НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Волощук Михайло Володимирович

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: к.фіз.-мат.н., доцент
Черевко Євген Володимирович

Одеса – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
___ _____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Волощуку Михайлу Володимировичу

1. Тема роботи: «Методи захисту інформації в комп'ютерних системах від несанкціонованого доступу»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
затверджені наказом НУ ОЮА від «18» березня 2025 року № 548-6
2. Строк подання здобувачем роботи «19» травня 2025 року
3. Дата видачі завдання «16» вересня 2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Методи захисту інформації в комп'ютерних системах від несанкціонованого доступу» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125. Кібербезпека, освітньою програмою: Кібербезпека.

Кваліфікаційна робота містить 19 рисунків, 3 таблиці, 18 літературних джерел за переліком посилань. Робота виконана на 44 сторінках загального тексту і 37 сторінках основного тексту.

Метою роботи є аналіз методів захисту інформації від несанкціонованого доступу в комп'ютерних системах.

Розглянуто сучасні загрози інформаційній безпеці, міжнародні стандарти, а також нормативно-правову базу України у сфері кібербезпеки. У роботі проаналізовано ключові концепції побудови систем захисту, моделі управління доступом та механізми автентифікації. Надано порівняльну характеристику інструментів моніторингу та виявлення спроб несанкціонованого доступу, таких як IDS та IPS.

Практична частина роботи включає реалізацію окремих засобів захисту: шифрування даних за допомогою BitLocker, впровадження двофакторної автентифікації для SSH-доступу та використання Fail2Ban для блокування підозрілої активності. Проведено оцінку ефективності застосованих рішень в умовах сучасної кіберзагрозової обстановки.

Результати роботи можуть бути використані для підвищення рівня інформаційної безпеки у державних, корпоративних і приватних IT-системах.

ІНФОРМАЦІЙНА БЕЗПЕКА, НЕСАНКЦІОНОВАНИЙ ДОСТУП, МЕТОДИ ЗАХИСТУ, АВТЕНТИФІКАЦІЯ, КОНТРОЛЬ ДОСТУПУ КІБЕРЗАХИСТ

ABSTRACT

Qualification work on the topic "Methods of protecting information in computer systems from unauthorized access" for obtaining the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity.

Qualification work contains 19 figures, 3 tables, 18 literary sources according to the list of references. The work is performed on 44 pages of general text and 37 pages of the main text.

The purpose of the work is to analyze methods of protecting information from unauthorized access in computer systems.

Modern threats to information security, international standards, as well as the regulatory and legal framework of Ukraine in the field of cybersecurity are considered. The work analyzes key concepts for building protection systems, access management models and authentication mechanisms. A comparative characteristic of monitoring tools and detection of unauthorized access attempts, such as IDS and IPS, is provided.

The practical part of the work includes the implementation of individual security measures: data encryption using BitLocker, the implementation of two-factor authentication for SSH access and the use of Fail2Ban to block suspicious activity. The effectiveness of the applied solutions in the conditions of the modern cyber threat environment was assessed.

The results of the work can be used to increase the level of information security in public, corporate and private IT systems.

INFORMATION SECURITY, UNAUTHORIZED ACCESS, PROTECTION METHODS, AUTHENTICATION, ACCESS CONTROL CYBER SECURITY

ЗМІСТ

ВСТУП

У сучасному цифровому світі інформація є одним з найцінніших ресурсів. Її зберігання, обробка та передача здійснюються за допомогою комп'ютерних систем, які щодня зазнають численних кіберзагроз. Однією з найпоширеніших і найнебезпечніших є загроза несанкціонованого доступу (НСД) до інформаційних ресурсів. Витоки даних, втручання у функціонування систем, крадіжки персональної або комерційної інформації – все це наслідки таких дій.

З огляду на динамічний розвиток IT-сфери та зростання кількості атак, питання захисту комп'ютерних систем від несанкціонованого доступу є надзвичайно актуальним як для бізнесу, так і для державних установ та приватних осіб.

Метою дипломної роботи є аналіз існуючих методів захисту інформації від несанкціонованого доступу в комп'ютерних системах, а також формування практичних рекомендацій щодо їх ефективного застосування.

Для досягнення поставленої мети необхідно вирішити такі завдання:
дослідити основні поняття та класифікації загроз інформаційній безпеці; розглянути нормативно-правову базу, яка регулює захист інформації; проаналізувати сучасні методи захисту від НСД: криптографічні, мережеві, програмні, організаційні; провести порівняльний аналіз ефективності обраних методів; сформулювати висновки та рекомендації щодо їх використання в різних умовах.

Об'єктом дослідження є комп'ютерні системи, які потребують захисту від несанкціонованого доступу. Предметом дослідження є методи та засоби захисту інформації в таких системах, включаючи технічні, програмні та організаційні рішення.

Під час написання роботи застосовувалися теоретичні методи (аналіз, класифікація, порівняння), а також вивчення прикладів практичного застосування захисних технологій та їх ефективності в різних умовах.

Робота містить комплексне дослідження сучасних підходів до захисту інформації в умовах зростаючих кіберзагроз. Практичне значення полягає в систематизації знань про методи захисту, а також у формуванні рекомендацій, які можуть бути використані фахівцями з кібербезпеки, IT-адміністраторами та розробниками безпечних систем.

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

1.1 Поняття інформаційної безпеки

У сучасному суспільстві інформаційні дані набули значення одного із ключових ресурсів. Вони використовуються в державному управлінні, бізнесі, науці, медицині, обороні, освіті та звичайному житті. Втрата, викривлення або несанкціонований доступ до важливої інформації може призвести до серйозних наслідків, наприклад, фінансових збитків, загрозі національної безпеки, порушення репутації, зупинки бізнес-процесів, тощо. Саме тому питання забезпечення інформаційної безпеки є одним із пріоритетних у нашу цифрову епоху.

Історично проблема захисту інформації виникла ще задовго до появи комп'ютерних систем. Перші відомі криптографічні методи – шифр Цезаря використовувалися ще в давньоримські часи для збереження секретності військових повідомлень. З розвитком комп'ютерної техніки з'явилися нові виклики: несанкціонований доступ до даних, комп'ютерні віруси, кібершпигунство, цифрове шахрайство. Тому важливо розуміти що це так, отже розберемо головні та основні поняття щодо інформації та її безпеки.

Інформаційна безпека – це стан захищеності інформації та інформаційної інфраструктури, при якому забезпечується цілісність, конфіденційність, доступність і, за потреби, автентичність даних, а також протидія загрозам, що можуть виникнути внаслідок навмисних або випадкових дій. Основу сучасної парадигми ІБ складає модель CIA-тріади, основні компоненти якої показано на рисунку 1.1. Розберемо значення кожного з них [1].

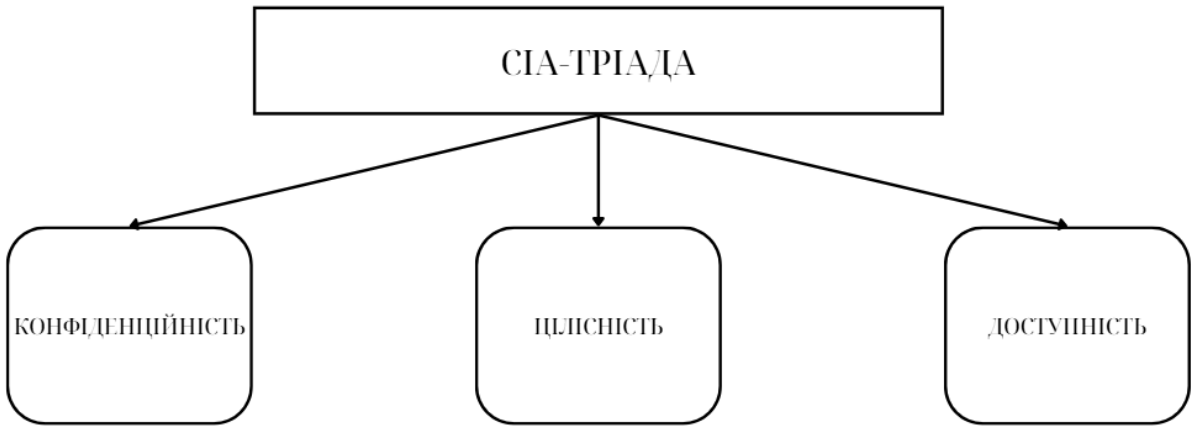

Рисунок 1.1 – Схема CIA-тріади

1. Конфіденційність передбачає захист інформації таким чином, щоб доступ до неї мали виключно авторизовані користувачі. Це означає, що дані необхідно убезпечити від несанкціонованого перегляду, копіювання або розголошення. Досягнення конфіденційності забезпечується застосуванням засобів шифрування, систем автентифікації та управління доступом.

2. Цілісність інформації вимагає гарантій того, що дані залишаються незмінними і не були модифіковані без належних прав або в незаконний спосіб. Для підтримки цілісності використовуються методи контролю цілісності, регулярне резервне копіювання, а також інструменти виявлення та запобігання вторгненням у систему.

3. Доступність означає забезпечення стабільного та безперебійного доступу до інформації та ресурсів уповноваженим користувачам у необхідний час. Це передбачає, що інформаційні системи повинні бути стійкими до технічних несправностей, природних катастроф чи зловмисних дій, які можуть порушити їх роботу. Для гарантування доступності застосовуються механізми резервного копіювання, реплікації даних та спеціалізовані засоби для швидкого відновлення працездатності систем після збоїв. Інформаційна безпека реалізується через

сукупність організаційних, технічних, програмних та правових заходів, що спрямовані на захист:

- інформаційних систем і технологій;
- мережевої інфраструктури;
- облікових записів користувачів;
- електронних документів, листування;
- персональних, фінансових та інших чутливих даних.

На практиці ІБ охоплює широкий спектр рішень: від елементарного обмеження фізичного доступу до серверної кімнати – до складних багаторівневих систем, які включають криптографічний захист, міжмережеві екрани, системи виявлення вторгнень, аудит дій користувачів, машинне навчання для виявлення аномалій.

Інформаційна безпека у сучасному світі є невід'ємною умовою сталого розвитку, економічної стабільності, надійного функціонування ІТ-інфраструктури та збереження цифрового суверенітету. Її забезпечення потребує постійного моніторингу загроз, впровадження нових технологій, розробки нормативно-правових актів і формування компетентних фахівців [2].

1.2 Актуальні загрози інформаційній безпеці

У сучасному світі стрімкий розвиток інформаційних технологій призвів не лише до нових можливостей обробки й передачі даних, але й до значного зростання ризиків для безпеки цих процесів. Інформаційна безпека вже давно перестала бути проблемою лише ІТ-відділів – вона перетворилася на стратегічне завдання для керівництва будь-якої організації.

Особливої актуальності питання безпеки набуває в умовах зростання кіберзлочинності, використання складних багатовекторних атак та появи нових технологій, таких як Інтернет речей, хмарні сервіси, штучний інтелект.

Щоб ефективно організувати захист інформаційних ресурсів, необхідно мати чітке уявлення про типи загроз, їх джерела та способи впливу. Для цього

використовується класифікація загроз інформаційній безпеці, яка дозволяє систематизувати знання та обрати адекватні методи протидії [3].

Нижче наведено узагальнену таблицю 1.1. класифікації основних типів загроз інформаційній безпеці в комп’ютерних системах.

Таблиця 1.1 – Класифікація загроз інформаційній безпеці

Тип загроз	Приклади загроз	Опис та потенційні наслідки	Засоби протидії
Фізичні	Втрата обладнання, крадіжка пристроїв, знищення носіїв інформації	Втрата або витік чутливих даних через фізичний доступ сторонніх осіб, потенційний фінансовий збиток	Шифрування дисків, фізичний контроль доступу, резервне копіювання
Програмно-технічні	Шкідливе ПЗ (віруси, трояни, бекдори, ransomware), технічні уразливості, помилки конфігурації	Несанкціонований доступ, витік або втрата даних, порушення роботи систем і сервісів	Антивірусний захист, регулярні оновлення, аудит безпеки
Мережеві	Brute-force атаки, DDoS-атаки, атаки типу людина посередині, несанкціоноване сканування портів	Порушення доступності систем, перехоплення трафіку, витік автентифікаційних даних	Firewall, IDS/IPS, використання захищених протоколів, VPN, двофакторна автентифікація

Продовження Таблиці 1.1.

Тип загроз	Приклади загроз	Опис та потенційні наслідки	Засоби протидії
Людський фактор	Соціальна інженерія, фішинг, помилки персоналу, інсайдерські загрози	Несанкціонований доступ через маніпуляції або людську помилку, витік корпоративних даних	Навчання персоналу, політики інформаційної безпеки, контроль доступу

Серед найпоширеніших загроз сучасності виокремлюють: несанкціонований доступ, шкідливе ПЗ, фішинг, атаки типу «людина посередині», DDoS-атаки, експлуатацію вразливостей ПЗ. Ці загрози можуть реалізовуватись як окремо, так і в комбінації, що робить їх вкрай небезпечними для інформаційної інфраструктури. Згідно з дослідженням IBM (2023), понад 80% кіберінцидентів так чи інакше пов’язані з помилками користувачів або недотриманням політик безпеки [16].

Одним із найбільш резонансних прикладів є кібератака вірусу NotPetya в червні 2017 року. Це шкідливе програмне забезпечення поширювалося через оновлення бухгалтерського ПЗ M.E.Doc, яким користувалися тисячі організацій в Україні. Вірус шифрував дані на комп’ютерах і вимагав викуп у криптовалюті. Постраждали десятки державних органів та великих компаній – «Укрзалізниця», Чорнобильська АЕС, НБУ, міжнародні корпорації Maersk, FedEx, Merck. Особливістю атаки було те, що вона імітувала програму-вимагач, проте мала ознаки деструктивного коду, метою якого було порушення роботи інфраструктури. За оцінками компанії WhiteScope, прямі збитки від NotPetya лише для Maersk сягнули $300 млн. Загальні збитки по світу оцінюються в понад $10 млрд. Після атаки було вжито серйозних заходів із кіберзахисту: оновлено

критичні системи, вдосконалено політики доступу, започатковано державні програми з кібербезпеки.

1.3 Міжнародні стандарти

Забезпечення інформаційної безпеки (ІБ) на міжнародному рівні вимагає уніфікованого підходу до оцінювання ризиків, управління системами, впровадження політик безпеки та постійного вдосконалення захисних заходів. Для цього були розроблені серії міжнародних стандартів, які є загальноприйнятими у світовій практиці забезпечення кіберзахисту, управління активами, а також у питаннях оцінювання загроз і реагування на інциденти.

Найбільш визнаною у сфері є серія стандартів ISO/IEC 27000, що розроблена Міжнародною організацією зі стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC). Вона охоплює всі аспекти управління інформаційною безпекою, від формування політик до технічної реалізації заходів контролю.

Стандарт ISO/IEC 27001 встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS). Він базується на моделі PDCA (Plan-Do-Check-Act) та передбачає інтеграцію безпеки в усі бізнес-процеси організації [5].

ISO/IEC 27002 надає практичні рекомендації щодо впровадження контролів безпеки, описаних у 27001. У новій редакції 2022 року стандарт об’єднує 93 заходи безпеки у 4 тематичні групи: організаційні, фізичні, технічні та людейські [6].

ISO/IEC 27005 присвячений управлінню ризиками в ІБ. У ньому детально описується процес ідентифікації інформаційних активів, виявлення вразливостей і загроз, оцінка ймовірності інцидентів і визначення способів їх обробки [7].

Національний інститут стандартів і технологій США (NIST) розробив численні публікації, серед яких: NIST SP 800-53 – каталог технічних і

адміністративних заходів для безпеки урядових систем, та NIST SP 800-30 – методологія управління ризиками [8].

COBIT – фреймворк для управління IT-процесами та аудиту IT-інфраструктури. Його використовують для синхронізації IT-завдань із бізнес-цілями та підвищення контролю над інформаційними ресурсами.

ITIL – це бібліотека найкращих практик для управління IT-сервісами, що містить процеси моніторингу доступу, реагування на інциденти, управління ризиками і безперервністю послуг.

Серед інших стандартів, що набувають популярності у сфері ІБ, варто згадати ISO/IEC 27701 щодо захисту персональних даних, ISO/IEC 22301 з безперервності бізнесу, а також рекомендації ENISA – Європейської агенції з кібербезпеки.

Впровадження міжнародних стандартів дозволяє уніфікувати підходи до безпеки, підвищити довіру до організації, відповідати юридичним вимогам, зменшити ймовірність інцидентів і полегшити проходження аудитів [11].

1.4 Правова основа систем захисту інформації в Україні

Нормативно-правове забезпечення інформаційної безпеки в Україні є однією з ключових складових національної безпеки. В умовах зростання рівня кіберзагроз, цифровізації економіки, електронного урядування та війни в інформаційному просторі питання правового регулювання захисту інформації набуває стратегічного значення.

Законодавча база в сфері інформаційної безпеки формується на основі Конституції України, міжнародних угод, законів, указів Президента, постанов Кабінету Міністрів, а також нормативних актів НБУ, СБУ, Держспецзв’язку.

Закон України «Про інформацію» закладає основи правовідносин у сфері створення, зберігання, поширення, захисту інформації, визначає принципи відкритості, доступності, конфіденційності [1].

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» регламентує порядок забезпечення захисту інформації в ІТ-системах, визначає вимоги до технічного та криптографічного захисту.

Закон України «Про основні засади забезпечення кібербезпеки України» є ключовим нормативним актом у сфері кіберзахисту. Він визначає основні суб'єкти, принципи взаємодії, права та обов'язки у сфері кібербезпеки, порядок реагування на інциденти [12].

Закон України «Про електронні довірчі послуги» регламентує використання електронного підпису, печатки, сертифікації та захисту електронних транзакцій, що є критичним у цифровій державі [14].

Кримінальний кодекс України містить статті щодо відповідальності за порушення у сфері інформаційної безпеки, зокрема несанкціоноване втручання в ІТ-системи, пошкодження даних, розповсюдження шкідливого ПЗ [15].

Серед підзаконних нормативів важливе місце займають постанови Кабінету Міністрів України. Наприклад, Постанова №518 встановлює процедури реагування на кіберінциденти та визначає рівні критичності подій. Також Постанова №821 регламентує функціонування урядової команди реагування на комп'ютерні інциденти CERT-UA.

Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) розробляє спеціалізовані нормативні документи, зокрема:

- ТЗІ-1.1-003-2002 – класифікація інформаційно-телекомунікаційних систем за ступенем важливості інформації;
- Вимоги до побудови комплексної системи захисту інформації (КСЗІ), обов'язкові для державного сектору;
- Положення про державну експертизу у сфері технічного захисту інформації, яке визначає процедуру узгодження систем із безпековими нормами.

У рамках євроінтеграційного курсу Україна адаптує своє законодавство до норм ЄС. Зокрема, імплементуються вимоги NIS-директиви, GDPR, а також адаптуються положення стандартів ISO до національних – через ДСТУ ISO/IEC 27001, 27002 тощо.

Завдяки гармонізації правової бази Україна поступово долучається до єдиного цифрового простору Європи, що є критичним для транскордонного захисту даних і підвищення довіри до держави як партнера в сфері кібербезпеки.

Таким чином, нормативно-правова база України в сфері інформаційної безпеки є багаторівневою та динамічною. Вона охоплює як загальні принципи та закони, так і галузеві вимоги, підзаконні акти та технічні стандарти, орієнтовані на найкращі міжнародні практики [13].

2 МЕТОДИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

2.1 Сучасні підходи до захисту інформації від несанкціонованого доступу

У відповідь на зростання кількості кіберзагроз було сформовано ряд сучасних концепцій та підходів до захисту від несанкціонованого доступу, що спрямовані на зниження ймовірності компрометації інформаційних систем і мінімізацію ризиків втрати конфіденційної інформації.

Зокрема, велике значення набули багаторівнева аутентифікація, моделі нульової довіри (Zero Trust), проактивний моніторинг безпеки, а також використання штучного інтелекту для виявлення аномалій. Упровадження цих рішень дозволяє не лише оперативно реагувати на потенційні загрози, а й запобігати їм на ранніх етапах, забезпечуючи високий рівень стійкості кіберінфраструктури.

Zero Trust (Нульова довіра) – це сучасна концепція кібербезпеки, яка передбачає докорінну зміну традиційного підходу до організації захисту інформаційних систем. На відміну від класичних моделей, які засновані на припущенні про надійність внутрішнього середовища, модель Zero Trust виходить із постулату, що жоден елемент системи будь то користувач чи пристрій – не заслуговує на довіру за замовчуванням. Це формулює систему, в котрій кожен запит на доступ до ресурсів має бути ретельно перевірений незалежно від того, з якого середовища – внутрішнього чи зовнішнього – він надходить.

Така модель зосереджується на захисті окремих ресурсів, а не лише на побудові захищеного периметра мережі, що дозволяє зменшити ризики, пов’язані з внутрішніми загрозами та компрометацією облікових записів. Основні принципи моделі Zero Trust зображені на рисунку 2.1.

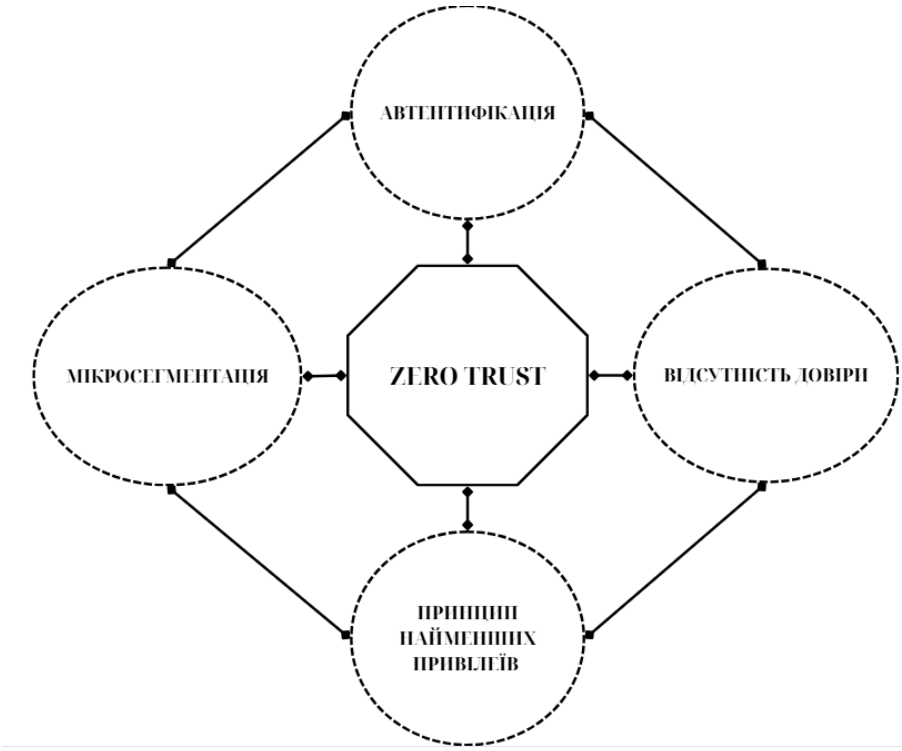

Рисунок 2.1 – Принципи моделі Zero Trust

Одже основа моделі складається з чотирьох принципів:

– відсутність довіри за замовчуванням (усі запити на доступ розглядаються як потенційно небезпечні);

– постійна автентифікація та верифікація (перевірка кожного доступу в режимі реального часу з урахуванням контексту);

– принцип найменших привілеїв (користувачі та програми отримують лише той рівень доступу, який є необхідним для виконання конкретних функцій);

– мікросегментація (поділ мережі на логічні сегменти для обмеження розповсюдження загроз у разі їх проникнення до системи).

На практиці така модель вже реалізована або активно впроваджується у низці провідних компаній, серед яких Google, Microsoft, Zscaler, Palo Alto Networks та інші. Ці компанії демонструють ефективність підходу в реальних умовах, що сприяє зростанню зацікавленості до нього серед представників академічного й професійного середовища.

Слід зауважити, що впровадження Zero Trust потребує комплексного переосмислення архітектури IT-інфраструктури організації, інвестицій у засоби

багатофакторної автентифікації, системи управління ідентичностями, засоби моніторингу та аналітики. Водночас очікуваний ефект від такого впровадження полягає в підвищення загального рівня кіберзахисту, адаптивність до сучасного середовища загроз, мінімізація ризиків витоку конфіденційних даних.

Одним з базових принципів побудови ефективної системи інформаційної безпеки є принцип найменших привілеїв (Least Privilege Principle). Він передбачає надання користувачам, службам та процесам мінімально необхідного рівня доступу для виконання їхніх функціональних обов'язків, без можливості здійснювати дії, що виходять за межі передбачених повноважень.

Такий підхід дозволяє значною мірою обмежити вектори потенційних атак, а також зменшити ризик несанкціонованого доступу до критично важливих ресурсів. Зокрема, він запобігає ситуаціям, коли окремі користувачі мають надмірні права, які можуть бути використані як унаслідок зловмисних дій (інсайдерських атак), так і через компрометацію облікових даних. Наприклад, співробітник відділу бухгалтерії не повинен мати доступ до інструментів адміністрування серверів, а фахівець технічної підтримки – до особистих даних працівників кадрового підрозділу [17].

Реалізація такого принципу сприяє проявлення таких явищ:

– зменшенню ризику внутрішніх загроз;

– локалізації та швидшій нейтралізації інцидентів безпеки;

– мінімізації наслідків успішної кібератаки, зокрема у разі фішингового впливу чи експлуатації вразливостей.

З технічної точки зору підтримка даного принципу забезпечується через впровадження політик доступу, використання систем контролю на основі ролей RBAC, а також засобів ізоляції облікових записів. У контексті масштабних IT-інфраструктур ці механізми дозволяють забезпечити структуроване й контрольоване середовище з мінімальними ризиками доступу до незареєстрованих або надмірних ресурсів.

Таким чином, принцип найменших привілеїв є непоганим концептуальним фундаментом для формування політик доступу в сучасних інформаційних

системах. Його дотримання є критично важливим у межах комплексної стратегії забезпечення кібербезпеки.

Мінімізація атакуючої поверхні (Attack Surface Reduction, ASR) передбачає зменшення кількості потенційних точок входу для зловмисника. Атакуюча поверхня охоплює всі можливі вектори взаємодії із системою, через які може бути реалізована атака: мережеві порти, служби, API, скрипти, інтерфейси користувача тощо.

Основною метою мінімізації атакуючої поверхні є ускладнення процесу несанкціонованого доступу до інформаційних ресурсів шляхом зменшення числа доступних або вразливих елементів. До реалізуючих методів можна віднести наступні: видалення або відключення невикористовуваних служб і сервісів, які можуть мати відомі вразливості або відкриті порти; оновлення програмного забезпечення до актуальних версій, що дозволяє усунути відомі вразливості, закриті у нових патчах; обмеження мережевої взаємодії, зокрема закриття невикористовуваних портів та протоколів; ізоляція критичних компонентів (наприклад, серверів баз даних) у захищених сегментах мережі; використання технологій віртуалізації, контейнеризації та sandboxing, які дозволяють обмежити наслідки компрометації окремих компонентів системи.

У практичній реалізації використовується провідними розробниками програмного забезпечення. Зокрема, корпорація Microsoft інтегрувала функціональність ASR у компонент Windows Defender Exploit Guard, який дозволяє блокувати запуск потенційно небезпечних скриптів, макросів, стороннього програмного забезпечення, а також виконання підозрілих дій без участі користувача. Такі механізми особливо ефективні в контексті запобігання фішинговим атакам, шкідливим макросам у файлах Microsoft Office, та експлуатації вразливостей нульового дня.

Можливість поєднання з іншими принципами, зокрема Zero Trust та найменших привілеїв, яке забезпечує більш високий рівень кіберстійкості організації, показує, що принцип зменшення атакуючої поверхні є технічно

доцільним компонентом комплексної системи захисту сучасних інформаційних інфраструктур.

Багаторівневий підхід до безпеки (Defense-in-Depth) передбачає створення системи з декількох послідовних та взаємопов’язаних рівнів захисту. Головна ідея цього підходу полягає у забезпеченні глибокої оборони: навіть у випадку подолання одного з бар'єрів, інші рівні залишаються активними та здатними запобігти подальшому поширенню атаки.

У межах даного підходу до захисту інформаційної інфраструктури реалізуються компоненти що зображені на рисунку 2.2.

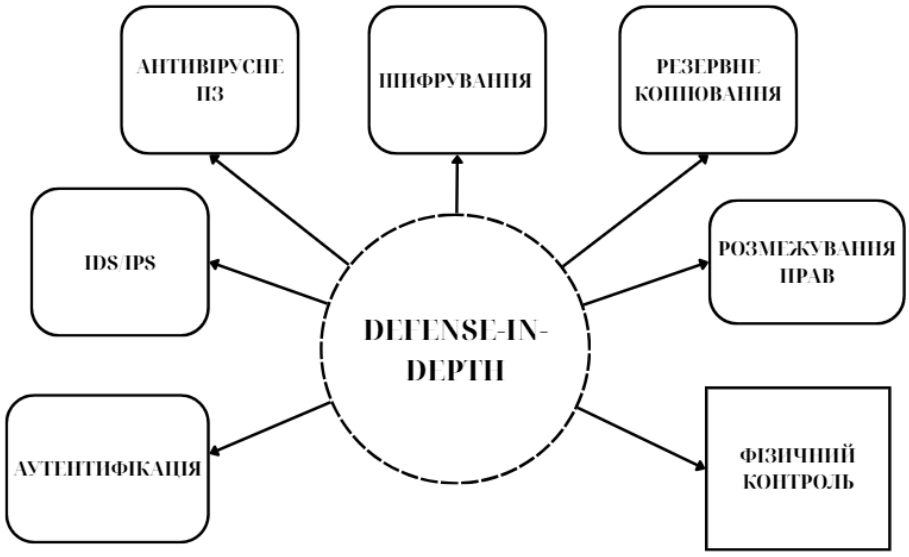

Рисунок 2.2 – Схема компонентів Defense-in-Depth

Перевага Defense-in-Depth полягає в його здатності забезпечувати адаптивний захист, здатний реагувати на динамічні кіберзагрози. При цьому кожен рівень функціонує як незалежний механізм, що ускладнює повну компрометацію системи. Більшість сучасних корпоративних архітектур безпеки, розроблених провідними IT-компаніями – такими як Cisco, Microsoft, Fortinet – ґрунтуються саме на концепції Defense-in-Depth, визнаючи її ефективність в умовах зростання складності атак і різноманітності загроз.

2.2 Механізми автентифікації та управління доступом

Автентифікація та управління доступом є фундаментальними компонентами системи інформаційної безпеки, що забезпечують перевірку правомірності доступу до інформаційних ресурсів. У сучасному кіберсередовищі, де зростає кількість загроз, реалізація надійних механізмів автентифікації та контролю доступу є критично важливою для зниження ймовірності несанкціонованого проникнення.

Автентифікація – процес встановлення відповідності між об'єктом доступу та його ідентифікатором. Метою автентифікації є підтвердження того, що суб’єкт (користувач, пристрій або процес) дійсно є тим, за кого себе видає. Загальний принцип процесу автентифікації показано на рисунку 2.3.

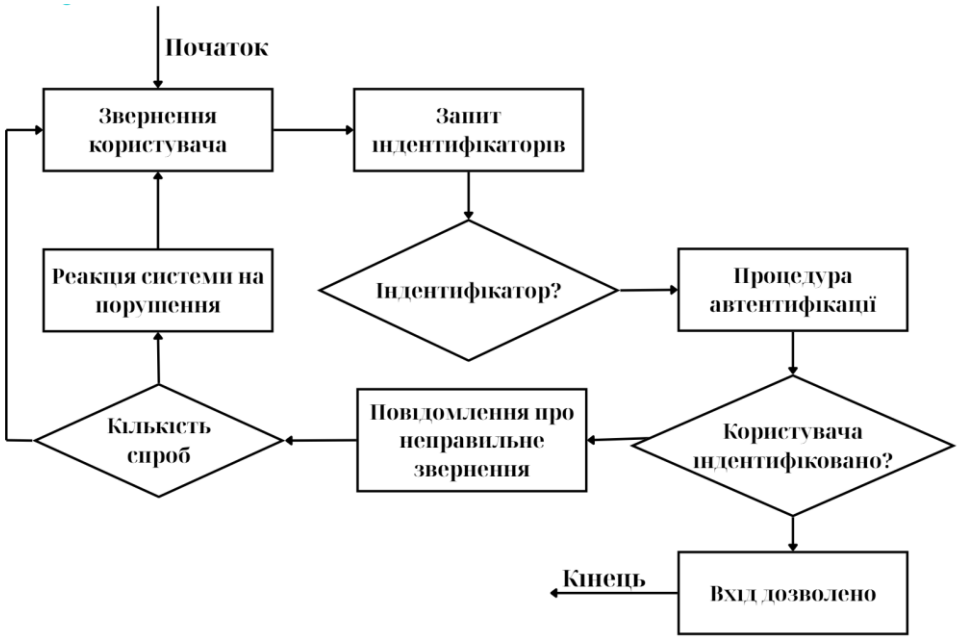

Рисунок 2.3 – Блок-схема процесу автентифікації

Автентифікація може містити в собі як один так і багато факторів за яким система може встановити чи дійсно це ми та чи можна нам надати доступ до запитаного ресурсу. В залежності від кількості таких факторів існують такі типи автентифікації:

– Однофакторна автентифікація (SFA) базується на використанні одного фактора, зазвичай паролю. Це найпростіший та найменш захищений метод, який піддається атакам типу перебору паролів або соціальної інженерії. Його застосування є доцільним лише в низькоризикових середовищах або в поєднанні з іншими засобами безпеки.

– Двофакторна автентифікація (2FA) передбачає використання двох незалежних факторів з трьох категорій: знання (наприклад, пароль), володіння (наприклад, мобільний пристрій з токеном або смарт-карта) та індивідуальні фізичні характеристики (наприклад, відбитки пальців). Цей підхід значно ускладнює несанкціонований доступ і використовується у більшості сучасних систем, включаючи банківські сервіси та хмарні платформи.

– Багатофакторна автентифікація (MFA) включає три або більше факторів автентифікації та забезпечує найвищий рівень безпеки. Вона є обов’язковою у середовищах з підвищеними вимогами до захисту даних, зокрема в урядових установах, критичних інфраструктурах, фінансових установах тощо.

Серед поширених технологічних засобів автентифікації варто виділити використання біометричних методів (наприклад, ідентифікація за сітківкою ока, обличчям або голосом), токенів (апаратних або програмних), а також одноразових паролів (OTP), які можуть генеруватись мобільними додатками або надсилатись через SMS. Крім того, у високозахищених середовищах застосовуються цифрові сертифікати (X.509), що підтверджують особу за допомогою криптографічних ключів. Такі сертифікати активно використовуються у протоколах SSL/TLS, віртуальних приватних мережах (VPN) та в системах електронного документообігу [9].

Після автентифікації наступним кроком є авторизація – процес визначення обсягу прав доступу користувача до ресурсів системи. Управління доступом дозволяє реалізувати політики безпеки, що визначають, хто, до чого і на яких умовах може отримати доступ. Сучасні системи контролю доступу спираються на різні моделі, кожна з яких має свої переваги та сфери застосування. Розберемо чотири таких моделей.

1. Дискреційна модель доступу (DAC) базується на праві власника об’єкта (файлу, каталогу, ресурсу) самостійно визначати, хто матиме до нього доступ. Ця модель є гнучкою, однак уразливою до помилок користувачів і не завжди забезпечує належний рівень безпеки в масштабних системах.

2. Примусова модель доступу (MAC), навпаки, передбачає централізоване встановлення політик доступу, які не можуть бути змінені користувачами. Її застосовують у військових та урядових структурах, де критично важливо контролювати всі аспекти доступу до класифікованої інформації.

3. Модель доступу, заснована на ролях (RBAC), є однією з найпоширеніших у корпоративному середовищі. Вона базується на принципі прив’язки прав доступу до ролей, що відповідають функціональним обов’язкам користувачів. Це дозволяє централізовано управляти доступом, підвищує прозорість та спрощує аудит безпеки.

4. Атрибутивна модель доступу (ABAC) забезпечує найвищий рівень гнучкості, оскільки дозволяє враховувати не лише роль користувача, а й інші атрибути – тип пристрою, місце розташування, час доби тощо. Ця модель знаходить застосування у складних динамічних середовищах, таких як хмарні сервіси та організації з розподіленою інфраструктурою[18].

Для узагальнення інформації та видимого порівняння було створено таблицю 2.1.

Таблиця 2.1 – Основні моделі авторизації та їх особливості

Модель	Основний принцип	Гнучкість	Сфера застосування
DAC	Власник ресурсу визначає права доступу.	Висока	Персональні системи, невеликі організації
MAC	Централізовані політики безпеки, що не змінюються користувачами.	Низька	Військові та урядові структури
RBAC	Права доступу визначаються ролями користувачів.	Середня	Корпоративне середовище

Продовження таблиці 2.1

Модель	Основний принцип	Гнучкість	Сфера застосування
ABAC	Права доступу визначаються атрибутами користувача та контекстом.	Висока	Хмарні сервіси, динамічні середовища

У корпоративному середовищі моделі RBAC і ABAC дозволяють ефективно контролювати доступ до конфіденційної інформації відповідно до посадових обов’язків і контексту користувачів. Це особливо важливо у великих компаніях з великою кількістю працівників, де ручне керування правами доступу є неефективним.

2.3 Засоби моніторингу та виявлення спроб несанкціонованого доступу

Враховуючи сучасні умови, коли зловмисники використовують дедалі витонченіші методи для проникнення в інформаційні системи, важливого значення набувають засоби моніторингу подій безпеки та своєчасного виявлення несанкціонованих дій. Ефективність таких засобів безпосередньо впливає на здатність організації швидко реагувати на інциденти, мінімізувати наслідки атак і забезпечити неперервність функціонування критичних сервісів.

До найважливіших категорій засобів контролю належать системи виявлення (IDS – Intrusion Detection System) та запобігання (IPS – Intrusion Prevention System) вторгненням. Вони є центральними елементами архітектури інформаційної безпеки, які дозволяють здійснювати аналіз подій у реальному часі, ідентифікувати загрози, порушення політик доступу або відхилення в поведінці користувачів, а в деяких випадках – автоматично вживати контрзаходів.

Системи виявлення вторгнень здійснюють постійний контроль за подіями, що відбуваються у мережевому трафіку або на окремих хостах. Основним їхнім завданням є фіксація підозрілих активностей, які можуть свідчити про спроби атак, витоки інформації або порушення політик безпеки. IDS зазвичай не

змінюють роботу системи, а лише генерують сповіщення для адміністраторів безпеки, що дозволяє зберегти цілісність середовища. Принцип роботи IDS складається з чотирьох ключових дій (рис.2.4):

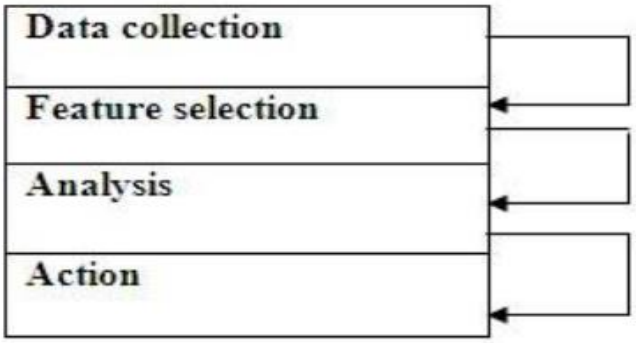

Рисунок 2.4 – Функції IDS

По-перше відбувається збір даних. Під час виконання цей модуль передає дані як вхідні для IDS. Інформація спочатку записується у файл, а потім аналізується, мережева IDS збирає та обробляє пакети даних, тоді як хостова IDS фіксує деталі, такі як використання дискового простору та системні процеси.

Другим етапом є вибір функції. Для вибору конкретних функцій у мережі доступні великі обсяги даних, які зазвичай оцінюються на предмет можливих вторгнень. Наприклад, такі параметри, як IP-адреси вихідної та цільової систем, тип протоколу, довжина заголовка та розмір, можуть слугувати ключовими індикаторами для виявлення вторгнень.

По-третє аналіз. Дані проходять аналіз для перевірки їх достовірності. У IDS, заснованій на правилах, вхідний трафік порівнюється з попередньо визначеними сигнатурами чи шаблонами. Альтернативним методом є IDS, орієнтована на аномалії, де вивчається поведінка системи і застосовується математична модель для виявлення відхилень.

Заключним етапом є дія. Система не лише виявляє атаку, а й формує відповідь відповідно до налаштувань безпеки. Вона може повідомити системного адміністратора через електронну пошту або сигналізацію з усіма необхідними

даними, а також може діяти активно, блокуючи пакети, щоб вони не потрапили в систему, або закриваючи порти для захисту.

В свою чергу IPS-системи, функціонують як активні елементи захисту. Тобто вони не тільки виявляють потенційні атаки, а й здатні самостійно переривати сесії, блокувати IP-адреси джерела загроз або змінювати конфігурацію мережевого середовища. Такі системи часто використовуюсь та інергрують у міжмережеві екрани та шлюзи безпеки для забезпечення комплексної протидії кіберзагрозам [10].

Розгортання IDS/IPS можно поділити на мережеві (NIDS/NIPS) та хостові (HIDS/HIPS). Мережеві системи здійснюють моніторинг у точках входу та виходу мережі, забезпечуючи аналіз усього вхідного й вихідного трафіку. Вони особливо ефективні для виявлення атак типу DoS, сканування портів, спроб експлуатації мережевих вразливостей. Хостові системи зосереджуються на окремих пристроях таких як сервери, робочі станції, критичні сервіси. Вони аналізують журнали подій, зміни файлів, запущені процеси й інші параметри роботи ОС. Поєднання обох підходів дозволяє досягти вищого рівня контролю, що характерно для комплексних SIEM-рішень (Security Information and Event Management), які забезпечують централізоване збирання, кореляцію та аналіз даних безпеки.

Впровадження IDS/IPS дозволяє значно підвищити загальну стійкість інформаційної інфраструктури до загроз. Своєчасне виявлення атак, зменшення часу реагування, можливість архівації журналів позитивно сприяє підвищенню рівня інформаційної безпеки. Інтеграція з SIEM-системами надає змогу здійснювати кореляцію подій з різних джерел, що підвищує точність виявлення.

Водночас, слід враховувати певні обмеження: IDS/IPS можуть створювати значне навантаження на інфраструктуру, особливо в умовах великих обсягів трафіку. Хибні спрацювання, складність налаштування й необхідність постійного оновлення сигнатур вимагають залучення кваліфікованого персоналу. Попри це, їх роль у багаторівневій архітектурі захисту залишається ключовою.

3 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

3.1 Реалізація та демонстрація методів захисту від несанціонованого доступу

Практична частина дипломного дослідження спрямована не лише на демонстрацію процесу впровадження окремих методів захисту інформації від несанкціонованого доступу, а й на оцінювання їх реальної ефективності, порівняння переваг та недоліків, а також визначення можливостей комплексного застосування цих методів у практичних умовах.

Окрему увагу в роботі приділено гібридному (комплексному) підходу до забезпечення інформаційної безпеки, який охоплює кілька рівнів інформаційної системи – від захисту локальних ресурсів і збережених даних до контролю віддаленого доступу й моніторингу мережевої активності.

Жоден із методів не забезпечує повного захисту від несанкціонованого доступу сам по собі. Це пов'язано з тим, що сучасні загрози інформаційній безпеці характеризуються складністю, багатовекторністю та постійною зміною тактик атакуючих. Окремий метод може ефективно запобігати лише певним типам загроз або покривати конкретний рівень системи, залишаючи інші вектори незахищеними. Саме тому для створення надійного та ефективного захисту інформації необхідно використовувати багаторівневий підхід, який передбачає комбінування кількох різнорідних методів захисту в єдину комплексну систему.

Для реалізації практичної частини дослідження було обрано типові корпоративні операційні системи – Windows 10 Pro та Ubuntu 22.04 LTS. На базі Windows реалізовано шифрування локальних даних за допомогою BitLocker, а в середовищі Ubuntu – впроваджено двофакторну автентифікацію та систему блокування підозрілої активності Fail2Ban.

Такий вибір зумовлений необхідністю побудови багаторівневої системи захисту, яка охоплює фізичний рівень (захист збережених даних), логічний рівень

(перевірка автентичності користувача) та мережевий рівень (виявлення підозрілої поведінки). Розглянуто практичне впровадження кожного з цих методів окремо.

Захист даних за допомогою BitLocker

BitLocker – це вбудований засіб шифрування дисків у Windows, який використовує алгоритм AES для захисту інформації від несанкціонованого доступу. Він дозволяє шифрувати як системні, так і несистемні логічні розділи, а також знімні носії, такі як USB-накопичувачі. BitLocker є частиною Windows, починаючи з версій Vista та Windows Server 2008, і доступний у редакціях Pro, Enterprise та Education.

Можливий функціонал як у поєднанні з апаратним модулем TPM (Trusted Platform Module), так і без нього, використовуючи лише пароль або ключ на зовнішньому носії. У разі використання TPM шифрувальний ключ надійно зберігається у спеціальному мікрочипі, що унеможливлює його викрадення програмним шляхом. Крім того, він підтримує багатофакторну автентифікацію, включно з PIN-кодом, USB-ключем та паролем.

Застосування BitLocker забезпечує конфіденційність та цілісність даних навіть у випадках фізичної крадіжки пристрою або втрати носія. Шифрування відбувається на рівні блочного доступу до диска, що гарантує неможливість читання інформації без попередньої автентифікації.

Алгоритм дій даного методу наочно:

1. Відкрито Панель керування: Система і безпека → Шифрування диска BitLocker. Демонстрацію зображено на рисунку 3.1.

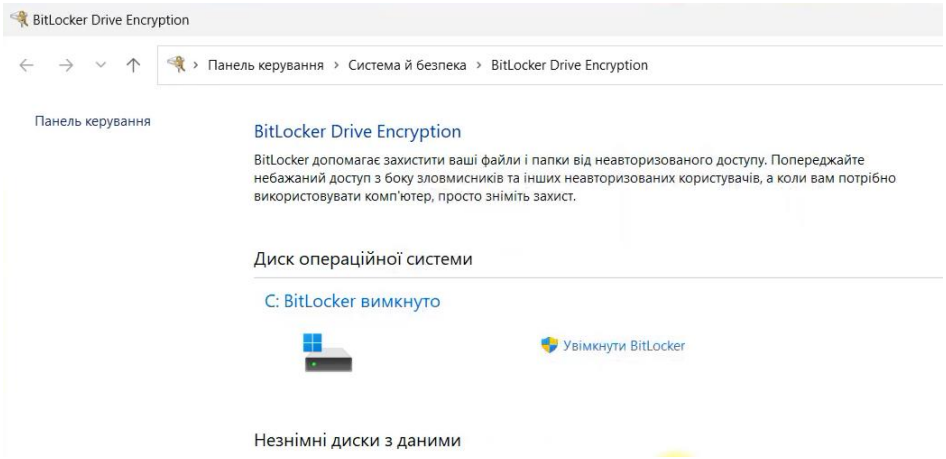

Рисунок 3.1 – Вікно «Про систему»

2. Обрано спосіб зберігання ключа шифрування. Демонстрацію зображено на рисунку 3.2.

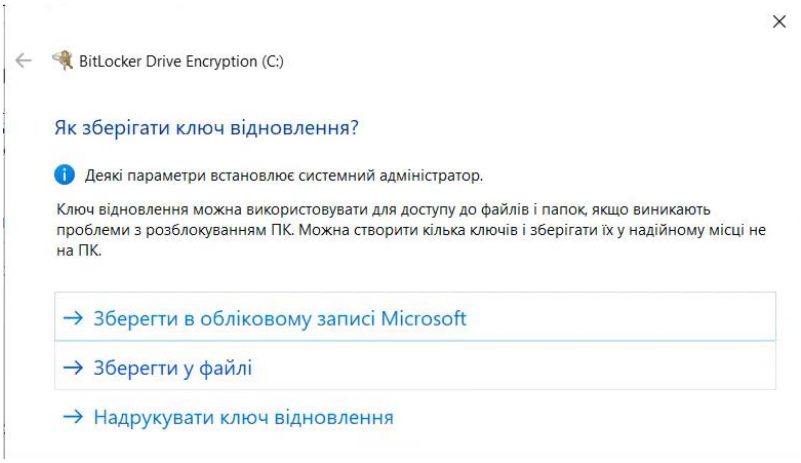

Рисунок 3.2 – Вибір методу зберігання ключа відновлення

3. Збережено ключ відновлення на інший носій. Демонстрацію зображено на рисунку 3.3.

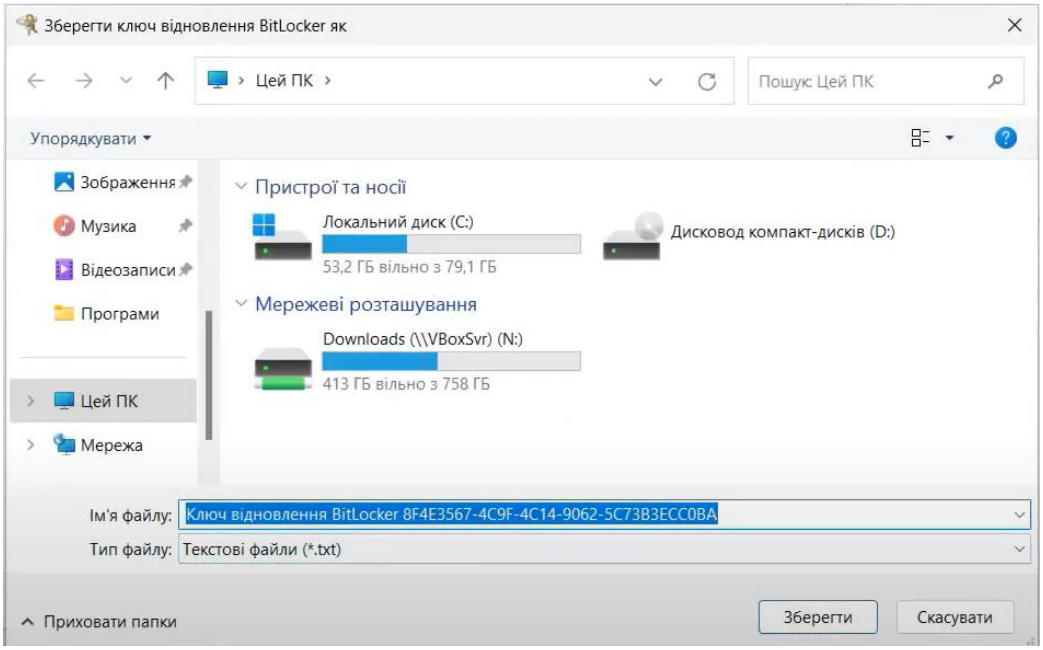

Рисунок 3.3 – Збереження ключа відновлення на зовнішньому носії N

4. Вибрано обсяги шифрування, а саме весь диск для більшого захисту. Демонстрацію зображено на рисунку 3.4.

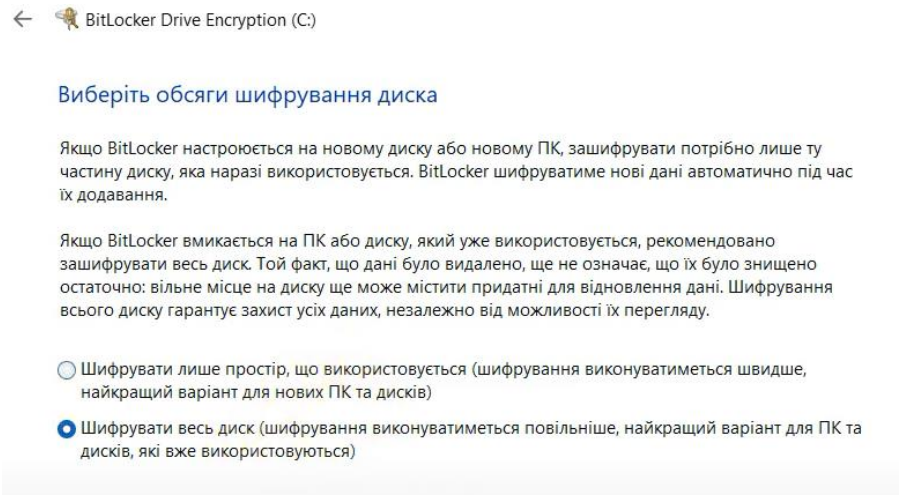

Рисунок 3.4 – Вибір параметрів шифрування

5. Вибрано повне шифрування з використанням режиму XTS-AES. Демонстрацію зображено на рисунку 3.5.

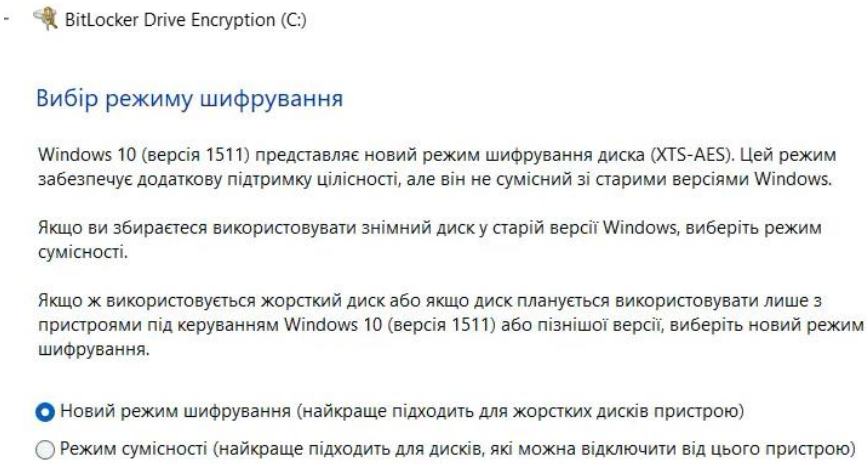

Рисунок 3.5 – Новий режим шифрування XTS-AES

6. Запущено процес шифрування та після завершення перевірено чи збережено ключ відновлення. Демонстрацію зображено на рисунку 3.6.

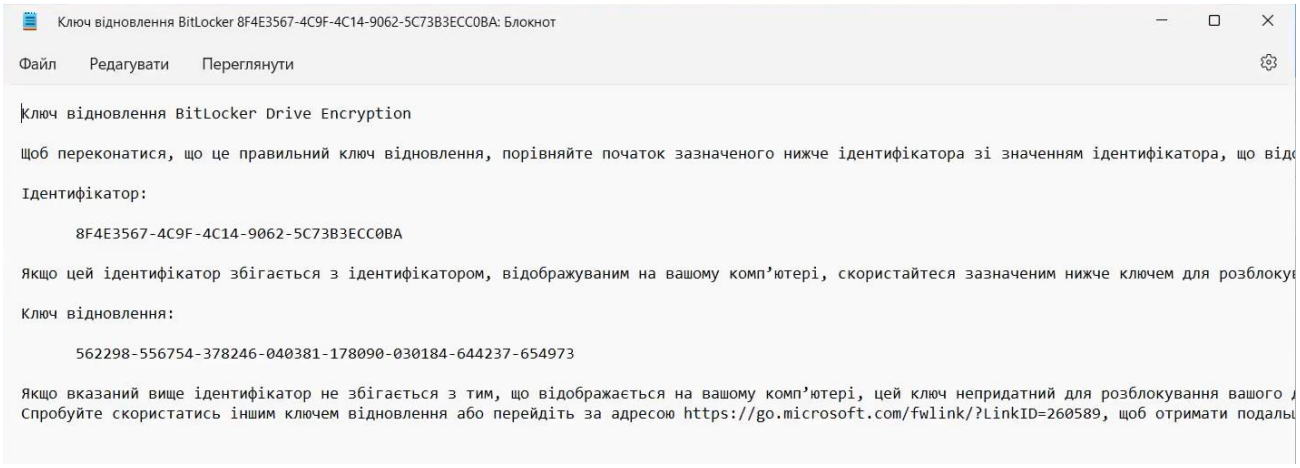

Рисунок 3.6 – Ключ відновлення після вдалого шифрування диску

7. Спроба несанкціонованого доступу від іншого користувача призводить до того, що для входа в систему потрібно ввести наш ключ відновлення. Демонстрацію зображено на рисунку 3.7.

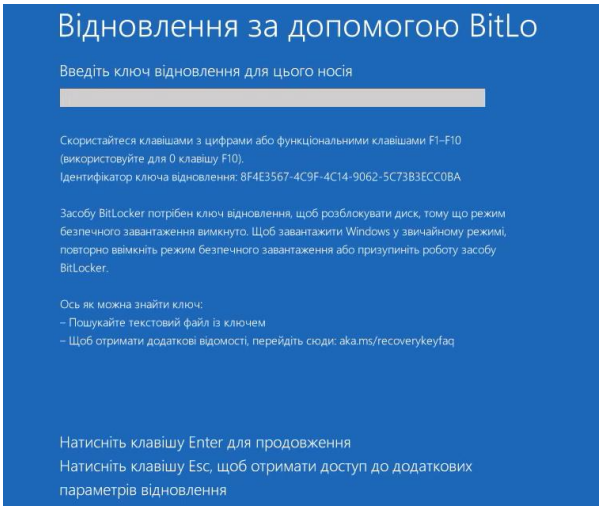

Рисунок 3.7 – Запит ключа при доступі до зашифрованого диска

BitLocker є ефективним інструментом захисту даних на комп'ютерах під управлінням Windows. Він дозволяє запобігти доступу до чутливої інформації у випадку втрати або крадіжки пристрою. Його використання є виправданим у державних установах, компаніях та для особистого користування, особливо при роботі з ноутбуками, що зберігають резервні копії або службову інформацію.

Реалізація двофакторної автентифікації для SSH-доступу

Двофакторна автентифікація (2FA) є методом посиленого захисту, при якому користувач повинен надати два різні типи автентифікаційних даних для доступу до системи. У контексті SSH-з'єднання зазвичай застосовується комбінація: щось, що користувач знає – наприклад, пароль, щось, що користувач має – мобільний пристрій із додатком Google Authenticator, який генерує одноразові паролі (OTP).

Такий підхід суттєво знижує ризик несанкціонованого доступу, навіть якщо пароль було скомпрометовано. Одноразові паролі генеруються за алгоритмом TOTP (Time-Based One-Time Password) і мають термін дії близько 30 секунд, що унеможливлює їх повторне використання.

Для реалізації 2FA на сервері з Linux/Ubuntu найчастіше використовується модуль libpam-google-authenticator, який інтегрується з PAM (Pluggable Authentication Modules) та дозволяє серверу перевіряти OTP-коди, створені на основі секретного ключа, що зберігається на стороні користувача. Додаткову зручність забезпечує мобільний додаток (Google Authenticator, FreeOTP, Authy), який генерує коди автоматично.

Усі OTP-коди генеруються на основі унікального секретного ключа, який встановлюється при першому налаштуванні, тому важливо зберегти резервні коди та QR-код під час генерації. У разі втрати телефону або видалення додатку, без резервного ключа доступ до системи може бути втрачено.

Розроблено алгоритм поступових кроків для роботи такого методу.

1. Встановлено на сервері Ubuntu модуль Google Authenticator. Для цього використовується пакет libpam-google-authenticator, який містить PAM-модуль для двоетапної автентифікації. Встановлення виконується через стандартний менеджер пакетів APT. Від імені адміністратора або через sudo виконуємо команду:

```
sudo apt install libpam-google-authenticator
```

Команда завантажує пакет з репозиторію і додає модуль Google Authenticator до системи.

2. Налаштовано автентифікатор для конкретного користувача. Для цього виконано команду google-authenticator. Програма запитає, чи потрібно використовувати токени, що базуються на часі. Далі утиліта згенерує секретний ключ і відобразить QR-код прямо в консолі, цей код кодує секретний ключ, відомий лише серверу та додатку Google Authenticator.

Окрім QR-коду, виводяться також текстові дані, такі як: секретний ключ; одноразовий верифікаційний код для перевірки та кілька аварійних кодів на випадок втрати доступу до генератора кодів. Демонстрацію цих всіх даних зображено на рисунку 3.8.

Рисунок 3.8 – Результат генерації секретний ключів та даних для користувача

3. На смартфоні відкрито мобільний додаток Google Authenticator, далі вибрано режим сканування QR-коду, після чого потрібно відсканувати QR-код з терміналу за допомогою камери телефону. Після успішного сканування додаток додасть новий запис і почне генерувати шестизначні одноразові паролі для цього облікового запису. Приклад зображено на рисунку 3.9. Такий код генерується на основі секретного ключа і часу і оновлюється кожні 30 секунд.

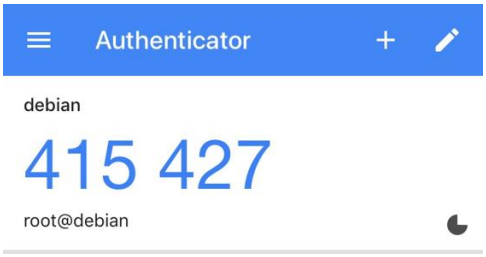

Рисунок 3.9 – Відображення поточного одноразового коду

4. Введення одноразового коду під час автентифікації. Тепер при спробі SSH-з’єднання, сервер спочатку запитує Verification code – тобто одноразовий код з Google Authenticator, а потім запитує звичайний пароль користувача. Лише після успішного введення обох цих значень автентифікація буде пройдена. На наведеному нижче на рисунку 3.10. показано сесію SSH-входу, де користувач вводить спочатку 6-значний код з додатку, потім свій пароль, і в результаті отримує доступ до сервера.

```
$ ssh user@server
Verification code: 123456
Password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-42-generic x86_64)
user@server:~$
```

Рисунок 3.10 – SSH-з’єднання до серверу за допомогою коду та паролю

5. Відмова в доступі при неправильному або відсутньому коді. Якщо ми спробуємо ввести код невірно, або надамо його взагалі, автентифікація не буде успішною. Тобто SSH-сервер повідомить про помилку і відмовить у доступі. Приклад показано на рисунку 3.11.

```
$ ssh user@server
Verification code: 000000
Password:
Permission denied, please try again.
Verification code: 111111
Password:
Permission denied (keyboard-interactive).
```

Рисунок 3.11 – Результат введення неправильного коду

Робимо висновок, що реалізація двофакторної автентифікації для SSH на Ubuntu за допомогою Google Authenticator значно підвищує безпеку. Для успішного входу тепер потрібні дві речі: знання пароля користувача і фізичний доступ до мобільного пристрою з генерованим одноразовим кодом. Такий підхід унеможливлює несанкціонований доступ тільки з паролем і є рекомендованою практикою захисту серверів. Зрештою, навіть якщо зловмисник підбере або дізнається ваш пароль, без другого фактору він не зможе увійти в систему. Це істотно покращує загальну безпеку SSH-доступу до сервера.

Захист доступу за допомогою Fail2Ban

Fail2Ban це система активного захисту для UNIX-подібних операційних систем, яка автоматично блокує підозрілі IP-адреси, аналізуючи журнали логів різних сервісів. Основна мета це захист системи від brute-force атак, спроб підбору паролів, DOS-атак на автентифікаційні механізми та інших проявів несанкціонованої активності.

Принцип роботи полягає у створенні спеціальних «в'язниць», де вказуються правила моніторингу логів певного сервісу (наприклад, SSH), шаблони для пошуку невдалих спроб автентифікації, а також дії, які слід виконати після досягнення заданого порогу спроб.

Fail2Ban не потребує постійної роботи в пам’яті системи на рівні перехоплення мережевого трафіку, що дозволяє зменшити навантаження на систему. Він є зручним у налаштуванні, підтримує автоматичне розблокування після закінчення часу «бана» та веде повний журнал подій. Серед його головних переваг – простота реалізації, розширюваність (можна створювати власні фільтри), а також інтеграція з системними брандмауерами та службами сповіщення таких як email, тощо.

Fail2Ban є особливо ефективним у ситуаціях, коли доступ до сервера відкритий для зовнішнього світу і використовуються стандартні протоколи на зразок SSH, FTP або HTTP, які часто є ціллю атак зловмисників.

Розробимо невеликий алгоритм для базового налаштування на сервері Ubuntu для захисту SSH:

1. Встановлено Fail2Ban звичайною консольною командою так як він входить до стандартного репозиторію Ubuntu. Спочатку оновлено індекс пакетів, а потім встановлюємо пакет Fail2Ban командою:

```
sudo apt install fail2ban -y
```

Пакет Fail2Ban та необхідні залежності будуть завантажені та встановлені з репозиторію.

2. Налаштовано роботу Fail2Ban за допомогою файлу конфігурації /etc/fail2ban/jail.local (копію стандартного jail.conf). У цьому файлі і будуть визначатися правила моніторингу логів для різних сервісів та параметри блокування. Відкрито файл jail.local у редакторі і у секції [sshd] вставлено для неї потрібні параметри. Демонстрація на рисунку 3.12. Розберемо строки які вписано: enabled = true (вмикає захист SSH); port = ssh (порт 22 який відповідає за роботу SSH); maxretry = 5 (максимальна кількість невдалих спроб); bantime = 1h (час блокування), ignoreip (для довірених IP, що не блокуватимуться).

Рисунок 3.12 – Файл конфігурації jail.local

3. Перезапуск служби Fail2Ban для застосування налаштувань. Це можна зробити наступною командою:

```
systemd: sudo systemctl restart fail2ban
Sudo systemctl restart fail2ban
```

Fail2Ban перезапускається без виводу повідомлень Після перезапуску Fail2Ban почне використовувати нову відредаговану конфігурацію jail.local.

4. Перевірено статус Fail2Ban. Для цього було використано команду:

```
sudo fail2ban-client status sshd
```

Результат цієї команди можна побачити на рисунку 3.13. Тут виводиться інформація фільтра і дій для служби SSHD. У даному випадку кількість поточних

та загальних невдалих спроб дорівнює 0, і жодна IP-адреса не заблокована (Currently banned: 0).

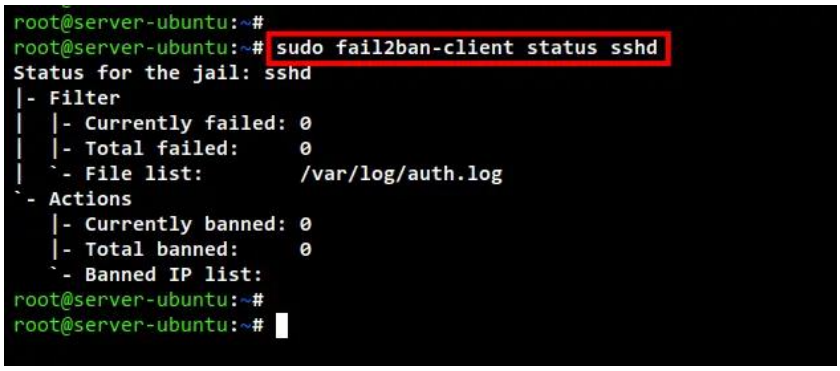

Рисунок 3.13 – Виконання команди на перевірку статусу робити

5. Імітовано декілька невдалих спроб SSH-входу для перевірки роботи Fail2Ban. Після перевищення ліміту спроб він блокує IP-адресу порушника на визначений нами раніше час. Ознаки блокування можна перевірит у логах, що знаходяться у журналі /var/log/fail2ban.log. На рисунку 3.14. показано фрагмент логу з повідомленнями про блокування IP-адреси.

Рисунок 3.14 – Записи логів в яких вказано заблоковану адресу

Fail2Ban регулярно аналізує журнали, і при виявленні багаторазових невдалих спроб входу автоматично блокує підозрілі IP-адреси, ефективно захищаючи сервер від brute-force атак. Його впровадження рекомендоване на всіх серверах з відкритим SSH, особливо у випадках, коли немає централізованої системи моніторингу.

3.2 Порівняльний аналіз методів захисту від несанкціонованого доступу

З кожним днем атаки стають багаторівневими, методи проникнення – дедалі витонченішими, а самі IT-системи – більш гібридними й розподіленими. У зв’язку

з цим, дедалі частіше виникає необхідність у більш комплексному підходу забезпечення безпеки, де застосовуються різні механізми одночасно. Нами було реалізовано та протестовано три різні методи: BitLocker, 2FA для SSH та Fail2Ban. Для аналізу цих методів обрано низку критеріїв, наведених у таблиці 3.1.

Таблиця 3.1 – Аналітична таблиця методів

Критерій	BitLocker	2FA SSH	Fail2Ban
Тип захисту	Шифрування диску	Двофакторна автентифікація	Блокування IP після підозрілих дій
Цільова загроза	Несанкціонований фізичний доступ	Компрометація пароля	Brute-force, сканування
Реакція на атаку	Забороняє доступ до розділу без розшифрування	Блокує вхід без TOTP-коду	Автоматичне банення IP через iptables
Алгоритм / Механізм	AES-шифрування, TPM/пароль/ключ	TOTP (time-based одноразовий код)	Аналіз логів + iptables/dynamic rules
Рівень автоматизації	Високий	Середній	Високий
Складність впровадження	Низька	Середня	Низька
Зручність для користувача	Висока	Середня	Висока
Гнучкість у налаштуванні	Низька	Середня	Висока
Потреба в сторонньому ПЗ	Ні (вбудований)	Так (Google Authenticator)	Ні (APT)

Продовження таблиці 3.1.

Сумісність із ОС	Windows Pro/Enterprise	Linux (Ubuntu, Debian)	Linux (Ubuntu, Debian)
Критерій	BitLocker	2FA SSH	Fail2Ban
Масштабованість	Середня (на рівні окремих ПК)	Висока (сотні користувачів)	Висока (мережеві інфраструктури)
Типова сфера використання	Персональні та корпоративні ПК	Сервери, хостинг, dev-середовище	Публічні сервери, ssh/gateway вузли

Як свідчать дані таблиці, кожен із методів зосереджується на окремому аспекті захисту й доповнює інші, формуючи багаторівневу систему безпеки.

– BitLocker є ефективним інструментом забезпечення фізичної безпеки даних на рівні пристрою. У разі втрати або викрадення комп’ютера доступ до інформації без відповідного ключа розшифрування стає неможливим. Завдяки інтеграції в операційну систему Windows, простоті налаштування та відсутності необхідності у додатковому програмному забезпеченні, BitLocker становить доцільне рішення як для індивідуального використання, так і для корпоративного середовища.

– Механізм двофакторної автентифікації, реалізований на основі одноразових кодів, забезпечує додатковий рівень безпеки при автентифікації користувачів. Навіть у випадку компрометації основного пароля, зловмисник не зможе здійснити несанкціонований доступ без підтвердження другого фактора. Хоча впровадження даного підходу передбачає участь користувача на етапі входу, воно істотно знижує ризик несанкціонованого проникнення до системи.

– Fail2Ban є засобом автоматизованого реактивного захисту, що функціонує на основі аналізу системних журналів подій. Його основне завдання полягає у виявленні ознак підозрілої активності – таких як багаторазові невдалі

спроби автентифікації з подальшим блокуванням IP-адрес джерел загроз шляхом створення відповідних правил у системному брандмауері. Завдяки своїй простоті впровадження, адаптивності до різних сервісів і здатності виявляти мережеву поведінкову активність, Fail2Ban становить ефективне рішення для додаткового захисту.

Проведений аналіз та практичне застосування трьох методів захисту дозволяють зробити висновок про відсутність універсального рішення, адже кожен метод має чітко окреслені рамки ефективності, власні переваги та обмеження у використанні. У сучасному середовищі, де інформаційні системи дедалі частіше стають розподіленими, мобільними, а загрози – складними й багаторівневими, застосування лише одного методу є недостатнім. Комбінація різних методів захисту стає не просто рекомендованою, а необхідною умовою безпеки. Аргументи на користь багаторівневого підходу:

- Сучасні атаки комплексні: один метод не здатний ефективно протистояти всім типам загроз.
- Кожен інструмент охоплює окремий напрямок або вектор атаки.
- Використання комбінації методів дозволяє мінімізувати ризик від помилок або уразливостей будь-якого окремого компонента.
- Запропоновані рішення є безкоштовними або вже інтегрованими в систему, що забезпечує економічну доцільність.
- Є можливість гнучко масштабувати систему захисту – від окремого персонального комп’ютера до рівня великих корпоративних мереж.

При практичному впровадженні ці методи діють спільно: BitLocker здійснює шифрування даних, 2FA забезпечує надійну ідентифікацію користувача, а Fail2Ban швидко реагує на будь-які підозрілі спроби доступу.

Отже, багаторівнева система захисту на основі BitLocker, 2FA та Fail2Ban є комплексним і логічно завершеним рішенням, оптимально пристосованим до потреб сучасних інформаційних систем.

ВИСНОВКИ

У цій кваліфікаційній роботі було проведено дослідження теоретичних і практичних аспектів захисту інформації від несанкціонованого доступу в комп’ютерних системах, зосереджуючи увагу на методах і засобах, що використовуються в сучасних умовах кіберзагроз.

Проаналізовано основні принципи кіберзахисту, що лежать в основі побудови ефективних систем інформаційної безпеки. Застосування цих принципів дає змогу зменшити ризики компрометації ресурсів, локалізувати потенційні порушення безпеки та підвищити загальну стійкість систем до атак.

Окрему увагу приділено механізмам авентифікації та засобам моніторингу, таким як IDS/IPS. Зазначено, що вибір автентифікаційної моделі має здійснюватися з урахуванням рівня критичності інформації, кількості користувачів, гнучкості вимог до доступу та необхідного рівня контролю.

У кваліфікаційній роботі була також практична частина, дослідження якої продемонстрували застосування реальних механізмів захисту – шифрування даних засобами BitLocker, реалізацію двофакторної автентифікації для SSH-доступу, а також використання системи Fail2Ban як елемента запобігання автоматизованим атакам. Усі реалізовані програми підтвердили, що їх можна використовувати та працювати з ними.

Результати засвідчують, що комплексне впровадження сучасних концепцій, моделей доступу та технічних засобів захисту дозволяє істотно підвищити рівень кіберзахищеності комп’ютерних систем. Це є необхідною умовою для забезпечення стабільного функціонування як державних інформаційних ресурсів, так і корпоративної інфраструктури в умовах зростаючої складності кіберзагроз.

Отже, можна зробити висновок, що для захисту від несанкціонованого доступу до інформації доцільно буде використовувати низку заходів для більш вдалого захисту. Ні один метод без синергії з іншими не зможе захистити від всіх типів атак. Потрібно використовувати цілі системи методів аби ваша інформація не потрапила у руки зловмисників.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення 01.01.2023 р. № 2801-IX. URL: https://zakon.rada.gov.ua/laws/show/2657-12
2. Лужецький В. А., Кожухівський А. Д., Войтович О. П. Основи інформаційної безпеки: навчальний посібник. – Вінниця: ВНТУ, 2013. – 221 с.
3. Theoretical and Applied Cybersecurity (TACS-2023): зб. матеріалів наук. – практ. конф. – Київ: Ін-т спец. зв'язку та захисту інформації НТУУ «КПІ», 2023. – 124 с. URL: https://is.ipt.kpi.ua/pdf/TACS-23.pdf
4. Зубок В. Ю., Мохор В. В. Кібербезпека топології INTERNET: монографія – Київ: ІПМЕ ім. Г.М. Доброва НАН України, 2022. – 260 с.
5. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. Geneva: International Organization for Standardization, 2013.
6. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva: International Organization for Standardization, 2022.
7. ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management. Geneva: International Organization for Standardization, 2018.
8. National Institute of Standards and Technology (NIST). SP 800-53 Rev.5, SP 800-30 Rev.1. URL: https://csrc.nist.gov/publications
9. Волинець О. Ю., Куліш Д. В., Приймак А. В., Яремчук Я. Ю. Удосконалення моделі керування доступом на основі ролей у приватних хмарних середовищах // Реєстрація, зберігання і обробка даних. – 2019. – Т. 21, № 4. – С. 49–56.
10. Сидоренко В. І., Яковенко В. В. Інформаційна безпека: навчальний посібник. Київ: Центр учбової літератури, 2017. – 248 с.

11. International Organization for Standardization. ISO/IEC 27000 family – Information security management systems. URL: https://www.iso.org/isoiec-27001-information-security.html
12. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. Дата оновлення 19.04.2023 р. № 2974-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр
13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. Дата оновлення 01.01.2023 р. № 2801-IX. URL: https://zakon.rada.gov.ua/laws/show/2163-19
14. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. Дата оновлення 19.07.2023 р. № 3272-IX. URL: https://zakon.rada.gov.ua/laws/show/2155-19
15. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. Статті 361–363-1. Дата оновлення 16.01.2024 р. № 3504-IX. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
16. IBM. Cost of Data Breach Report 2023. URL: https://www.ibm.com/reports/data-breach
17. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г. М. Гулак. – Київ: ІММСП, 2020. – 312 с.
18. Kubernetes Security Best Practices -Part 1: Role Based Access Control (RBAC) – URL: https://engineering.dynatrace.com/blog/kubernetessecurity-part-1-role-based-access-control-rbac/