного забезпечення та даних від випадкових чи навмисних змін.	Налаштування прав доступу на модифікацію системних каталогів засобами Active Directory та NTFS.
ДВ-1	Ручне відновлення системи. Забезпечення можливості адміністративного відновлення працездатності АС після збоїв.	Організація процедур регулярного резервного копіювання (Backup) конфігурацій та баз даних на ізольовані сховища.
НР-2	Захищений журнал реєстрації подій. Виключення можливості несанкціонованого видалення або модифікації логів аудиту.	Налаштування прав доступу до вбудованого журналу Windows Event Logs, обмеження прав доступу користувачів до служб аудиту.

Кінець таблиці 2.2

1	2	3
НИ-2	Одиночна ідентифікація та автентифікація. Обов'язкова перевірка автентичності користувача за унікальним ідентифікатором та паролем.	Реалізація підсистеми облікових записів Windows, встановлення суворих вимог до парольної політики.
НК-1	Односпрямований достовірний канал. Надійний захист даних ідентифікації під час їхнього передавання в межах АС від перехоплення.	Застосування вбудованих захищених протоколів автентифікації ОС Windows (Kerberos v5 / NTLMv2).
НО-1	Виділення адміністратора безпеки. Організаційне та логічне відокремлення функцій керування системою захисту від звичайних користувачів.	Створення окремого облікового запису адміністратора безпеки з повними правами управління політиками без права повсякденної обробки даних.
НЦ-2	Комплекс засобів захисту з контролером цілісності. Автоматичний інструментальний контроль цілісності критичних компонентів КЗЗ.	Впровадження підсистеми контролю цілісності Windows (SFC, DISM) та інтегрованих засобів антивірусного захисту з функцією самозахисту.

Окремим критично важливим аспектом функціонування системи є забезпечення невідмовності та контролю цілісності під час роботи з критичними даними ТОВ «ПРАЩУР». У межах розробленого безпекового середовища підсистема аудиту фіксує всі дії з інформаційними ресурсами. Система в автоматичному режимі забезпечує безумовну фіксацію трьох ключових параметрів для кожної операції підвищеної важливості:

– ідентифікацію особи (працівника), яка отримала доступ до захищених файлів чи баз даних.

– точну часову мітку кожної дії, синхронізовану із сервером точного часу.

– деталізований перелік проведених маніпуляцій (читання, модифікація, копіювання тощо).

Такий рівень деталізації аудиту дозволяє відстежити повну історію роботи з корпоративними документами. Це є дієвим інструментом внутрішньої безпеки: будь-яка спроба несанкціонованого доступу до комерційної таємниці буде негайно зафіксована, що дозволяє чітко локалізувати інцидент та встановити винних осіб.

Комплексна реалізація зазначених організаційних заходів разом із правовими нормами та програмно-апаратними механізмами гарантує побудову надійної та легітимної КСЗІ, яка повністю нівелює актуальні загрози та відповідає чинному законодавству України у сфері технічного захисту інформації.

2.3 Конфігурування параметрів безпеки операційного середовища Windows

Реалізація технічних заходів кіберзахисту передбачає конфігурування параметрів операційного середовища. Для цього можуть застосовуватися як спеціалізовані захисні комплекси (наприклад, «ЛОЗА™-1», «Гриф» версії 3, «Рубіж»), так і вбудовані інструменти та служби операційної системи MS Windows 10.

Комплекс засобів захисту (КЗЗ) утворює сукупність апаратно-програмних елементів, серед яких ключову роль відіграють захищені механізми Windows та підсистема антивірусного контролю. Далі розглянемо детальний алгоритм налаштування захисту робочої станції засобами ОС.

Щоб розпочати конфігурування, необхідно перейти до панелі «Безпека у

Windows». Стандартний шлях через графічний інтерфейс виглядає наступним чином: Параметри – Оновлення та захист – Безпека у Windows, або за допомогою системного рядка пошуку. Після виконання цієї дії перед користувачем з'явиться вікно, візуалізоване на рисунку 2.4.

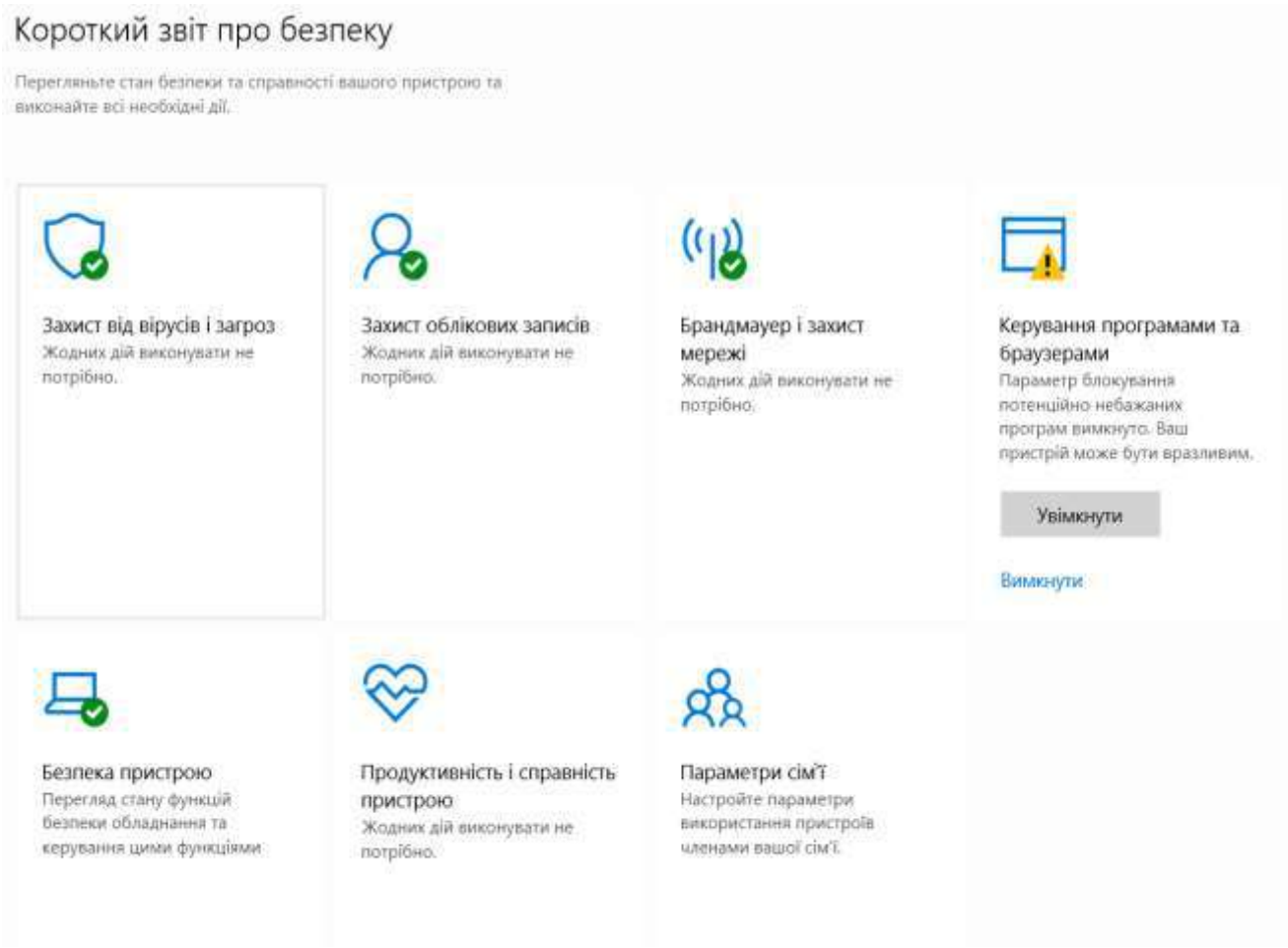


Рисунок 2.4 – Загальний вигляд панелі керування безпекою середовища Windows

У цьому модулі передбачено тестування та керування такими блоками:

– захист від вірусних загроз: запуск швидкого чи повного сканування, налаштування параметрів безпеки в режимі реального часу, перевірка оновлень тощо;

– безпека облікових записів: вибір та модифікація способу верифікації при вході в систему (використання парольних фраз, апаратних ключів тощо);

– активація брандмауера (файрвола) для ефективного запобігання

несанкціонованому віддаленому доступу;

– керування програмами та браузером: фільтрація потенційно небезпечного чи шкідливого програмного забезпечення та блокування підозрілих веб-ресурсів;

– моніторинг стану апаратної частини: перевірка працездатності батареї, накопичувачів та встановленого софту.

Редагування групових політик відбувається згідно з чинними нормативними рекомендаціями для наступних категорій безпекових параметрів ОС:

– політики облікових записів;

– параметри локальних політик;

– конфігурація журналу подій;

– керування системними службами;

– редагування реєстру;

– права доступу до файлової системи;

– адміністративні шаблони;

– політики обмеження запуску програмного забезпечення.

Зміна параметрів безпеки здійснюється через системні редактори об'єктів групових політик, зокрема:

– «Локальна політика безпеки» (Local Security Policy) – для редагування політик локальної машини;

– редактор групової політики – для внесення змін у централізовану базу домену Active Directory.

Швидкий виклик оснастки через комбінацію Пуск – Пошук – Local Security Policy відкриває доступ до глибоких налаштувань платформи (рисунок 2.5).

Локальні політики надають адміністраторам інструментарій для гнучкого керування конфігураціями захисту, правами доступу та мережевими параметрами робочих станцій. Це дозволяє встановлювати обмеження на запуск певних утиліт, задавати складність паролів та вести детальний облік системних подій.

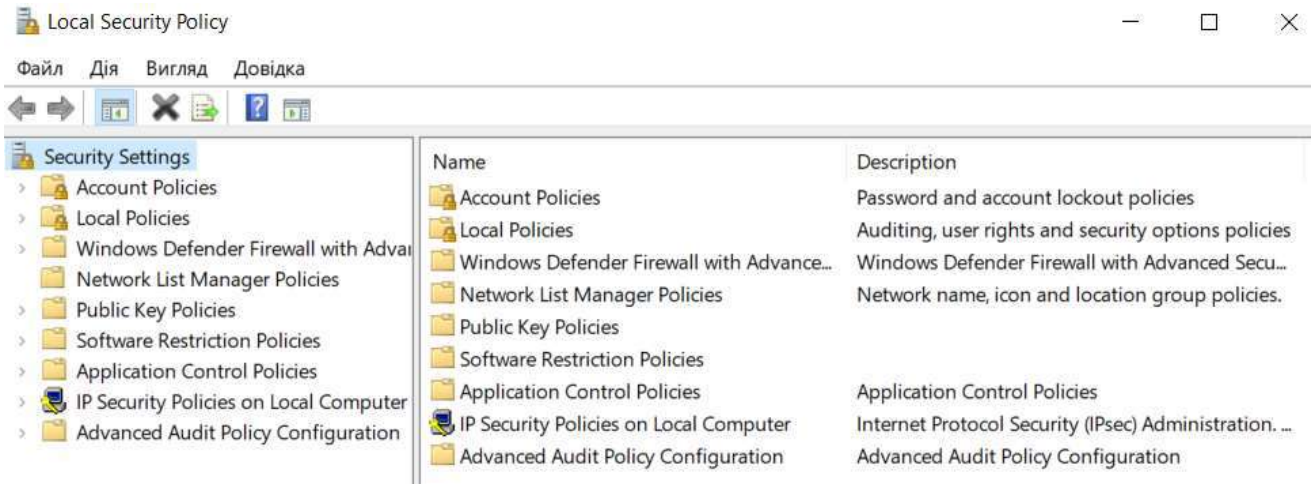


Рисунок 2.5 – Налаштування безпеки

Інтерфейс керування локальними політиками безпеки наведено на (рисунок 2.6). Цей інструмент є базовим для адміністраторів з метою ізоляції та захисту корпоративних ресурсів.

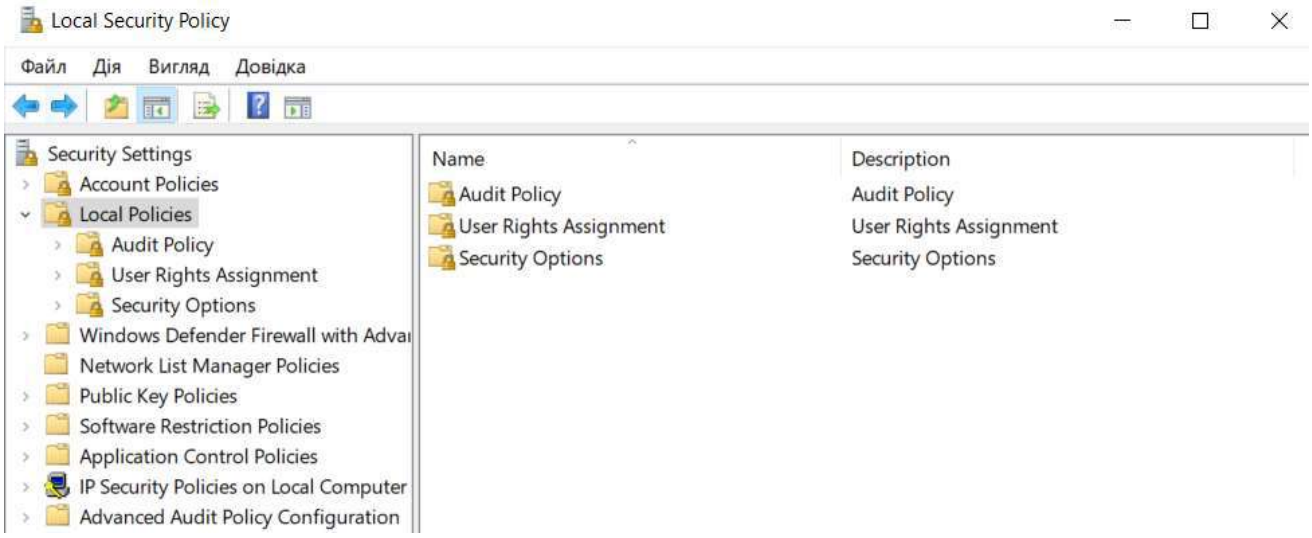


Рисунок 2.6 – Локальні політики безпеки

Аналізуючи зображення на рисунку 2.7, можна помітити, що за замовчуванням підсистема аудиту є деактивованою (навпроти кожної позиції фіксується статус No auditing). Для побудови повноцінного контуру безпеки необхідно налаштувати реєстрацію таких подій:

– аудит спроб входу до облікового запису;

– фіксація керувальних дій у системі;

– аудит звернень до системних каталогів;

– реєстрація успішних/невдалих входів у систему;

– аудит доступу до захищених файлових об'єктів.

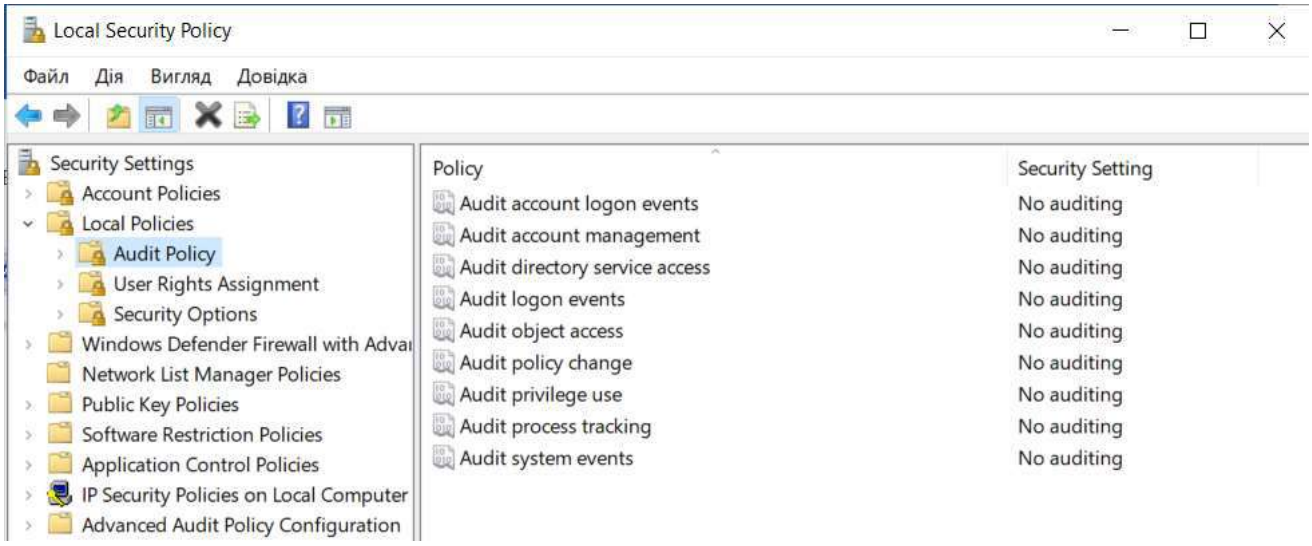


Рисунок 2.7 – Політики аудиту системи

На рисунку 2.8 продемонстровано стан системи після успішної активації політики аудиту подій входу до облікового запису.

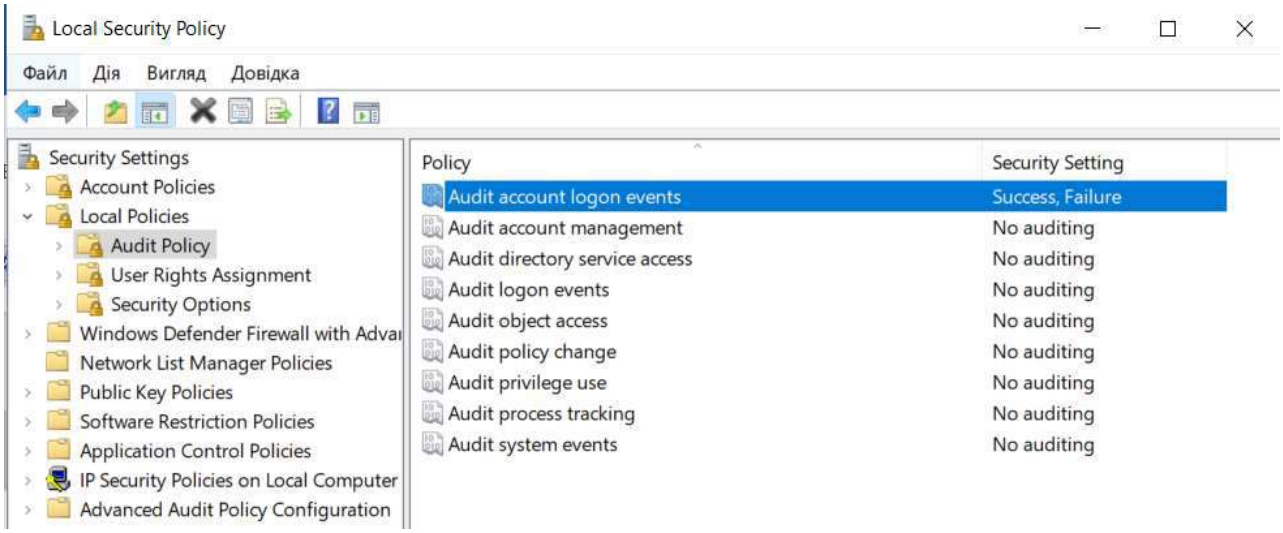


Рисунок 2.8 – Приклад активованої політики безпеки

Візуальне відображення призначених прав користувачів та екрани конфігурації парольних політик проілюстровано на рисунках 2.9 та 2.10 відповідно.

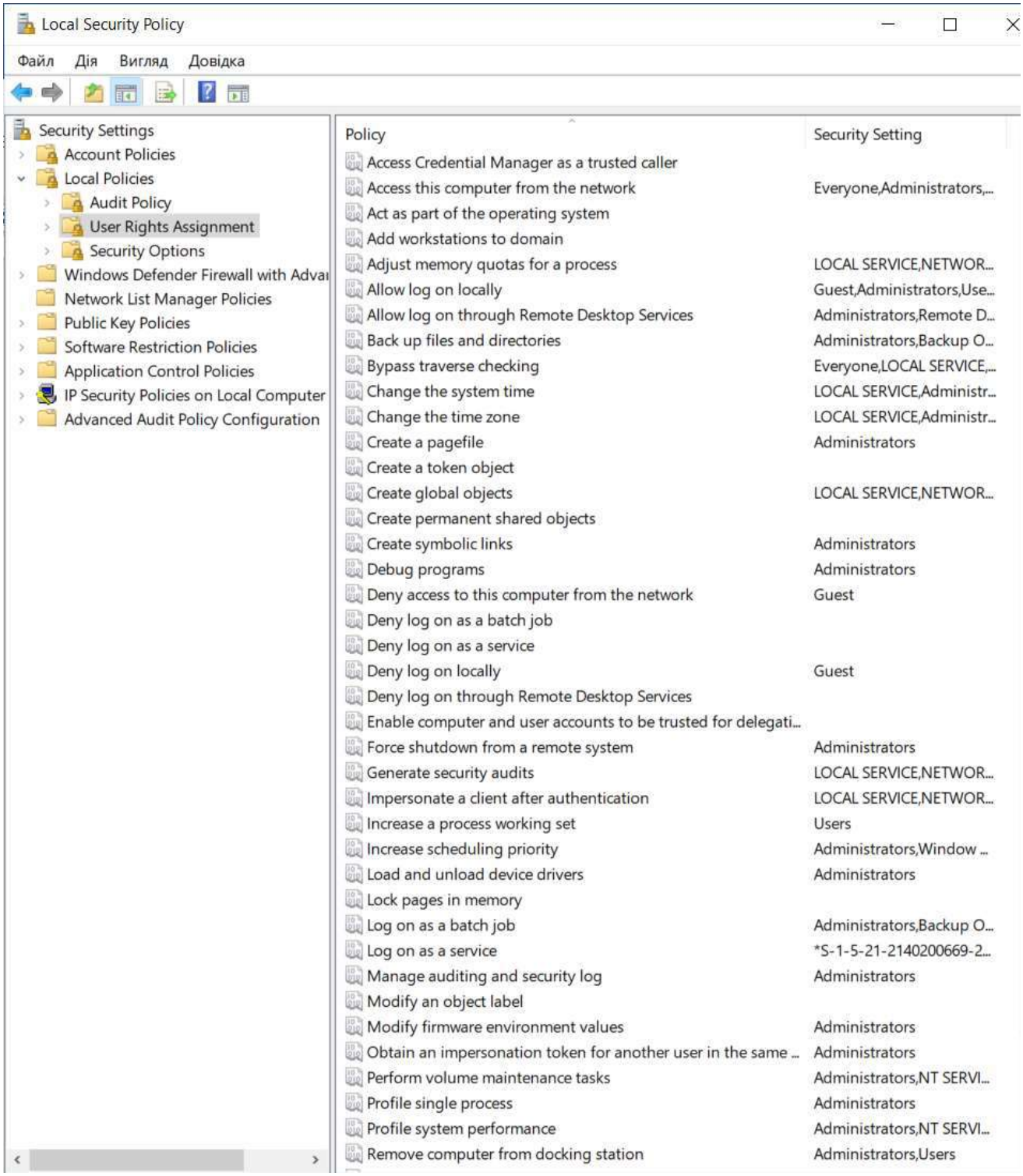


Рисунок 2.9 – Доступи користувачів системи

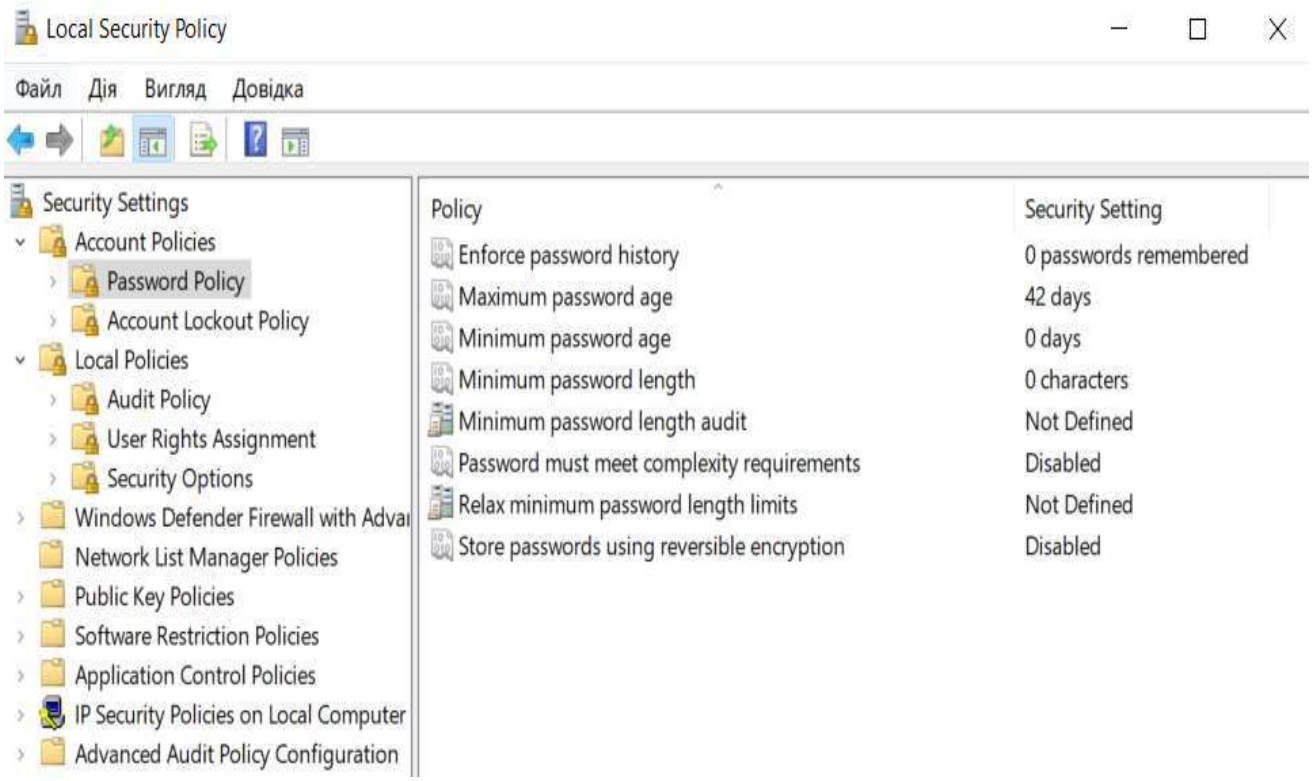


Рисунок 2.10 – Налаштування паролів системи

Загалом за допомогою цього інструментарію вирішується широкий спектр завдань:

– визначення критеріїв стійкості паролів;

– встановлення ліміту невдалих спроб введення пароля для блокування облікового запису;

– налаштування журналювання безпекових подій;

– обмеження запуску нерегламентованого софту;

– встановлення захисних атрибутів для папок і файлів;

– керування процесом встановлення оновлень.

Застосування таких політик можливе як на окремому комп'ютері, так і в межах доменної структури під керуванням контролера. Це дозволяє реалізовувати різнорівневі стратегії безпеки, спираючись на актуальні потреби організації та специфіку обробки інформації.

Окрім налаштування базових локальних політик безпеки, критично важливим ешелоном захисту робочої станції ізольованого типу є блокування

каналів витоку інформації через неконтрольовані змінні носії інформації. Засобами редактора групових політик за шляхом: Конфігурація комп'ютера - Адміністративні шаблони – Система – Доступ до знімних запам'ятовувальних пристроїв реалізується комплексна заборона. Активація параметра «Знімні диски: заборонити читання» (Removable Disks: Deny read access) [37] та запис унеможливлюють підключення будь-яких нерегламентованих USB-накопичувачів (флешок, зовнішніх жорстких дисків), що повністю нівелює вектор атаки, пов'язаний із зараженням робочої станції шкідливим ПЗ через флеш-носії (рисунок 2.11).

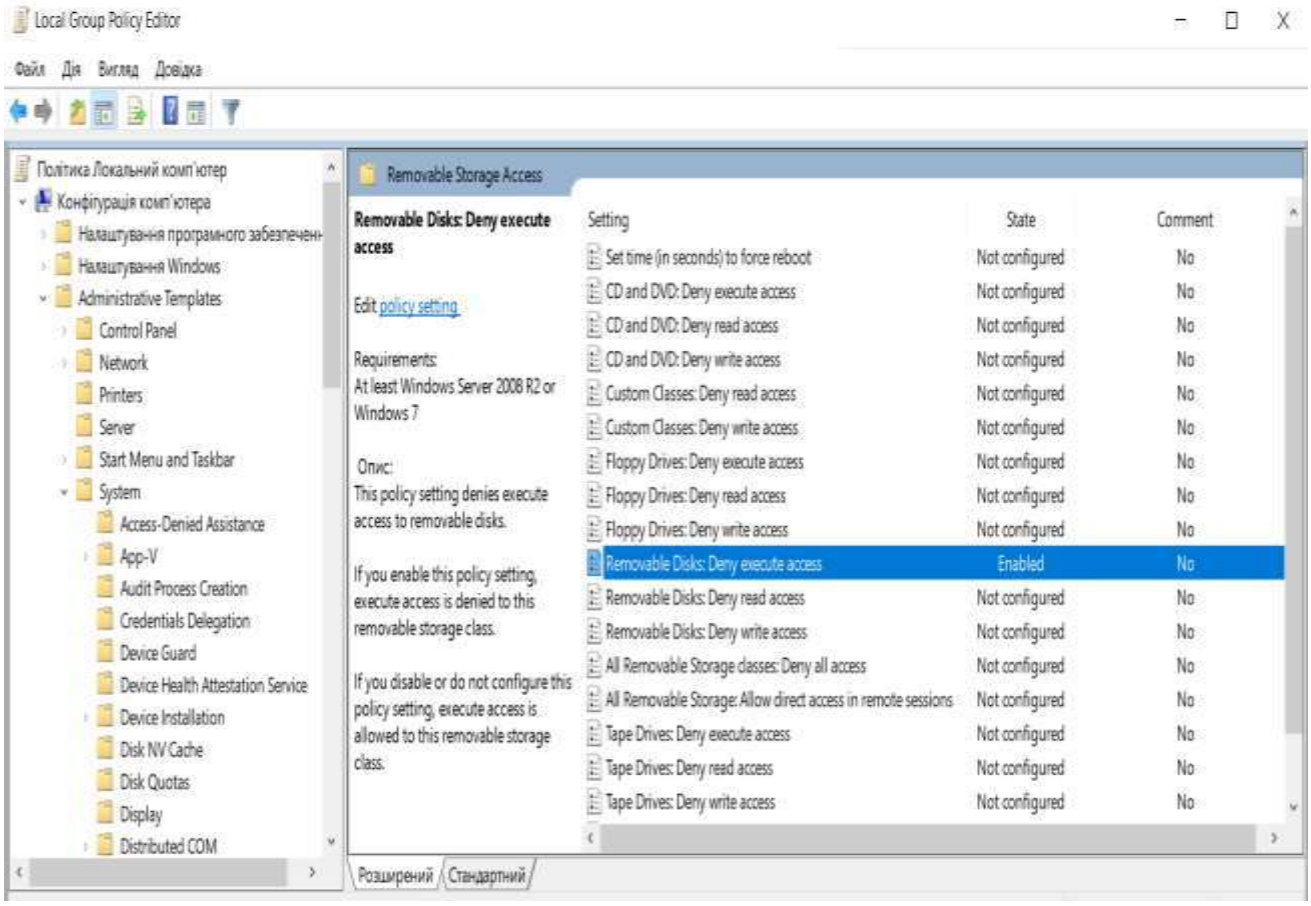


Рисунок 2.11 – Політика обмеження доступу до знімних накопичувачів

Додатково, для забезпечення конфіденційності інформації на випадок фізичної крадіжки обладнання або несанкціонованого демонтажу жорсткого диска зловмисниками, на робочій станції розгортається вбудований

криптографічний механізм захисту - шифрування дисків BitLocker [38]. Використання алгоритму XTS-AES зі 128- або 256-бітним ключем гарантує, що зчитування даних шляхом прямого підключення носія до іншого ПК стане неможливим.

Перевірка статусу шифрування системного диска здійснюється через відповідний модуль панелі керування (рисунок 2.12).

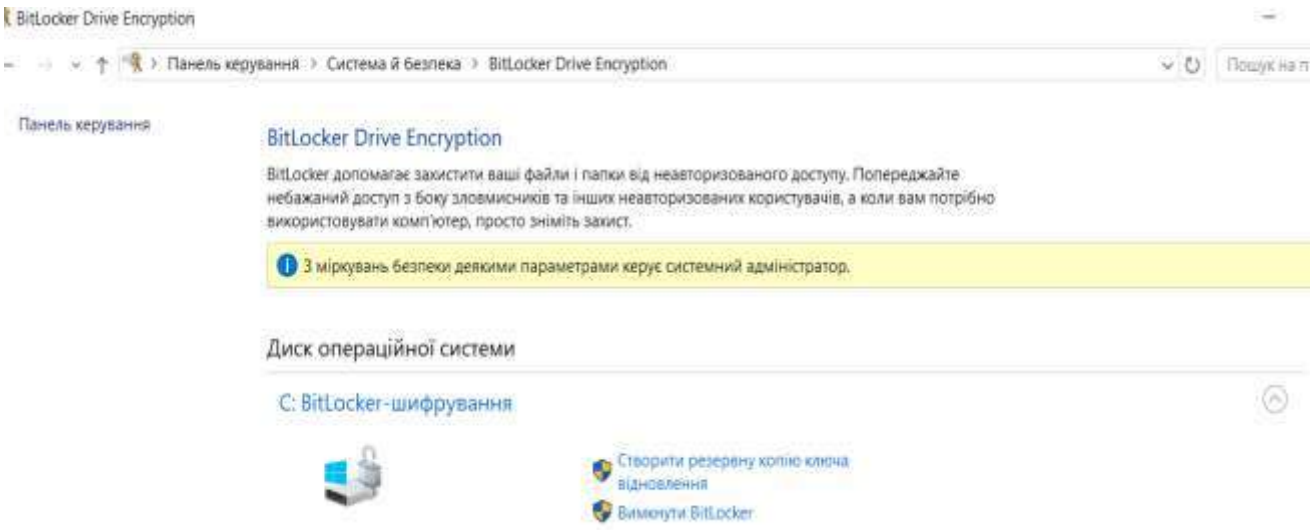


Рисунок 2.12 – Візуалізація статусу активації шифрування BitLocker

Застосування вищенаведеного комплексу політик та захисних параметрів можливе як на окремій автономній машині (АРМ-1), так і в межах локальної інфраструктури, забезпечуючи високий рівень кібернетичної стійкості, цілісності корпоративних даних та захищеності від широкого спектра внутрішніх і технічних загроз.

2.4 Реалізація комплексної системи захисту інформації на об’єкті

Після розробки всієї необхідної документації, технічного проєкту та підготовки теоретичної бази настає етап практичної реалізації. Першим кроком є введення КСЗІ в дію.

Робота із системою на цьому етапі передбачає правильне розміщення автоматизованої системи відповідно до вимог, а також тонке налаштування середовища Windows та антивірусного захисту.

Навчання персоналу проводиться для всіх категорій працівників підприємства, які мають допуск до приміщення з КСЗІ. До списку таких осіб належать: власник системи, безпосередні користувачі, технічний персонал та охорона. Кожен з них має власний рівень допуску, тому інструктаж здійснюється суворо відповідно до посадових повноважень. Обслуговуючий персонал навчають правильного поводження з елементами системи. Наприклад, технікам демонструють обладнання, до якого вони мають доступ, а охороні - розташування систем сигналізації та пожежної безпеки з поясненням алгоритму дій у нештатних ситуаціях. Також їх навчають базових засад безпеки для усвідомлення відповідальності.

Користувачам демонструють інтерфейс входу та виходу, правила збереження даних та роз'яснюють їхні персональні права доступу. Обов'язково проводяться лекції з кібербезпеки для підтримки високого рівня обізнаності.

Важливим аспектом є розпізнавання вразливостей та реагування на загрози – користувачі повинні вчасно реагувати на інциденти, знати алгоритм дій у непередбачуваних ситуаціях та володіти навичками заповнення звітів. Навчання користувачів має циклічний характер і проводиться також після введення системи в експлуатацію для актуалізації знань відповідно до нових тенденцій у сфері кіберзлочинності.

Окрім технічного навчання, всіх працівників ознайомлюють під підпис із документацією, а саме: з планом захисту, політиками безпеки та інформацією про їхні персональні доступи.

Етап введення КСЗІ в дію супроводжується практичними роботами. Відповідно до плану захисту інсталюються всі програмні засоби, що мають експертний висновок, і проводиться перевірка працездатності комплексу.

Мають бути встановлені всі захисні механізми згідно з проєктом.

Здійснюється реєстрація користувачів, налаштовуються їхні індивідуальні права та вводяться особисті паролі. Права доступу диференціюються: наприклад, перегляд та редагування документів, тоді як додавання чи видалення інформації дозволено виключно адміністратору системи.

Коли система повністю готова, починається етап попередніх випробувань та дослідної експлуатації [39].

Випробування проводяться розробником КСЗІ для визначення готовності комплексу до повноцінної роботи, при цьому перевірка безпеки здійснюється всіма доступними інструментами.

Після тестувань, за потреби, доставляється відсутнє програмне забезпечення, замінюються апаратні компоненти, що не відповідають вимогам, або проводяться додаткові налаштування. Якщо виявляється, що певне ПЗ не має експертного висновку, його негайно замінюють.

Останнім етапом є державна експертиза, яка проводиться Державною службою спеціального зв'язку та захисту інформації України відповідно до регламентних положень [40]. За результатами випробувань та підтвердження відповідності системи технічному завданню об'єкт отримує Атестат відповідності.

Після отримання атестата, на підставі наказу керівника установи, починається штатна експлуатація системи. В силу вступають план захисту та політики безпеки.

Служба захисту інформації зобов'язана фіксувати всі аспекти використання, пропонувати заходи з модернізації комплексу, вчасно проходити переатестації та забезпечувати відповідність актуальним вимогам законодавства.

Ці політики можуть бути налаштовані як для локального комп'ютера, так і для комп'ютерів у мережі, які керуються контролером домену. Вони дозволяють створювати і реалізувати різні стратегії безпеки в залежності від потреб організації або конкретного випадку використання.

2.5 Висновок до розділу

У цьому розділі було розроблено архітектуру та здійснено практичну реалізацію комплексної системи захисту інформації для автоматизованого робочого місця керівника ТОВ «ПРАЩУР», що функціонує як ізольована інформаційна система класу «1». Під час виконання роботи було послідовно пройдено всі етапи створення системи захисту. На організаційно-розпорядчому етапі сформовано повний пакет внутрішньої документації, який створив легітимне правове поле для впровадження заходів кіберзахисту відповідно до чинних нормативних документів НД ТЗІ. У межах аналізу ризиків та моделювання загроз розроблено детальні моделі загроз і порушника, складено генеральний та ситуаційний плани контрольованої зони, а також обґрунтовано функціональний профіль безпеки згідно з критеріями НД ТЗІ 2.5-004-99, що забезпечило належний рівень конфіденційності, цілісності та аудиту. На етапі технічного конфігурування на базі вбудованих інструментів операційного середовища MS Windows 10 налаштовано суворі локальні політики безпеки, розгорнуто підсистему аудиту подій, активовано механізми блокування знімних USB-накопичувачів та запроваджено криптографічний захист інформації за допомогою шифрування системних дисків засобами BitLocker. Загалом спроєктований комплекс заходів та технічних рішень утворює надійний, ешелонований і доказовий контур безпеки, який повністю відповідає національним стандартам кіберзахисту унеможливлює несанкціонований доступ.

3 РОЗГОРТАННЯ ТА ЕКСПЛУАТАЦІЙНЕ ОБСЛУГОВУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТОВ "ПРАЩУР"

3.1Технічна підтримка та обслуговування програмного забезпечення в процесі розгортання та експлуатації

Цифровізація усіх інформаційних просторів суттєво розширює межі обробки, зберігання та передачі даних. Кожна ланка сучасного суспільства стикається з автоматизованими системами, що неабияк полегшує виконання щоденних завдань. Проте стрімкий розвиток технологій змінює світ, а еволюція кіберзлочинності вимагає постійного вдосконалення методів кібербезпеки. Найкращим варіантом для установ та підприємств є комплексний підхід до захисту, який унеможливлює реалізацію атак за різними векторами.

Комплексна система захисту інформації є сукупністю організаційних та технічних засобів, спрямованих на запобігання несанкціонованим діям, витоку, крадіжці, модифікації чи видаленню даних без відповідних повноважень.

Типова схема системи захисту інформації складається з трьох взаємопов'язаних складових: нормативно-правової (закони та внутрішні положення), організаційної (заходи безпеки на фізичному рівні) та інженерно-технічної (налаштування апаратно-програмних комплексів, охоронно-пожежної сигналізації). Усі ці складники тісно переплітаються між собою. Завдання, що виконуються на етапі проєктування, часто плавно переходять в інші стадії: наприклад, фізичний захист нерозривно пов'язаний з організацією пропускного режиму, а технічні обмеження доповнюють адміністративні правила.

Нормативно-правова база враховує специфіку конкретного підприємства. Однак кіберзлочинність розвивається надзвичайно швидко, що зумовлює постійні зміни в законодавчій базі України. З огляду на це, нормативні акти та закони необхідно переглядати на кожному етапі створення системи. Для економії фінансів, часу та забезпечення безперебійного введення КСЗІ в експлуатацію доцільно здійснювати постійний моніторинг регуляторних вимог.

Організаційні заходи КСЗІ націлені на гарантування безпеки та конфіденційності інформації впродовж усього її життєвого циклу. До базових організаційних процедур належать розробка політик і регламентів безпеки, що визначають правила збереження, обробки та знищення даних. Величезне значення має підвищення обізнаності персоналу через регулярні тренінги та інструктажі. Управління доступом базується на суворому дотриманні принципу службової необхідності із застосуванням надійних механізмів автентифікації. Також обов'язковими є систематичний аудит безпеки, контроль фізичного периметра приміщень, чіткі алгоритми реагування на інциденти та впровадження національних стандартів захисту.

Технічні заходи захисту охоплюють використання спеціалізованих технологій, програмного та апаратного забезпечення для запобігання несанкціонованому доступу. Ключовим елементом тут є розмежування ідентифікації (логін) та автентифікації (пароль), включно з використанням двофакторної верифікації. Для захисту інформації під час зберігання та передачі застосовується надійне криптографічне шифрування дисків і комунікаційних каналів. Антивірусне програмне забезпечення забезпечує блокування шкідливого софту, а регулярне резервне копіювання гарантує відновлення інформації у разі кібератак чи аварій. Додатково використовуються апаратні модулі безпеки та захищені носії.

Усі перераховані технічні, організаційні та фізичні заходи в синергії формують надійну КСЗІ. Основне завдання полягає в правильному визначенні меж та категорій об'єкта. Грамотно побудована організаційна структура створює непрохідний фізичний бар'єр, унеможливлюючи нелегітимний доступ порушників до обладнання, тоді як технічна складова забезпечує стабільну роботу уповноважених працівників.

Життєвий цикл захисту інформації охоплює кілька послідовних етапів. На першому етапі проводиться глибокий аналіз ризиків і визначення потенційних загроз та вразливостей. Далі розробляється детальна політика безпеки, яка

встановлює правила, парольні вимоги та стандарти роботи. Наступним кроком є практичне впровадження технічних і організаційних засобів, після чого починається безпосередня експлуатація КСЗІ з постійним моніторингом подій. Завершується цикл постійним удосконаленням системи відповідно до еволюції загроз та технологій, що дозволяє уникнути помилок і знизити навантаження на фахівців із безпеки.

Для забезпечення ефективного захисту необхідно реалізовувати дворівневу архітектуру. Організація зовнішнього захисту включає аудит фізичних подій, охорону території та контроль доступу до приміщень, обладнаних сигналізацією і відеоспостереженням. Внутрішній захист фокусується на програмному середовищі – встановленні антивірусів, веденні журналів реєстрації та блокуванні спроб несанкціонованого доступу. Особлива увага приділяється аудиту подій, який фіксує кожен крок користувача в системі. Хоча сам по собі аудит не зупиняє атаку, він дозволяє реконструювати інцидент, виявити порушника та відновити справедливість. Варто пам'ятати, що витік інформації тягне за собою сувору кримінальну, адміністративну або дисциплінарну відповідальність. Етап реагування передбачає фіксацію порушення, ліквідацію наслідків та глибокий аналіз причин для недопущення подібних інцидентів у майбутньому.

Розглядаючи безпековий контур, не можна нехтувати людським фактором та випадковими подіями. Уявімо ситуацію, коли обслуговуючий персонал, який не має доступу до державної таємниці, випадково вимикає електроживлення в сусідній кімнаті під час прибирання. Якщо політики безпеки та резервного живлення налаштовані неналежним чином, це може призвести до втрати критичних даних. Грамотне проєктування КСЗІ обов'язково враховує такі ризики через впровадження джерел безперебійного живлення, автоматичне збереження сесій та ізоляцію апаратної частини.

Етап попередження загроз пронизує всі рівні створення системи захисту – від написання перших наказів до фізичного розміщення технічних засобів.

Наприклад, елементарний вибір кута нахилу монітора відносно вікна чи дверей може стати вирішальним для запобігання візуальному витоку інформації. Ситуації з випадковими збоями також успішно нівелюються завдяки якісному навчанню не лише основних користувачів, а й усього залученого персоналу [41].

Психологічний аспект безпеки є не менш важливою складовою, оскільки ризик підкупу працівників або недбалості через людський фактор залишається актуальним. Детальне роз'яснення посадових обов'язків та рівня відповідальності за розголошення комерційної таємниці формує у колективі правильну культуру кібергігієни. Логічним завершенням комплексу є безперебійна робота інженерно-технічних систем — надійного заземлення, промислових джерел живлення та протипожежних комплексів, які гарантують цілісність корпоративних ресурсів на всіх рівнях.

3.2 Політика та регламент антивірусного захисту в ТОВ «ПРАЩУР»

Безпека інформаційних ресурсів ТОВ «ПРАЩУР» ґрунтується на використанні сертифікованих засобів антивірусного захисту, що відповідають чинним вимогам Держспецзв'язку України. Легітимність захисного ПЗ на підприємстві підтверджується наявністю експертного висновку та чинного атестата відповідності, що є обов’язковим для АС будь-якого класу. Процедура впровадження розпочинається з офіційної реєстрації ТОВ «ПРАЩУР» у центрі управління безпекою розробника, де фіксуються дані про власника системи, мережеві параметри та конкретні ідентифікатори доменів. Це забезпечує не лише легальність програмного забезпечення, а й доступ до щоденних оновлень, які є критичними для протидії новим векторам атак.

Для забезпечення актуальності захисту в ТОВ «ПРАЩУР» впроваджено багаторівневу архітектуру оновлень. У сегментах мережі, підключених до інтернету, антивірусні бази оновлюються автоматично з обов'язковим

логуванням успішності кожної сесії. Натомість, для ізольованих інформаційних систем, де доступ до глобальної мережі фізично обмежений, діє суворий «шлюзовий» протокол. Адміністратор безпеки ТОВ «ПРАЩУР» завантажує оновлення на виділену «станцію адміністрування», після чого вони переносяться на ізольовані вузли через спеціально зареєстровані USB-носії. Кожне використання носія супроводжується записом у журналі аудиту із зазначенням часових міток, ідентифікатора носія та підписом відповідальної особи, що мінімізує ризики внесення шкідливого коду через зовнішні пристрої.

Станом на 2026 рік технічну базу захисту ТОВ «ПРАЩУР» складають рішення класу ESET Endpoint Security [42]. Обрання цього продукту обумовлене його високою ефективністю у виявленні багатовекторних загроз. Завдяки технологіям багаторівневого захисту, зокрема використанню двигуна ESET LiveSense, антивірус здійснює не лише традиційне порівняння з базою сигнатур, а й глибокий евристичний аналіз поведінки програм. Це дозволяє системі ефективно ідентифікувати загрози «нульового дня», які ще не мають офіційних описів, шляхом аналізу підозрілої активності в оперативній пам’яті та на рівні системних викликів.

Важливим компонентом безпеки є впроваджений у ТОВ «ПРАЩУР» модуль контролю пристроїв (Device Control), який блокує неавторизоване підключення зовнішнього обладнання до АС. Будь-який змінний носій перед початком роботи проходить примусове глибоке сканування, а перевірка цілісності файлів здійснюється шляхом контролю хеш-сум. Додатково, використання інструментів ESET дозволяє адміністраторам підприємства проводити централізоване управління політиками, блокувати потенційно небезпечні вебресурси та контролювати шифрування даних на дисках. Така комплексна стратегія, що інтегрує міжнародні стандарти серії ISO/IEC 27001 з національними вимогами, дозволяє ТОВ «ПРАЩУР» підтримувати високий рівень стійкості інформаційного середовища та оперативно реагувати на спроби несанкціонованого втручання в діяльність системи [43].

3.3 Регламентація повноважень персоналу ТОВ «ПРАЩУР»

Формування безпекового середовища в ТОВ «ПРАЩУР» базується на чіткому розмежуванні прав та обов'язків між суб'єктами інформаційних відносин. Політики безпеки, що розробляються як індивідуальні інструкції, є обов'язковими для виконання всіма працівниками. Уся ієрархія захисту в компанії вибудовується навколо трьох напрямків: програмного (налаштування та підтримка ПЗ), системно-орієнтованого (адміністрування та функціонування КСЗІ) та проблемно-орієнтованого (алгоритми реагування на непередбачувані інциденти).

Формування безпекового середовища в ТОВ «ПРАЩУР» базується на чіткому розмежуванні прав та обов'язків між суб'єктами інформаційних відносин. Політики безпеки, що розробляються як індивідуальні інструкції, є обов'язковими для виконання всіма працівниками. Уся ієрархія захисту в компанії вибудовується навколо трьох напрямків: програмного, системно-орієнтованого та проблемно-орієнтованого. Ключовим суб'єктом, що забезпечує функціонування КСЗІ, є адміністратор безпеки ТОВ «ПРАЩУР». Його повноваження охоплюють повний цикл контролю: від управління автентифікацією та моніторингу системних журналів до конфігурації засобів виявлення вторгнень. Для кінцевих користувачів інструкції безпеки фокусуються на мінімізації людського фактора. У випадку виявлення загрози персонал діє згідно із затвердженим протоколом реагування. Власник системи несе стратегічну відповідальність за стан КСЗІ. Весь комплекс документів, що регламентує ці вимоги, утворює єдиний нормативний контур підприємства.

Ефективність функціонування комплексної системи захисту інформації значною мірою залежить не лише від наявності сучасних технічних засобів захисту, а й від рівня організаційної зрілості підприємства. У ТОВ «ПРАЩУР» безпекова діяльність розглядається як безперервний процес, що охоплює всі етапи життєвого циклу інформації: від її створення та оброблення до

архівування або знищення. Такий підхід дозволяє забезпечити належний рівень конфіденційності, цілісності та доступності інформаційних ресурсів незалежно від характеру потенційних загроз та змін у зовнішньому середовищі. Ключовим суб’єктом, що забезпечує функціонування КСЗІ, є адміністратор безпеки ТОВ «ПРАЩУР». Його повноваження охоплюють повний цикл контролю: від управління автентифікацією та моніторингу системних журналів до конфігурації засобів виявлення вторгнень. До його розширеного переліку обов'язків входить:

- контроль ідентифікації;
- аудит та моніторинг;
- управління вразливостями;
- підготовка звітності.

Контроль ідентифікації передбачає ведення реєстру облікових записів, регулярний перегляд прав доступу та анулювання доступу для звільнених працівників. Аудит та моніторинг передбачає щоденний аналіз журналів подій на предмет виявлення аномальної активності (наприклад, спроб підбору паролів чи масового копіювання даних). Управління вразливостями передбачає встановлення критичних оновлень безпеки та патчів на всі вузли мережі, включаючи захищені АС. Підготовка звітності передбачає формування періодичних звітів про стан захищеності для керівництва підприємства, що є частиною обов’язкового внутрішнього аудиту.

Власник системи в ТОВ «ПРАЩУР» несе стратегічну відповідальність за стан КСЗІ. До його обов’язків входить визначення ризик-апетиту компанії, забезпечення належного фінансування організаційно-технічних заходів, затвердження планів відновлення діяльності (DRP – Disaster Recovery Plan) та встановлення стандартів корпоративної кібергігієни. Такий підхід забезпечує не лише технічну стабільність, а й юридичну захищеність бізнес-процесів компанії. Весь комплекс документів, що регламентує ці вимоги (технічне завдання, проект захисту та план реалізації), утворює єдиний нормативний контур підприємства.

Кожен з цих документів тісно інтегрований з іншими: план захисту деталізує стратегічні завдання, сформульовані в технічному завданні, створюючи прозору структуру відповідальності на кожному рівні доступу до корпоративних активів.

Для кінцевих користувачів інструкції безпеки в ТОВ «ПРАЩУР» фокусуються на мінімізації людського фактора. Вимоги включають обов'язкове використання складних паролів довжиною не менше 14 символів та обов'язкове застосування двофакторної автентифікації. Повна заборона на використання несертифікованих USB-накопичувачів або персональних хмарних сховищ для зберігання робочих документів. Проходження щорічного онлайн-тренінгу з виявлення фішингових розсилок та інших методів соціальної інженерії.

У випадку виявлення загрози, персонал ТОВ «ПРАЩУР» діє згідно з затвердженим протоколом реагування, який мінімізує збитки:

– ідентифікація – користувач негайно повідомляє адміністратора про підозрілу активність (нетипові повідомлення, «зависання» ПЗ, блокування файлів);

– ізоляція – адміністратор безпеки миттєво відключає уражений сегмент ас від загальної мережі, щоб запобігти поширенню вірусу чи витоку даних;

– аналіз – проводиться аналіз журналів подій та дампів пам'яті для визначення джерела атаки та вектору проникнення;

– відновлення – після очищення системи та виправлення вразливості дані відновлюються з останньої перевіреної резервної копії, проведеної згідно з графіком;

– аналіз після інциденту – розробка коригувальних заходів для уникнення повторення подібних випадків у майбутньому.

Особливе значення приділяється класифікації інформаційних активів. Інформаційні ресурси підприємства розподіляються за рівнями критичності та важливості для бізнес-процесів. Подібна класифікація створює основу для вибору адекватних механізмів захисту та визначення пріоритетності заходів безпеки. Критично важливі дані потребують посиленого контролю доступу,

додаткового резервування та постійного моніторингу стану захищеності. Менш чутлива інформація також перебуває під контролем, однак до неї застосовуються пропорційні заходи безпеки, що дозволяє оптимально використовувати ресурси підприємства.

Важливим елементом організації захисту є управління ризиками. Процес аналізу ризиків проводиться на регулярній основі та передбачає ідентифікацію потенційних загроз, оцінювання можливих наслідків їх реалізації та визначення ймовірності виникнення інцидентів. Результати такого аналізу використовуються для коригування політик безпеки, удосконалення технічних засобів захисту та перегляду організаційних процедур. Регулярне оцінювання ризиків дозволяє підприємству своєчасно реагувати на зміни кіберзагроз і підтримувати актуальність захисних механізмів.

Система контролю доступу на підприємстві будується відповідно до принципу мінімально необхідних привілеїв. Працівники отримують лише ті права доступу, які потрібні для виконання їхніх службових обов'язків. Будь-яке розширення повноважень здійснюється виключно після погодження з відповідальними особами та документального оформлення. Такий підхід суттєво зменшує ризик несанкціонованого доступу до критичних інформаційних ресурсів і забезпечує прозорість процесів управління доступом.

Окрему увагу приділено питанням журналювання подій інформаційної безпеки. Усі суттєві дії користувачів, адміністраторів та програмних компонентів реєструються в системних журналах. Отримана інформація використовується для проведення аудиту, розслідування інцидентів та оцінювання ефективності захисних механізмів. Наявність централізованої системи збору подій дозволяє оперативно виявляти аномальну активність і своєчасно вживати необхідних заходів реагування.

Для забезпечення безперервності діяльності підприємства створюються резервні копії критично важливих даних та конфігураційних файлів. Процедури резервного копіювання виконуються відповідно до затвердженого графіка, а

результати регулярно перевіряються шляхом тестового відновлення інформації. Практика показує, що наявність резервних копій є одним із найбільш ефективних інструментів протидії наслідкам програм-вимагачів, технічних збоїв або помилок персоналу.

Сучасні інформаційні системи постійно перебувають під впливом нових кіберзагроз, тому значна роль відводиться процесу управління вразливостями. Підприємство забезпечує своєчасне встановлення оновлень програмного забезпечення, проводить сканування інформаційної інфраструктури та здійснює аналіз виявлених недоліків. Виявлені вразливості ранжуються за рівнем критичності, після чого визначаються строки та порядок їх усунення. Така практика сприяє зменшенню площини потенційної атаки та підвищує загальний рівень захищеності системи.

Не менш важливим напрямом є підготовка персоналу. Людський фактор традиційно залишається однією з основних причин виникнення інцидентів інформаційної безпеки. Саме тому працівники регулярно проходять навчання, під час якого розглядаються актуальні загрози, методи соціальної інженерії, правила безпечної роботи з електронною поштою та особливості захисту корпоративної інформації. Формування культури безпеки сприяє усвідомленому ставленню працівників до власної відповідальності.

Організаційні заходи безпеки доповнюються використанням технічних засобів захисту. До таких засобів належать міжмережеві екрани, системи виявлення та запобігання вторгненням, антивірусне програмне забезпечення, засоби криптографічного захисту інформації та системи централізованого моніторингу. Комплексне використання цих рішень дозволяє забезпечити багаторівневий захист інформаційної інфраструктури та знизити ризик успішної реалізації атак.

Важливим аспектом функціонування КСЗІ є забезпечення фізичної безпеки. Серверні приміщення обладнуються системами контролю доступу, відеоспостереженням та засобами пожежогасіння. Доступ до технічних

приміщень надається лише уповноваженим особам. Подібні заходи дозволяють мінімізувати ризики, пов’язані з несанкціонованим фізичним втручанням у роботу інформаційних систем.

У межах управління інцидентами особлива увага приділяється документуванню всіх етапів реагування. Фіксація обставин події, часу її виявлення, виконаних дій та отриманих результатів створює основу для подальшого аналізу та вдосконалення процесів безпеки. Накопичений досвід використовується для актуалізації внутрішніх регламентів і підвищення готовності персоналу до реагування на подібні ситуації в майбутньому.

Підприємство також враховує необхідність захисту інформації під час взаємодії з контрагентами. У договорах передбачаються вимоги щодо нерозголошення інформації, дотримання правил безпеки та відповідальності за порушення встановлених умов. Такий підхід дозволяє розширити контур захисту за межі внутрішнього середовища підприємства та знизити ризики, пов’язані із зовнішніми учасниками бізнес-процесів.

Важливим напрямом розвитку системи безпеки є проведення внутрішніх аудитів. Аудит дає можливість оцінити відповідність фактичного стану захисту встановленим вимогам, виявити недоліки та визначити напрями вдосконалення. За результатами перевірок формуються рекомендації щодо оптимізації процесів безпеки та підвищення ефективності функціонування КСЗІ.

Таким чином, функціонування КСЗІ в ТОВ «ПРАЩУР» являє собою комплекс взаємопов’язаних організаційних, технічних та правових заходів. Їх реалізація забезпечує належний рівень захисту інформаційних ресурсів, підтримує безперервність бізнес-процесів та створює умови для стабільного розвитку підприємства в умовах постійного зростання кіберзагроз. Послідовне вдосконалення системи безпеки, розвиток культури захисту інформації та впровадження сучасних технологій дозволяють забезпечити довгострокову стійкість підприємства та ефективно протидіяти актуальним викликам інформаційного суспільства.

3.4 Висновки

У третьому розділі роботи було завершено проєктування комплексної системи захисту інформації для автоматизованого робочого місця директора ТОВ «ПРАЩУР» та обґрунтовано вибір організаційних і програмно-технічних рішень, спрямованих на забезпечення конфіденційності, цілісності та доступності корпоративних інформаційних ресурсів.

На основі результатів попереднього аналізу загроз, вразливостей і особливостей функціонування підприємства сформовано цілісну архітектуру захисного контуру, яка відповідає вимогам чинної нормативно-правової бази України у сфері технічного захисту інформації.

У ході виконання робіт визначено склад і функції основних суб’єктів забезпечення безпеки, розроблено організаційно-розпорядчу документацію, регламентовано порядок адміністрування системи та розмежування прав доступу користувачів. Особливу увагу приділено впровадженню механізмів автентифікації, контролю доступу, журналювання подій безпеки, резервного копіювання та моніторингу стану захищеності інформаційної інфраструктури.

Розроблена система передбачає використання сучасних програмно-апаратних засобів захисту, включаючи антивірусні рішення, засоби криптографічного захисту інформації, міжмережеві екрани та механізми контролю цілісності даних.

Проведене обґрунтування підтвердило, що реалізація КСЗІ для АРМ директора є економічно та функціонально доцільною, оскільки дозволяє суттєво знизити ймовірність реалізації кіберзагроз, захистити комерційну таємницю, персональні дані працівників і клієнтів, а також забезпечити належний рівень інформаційної безпеки відповідно до вимог четвертої категорії об’єктів інформаційної діяльності. Отримані результати свідчать про досягнення поставленої мети роботи та підтверджують можливість практичного впровадження розробленої КСЗІ в діяльність ТОВ «ПРАЩУР».

ВИСНОВКИ

У кваліфікаційній роботі проведено комплексне дослідження та розроблено концептуальну архітектуру комплексної системи захисту інформації (КСЗІ) для ТОВ «ПРАЩУР», яка враховує сучасні вимоги до безпеки критичних даних, включаючи специфіку обробки об’єктів цифрової криміналістики та комерційної таємниці. Аналіз існуючого інформаційного середовища підприємства довів, що в умовах стрімкої цифровізації 2026 року інформація перетворилася на найбільш вразливий актив, а забезпечення її цілісності, автентичності та незмінності стало ключовим фактором стійкості та стабільності всіх бізнес-процесів компанії. Проведене дослідження дозволило сформувати цілісну картину вразливостей, притаманних корпоративним мережам, де ризик несанкціонованого втручання може призвести не лише до прямих фінансових втрат, а й до критичної втрати доказової сили цифрових матеріалів, що є неприпустимим при проведенні внутрішніх розслідувань або взаємодії з правоохоронними органами.

Під час виконання роботи було реалізовано послідовний аналітичний аудит, який дозволив чітко класифікувати категорії інформаційних потоків та визначити рівні пріоритетності захисту для кожного вузла мережі ТОВ «ПРАЩУР». На основі отриманих даних було побудовано детальну модель загроз та модель порушника, яка враховує актуальні вектори атак, притаманні для поточного технологічного етапу. Цей етап роботи став фундаментом для обґрунтування необхідності переходу від фрагментарних засобів захисту до багаторівневої системи, де технічні інструменти безпеки обов'язково підкріплюються жорсткими організаційними процедурами, що мінімізують вплив людського фактора. Важливо підкреслити, що побудована модель не є статичною, а передбачає динамічну адаптацію до змін у зовнішньому середовищі, що дозволяє підприємству зберігати технологічну перевагу в умовах постійного еволюціонування кіберзагроз.

Технологічна реалізація проєкту включала впровадження спеціалізованого програмного забезпечення класу ESET Endpoint Security, яке було інтегроване в загальну інфраструктуру підприємства. Особливу увагу в роботі приділено криптографічним механізмам, зокрема методам хешування, які забезпечують контроль незмінності даних. Для сегментів мережі, що функціонують в ізольованому режимі, було розроблено та успішно випробувано «шлюзову» модель оновлення антивірусних баз, яка виключає прямий доступ до інтернету та унеможливлює проникнення шкідливого коду через зовнішні USB-носії. Цей підхід забезпечує гарантований захист найбільш конфіденційних сегментів АС, зберігаючи при цьому необхідний рівень продуктивності системи.

Значний обсяг роботи було присвячено формуванню нормативної бази та системи інструктажу персоналу, оскільки технічні засоби без належного регулювання втрачають свою ефективність. Нами було розроблено ієрархію політик безпеки, яка включає деталізовані інструкції для адміністраторів безпеки, власників системи та рядових користувачів. Ці документи трансформують загальні вимоги безпеки у чіткі робочі алгоритми, такі як протоколи дій при виявленні несанкціонованої активності, правила ідентифікації користувачів, принципи роботи з конфіденційними файлами та процедури аварійного відновлення після інцидентів.

Підсумовуючи, можна стверджувати, що успіх впровадженої КСЗІ базується на синергії технічних рішень, організаційної дисципліни та нормативної відповідності. Спроєктована система дозволила ТОВ «ПРАЩУР» забезпечити належний рівень конфіденційності, цілісності та доступності інформаційних ресурсів, що безпосередньо впливає на рівень довіри з боку клієнтів та партнерів. Подальший розвиток системи вбачається у впровадженні інтелектуальних інструментів моніторингу типу SIEM, автоматизації контролю ланцюга зберігання даних та переході до хмарно-орієнтованих моделей безпеки. Реалізація цих кроків дозволить підприємству не лише підтримувати високі стандарти кібербезпеки в майбутньому, а й динамічно реагувати на виклики.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Комплексні системи захисту інформації : навчальний посібник / Ю. Є. Яремчук та ін. Вінниця : ВНТУ, 2018. 118с.

2. 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: 30.03.2026).

3. 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: 01.04.2026).

4. Про захист персональних даних: Закон України від 14.06.2025 URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 01.04.2026).

5. Про державну таємницю: Закон України від 27.08.2025 № 763-VII URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 01.04.2026).

6. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу Київ : ДСТСЗІ СБ України, 1999. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf (дата звернення: 26.03.2026).

7. 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: 26.03.2026).

8. 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).

9. 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: 12.04.2026).

10. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації : навчальний посібник. Одеса : Фенікс, 2015. 264 с.

11. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створеннякомплексної системи захисту інформації в автоматизованій системі Київ : ДСТСЗІ СБ України, 1999. URL: https://tzi.com.ua/downloads/3.7-001-99.pdf (дата звернення: 07.04.2026)

12. Автоматизоване робоче місце. URL: https://studfile.net/preview/9699901/page:39/ (дата звернення: 07.04.2026)

13. Порядок проведення робіт із створення КСЗІ в інформаційно-телекомунікаційній системі : Нормативний документ технічного захисту інформації від 28.12.2012 № z0910-19. Редакція від 25.04.2023. – Режим доступу: https://tinyurl.com/3kmdap98 (дата звернення 21.04.2026).

14. Розробка моделі загроз інформації та вибір методі в засобів технічного захисту інформації для об'єкта інформаційної діяльності. URL: https://tinyurl.com/4syckuj9 (дата звернення: 28.03.2026)

15. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96. URL: https://tinyurl.com/2dh5fwf8 (дата звернення: 21.04.2026).

16. Основи кібербезпеки. Розділ 17. Моделі загроз та моделі порушника. URL: https://tinyurl.com/vxc79473 (дата звернення: 27.03. 2026)

17. НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці ДСТСЗІ СБ України, 2013. URL: https://tzi.com.ua/downloads/1.6-005-2013.pdf (дата звернення: 08.04.2026)

18. Про затвердження Переліку відомостей, які містять службову інформацію, і яким надається гриф "Для службового користування" наказ від 31.05.2013 № 355 URL: https://zakon.rada.gov.ua/rada/show/v0355733-13#Text (дата звернення: 08.04.2026)

19. Про затвердження переліку об’єктів, проектна документація на будівництво яких повинна включати розділ інженерно-технічних заходів цивільного захисту від 9 січня 2014 р. № 6 https://tinyurl.com/4eh8maf3 (дата звернення: 08.04.2026)

20. Методичні вказівки щодо розробки технічного завдання на створення КСЗІ в автоматизованій системі : Нормативний документ технічного захисту інформації від 28.06.2002 №22 URL: https://tzi.com.ua/downloads/3.7-001-99.pdf (дата звернення 22.04.2026).

21. Розробка моделі загроз інформації та вибір методі в засобів технічного захисту інформації для об'єкта інформаційної діяльності. URL: https://tinyurl.com/4syckuj9 (дата звернення: 28.03.2026)

22. Богуш В. М., Настрадін В. П. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. Київ : Ліра-К, 2020. 553 с.

23. Політика інформаційної безпеки. URL: https://kitsoft.ua/ua/politika-informacijnoyi-bezpeki (дата звернення: 01.04.2026)

24. Організаційно-правові основи забезпечення кібербезпеки. / А. І. Марущак та ін. Київ: Ліра-К, 2023. 320 с.

25. Про електронні документи та електронний документообіг : Закон України від 31.12.2023 № 851-IV. Відомості Верховної Ради України. 2003. № 36. Ст. 275. URL: https://tinyurl.com/mwbs25jt5 (дата звернення: 27.04.2026).

26. Цифровий відбиток (дата звернення: 27.04.2026). URL: https://www.vpnunlimited.com/ua/help/cybersecurity

27. 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).

28. Інформаційна безпека: види загроз і методи їх усунення. URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/ (дата звернення: 04.04.2026)

29. Кібербезпека в Україні: нормативна база, коментарі та роз'яснення,

актуальна судова практика / С. В. Пєтков та ін. Київ: ЦУЛ, 2022. 460 с.

30. Проблеми нормативно-правової бази забезпечення кібербезпеки в Україні: стан і перспективи / З. Б. Живко та ін. Соціально-правові студії : науково-аналітичний журнал Львів : ЛьвДУВС, 2020. Вип. 3 (9). С48-57.

31. Мандзюк О.А. Роль аналітичної діяльності та аналітичних центрів у формуванні й реалізації кібербезпекової політики. URL: https://tinyurl.com/3sx9auw6 (дата звернення: 27.04.2026).

32. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку) URL: https://cip.gov.ua/ (дата звернення: 27.04.2026).

33. . Проект Концепції інформаційної безпеки України. URL: http://www.osce.org/uk/fom/175056?download=true (дата звернення: 06.04.2026).

34. Матриця ризиків: Ключовий інструмент в управлінні проектними ризиками. URL: https://flexi-project.com/uk (дата звернення: 27.04.2026).

35. Метод ідентифікації функціонального профілю захисту. URL: https://www.researchgate.net/publication/370830014_Metod_identifikacii_funkcionalnogo_profilu_zahistu. (дата звернення: 06.04.2026).

36. Впровадження КСЗІ. URL: https://tinyurl.com/n7kjb6j6 (дата звернення: 17.04.2026).

37. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації» від 26.03.2007 № 45. URL: https://zakon.rada.gov.ua/laws/show/z0320-07#Text (дата звернення: 18.05. 2026).

38. Необхідність створення КСЗІ. URL: https://tinyurl.com/y8ve3kh5 (дата звернення: 12.05. 2026).

39. Проектування, введення в дію та супроводження КСЗІ: навчальний посібник / В.Д. Козюра та ін. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. 240 с.

40. Світличний В.А. Дослідження атак на відмову в обслуговуванні інформаційно-телекомунікаційних систем. Кібербезпека в Україні: правові та організаційні питання : Матеріали III Всеукр. наук.-практ. конф. Одеса: ОДУВС, 2018. С. 88-89.

41. Removable Disks: Deny read access URL: https://gpedit.tplant.com.au/enus/policy/RemovableStorage/RemovableDisks_DenyRead_Access_2/ (дата звернення: 10.05.2026)

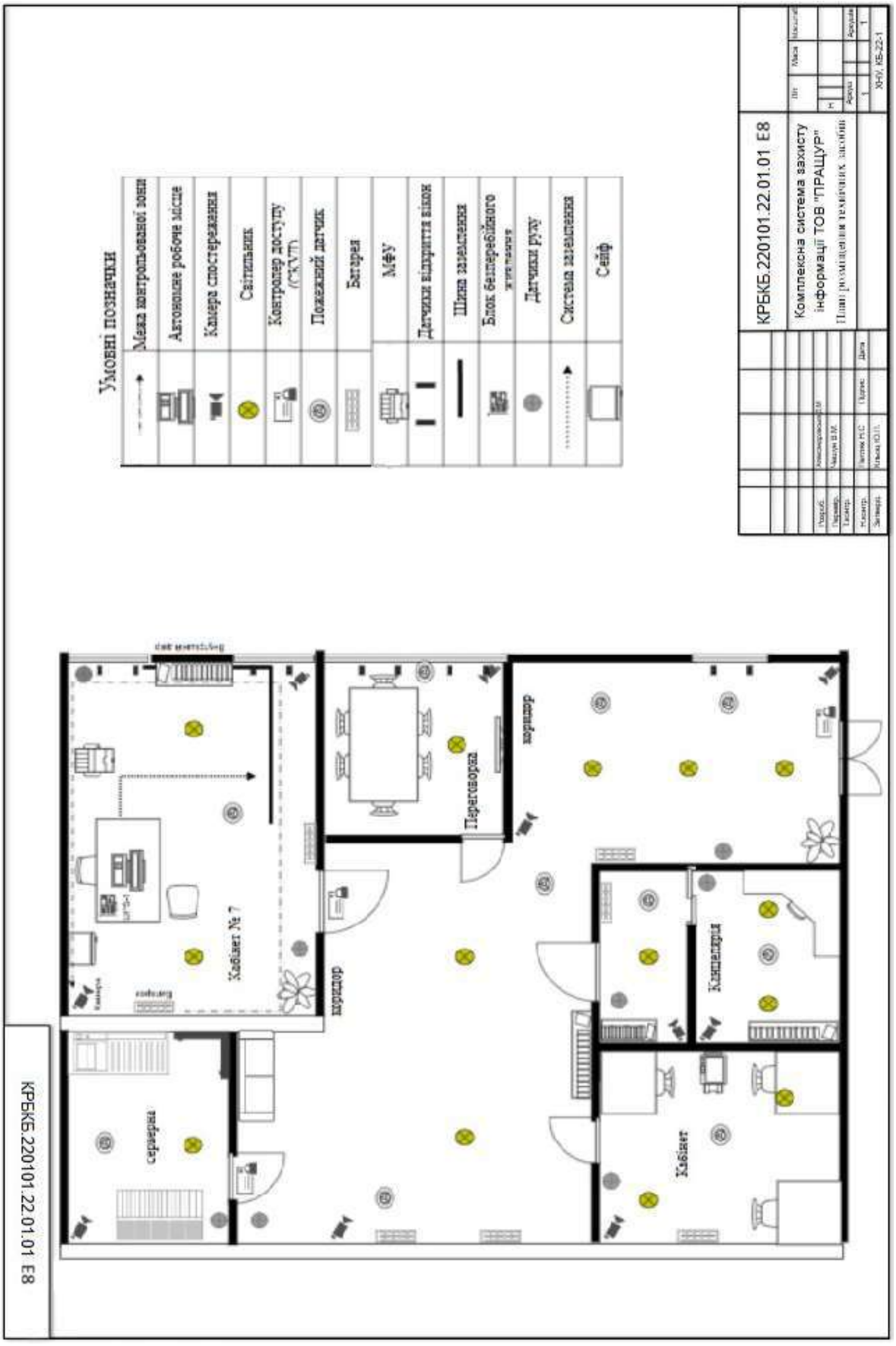
42. Огляд BitLocker. URL: https://support.microsoft.com/uk-ua/windows (дата звернення: 10.05.2026)

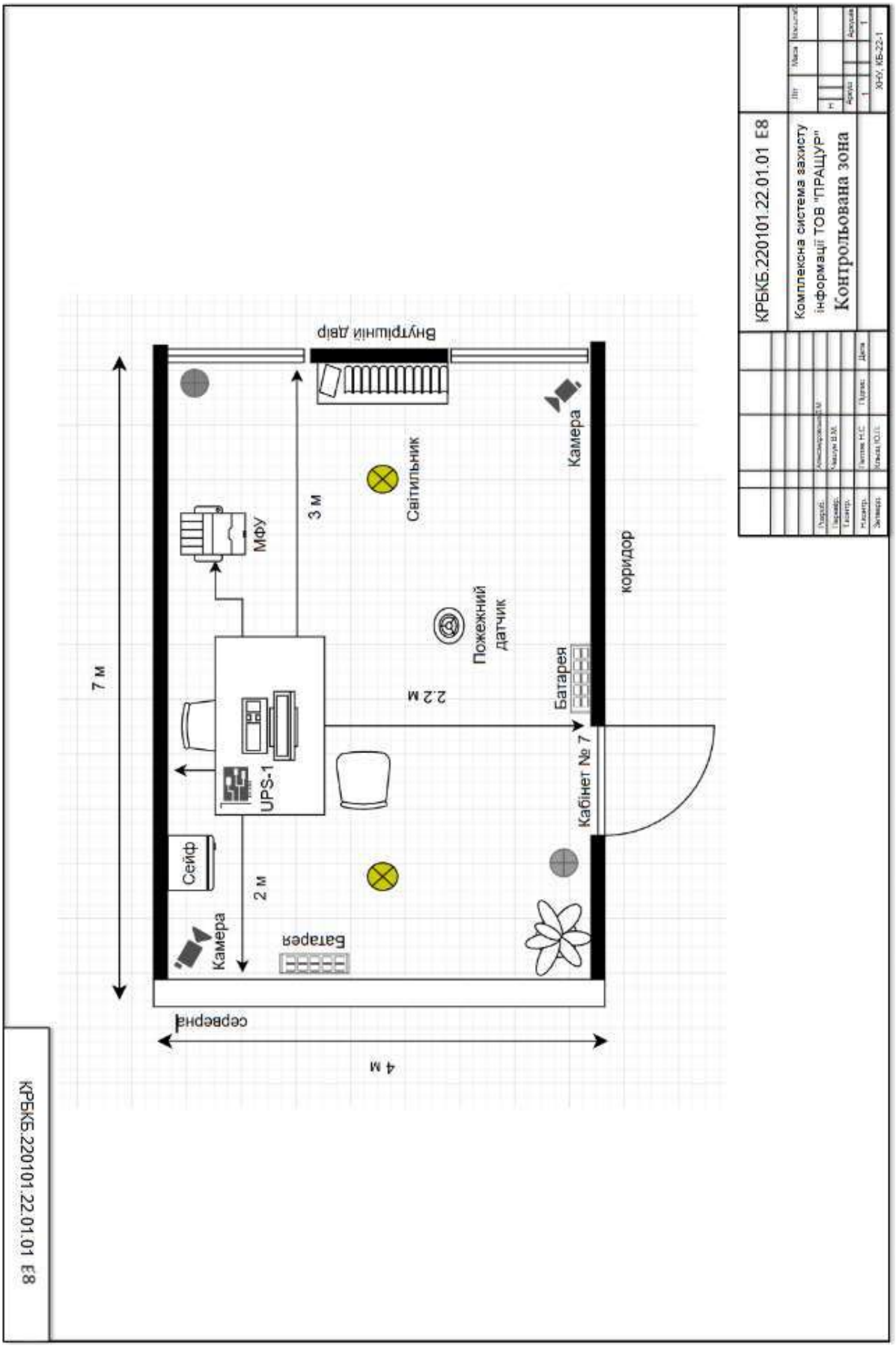
43. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf (дата звернення: 12.05.2026)

Додаток А

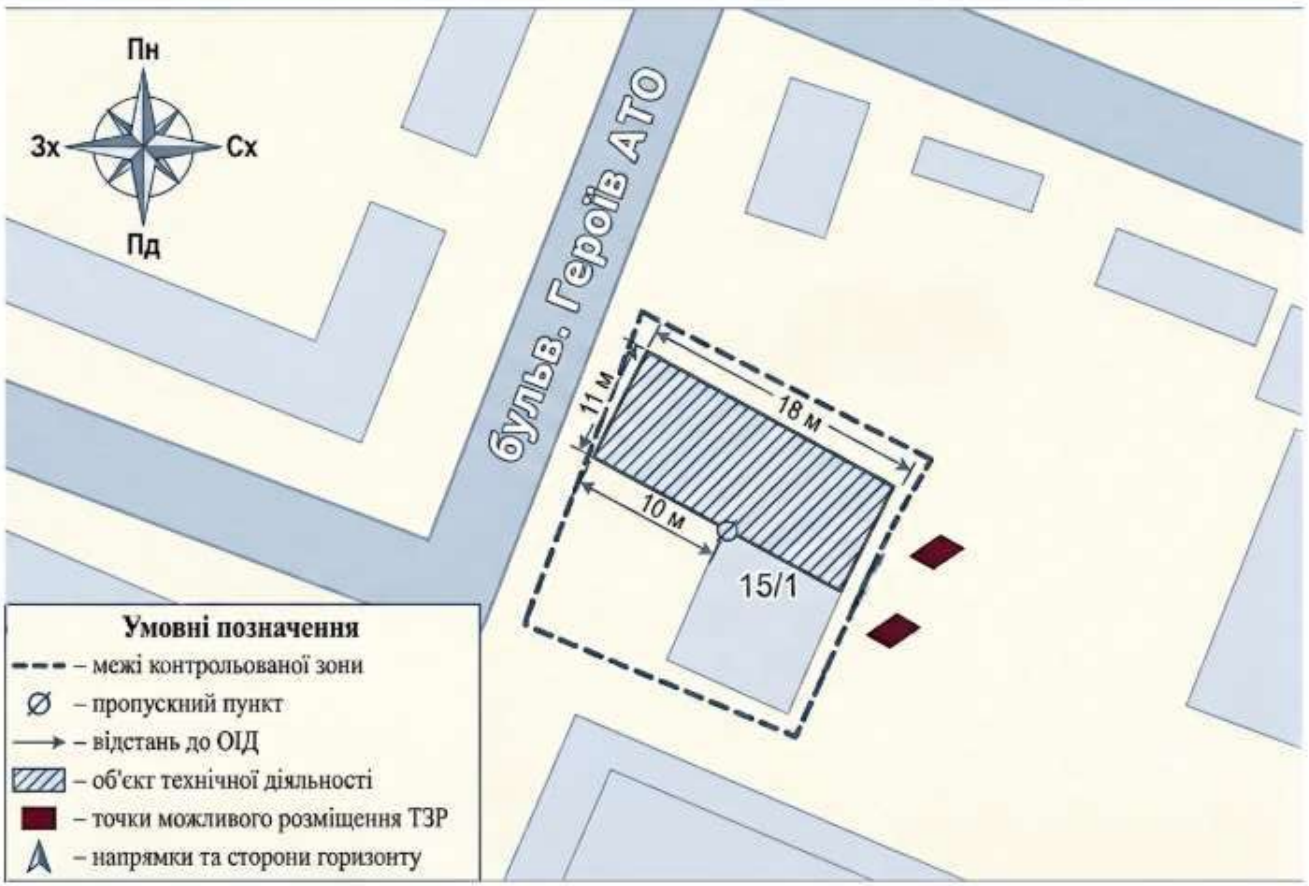
(обов’язковий)

Копії графічної частини




КРБКБ.220101.22.01.01 Е8
Комплексна система захисту інформації ТОВ "ПРАЦЮР"
Контрольована зона
Внутрішній двір
Світильник
Камера
МФУ
3 м
коридор
Пожежний датчик
2.2 м
Батарея
UPS-1
Кабінет № 7
Сейф
2 м
Камера
Батарея
4 м
КРБКБ.220101.22.01.01 Е8

КРБКБ.220101.22.01.01 Е8



					КРБКБ.220101.22.01.01 Е8	
					Комплексна система захисту інформації ТОВ "ПРАЩУР"	Літ. Маса Масштаб
Розроб.		Александровський Е.М.			Ситуаційний план	
Перевір.		Чащук В.М.				Аркуш Аркушів
Т.контр.						1 1
Н.контр.		Пилипів Н.С.	Підпис	Дата		ХНУ, КБ-22-1
Затверд.		Кільош Ю.І.				

Додаток Б

НАКАЗ

10.04.2026 Хмельницький №01

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 затверджене указом Президента України №1229/99 від 27.09.1999 та Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно- комунікаційних системах затвердженого постановою Кабінету Міністрів України №373 від 29.03.2006

НАКАЗУЮ:

1 Створити комплексну систему захисту інформації в автоматизованій системі класу «1» інв. № 111358760, в якій передбачається обробка інформації з грифом обмеження доступу «Для службового користування та конфіденційна інформація (персональні дані) ТОВ «ПРАЩУР».

2 Відповідальним за створення комплексної системи захисту інформації та впровадження заходів із захисту інформації призначити керівника ТОВ «ПРАЩУР» Хмель Євгенія Костянтиновича.

3 Контроль за виконанням цього наказу покласти на відповідального за технічний захист інформації Романенка Бориса Івановича.

Директор ПРАЩУР Дарина ПАВЛОВА

Додаток В
Наказ про створення служби захисту інформації

Н А К А З

09.05.2026 Хмельницький №01

Про створення служби
захисту інформації

Відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", Вимог у сфері електронних довірчих послуг, затверджених постановою Кабінету Міністрів України від 07.11.2018 № 992, 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 від 04.12.2000 № 53, з метою забезпечення завдань керування комплексною системою захисту інформації інформаційно-телекомунікаційної системи ТОВ «ПРАЩУР»

НАКАЗУЮ:

1. Створити службу захисту інформації ТОВ «ПРАЩУР» у складі:

ХМЕЛЬ Євгенія Костянтиновича	керівник служби захисту інформації ТОВ «ПРАЩУР»
БІЛІНСЬКОГО Валентина Віталійовича	системний адміністратор;
ПРІМАКОВА Кирила Максимовича	адміністратор
СУГАЙ Олександра Васильовича	спеціаліст з технічного захисту інформації;
ГУДІЛІНА Віктора Руслановича	спеціаліст з технічного захисту інформації;
ПРОЦЮКА Руслана Руслановича	системного адміністратора

2. Службі захисту інформації ТОВ «ПРАЩУР» забезпечити:

- виконання робіт з визначення вимог із захисту інформації в інформаційно-телекомунікаційній системі ТОВ «ПРАЩУР»;
- проєктування, розроблення і модернізацію комплексної системи захисту інформації інформаційно-телекомунікаційній системі ТОВ «ПРАЩУР»;
- експлуатацію, обслуговування, підтримку працездатності КСЗІ інформаційно-телекомунікаційній системі ТОВ «ПРАЩУР»;
- контроль за станом захищеності інформації в інформаційно-телекомунікаційній системі ТОВ «ПРАЩУР».

3. Затвердити Положення про службу захисту інформації ТОВ «ПРАЩУР», що додається.

4. Контроль за виконанням наказу покласти на першого заступника директора Говду Р.М.

Додаток Г

Наказ про створення комісії з обстеження об’єктів інформації діяльності

НАКАЗ

12.05.2026 Хмельницький №04

Про створення комісії з обстеження
об’єкту
інформаційної діяльності

Відповідно до закону України «Про захист інформації в інформаційно-комунікаційних системах» №80/94-ВР від 05.07.1994 (зі змінами), (НД ТЗІ 3.1-001-07) «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи»

НАКАЗУЮ:

Утворити комісію з обстеження об’єкту інформаційної діяльності (приміщення №17 ТОВ «ПРАЩУР»)

ГОЛОВА:

ХМЕЛЬ Євгеній Костянтинович	керівник ТОВ «ПРАЩУР»

ЧЛЕНИ КОМІСІЇ:

ГУДІЛІН Віктор Русланович	спеціаліст з технічного захисту інформації;
БІДІНСЬКИИ Валентин Віталійович	системний адміністратор;

Комісії з обстеження провести обстеження об’єкту інформаційної діяльності до 12.05.2026, скласти відповідний акт та подати його на затвердження.

Контроль за виконанням цього наказу покласти на відповідального за технічний захист інформації Романенка Бориса Івановича.

Директор Дарина ПАВЛОВА

Додаток Д

Акт категоріювання об’єкта ЕОТ

(автоматизованої системи класу 1 інв. № 111358760)

ЗАТВЕРДЖУЮ
Директор ТОВ “ПРАЩУР”
_____ Д. О. Павлова
«20» травня 2026 р
М.П.

АКТ
категоріювання автоматизованої системи класу 1 інв. № 111358760 розташованого в приміщенні № 7 кабінету
(найменування об’єкта категоріювання)

Підстава для категоріювання наказ №01 від 30.03.2026 про встановлення КСЗІ
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
зміна ознаки, за якоюбула встановлена категорія об’єкта, тощо;
наказ №01 від 09.04.2026 про утворення комісії зькатегріювання та обстеження об’єктів інформаційної діяльності
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

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)

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

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 (персональні дані)
Закону України “Про доступ до публічної інформації”; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

Встановлена категорія IV (четверта)

Голова комісії	_____	Є.К. Тарасенко
	(підпис)	(ініціали, прізвище)
Члени комісії:	_____	К.В. Стецько
	(підпис)	(ініціали, прізвище)
	_____	О.В. Коростюк
	(підпис)	(ініціали, прізвище)

Додаток Е

Акт обстеження на об’єкті інформаційної діяльності автоматизованої системи класу 1 інв. № 111358760

ЗАТВЕРДЖУЮ
Директор ТОВ “ПРАЩУР”
_____ Д. О. Павлова
«20» травня 2026 р
М.П.

АКТ

обстеження на об’єкті інформаційної діяльності

автоматизованої системи класу 1 інв. № 111358760 розташованого в приміщенні № 17 кабінету Бібліотеки

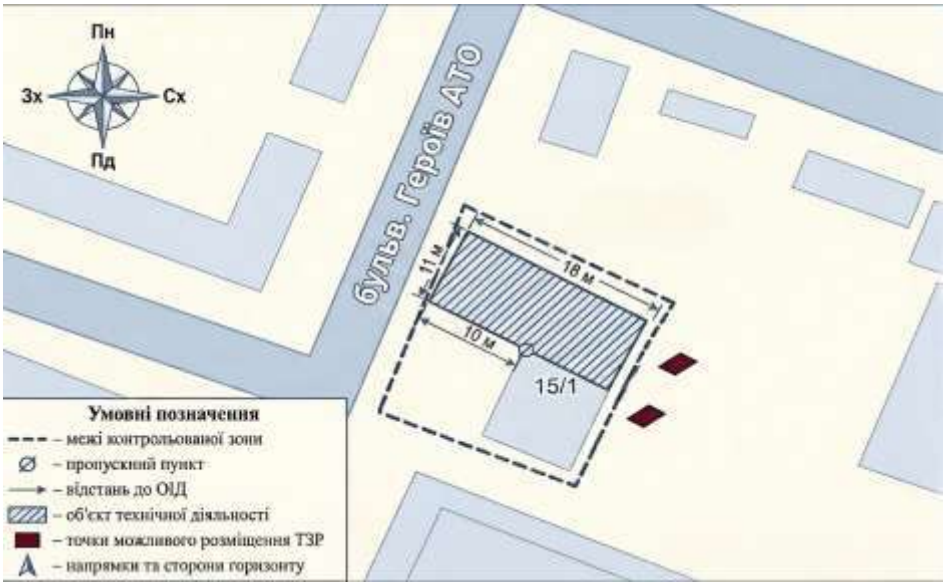
(назва, належність об'єкта інформаційної діяльності)

1. Обстеження ОІД проведено комісією у складі: голови комісії: керівника ВНД Тарасенка Євгенія Костянтиновича та членів комісії: спеціаліста з технічного захисту інформації Гуділіна Віктора Руслановича та системного адміністратора Гаєвського Валентина Віталійовича, призначеною наказом Секретаріату Кабінету Міністрів України від 12.01.2026 №01.

У цьому документі використовуються терміни та визначення згідно з ДСТУ 3396.2-97, НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу», а також такі терміни та визначення:

критична інформація	інформація, що вимагає захисту: будь-яка інформація, втрата або неправильне використання якої (модифікація, знищення, блокування, тощо) може нанести шкоду власникові інформації або АС, або будь-якій іншій фізичній (юридичній) особі чи групі осіб;
слабозв’язані об’єкти	відносно незалежні набори даних, що генеруються, модифікуються, зберігаються і обробляються в АС;
сильнозв’язані об’єкти	сукупність наборів даних, що характеризується наявністю мінімальної надлишковості і допускають їх оптимальне використання одним чи декількома процесами, як одночасно, так і в різні проміжки часу, і вимагають безумовного забезпечення цілісності цих наборів даних, як сукупності.

2. Ситуаційний план ОІД наведено на рисунку 1.



3. Опис ситуаційного плану ОІД.

ОІД знаходиться на 4 поверсі будинку за адресою: м. Київ, вул. Грушевського 12/2. Уся будівля належить Кабінету Міністрів України (далі – КМУ), бічні сторони будівлі мають сім поверхів, а середня частина - десятиповерхова та має пропускний пункт.

Межа контрольованої зони встановлена межами адміністративної будівлі КМУ.

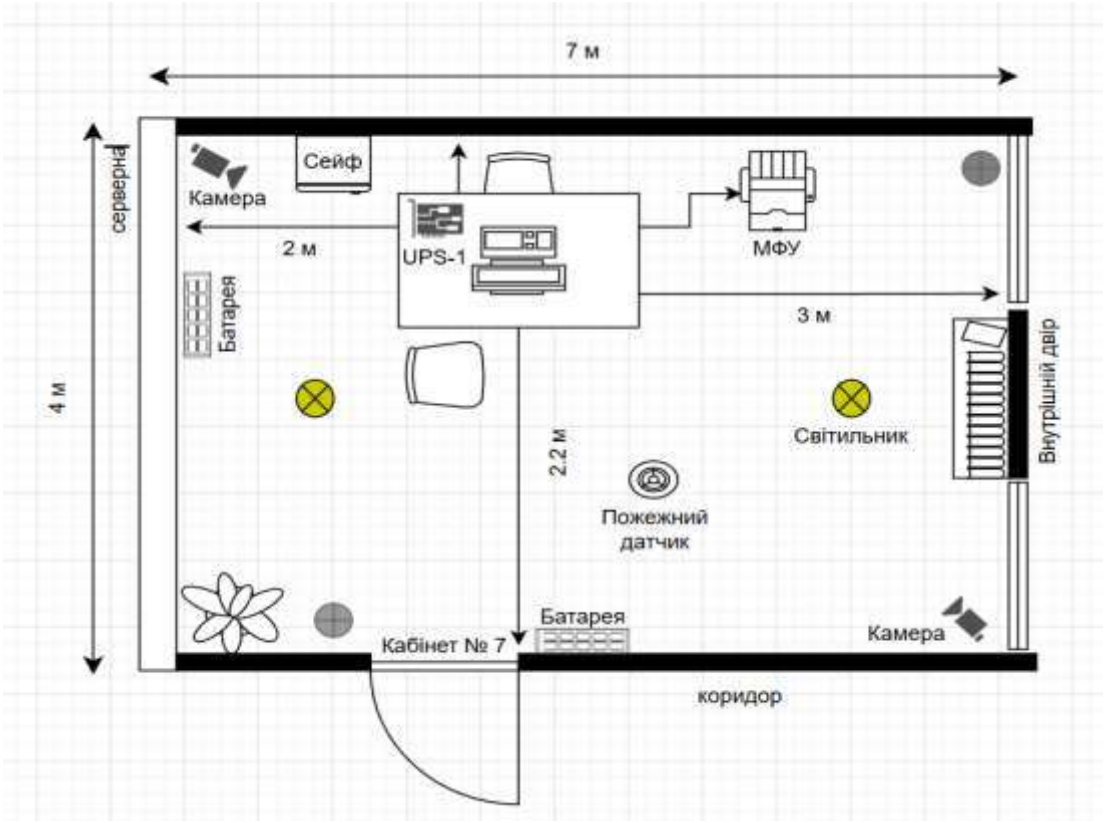
Охорона будівлі КМУ та пропускний режим забезпечується представниками підрозділу охорони КМУ. Територія навколо КМУ контролюється за допомогою системи відеоспостереження. Контроль моніторів проводиться охороною.

Відомості про будинки, будівлі та споруди, що оточують адміністративну будівлю КМУ, в якому знаходиться ОІД вказані в таблиці 1.

Таблиця 1. Об’єкти, що оточують будинок, в якому знаходиться ОІД

Розташування відносно ОІД	Кількість поверхів	Адреса	Характеристика об’єкта
північний схід	3	вул. Озерна, 8	Гкртожиток №8
схід	10	вул. Озерна 10	ОСББ «Озерний 10»
захід	5	вул. Озерна 3	Збірний пункт Хмельницького обласного військкомату
південь	10	вул. Грушевського, 12/2	ЖК Європейський

4. Генеральний план ОІД наведено на малюнку 2.



5. Опис генерального плану ОІД.

Загальна характеристика будинку, в якому розташовано ОІД.

Фундамент будинку – бетонний, стіни – цегляні. Бази колон і капітелі відлиті з чавуну. Нижні поверхи будівлі облицьовані великими необробленими блоками тульчинського лабрадориту, цоколь, пояски та портали – полірованим головинським гранітом. Перекриття між поверхами виконані з залізобетонних плит, оштукатурених. Підлога вкрита лінолеумом. Вікна – пластикові, двері – дерев'яні. АС (автоматизована система) розміщена в приміщенні кабінету №414 відділу надання допомоги Хмельницькому національному університету; вхід здійснюється з коридору 4 поверху будівлі.

Територія навколо будівлі впорядкована, має асфальтоване покриття, газони та бруківку.

Електроживлення – централізоване. Трансформаторна підстанція знаходиться за межами КЗ. Контур заземлення розташовано в межах КЗ. Пожежна сигналізація знаходиться в межах КЗ.Характеристика приміщення, в якому розташовано ОІД. Найвищий гриф, що обробляється на ОІД:

1. в електронному вигляді (в АС класу 1 «ВНД ХНУ») – конфіденційна інформація (персональні дані), інформація «Для службового користування»;
2. у мовному та електронному вигляді – відкрита інформація.

Приміщення обладнане наступними системами: електроживлення, освітлення, опалення та кондиціонування повітря.

Стіни приміщення виконані з цегли, пофарбовані у відтінок зеленого кольору. Товщина зовнішньої стіни та стіни складає 60 см. Покриття підлоги виконано з паркету. Стеля оштукатурена та пофарбована.

Наповнення вхідних дверей плита ДСП з трубчастими отворами.

Опис суміжних з ОІД приміщень.

В суміжних приміщеннях не працюють іноземні громадяни, в будівлі в цілому працюють іноземні громадяни.

Навпроти вхідних дверей в приміщення заходиться кабінет №405, в якому розташоване приміщення департаменту з питань інформації та комунікації з громадськістю. Найвищий гриф ІзОД, що обробляється в цьому приміщенні – для службового користування (у паперовому вигляді).

Суміжні кабінети №412 та №416 також використовуються департаментом з питань інформації та комунікації з громадськістю. Найвищий гриф ІзОД, що обробляється в цьому приміщенні – для службового користування (у паперовому вигляді).

Поверхом нижче (під ОІД) знаходяться службові кабінети департаменту територіального та місцевого розвитку та поверхом вище (над ОІД) знаходяться кабінети директорату публічної адміністрації. В цих приміщеннях обробляється конфіденційна інформація (персональні дані фізичних осіб) в електронному та в паперовому вигляді.

Неконтрольоване перебування сторонніх осіб не можливо в приміщеннях та коридорі, що знаходяться навколо ОІД, що належить Секретаріату Кабінету Міністрів України.

Основні та допоміжні технічні засоби.

1. Схема розташування ОТЗ наведена на Генеральному плані ОІД.
2. Опис ОТЗ та ДСТЗ.

До ОТЗ відноситься АС класу 1 «ВНД ХНУ», інв. № 111308860 (на мал. обведено пунктирним прямокутником), що складається з системного блоку, монітору, клавіатури та миші (системний блоку – під робочим столом). Лінії електроживлення АС мають вихід за межі КЗ.

3. Схема розташування ДСТЗ наведено на Генеральному плані ОІД. Перелік ДСТЗ, розміщених на ОІД, наведено в таблиці 2.

Таблиця 2. Перелік ДСТЗ, розміщених на ОІД.

Обладнання, розташоване в приміщенні	Серійний номер №	Місце розташування	К-сть, шт.
Принтер Canon	87150000598716	Кабінет №7	1
Кондиціонер Samsung	CQWJD2211	Кабінет №7	1
Настільна лампа Patrik	DK-8220 DK-8221 DK-8222	Кабінет №7	3
Системний блок Vinga	0000009854727-P002119 0000009854727-P002121	Кабінет №7	2
Монітор HP	LMN12345 LMN12346	Кабінет №7	2
Клавіатура Atech	A1B2C3D A1B2F9W	Кабінет №7	2
Миша Atech	21698-230506-05459 21698-230506-05567	Кабінет №7	2

Електроживлення ОІД здійснюється від трансформаторної підстанції, яка знаходиться за межами КЗ. Система вентиляції виходиться за межі КЗ. Система водяного опалення

складається з радіаторів і з'єднувальних труб, які виходять в суміжний кабінет.

Загальна класифікація загроз інформації, яка обробляється в АС

Під загрозою ресурсам комп'ютерної системи КМУ розуміється потенційне порушення безпеки інформації в Автоматизованій системі, чи будь-які обставини або події, що можуть бути причиною порушення політики безпеки і/або нанесення шкоди ресурсам КС.

Згідно з нормативними документами системи ТЗІ (НД ТЗІ 1.1-002-99, 1.4-001-2000) за результатом впливу на інформацію та автоматизовану систему її обробки, загрози для АС поділяються на чотири класи:

– порушення конфіденційності інформації – одержання інформації користувачами або процесами всупереч встановлених правил доступу;

– порушення цілісності інформації – повне або часткове знищення інформації, її викривлення або модифікація, нав'язування хибної інформації тощо;

– порушення доступності інформації – повна або часткова втрата працездатності системи, блокування доступу до інформації;

– втрата спостереженості або керованості системи обробки – порушення процедур ідентифікації та автентифікації користувачів і процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від одержання або пересилання повідомлень.

За типом основного засобу, який використовується для реалізації загрози, всі джерела загроз поділяються на такі групи:

– людина (співробітник КМУ, відвідувач);
– апаратура (основні та допоміжні технічні засоби і системи);
– програма;
– фізичне середовище.

Можливими каналами загроз ресурсам КС КМУ, які призначені для обробки службової та конфіденційної інформації, до яких відноситься й ОТЗ, що розташовані на ОІД, є канали та способи несанкціонованого доступу шляхом маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

Основними видами загроз ресурсам КС КМУ можуть бути:

– зміна умов фізичного середовища (стихійні лиха (землетрус, повінь, ураган), пожежа або інші випадкові події);

– збої та відмови у роботі обладнання та технічних засобів КС;

– наслідки помилок під час проектування та розробки компонентів КС КМУ (технічних засобів, технології обробки інформації, програмних засобів захисту, структур даних тощо);

– помилки під час експлуатації (персоналу, користувачів КС);

– навмисні дії порушників (спроби НСД).

Навмисні (у тому числі і пов'язані з діяльністю зареєстрованих користувачів) загрози з боку зловмисників спрямовуються на дезорганізацію роботи КС (її окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості НСД до її ресурсів.

Загрози, пов'язані з діяльністю зареєстрованих користувачів, у свою чергу можуть розподілятись на випадкові чи навмисні. Зрозуміло, що кожна із загроз здійснюється з деякою ймовірністю, може порушувати ту чи іншу функціональну властивість захищеної системи, має своїм наслідком (особливо навмисні загрози) певні втрати (шкоду) та джерело виникнення чи

активізації.

Перелік можливих загроз інформації, яка обробляється в АС та циркулює у відповідних приміщеннях, наводиться в таблиці 3.

Умовні позначення такі:

К – порушення конфіденційності інформації;

Ц – порушення цілісності інформації, програмного забезпечення, системних даних, даних реєстрації;

Д – порушення можливості доступу до інформації, системних даних, даних реєстрації;

С – порушення спостереженості, керованості процесу оброблення інформації.

Таблиця 3. Перелік загроз інформації для АС та оцінка можливої шкоди від їх реалізації

№	Види загроз	Рівень ризику	К	Ц	Д	С
1. Зовнішні загрози						
1.1	Стихійні явища (землетруси, урагани, пожежі)	середній		+	+	+
1.2	Збої та відмови системи електроживлення	низький		+	+	+
1.3	Ураження ПЗ комп'ютерними вірусами	високий	+	+	+	+
1.4	Використання системи з корисливою метою персоналу АС	високий	+	+	+	+
1.5	НСД до приміщення АС	середній	+	+	+	+
1.6	Вербування працівників КМУ	середній	+	+		
1.7	Розкрадання матеріальних носії інформації	високий	+	+		
2. Внутрішні загрози						
2.1	Збої та відмови ЕОТ	середній		+	+	
2.2	Збої, відмови та пошкодження носіїв інформації	середній		+	+	
2.3	Збої та відмови ПЗ	середній		+	+	
2.4	Відмова в доступі санкціонованому користувачу в результаті помилки ПЗ	низький			+	
2.5	Несанкціоноване внесення змін до технічних засобів, в ПЗ, що призводить до зміни роботи чи відмови АС	низький		+	+	+
2.6	Порушення адміністратором безпеки, системним адміністратором, спеціалістом з ТЗІ реалізації безпеки програмних рішень	середній	+	+	+	+
2.7	Неправомірне впровадження і використання забороненого політикою безпеки ПЗ	низький	+	+	+	+
2.8	Викрадення носіїв інформації	високий	+	+		
2.9	Читання залишеної інформації	низький	+			
2.10	Ненавмисне псування матеріальних носіїв інформації	низький			+	

АС призначена для обробки інформації, яка має гриф обмеження доступу не вище ніж «для службового користування» та «конфіденційна інформація». Згідно з НД ТЗІ вимоги щодо захисту такої інформації від витоку технічними каналами не висуваються. В зв'язку з цим, технічні канали витоку в даній Моделі загроз не розглядаються.

2. Модель порушника оцінюватимемо за такими критеріями:

1. Категорія порушника представлена у таблиці 4.

Таблиця 4. Категорії порушників

Позначення	Визначення категорії	Рівень загроз
Внутрішні порушники		
ВП 1	Технічний персонал (прибиральники, охоронці, електрики тощо)	1
ВП 2	Користувачі АС	2
ВП 3	Персонал, який обслуговує технічні засоби (інженери тощо)	2
ВП 4	Співробітники служби захисту інформації, керівники різних рівнів	4
Зовнішні порушники		
ЗП 1	Відвідувачі запрошені з будь-якого приводу	1
ЗП 2	Хакери	3

2. Мотив:

Основні мотиви порушень представлені у таблиці 5.

Таблиця 5. Мотиви порушень

Позначення	Мотив порушення	Рівень загроз
М 1	Безвідповідальність	1
М 2	Самоствердження	2
М 3	Корислива мета	3
М 4	Професійний обов’язок	4

3. Рівень обізнаності:

Основні кваліфікаційні ознаки порушника представлені у таблиці 6.

Таблиця 6. Рівні обізнаності

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К 1	Порушник володіє низьким рівнем знань, проте вміє працювати з технічними засобами АС	1
К 2	Порушник володіє середнім рівнем знань та практичними навичками роботи з технічними засобами АС та їх обслуговування	2
К 3	Порушник володіє високим рівнем знань у програмуванні та обчислювальної техніки, проєктування та експлуатації АС	3
К 4	Порушник знає структуру, функції та механізми дії засобів захисту інформації в АС, їх недоліки та можливості	4

4. Доступність:

Можливість доступу до АС порушника наведено у таблиці

Таблиця 7. Доступність до АС

Позначення	Доступність	Рівень загроз
Д 1	Дуже низька: доступ практично неможливий або вимагає особливих обставин	1
Д 2	Низька: доступ ускладнений і потребує значних зусиль	2
Д 3	Середня: доступ є, але вимагає певних зусиль	3
Д 4	Висока: легкий доступ до системи	4

Критерії оцінюють рівень загрози за шкалою від 1 до 4, де 1 – мінімальна загроза; 2 – загроза з незначними наслідками; 3 – можлива загроза з серйозними наслідками; 4 – максимальна загроза.

У КСЗІ на ОІД передбачаються, розглядаються і розробляються усі чотири рівні

загроз.

Модель порушника наведена у таблиці 8.

Таблиця 8. Модель порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності	Доступність	Сума загроз
Користувач	ВП 2	М 1, М 3	К 3	Д 4	13
Адміністратор безпеки	ВП 4	М 3	К 4	Д 4	15
Системний адміністратор	ВП 4	М 3	К 4	Д 4	15
Спеціаліст з ТЗІ	ВП 4	М 3	К 4	Д 4	15
Керівник відділу	ВП 4	М 1	К 4	Д 4	13
Електрик	ВП 1	М 1	К 2	Д 2	6
Прибиральник	ВП 1	М 3	К 1	Д 3	8
Охоронець	ВП 1	М 3	К 1	Д 2	7
Відвідувач	ЗП 1	М 3	К 1	Д 1	6
Хакер	ЗП 2	М 4	К 4	Д 1	11

Відповідно до останньої колонки таблиці 8 найбільше можливості нанести шкоди є у адміністратора безпеки, системного адміністратора та спеціаліста з ТЗІ, а отже робота даних осіб повинна постійно контролюватися, адже вони є потенційними порушниками безпеки інформації та мають можливість викрасти, модифікувати та видалити важливу інформацію, яка обробляється в АС.

Відповідальний за ТЗІ Б.І. Романенко

14.05.2026

Додаток Ж

Технічне завдання на створення комплексної системи захисту інформації в автоматизованій системі класу «1»

ЗАТВЕРДЖУЮ
Директор ТОВ “ПРАЩУР”
_____ Д. О. Павлова
«20» травня 2026 р

ТЕХНІЧНЕ ЗАВДАННЯ
для інформації, яка обробляється на об’єкті інформаційної діяльності
ТОВ “ПРАЩУР”
(назва установи, організації, підприємства)

Автоматизована система класу 1

м. Хмельницький, бул. Героїв АТО 8,
(місце розташування ОІД)

1. Перелік скорочень

АПЗ – Апаратно – програмний засіб
ДСТУ – Державний стандарт України
КЗЗ – Комплекс засобів захисту
КЗІ – Криптографічний захист інформації КМУ – Кабінет Міністрів України
КСЗІ – Комплексна система захисту інформації ЛОМ – локальна обчислювальна мережа
НЖМД – накопичувач на жорсткому магнітному диску НД – Нормативний документ
НСД – Несанкціонований доступ ОП – Оперативна пам'ять
ОС – Операційна система
ПЕОМ – Персональна електронно-обчислювальна машина ПЗ – Програмне забезпечення
ПК – Програмний комплекс РС – Робоча станція
СЗІ – Служба захисту інформації
СКМУ – Секретаріат Кабінету Міністрів України ТЗ – Технічне завдання
ТЗІ – Технічний захист інформації ФС – Файлова система

2. Терміни та визначення

У цьому ТЗ використовуються терміни та визначення згідно з ДСТУ 3396.2-97, НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», а також такі терміни та визначення:

– критична інформація – інформація, що вимагає захисту; будь-яка інформація, втрата або неправильне використання якої (модифікація, ознайомлення) може нанести шкоду власникові інформації або АС, або будь-якій іншій фізичній (юридичній) особі чи групі осіб;
– слабозв'язані об'єкти – відносно незалежні набори даних, що генеруються,
– модифікуються, зберігаються і обробляються в АС;
– сильнозв'язані об'єкти – сукупність наборів даних, що характеризується наявністю мінімальної надлишковості і допускають їх оптимальне використання одним чи декількома процесами як одночасно, так і в різні проміжки часу і вимагають безумовного забезпечення цілісності цих наборів даних як сукупності.

3. Загальні відомості

Це технічне завдання визначає вимоги до комплексу організаційних та технічних заходів щодо забезпечення захисту інформації в автоматизованій системі (АС) класу «1» відділу надання допомоги Хмельницькому національному університету.

Умовне позначення автоматизованої системи: АС БХТЛ.

Замовник – виконавець: ТОВ ПРАЩУР

Юридична адреса: 26005, місто Хмельницький, бульвар Героїв АТО, будинок 8. Код ЄДРПОУ: 00019442.

Початок робіт: розробка КСЗІ розпочинається з моменту призначення відповідального за технічний захист інформації.

Підстава для розробки: КСЗІ створюється 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 затверджене указом Президента України

№1229/99 від 27.09.1999 та Правил забезпечення захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах затвердженого постановою Кабінету Міністрів України №373 від 29.03.2006.

Фінансування роботи здійснюється за рахунок: джерелом фінансування робіт зі створення КСЗІ є кошти відділу надання допомоги Хмельницькому національному університету, де створюється КСЗІ.

Технічне завдання на комплексну систему захисту інформації оформлено відповідно до НД ТЗІ 3.7-001-99.

Мета й призначення комплексної системи захисту інформації

Метою створення комплексної системи захисту інформації (КСЗІ) в автоматизованій системі класу «1» є захист інформації з обмеженим доступом, вимога щодо захисту якої

встановлена законом, в процесі оброблення її засобами АС від загроз порушення конфіденційності, цілісності, доступності та спостереженості.

При розробці та впровадженні КСЗІ повинні бути враховані існуючі тенденції розвитку захищених інформаційних технологій, розробки відповідних засобів захисту інформації.

Для здійснення захисту інформації на всіх стадіях життєвого циклу у КСЗІ має бути передбачено застосування наступних заходів та засобів захисту інформації:

1. організаційно-правові заходи, які реалізуються поза обчислювальною системою БХТЛ;
2. програмні засоби (комплекси) захисту від несанкціонованого доступу до інформації, яка обробляється та зберігається в АС БХТЛ;
3. апаратні (або апаратно-програмні) та програмні засоби (комплекси) криптографічного захисту інформації.

Процес оброблення інформації складається з таких технологічних етапів:

1. Виготовлення документів за допомогою ПЕОМ; зберігання інформації на носіях: НЖМД, вбудовані в ПЕОМ, знімні НЖМД, ГМД, оптичні диски та носії типу USB-flash; копіювання інформації на знімні носії та між двома знімними носіями; друкування документів на принтері.
2. Функціональне призначення КСЗІ КСЗІ призначена для:

– реалізації політики безпеки інформації;
– ідентифікації та автентифікації користувачів;
– забезпечення цілісності та доступності відкритої інформації, що обробляється, а також конфіденційності та цілісності конфіденційної інформації (персональних даних);

4. створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації та оперативного оповіщення працівників служби захисту інформації про факти несанкціонованого доступу до інформації;
5. ефективного попередження, своєчасного виявлення та знешкодження загроз для ресурсів обчислювальної системи , причин та умов, які спричиняють або можуть призвести до порушення її нормального функціонування;
6. керування засобами захисту інформації, розмежування доступу користувачів до ресурсів АС, контроль за їхньою роботою з боку осіб, які відповідають за забезпечення безпеки інформації;

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 облікові 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

5. Вимоги до комплексної системи захисту інформації

1. Загальні вимоги

Конфігурація ПЕОМ, що входить до складу АС, повинна відповідати функціональному призначенню. Непотрібні пристрої знімаються (демонтуються) або фізично відключаються.

Робота АС у штатних режимах повинна бути можливою лише за умови функціонування системи захисту інформації.

Розташування, монтаж та прокладку інженерно-технічних комунікацій АС, в тому числі систем заземлення та електроживлення технічних засобів, які приймають участь у обробці інформації, необхідно виконувати з дотриманням вимог відповідних стандартів та нормативних документів системи ТЗІ.

Неформалізована «Модель загроз» та «План захисту інформації», які розроблені із врахуванням результатів обстеження середовища функціонування, технічних засобів та систем забезпечення інформаційної діяльності АС, включають:

1. ситуаційний план розташування структурних елементів АС із зазначенням місць розташування технічних засобів та систем обробки інформації і життєзабезпечення, джерел електроживлення, контурів заземлення, енергетичних мереж, а також інженерних комунікацій, що виходять за межі зони безпеки інформації;
2. опис можливих способів реалізації несанкціонованого доступу до інформації;
3. політику безпеки інформації;
4. оцінку обсягів можливих збитків від реалізації загроз безпеці інформації.

Для реалізації частини політики безпеки інформації, яка покладається на технічні заходи і відповідає реальній моделі загроз, КЗЗ повинен мати такі функціональні можливості:

5. забезпечення входу в систему та завантаження операційної системи за умови введення особистого паролю;
6. контроль за інсталяцією програмного забезпечення;
7. контроль за виведенням інформації на носії, що вилучаються;
8. реєстрація дій користувачів по відношенню до ресурсів системи;
9. забезпечення цілісності інформаційних ресурсів (у тому числі і антивірусний захист);
10. перевірка цілісності та працездатності КСЗІ;
11. надання користувачам прав доступу до ресурсів АС згідно з прийнятою політикою безпеки, та їх ліквідація по закінченню строку дії;
12. багаторівневе розмежування повноважень персоналу АС по відношенню до ресурсів АС;
13. контроль за запуском процесів та їх виконанням;
14. автоматичне блокування екрану робочої станції на час відсутності користувача;
15. автоматизований облік завдань, які сформовані для принтерів системи.

Виконання завдань повинне здійснюватися зареєстрованими користувачами у функціонально замкненому середовищі із забезпеченням доступу до ресурсів, що обмежені рамками завдань.

Інформація, яка оброблюється в АС, за змістом вимог щодо захисту підрозділяється на такі групи:

16. дані та програмні коди у вигляді файлів різних форматів, записів баз даних та інших структур машинного представлення, які містять ІЗОД;
17. бази даних захисту (списки зареєстрованих користувачів, їх ідентифікаторів, повноважень користувачів, права доступу, журнали реєстрації подій комплексу засобів захисту та ін.);
18. дані загального користування.

КСЗІ повинна забезпечувати підтримку не менше 4 рівнів повноважень користувачів (адміністратор безпеки – особа, що має повноваження щодо встановлення та керування комплексом засобів захисту інформації, системний адміністратор – особа, що має повноваження щодо встановлення

програмного забезпечення, спеціаліст з ТЗІ – особа, що має повноваження щодо впровадження криптографічного захисту інформації, користувач – особа, чиї повноваження обмежені функціями, необхідними для роботи із захищеними даними);

Комплексна система захисту інформації повинна реалізовуватися як сукупність узгоджених за часом та місцем застосування організаційних, підготовчих технічних і технічних заходів.

Організаційні заходи повинні включати:

19. визначення та встановлення обов'язків із захисту інформації осіб, що приймають участь в обробці інформації;
20. визначення технологічних процесів обробки інформації з урахуванням вимог із захисту інформації;
21. встановлення порядку впровадження та модернізації засобів обробки інформації, програмних та технічних засобів захисту інформації;
22. організацію фізичного та протипожежного захисту АС;
23. розробку правил та порядку контролю функціонування КСЗІ.

Під час створення КЗЗ для забезпечення вимог щодо захисту інформації повинні використовуватися засоби технічного захисту інформації з «Переліку засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України».

1. Вимоги до КСЗІ в частині захисту від несанкціонованого доступу

Нейтралізація загроз несанкціонованого доступу до інформації в АС повинна забезпечуватися реалізацією КЗЗ політики функціональних послуг, які визначаються профілем захищеності АС від НСД.

Усі запити користувачів на доступ до об'єктів захисту повинні оброблятися КЗЗ. Доступ до пасивного об'єкту захисту має дозволятися/заборонятися згідно правил розмежування доступу за результатами порівняння атрибутів доступу об'єкта-користувача та призначених йому прав.

При розмежуванні доступу до об'єктів захисту, що обробляються використовується адміністративний принцип керування доступом. Адміністратор надає доступ об'єкту- користувачу до об'єкта захисту, тільки якщо: у асоційованому списку об'єкта захисту для об'єкта-користувача (або ролі до якої він входить) у явному вигляді надано необхідний вид доступу та відсутні заборони на здійснення необхідного виду доступу.

Реалізація політики функціональних послуг та виконання основних функцій АС здійснюється за участю активних та пасивних об'єктів.

До активних об'єктів відносяться користувачі АС. Користувачі АС поділяються за функціональними обов'язками на:

1. адміністратори безпеки;
2. системні адміністратори;
3. спеціалісти з технічного захисту інформації;
4. користувач.

До пасивних об'єктів відносяться:

5. процеси;
6. файлова система;
7. програмне забезпечення ;
8. пристрої введення/виведення (НГМД, CD ROM, FDD, порти USB, принтер, монітор, клавіатура).

Основними атрибутами доступу користувачів є:

1. ім'я користувача (групи користувачів);
2. пароль.

3. Для реалізації необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в АС, обрано рекомендований НД ТЗІ 2.5-005-99 КЗЗ профіль захищеності: {КА- 2, КД-2, КО-1, ЦА-2, ЦО-2, ДВ-3, НР-2, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1}.

Вимоги до функціональних послуг:

КА-2. Базова адміністративна конфіденційність

Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

КД-2. Базова довірча конфіденційність

Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

КО-1. Повторне використання об’єктів.

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

ЦА-2. Базова адміністративна цілісність.

Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

ЦО-2. Повний відкат.

Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити всі операції, виконані над захищеним об'єктом за певний проміжок часу.

ЦВ-1. Мінімальна цілісність при обміні.

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається.

ДВ-3. Вибіркове відновлення

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС.

Після будь-якої відмови КС або переривання обслуговування, що не призводить до необхідності заново інсталювати КС, КЗЗ повинен бути здатним виконати необхідні процедури і безпечним чином повернути КС до нормального функціонування або, в гіршому випадку, функціонування в режимі з погіршеними характеристиками обслуговування.

Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС з режиму з погіршеними характеристиками обслуговування в режим нормального функціонування.

НР-2. Захищений журнал

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються.

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

НИ-2. Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Однонаправлений достовірний канал

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ.

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО-3. Розподіл обов’язків на підставі привілеїв

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

Політика розподілу обов'язків повинна визначати множину ролей користувачів.

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

НЦ-2. КЗЗ з гарантованою цілісністю

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів.

КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх

впливів і несанкціонованої модифікації і/або втрати керування.

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НТ-2. Самотестування при старті

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

НВ-1. Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ.

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

2. Вимоги до гарантій

Рівень гарантій реалізації функціонального профілю має бути не нижчим за Г-2. Специфікація рівнів критеріїв гарантій наведена в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

1. Вимоги до гарантій архітектури КЗЗ

Архітектура КЗЗ повинна бути у змозі повністю реалізувати обрану політику безпеки і складатися із достатньо визначених і максимально незалежних програмних компонентів (модулів), які ідентифікуються.

Структура модулів повинна дозволяти тестування КЗЗ на рівні функціонально-завершених вузлів.

2. Вимоги до гарантій середовища розробки та керування конфігурацією.

Мають бути визначені всі стадії та етапи життєвого циклу АС, а для кожної стадії та етапу – перелік і обсяги необхідних робіт та порядок їх виконання. Якщо для якихось робіт вимагається створення особливих умов – це повинно бути визначено окремо. Всі стадії та етапи робіт повинні бути задокументовані. Види та зміст документів встановлено державними стандартами.

На всіх стадіях життєвого циклу повинні існувати процедури керування конфігурацією АС. Ці процедури повинні визначати технологію відслідковування та внесення змін в апаратне та програмне забезпечення КСЗІ, тестове покриття і документацію та гарантувати, що без дотримання цієї технології ніякі зміни не можуть бути внесені. Технологія відслідковування та внесення змін повинна гарантувати постійну відповідність між документацією й реалізацією поточної версії КЗЗ (інших компонентів КСЗІ).

3. Послідовність розробки

На стадії виконання технічного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними.

Документально оформити методики діяльності на кожному етапі життєвого циклу та умови переходу від одного етапу до наступного. Необхідно визначити процедури внесення змін та фіксувати всі зміни на кожному етапі.

4. Вимоги до гарантій середовища функціонування

Розробник повинен представити засоби інсталяції, генерації і запуску АС, які гарантують, що експлуатація АС починається з безпечного стану. Розробник повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску.

Повинна існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ, що поставляється Замовнику, точно відповідає еталонній копії.

5. Вимоги до гарантій експлуатаційної документації

Розробник повинен надати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратора щодо послуг безпеки, настанови користувача щодо послуг безпеки у вигляді окремих документів або розділів (підрозділів) інших документів.

В опису функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ, а також самі послуги.

Настанови адміністратора, системного адміністратора, спеціаліста з ТЗІ щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску АС, опис усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску АС, опис властивостей АС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує АС.

Настанови користувача щодо послуг безпеки мають містити інструкції стосовно використання функцій безпеки звичайним користувачем (не адміністратором).

Настанови адміністратора, системного адміністратора, спеціаліста з ТЗІ і настанови користувача можуть бути об'єднані в настанови з установлення та експлуатації.

6. Вимоги до гарантій випробувань комплексу засобів захисту

КЗЗ повинен відповідати вимогам чинного законодавства та нормативних документів, а також повинен мати обов'язковим чинний експертний висновок від Державної служби спеціального зв'язку та захисту інформації України.

11. Вимоги до складу проектної та експлуатаційної документації КСЗІ

Проектна документація на комплексну систему захисту інформації повинна включати:

1. Акт категоріювання об'єкта ЕОТ (автоматизованої системи класу 1 інв. № 111308860) розташованого в приміщенні №414 відділу надання допомоги ХНУ.

2. Акт категоріювання ОІД (приміщення №414 відділу надання допомоги Хмельницькому національному університету).

3. Положення про службу захисту інформації в автоматизованій системі класу «1» відділу надання допомоги Хмельницькому національному університету.

4. Акт обстеження на об'єкті інформаційної діяльності автоматизованої системи класу «1» інв. №111308860, приміщення №414 відділу надання допомоги Хмельницькому національному університету.

5. Модель загроз для інформації, яка обробляється на об'єкті інформаційної діяльності №414 відділу надання допомоги Хмельницькому національному університету.

6. План захисту інформації, що обробляється в автоматизованій системі класу 1 об'єкту інформаційної діяльності №414 відділу надання допомоги Хмельницькому національному університету.

7. Календарний план робіт із захисту інформації в АС класу «1» відділу надання допомоги Хмельницькому національному університету.

8. Технічне завдання на створення комплексної системи захисту інформації в автоматизованій системі класу «1» об'єкту інформаційної діяльності №414 відділу надання допомоги Хмельницькому національному університету.

9. Інструкція щодо забезпечення правил оброблення ІзОД в АС класу «1» відділу надання допомоги Хмельницькому національному університету.

10. Інструкція про порядок введення в експлуатацію КСЗІ.

11. Інструкція про порядок модернізації КЗСІ.

12. Інструкція про порядок резервування та відновлення інформації в АС.

13. Інструкція про порядок оперативного відновлення функціонування АС.

14. Інструкція про порядок проведення ремонтних робіт.

15. Інструкція про організацію контролю за функціонуванням КСЗІ.

16. Інструкція про порядок розроблення, впровадження та модернізації програмного забезпечення АС.

17. Інструкція про порядок реєстрації користувачів АС.

18. Інструкція про порядок створення захищених інформаційних ресурсів в АС.

19. Інструкція про порядок надання доступу до захищених інформаційних ресурсів в АС.

20. Інструкція про порядок забезпечення антивірусного захисту в АС.

21. Інструкція по правилам видачі, вилучення та обліку персональних ідентифікаторів користувачів АС.

22. Інструкція із забезпечення безпеки експлуатації засобів КЗІ.

23. Інструкція щодо порядку генерації ключових даних та поводження з ключовими документами.

24. Етапи виконання робіт

1. Проектування та створення КСЗІ.

2. Розробка робочої документації на КСЗІ.
3. Проведення попередніх випробувань КСЗІ.
4. Відпрацювання КСЗІ в процесі дослідної експлуатації.
5. Проведення приймальних випробовувань КСЗІ.
6. Підготовка персоналу.
7. Проведення експертизи КСЗІ та отримання «Атестату відповідності».

25.Порядок внесення змін і доповнень до ТЗ Зміни та доповнення до розділів ТЗ на комплексну систему захисту інформації в АС

оформлюються окремим доповненням, яке погоджується та затверджується у порядку погодження та затвердження самого ТЗ.

26.Порядок проведення випробувань комплексної системи захисту інформації

1. Об'єктом випробувань є КСЗІ.

Метою випробувань є визначення відповідності досягнутого в КСЗІ рівня захищеності інформації вимогам ТЗ і визначення готовності до експлуатації.

2. Випробування КСЗІ здійснюється з врахуванням змісту етапів та черговості виконання робіт з побудови КСЗІ.

3. Проводяться наступні види випробувань: попередні, дослідна експлуатація, державна експертиза КСЗІ.

4. Попередні випробування КСЗІ проводить комісія, яка призначається наказом керівника установи, де створюється КСЗІ, відповідно до затвердженої встановленим порядком програми та методики випробувань. Обсяг випробувань повинен бути достатнім для оцінки всіх показників захисту інформації і вказується в програмі випробувань. За результатами попередніх випробувань складається акт, у якому зазначаються результати випробувань і дається висновок щодо можливості впровадження КСЗІ у дослідну експлуатацію.

5. КСЗІ вводиться у дослідну експлуатацію згідно з наказом керівника, де створюється КСЗІ. Для КСЗІ, що створюється у ході виконання робіт другої черги, після завершення дослідної експлуатації складається акт, у якому наведені результати дослідної експлуатації і дається висновок про можливість представлення КСЗІ на державну експертизу. Для КСЗІ, що створюється у ході виконання робіт третьої черги, після завершення дослідної експлуатації складається акт відповідності введеного в експлуатацію АС організаційно- технічному рішенню «КСЗІ, що знаходиться у розпорядженні (володінні) організації». Затверджені «Акт відповідності» та відповідні протоколи випробувань є підставою для вводу КСЗІ , що створений на конкретному об’єкті інформаційної діяльності організації в експлуатацію.

6. Державна експертиза КСЗІ здійснюється організатором експертизи відповідно до

«Положення про державну експертизу в сфері технічного захисту інформації», яке затверджено наказом ДССЗЗІ України від 16.05.2007 р. № 93 (із змінами затвердженими наказом Адміністрації Держспецзв’язку України від 10.10.2012 р. № 567).

Відповідальний за ТЗІ Б.І. Романенко

20.05.2026