Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

**КВАЛІФІКАЦІЙНА РОБОТА**
Коцюка Миколи Миколайовича

на здобуття ступеня вищої освіти Бакалавра

Система захисту комп'ютеризованого робочого місця від інформаційних витоків

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

Шифр КРБКБ.2102150.21.02.13 ПЗ

Виконав студент 4 курсу група КБ-21-2 Микола КОЦЮК

Керівник кандидат технічних наук, доцент Віктор ЧЕШУН

Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

10 06 2025 р.

Хмельницький 2025

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
15 лютого 2025 р.

**З А В Д А Н Н Я**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ**
Коцюка Миколи Миколайовича

1 Тема роботи Система захисту комп'ютеризованого робочого місця від інформаційних витоків

Керівник роботи канд. техн. наук, доцент Віктор ЧЕШУН

Затверджено наказом ректора університету від 07 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру 1.06.2025

3 Вихідні дані до роботи Проаналізувати проблеми специфіки та типової проблематики інформаційних витоків. Дослідити існуючі рішення систем протидії інформаційним витокам. Дослідити на законодавчому рівні рішення проблематики інформаційних витоків. Розробка моделі загроз та моделі порушника типового коип'ютеризованого робочого місця. Проаналізувати канали витоку інформації на комп'ютеризованому робочому місці та проектуванняпротидії витоку інформації по цим каналам. Імплементація системи на експереминтальному робочому місці. Тестування та апробація імплементованої системи. Підбивання фінансових підсумків розорбленої системи захисту від інформаційних витоків.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз предметної області роботи та типової проблематики інформаційних витоків. Дослідження існуючих систем протидії інформаційним витокам. Дослідження державної та міжнародної нормативно – правової бази за темою роботи. Постановка задачі проєктування. Висновок. Визначення найбільш загрозливих каналів витоку інформації в контексті окремого коип'ютеризованого робочого місця. Побудова моделі загроз та моделі порушника типового комп'ютеризованого робочого місця. Проєктування системи запобігання інформаційним витокам. Висновок. Імплементація системи запобігання інформаційним витокам на експерементальному робочому місці. Апробація та тестування імплементованої системи. Розробка настанов що до її експлуатації. Оцінка затрачених ресурсів. Висновок. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Таблиці оцінювання критичності оптичного, акустичного, вібро акустичного та мережевого каналів витоків інформації. Таблиці визначення найбільш загрозливих каналів витоку інформації. Таблиця моделі загроз на комп'ютеризованому робочому місці. Таблиця моделі порушника на комп'ютеризованому робочому місці. Налаштування політики безпеки ОС Windows. Політика паролів комп'ютеризованого робочого місця. Робота у програмному комплексі ЛОЗА-1. Атрибути доступів до файлів. Правило заборони вихідного трафіку за незахищеним протоколом. Робота у програмному комплексі Norton. Налаштування лонгування та моніторингу. Робота з портами за допомогою Nmap.
.

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 16 лютого 2025 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 | Червень | |
| Захист КР | Червень | |

Студент _____ Микола КОЦЮК

Керівник кваліфікаційної роботи _____ Віктор ЧЕШУН

# АНОТАЦІЯ

Тема кваліфікаційної роботи: Система захисту комп'ютеризованого робочого місця від інформаційних витоків.

Автор роботи: Коцюк Микола Миколайович.

Керівник роботи: Чешун Віктор Миколайович

Пояснювальна записка: 81 с., 12 додатків, 18 рисунків, 21 таблиці, 47 джерел.

Графічна частина: 12 плакатів.

КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ, МЕРЕЖЕВИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ, ОПТИЧНИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ, ВІБРО-АКУСТИЧНИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ, АКУСТИЧНИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ, ЗАХИСТ КОМП'ЮТЕРИЗОВАНОГО РОБОЧОГО МІСЦЯ.

Кваліфікаційна робота бакалавра присвячена розробці системи запобігання інформаційним витокам комп'ютеризованого робочого місця.

У роботі проаналізовано сучасні загрози витоку інформації, оцінено рівень безпеки комп'ютеризованого робочого місця та визначено ключові вразливості. Розроблено комплекс заходів для запобігання витокам даних, що включає організаційні, програмно-апаратні та криптографічні методи захисту інформації.

В результаті роботи створено супровідну документацію до системи запобігання інформаційним витокам: модель загроз, політику безпеки, технічне завдання, план впровадження заходів захисту, рекомендації щодо контролю доступу, акт оцінки рівня ризиків, регламент роботи з конфіденційною інформацією та протокол тестування ефективності запропонованих рішень.

Здійснено підготовку до впровадження розробленої системи, що забезпечить надійний захист інформації та мінімізує ризики несанкціонованого розголошення даних.

05.06.2025 _____

# ABSTRACT

Subject of qualification work: A system for protecting a computerized workplace from information leaks.

Author: Kotsyuk Mykola Mykolayovych.

Head of work: Cheshun Viktor Mykolayovych.

Explanatory note: 81 p., 12 appendices, 18 figures, 21 tables, 47 sources

Graphic part: 12 posters.

INFORMATION FLOW CHANNELS, NETWORK INFORMATION FLOW CHANNEL, OPTICAL INFORMATION FLOW CHANNEL, VIBRO-ACOUSTIC INFORMATION FLOW CHANNEL, ACOUSTIC INFORMATION FLOW CHANNEL, COMPUTERIZED WORKPLACE PROTECTION.

The bachelor's qualification work is devoted to the development of an information leakage prevention system for a computerized workplace.

The study analyzes modern threats of information leakage, assesses the security level of a computerized workplace, and identifies key vulnerabilities. A comprehensive set of measures to prevent data leaks has been developed, including organizational, software-hardware, and cryptographic methods of information protection.

As a result of the work, accompanying documentation for the information leakage prevention system has been created: a threat model, security policy, technical specifications, implementation plan for protective measures, recommendations for access control, risk assessment report, confidential information handling regulations, and a protocol for testing the effectiveness of the proposed solutions.

Preparations for the implementation of the developed system have been carried out to ensure reliable information protection and minimize the risks of unauthorized data disclosure.

05.06.2025 _____

ЗМІСТ

# ВСТУП

У сучасному інформаційному суспільстві, де цифрові технології охоплюють усі сфери діяльності від бізнесу до управління, захист інформаційних ресурсів є стратегічно важливим питанням. Зі збільшенням обсягів оброблюваних даних та ускладненням IT-інфраструктур зростають і загрози, пов'язані з несанкціонованим доступом, витоком конфіденційної інформації та цілеспрямованими кіберінцидентами. Це питання особливо актуальне в контексті широкого використання комп'ютеризованих робочих місць, які часто мають доступ до внутрішніх мереж, електронного документообігу, баз даних і зовнішніх інформаційних каналів.

Витоки інформації, незалежно від того, чи мають вони технічне, організаційне або людське походження, несуть серйозні ризики для організації, включаючи втрату комерційної таємниці, порушення законів про конфіденційність, фінансові санкції та шкоду репутації. З цієї причини існує потреба не лише у швидкому реагуванні на інциденти, але й в активному впровадженні систем запобігання витоку інформації. У цьому контексті створення ефективних, надійних і адаптивних систем захисту інформації на комп'ютеризованих робочих місцях є ключовим завданням.

Метою роботи є проєктування системи запобігання інформаційним витокам комп’ютеризованого робочого місця, експериментальне впровадження та апробація створеної системи.

Для досягнення мети кваліфікаційної роботи необхідно виконати такі завдання:

– проаназілувати предметну область кваліфікаційної роботи;

– дослідити існуючі системи запобігання інформаційним витокам, методи їх роботи;

– проаналізувати типові загрози комп’ютеризованого робочого місця;

– побудувати модель загроз типового комп’ютеризованого робочого місця;

– визначити найбільш загрозливі потенційні канали витоку інформації;

– побудувати модель порушника типового комп’ютеризованого робочого місця;

– спроєктувати систему запобігання інформаційним витокам комп’ютеризованого робочого місця;

– імплементувати спроєктовану систему в рамках експериментального робочого місця;

– провести тестування та апробацію реалізованої системи;

– провести оцінку захищеності та оцінку затрат реалізації спроєктованої системи запобігання інформаційним витокам.

За темою кваліфікаційної роботи було опубліковано тези конференції.

Особливістю цієї роботи є комплексний підхід, що поєднує технічні, організаційні та правові аспекти захисту інформації. Вона враховує чинне українське законодавство, таке як Закон «Про інформацію», Закон «Про захист інформації в інформаційно-комунікаційних системах», Закон «Про державну таємницю», а також міжнародні стандарти, такі як ISO/IEC 27001, NIST SP 800-53 та GDPR. Розроблена система повинна бути не тільки технічно ефективною, але й відповідати цим вимогам. Крім того, враховуються сучасні тенденції у сфері кібербезпеки, такі як розвиток методів соціальної інженерії, зростання активності APT-груп та використання штучного інтелекту в атаках на корпоративну інфраструктуру. Це вимагає динамічного, гнучкого та адаптивного підходу до проектування системи безпеки.

# 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ РОБОТИ. ДОСЛІДЖЕННЯ ІНСУЮЧИХ ПРОТОТИПІВ ТА МЕТОДІВ ЗАПОБІГАННЯ ІНФОРМАЦІЙНИМ ВИТОКАМ

## 1.1 Аналіз предметної області роботи та типової проблематики інформаційних витоків.

Розпочнемо роботу з визначення ключових аспектів предметної області, що стосується інформаційних витоків, а також типових проблем, які виникають у процесі забезпечення інформаційної безпеки. Інформаційні витоки є однією з головних загроз для організацій різних масштабів та сфер діяльності. Вони можуть відбуватися через різні фактори, включаючи технічні недоліки, людський фактор, внутрішні та зовнішні атаки. Основна мета аналізу предметної області – виявлення ключових джерел ризиків, що можуть призвести до витоку конфіденційної інформації. Однією з основних причин витоків є неналежний контроль за доступом до конфіденційних даних, що може спричиняти ситуації, коли співробітники мають доступ до інформації, яка не стосується їхніх посадових обов’язків. Це може стати передумовою для зловживань або ненавмисного розголошення інформації [1-2].

Витоки можуть виникати через використання ненадійних програмних рішень, які містять вразливості та можуть бути атаковані зловмисникам. Оновлення програмного забезпечення та використання сучасних технологій шифрування відіграють ключову роль у забезпеченні безпеки даних. Крім того, важливим аспектом є соціальна інженерія – методи психологічного впливу на співробітників з метою отримання конфіденційної інформації. Недостатня обізнаність персоналу щодо таких методів може призводити до того, що співробітники добровільно розкривають важливі дані шахраям або залишають їх доступними для сторонніх осіб [3]. Відсутність чітких політик інформаційної безпеки та їх несвоєчасне оновлення також є проблемою, що сприяє витокам. Організації повинні розробляти та впроваджувати стандартизовані підходи до контролю доступу, моніторингу дій користувачів, а також проведення регулярних

аудитів системи безпеки. Неналежний контроль над передачею даних та відсутність механізмів моніторингу можуть призводити до несанкціонованого розповсюдження інформації за межі компанії [4]. Компанії можуть зазнавати значних фінансових втрат через штрафи, судові позови, втрату клієнтів та зниження репутації. Дослідження показують, що наслідки витоку конфіденційних даних можуть мати довгостроковий негативний вплив на діяльність організації, особливо якщо вона працює в сферах, що потребують високого рівня довіри, таких як фінансові послуги чи медицина [5].

Багато країн мають жорсткі законодавчі вимоги щодо збереження конфіденційності даних, зокрема GDPR в Європі та CCPA у США. Відповідність цим стандартам стає важливим завданням для компаній, оскільки недотримання може призводити до серйозних санкцій та репутаційних втрат. Таким чином, аналіз предметної області дозволяє сформувати комплексний підхід до управління ризиками інформаційних витоків і розробити ефективні стратегії для їх запобігання [6-9]. Запровадження комплексних заходів, таких як багаторівневий контроль доступу, навчання персоналу, шифрування даних та постійний моніторинг інформаційних потоків, дозволяє мінімізувати ризики та створити надійну систему захисту інформації. Успішна стратегія інформаційної безпеки має базуватися не лише на технологічних рішеннях, а й на усвідомленні працівниками важливості захисту даних та відповідальному ставленні до обробки інформації. Відповідно, розуміння предметної області та її проблематики допомагає розробити комплексний підхід до захисту інформаційних активів та підвищити загальний рівень безпеки в організації [10].

Дослідження "Wirtschaftsschutz 2022" (Захист бізнесу 2022) німецької галузевої асоціації Bitkom підтверджує, що хакери добре усвідомлюють економічну цінність інформації та даних у сучасному діловому світі: 36 відсотків опитаних компаній вже постраждали від крадіжки конфіденційних даних та цифрової інформації. Особливо популярними цілями є комунікаційні дані (68%) та дані клієнтів (45%). Збитки, спричинені шантажем, порушенням патентів і втратою продажів, безпосередньо пов'язаними з крадіжкою даних, становлять

кілька мільярдів євро щорічно. Компаніям і організаціям необхідно ще більше посилити захист при обробці своїх критично важливих даних. Додаткові рекомендації допоможуть ще більше вдосконалити загальну концепцію безпеки і зменшити можливості атаки [11].

Витоки комерційної інформації з комп'ютеризованих робочих місць залишаються актуальною проблемою для сучасних підприємств. Зростання обсягів електронної інформації та використання мережевих технологій підвищує ризики несанкціонованого доступу та розповсюдження конфіденційних даних. Основними причинами витоків інформації є як технічні, так і організаційні фактори. До технічних відносяться вразливості в програмному забезпеченні, недостатній захист мереж та відсутність сучасних засобів кібербезпеки. Організаційні фактори включають недостатню обізнаність співробітників щодо правил інформаційної безпеки, відсутність чітких політик захисту даних та недоліки в управлінні доступом до інформації [12].

Кібербезпека є ключовим елементом у сучасному цифровому суспільстві. Оскільки суспільство стає все більш залежним від інтернету та цифрових технологій, кількість потенційних загроз також зростає. Зловмисники постійно розробляють нові та витончені методи атак, ставлячи під загрозу дані, фінанси та репутацію компаній і приватних осіб. Спектр загроз кібербезпеці широкий і різноманітний - від фішингових атак до складних цілеспрямованих атак. Для ефективної протидії цим загрозам важливо розуміти їхню природу та механізми [13]. Фішинг - це форма соціальної інженерії, коли зловмисник видає себе за довірену особу, щоб спонукати жертву надати конфіденційну інформацію, таку як паролі або номери банківських карток [14]. Існують різні види фішингу, зокрема spear phishing (цільовий фішинг) і vishing (націлений на високопоставлених співробітників). Криптоджекінг – це несанкціоноване використання обчислювальних ресурсів жертви шляхом впровадження скриптів для майнінгу криптовалют на чужі комп’ютери або веб-сайти, що уповільнює роботу системи, збільшує витрати на електроенергію та спричиняє знос обладнання, підвищуючи ризик його збоїв [15-16]. Одночасно з цим новим

поколінням кіберзагроз стають атаки на основі штучного інтелекту, де зловмисники застосовують передові технології для підсилення й оптимізації атак, роблячи їх більш ефективними та складними для виявлення, (рис. 1.1) [17-18].


Рисунок 1.1 – Схема розміщення декількох комп'ютеризованих робочих місць у компанії

Відповідно до рисунка, ми бачимо розміщення декількох комп'ютиризованих робочих місць в компанії. Дана схема не є стандартною і офіційно обов'язковою. Але, на разі, дане зображення допомагає усвідомити як виглядає схема системи в корпорації або у інших офісах, де працюють та проводять свій час працівники.

У корпоративних комп'ютерних системах існує широкий спектр загроз, кожна з яких становить серйозну небезпеку для конфіденційності, цілісності та доступності даних. Навіть одна проігнорована загроза може призвести до масштабного витоку конфіденційних даних або порушення критично важливих процесів. В наступній таблиці показано більше інформації про них.

Таблиця 1.1 – Порівняння типових потенційних загроз

| Назва загрози | Ризики | Протидія |
|---|---|---|
| 1 | 2 | 3 |
| Фішинг | Фішингові атаки спрямовані на викрадення конфіденційних даних, таких як паролі та фінансова інформація, шляхом маніпуляцій користувачами через підроблені вебсайти або електронні листи [19-20]. Це може призвести до витоку корпоративних даних, фінансових втрат і репутаційних ризиків. | Використання багатофакторної автентифікації (MFA), фільтрація електронної пошти, навчання співробітників та впровадження засобів виявлення шкідливих посилань [21]. |
| Шкідливе програмне забезпечення | Віруси, трояни та програми-вимагачі можуть пошкоджувати або шифрувати файли, вимагати викуп за відновлення доступу до даних, а також створювати бекдори для атакуючих [22]. | Антивірусний захист, регулярне оновлення програмного забезпечення, сегментування мережі, резервне копіювання даних [23]. |
| DDoS-атаки | DDoS-атаки можуть вивести з ладу корпоративні сервіси, створити фінансові збитки та підірвати довіру клієнтів через недоступність ресурсів [24]. | Використання систем виявлення та запобігання вторгненням (IDS/IPS), балансувальники навантаження, мережеві. |

Закінчення таблиці 1.1

| 1 | 2 | 3 |
|---|---|---|
| Атаки на паролі | Використання слабких або повторюваних паролів може сприяти компрометації облікових записів та несанкціонованому доступу до конфіденційної інформації. | Застосування комплексної політики паролів, застосування менеджерів паролів, політики регулярної зміни паролів та багатофакторної автентифікації [25-26]. |
| Слабка мережева безпека | Відсутність належного контролю мережевого трафіку може призвести до проникнення атакуючих у внутрішню мережу організації. | Використання брандмауерів, VPN, регулярний аудит безпеки, сегментація мережі та впровадження політик мінімальних привілеїв [27]. |

За підсумками аналізу літератури та відкритих джерел було встановленно, найбільш поширенні загрози та можливі способи протидії їм. Результати даного аназілу будуть використанні в наступних кроках проектування та імплементації системи захисту робочого місця.

Окрему небезпеку становлять атаки на паролі, зокрема підбір слабких або викрадених паролів. Зокрема, атаки на паролі можуть реалізовуватись через методи перебору (brute force). Грубий перебір - це метод, заснований на переборі всіх можливих варіантів ключа (пароля, PIN-коду або ключа шифрування) до тих пір, поки не буде знайдений правильний [28]. Щоб зменшити ризик таких атак, компанії впроваджують політики мінімальної довжини пароля, обов’язкове використання спеціальних символів, а також обмеження кількості спроб входу.,

що дає змогу зловмисникам отримати несанкціонований доступ до акаунтів і систем. Слабка мережева безпека - це недоліки в проектуванні та захисті комп'ютерних мереж, які створюють можливості для зловмисників отримати несанкціонований доступ до даних, внутрішніх систем та інтерфейсів управління. Найпоширенішими прикладами є використання незахищених або застарілих мереж Wi-Fi, вразливих до перехоплення трафіку та атак типу «людина посередині» (MITM). Передача інформації через відкриті незашифровані протоколи, такі як HTTP, FTP і Telnet, де логіни та паролі можуть бути перехоплені. Наявність відкритих або погано налаштованих портів, які створюють точки входу, такі як: відсутність контролю доступу до мережевих ресурсів, наприклад, відсутність сегментації VLAN або фільтрації доступу за MAC або IP-адресою. VPN при віддаленому доступі до внутрішніх ресурсів не використовується, існує ризик витоку інформації під час передачі [29].

Відсутність систем виявлення та запобігання вторгнень (IDS/IPS), що може призвести до того, що атаки залишаться невиявленими, поки не буде завдано шкоди.

Використання застарілого програмного забезпечення та вразливих версій систем є однією з основних причин кіберінцидентів. Застарілі операційні системи, програми та драйвери часто містять відомі вразливості, більше не підтримуються виробниками та не надають оновлень безпеки. Зловмисники активно використовують ці вразливості для запуску експлойтів та інших атак. Наприклад, атака WannaCry 2017 – це комп'ютерний вірус, що вражає операційну систему Microsoft Windows шляхом шифрування файлів. Цей вірус був поширений саме через вразливість у старій версії Windows, яку більшість жертв не оновили [30]. Крім того, використання ненадійних мережевих протоколів, таких як FTP, Telnet і HTTP (без SSL/TLS), дозволяє перехоплювати дані, що передаються, включаючи логіни, паролі та конфіденційну інформацію. Замість них слід використовувати сучасні безпечні протоколи: sftp, ssh, https, tls 1.2/1.3. Окрім технічних аспектів, важлива також кібергігієна. Це включає регулярне оновлення програмного забезпечення, використання антивірусу, складних паролів, двофакторної

автентифікації, уникнення підозрілих посилань та резервне копіювання даних.

## 1.2 Дослідження існуючих систем протидії інформаційним витокам

Системи запобігання витоку інформації на комп'ютеризованих робочих місцях є ключовим компонентом сучасних систем інформаційної безпеки, а їх впровадження є пріоритетним завданням для всіх організацій та установ.

Однією з найкращих практик в області DLP є захист даних від передачі всередині організації та захисту даних від передачі всередині організації та в зовнішнє середовище, є використання інтегрованих систем, які можуть відстежувати та контролювати передачу даних при взаємодії із зовнішнім середовищем [31]. Іншим поширеним підходом до захисту інформації на робочому місці є впровадження політик доступу та обмеження функціональності робочих станцій, наприклад, шляхом використання режиму кіоску. У цьому режимі доступ можна обмежити лише певними програмами та функціями, що значно знижує ризик несанкціонованого використання інформації [32]. Основними особливостями комп'ютерних кіосків є обмежений інтерфейс, який дозволяє користувачам взаємодіяти лише з авторизованим програмним забезпеченням, відсутність доступу до налаштувань системи, автоматичний запуск певних програм після увімкнення або перезавантаження, а також захист від несанкціонованого доступу або модифікації. Такі обмеження є актуальними в середовищах, де можливий доступ до робочих станцій неавторизованих користувачів, наприклад, у відділеннях банків та службах обслуговування клієнтів.

Основними компонентами типовою DLP-системи є: сервіс моніторингу та контролю за передачею конфіденційної інформації.

Аналіз моделей поведінки користувачів для виявлення нетипової поведінки, можливість запуску обраного програмного забезпечення, а також DLP забезпечує захист шляхом встановлення правил доступу до даних, а також запобігання

спробам копіювання або передачі конфіденційної інформації через зовнішні пристрої або мережеві канали за допомогою засобів копіювання та запису DLP запобігає спробам копіювання або передачі конфіденційної інформації через зовнішні пристрої або мережеві канали за допомогою засобів копіювання та запису. Запобігає спробам копіювання або передачі конфіденційної інформації. Поведінковий аналіз використовує алгоритми для відстеження та аналізу поведінки користувачів і автоматично виявляє аномалії, які можуть свідчити про потенційні загрози. Разом ці елементи створюють багаторівневу систему захисту, яка посилює безпеку на робочому місці, запобігаючи витоку даних як від зовнішніх загроз, так і від внутрішніх ризиків. Задачею будь-якої системи запобігання інформаційним витокам є встановлення можливих каналів витоку інформації та блокування несанкціонованої передачі по них [33].

Розглянемо можливі канали витоку інформації, найбільш поширеними серед них є:

– акустичні канали витоку інформації;
– віброакустичні канали витоку інформації;
– акустико-електричні канали витоку інформації;
– мережеві канали витоку інформації;
– оптичні канали витоку інформації.

Розглянемо, усі ці канали по черзі, та як саме витік інформації може бути саме серед перечислених каналах.

Акустичні канали витоку інформації середовищем поширення звукового сигналу є повітря.

Через «мембранний ефект» викликаний коливаннями в тонких (відносно довжини) і зазвичай відносно легких елементах огороджувальних конструкцій будівлі, які прогинаються під впливом звуку.

Через тріщини, отвори, пази та інші акустичні отвори, тобто шляхом прямого поширення акустичних коливань.

Віброакустичні канали витоку інформації основним середовищем поширення звукового сигналу є огороджувальні конструкції будівлі (стіни, вікна,

двері, підлога тощо) та інженерні комунікації. У цьому випадку для перехоплення звукового сигналу використовуються контактні мікрофони (акселерометри).

Віброакустичні канали також використовуються для перехоплення інформації за допомогою підслуховуючих пристроїв. Радіоканали часто використовуються для передачі інформації, і такі пристрої часто називають радіостетоскопами. Датчики також можуть використовуватися для передачі інформації оптичними каналами в ближньому інфрачервоному діапазоні довжин хвиль або ультразвуковими каналами (через інженерні комунікації).

Акустико-електричні канали витоку інформації виникає при перетворенні акустичного каналу в електричний. Деякі елементи допоміжних технічних засобів і систем (ДТС), такі як трансформатори, котушки індуктивності, електромагніти у вторинних годинниках і телефонних дзвінках, мають здатність змінювати свої параметри (ємність, індуктивність, опір) під впливом звукового поля, що генерується джерелом звукового сигналу [34].

Мережеві шляхи витоку інформації - це використання мережевої інфраструктури для несанкціонованої передачі конфіденційних або критично важливих даних назовні або між підрозділами всередині організації. Сюди входять легальні протоколи передачі даних, такі як HTTP, FTP і SMTP, а також нелегальні методи передачі, які маскують інформацію в легальному трафіку, наприклад, тунелювання і стеганографічні приховані канали. Крім того, бездротові мережі Wi-Fi і Bluetooth, VPN і проксі-сервери можуть використовуватися для обходу систем контролю, що збільшує ризик витоку. Використання хмарних сервісів обміну файлами також може бути джерелом витоку, особливо якщо немає відповідних політик безпеки. Витоки через мережі важко виявити, оскільки вони часто відбуваються через стандартні мережеві порти та протоколи, і тому їх важко запідозрити. Тому для захисту від витоків використовуються комплексні системи моніторингу мережевого трафіку, аналіз поведінки користувачів, фільтрація контенту, шифрування даних і суворі політики контролю доступу. Важливо виявляти аномалії в мережевому трафіку, які можуть свідчити про передачу конфіденційної інформації, наприклад, раптове

збільшення обсягу відправлених даних або незвичні адреси призначення [35].

Оптичні канали витоку інформації передбачають передачу конфіденційних даних за допомогою оптичних сигналів, які можуть бути виявлені зловмисниками, що не мають прямого доступу до обладнання або мережі. Такі витоки інформації можуть відбуватися через спонтанні випромінювання з екранів моніторів, індикаторів обладнання, мерехтіння світлодіодів на мережевих адаптерах, лазерне зчитування вібрацій на віконному склі та використання інфрачервоних каналів на камерах спостереження. Одним з найвідоміших методів витоку інформації є використання високочутливих телевізійних камер та оптичних датчиків для зчитування інформації з екранів через вікна або на відстані.

Лазерні мікрофони також можуть перехоплювати звукові коливання, викликані розмовами в приміщенні, фіксуючи найдрібніші коливання віконного скла, яке деформується під впливом звукових хвиль. В результаті утворюється фотоелектричний шлях витоку інформації, що дозволяє зловмиснику відновити зміст переданої інформації без фізичного проникнення в приміщення.

Для протидії такому витоку інформації використовуються такі методи, як екранування вікон спеціальними плівками, використання жалюзі, створення захищених приміщень без вікон, а також виявлення активних джерел оптичного випромінювання поблизу об'єкта [36].

DLP-системи як засіб запобігання витокам інформації системи запобігання витокам інформації (Data Loss Prevention, DLP) відіграють ключову роль у забезпеченні безпеки даних. Вони працюють шляхом моніторингу та аналізу потоків інформації в мережі, на пристроях та в хмарних середовищах. DLP-системи розпізнають конфіденційну інформацію, використовуючи попередньо задані правила та шаблони, а також можуть блокувати її передачу через незахищені канали. Наприклад, такі продукти як McAfee Total Protection for Data Loss Prevention та Symantec Data Loss Prevention забезпечують контроль за передачею файлів, електронної пошти та знімних носіїв.

Системи з протидії інформаційним витокам можуть бути складовою

частиною комплексної системи захисту інформації (Далі – КСЗІ). КСЗІ охоплюють сукупність організаційних та технічних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. Вони включають впровадження політик безпеки, регулярний аудит систем, шифрування даних, а також багаторівневий контроль доступу [37].

Таким чином, ми дослідили системи протидії інформаційним витокам та встановили, що DLP-рішення є важливою складовою захисту даних. Вони забезпечують контроль доступу, моніторинг, поведінковий аналіз і блокування несанкціонованих передач. Ефективним доповненням є використання режиму кіоску, що обмежує функціональність робочих місць. Окрему загрозу становлять технічні канали витоку, для захисту від яких застосовуються екрани, фільтри та шифрування.

## 1.3 Дослідження державної та міжнародної нормативно-правової бази та темою роботи

Нормативно-правова база відіграє важливу роль у регулюванні правовідносин як на державному, так і на міжнародному рівнях, дозволяючи виявити правові прогалини, забезпечити ефективне застосування законодавства та узгодити внутрішні норми з міжнародними стандартами. Конституція України визначає основні права і свободи людини, а також принципи функціонування правової системи, зокрема, у контексті досліджуваної теми важливими є статті, що регламентують принципи державного управління та гарантії прав суб’єктів правовідносин.

У сфері кібербезпеки, запобігання інформаційним витокам на робочому місці є однією з ключових задач, адже витік даних може мати критичні наслідки як для державного сектору, так і для приватних компаній. В Україні правову основу складають такі закони, як «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» та «Про державну таємницю», що

регулюють обіг, доступ та захист як публічної, так і класифікованої інформації, а також передбачають відповідальність за порушення режимів захисту. Окрему роль відіграють норми Кримінального кодексу України, які встановлюють покарання за комп'ютерні злочини, несанкціонований доступ, перехоплення даних або незаконне використання службової/комерційної інформації.

Організаційно-технічну основу формують, наприклад ДСТУ ISO/IEC 27001:2015, що є основою для впровадження систем управління інформаційною безпекою (ISMS), та ДСТУ 2737-94, який описує термінологічну базу у сфері захисту інформації. Важливими для фахівців з кібербезпеки є також нормативні документи з технічного захисту інформації (НД ТЗІ), які описують критерії оцінки захищеності систем та порядок сертифікації засобів захисту [38].

Нормативні документи з технічного захисту інформації (НД ТЗІ) є важливим елементом нормативно-правової бази України у сфері інформаційної безпеки. Особливе значення мають НД ТЗІ 1.1-003-99 та НД ТЗІ 2.5-010-03, які визначають термінологію та основні процедури забезпечення технічного захисту інформації в інформаційно-телекомунікаційних системах.

НД ТЗІ 1.1-003-99 має назву «Технічний захист інформації. Терміни та визначення» і є базовим документом, що уніфікує термінологію в галузі технічного захисту інформації. Він містить визначення основних понять, що використовуються при проектуванні, впровадженні та оцінці систем захисту інформації: «технічний захист інформації», «заходи захисту інформації», «автоматизовані системи», «несанкціонований доступ», «інформаційна безпека» тощо. Використання узгодженої термінології має вирішальне значення для взаємодії між державними органами, організаціями, розробниками, аудиторами та експертами у сфері інформаційної безпеки. Цей документ буде використано як методологічну основу для розробки інших нормативних документів, стандартів, глосаріїв та навчальних матеріалів з питань кібербезпеки та ТЗІ.

Іншим важливим стандартом є НД ТЗІ 2.5-010-03 «Захист інформації в інформаційно-телекомунікаційних системах. Процедури забезпечення технічного захисту інформації». Цей документ визначає алгоритм дій для організацій, які

обробляють інформацію з обмеженим доступом, що не становить державної таємниці. Основним завданням є впровадження ефективної системи технічного захисту відповідно до виявлених загроз.

Процес створення системи захисту інформації починається з обстеження об'єкта інформатизації відповідно до вимог НД ТЗІ 2.5 з метою визначення конфігурації та структури системи, а також аналізу потоків інформації та можливостей її витоку. Потім ІТС класифікуються відповідно до важливості інформації, що обробляється, та наслідків її витоку. Далі будується модель загроз і визначається модель зловмисника, щоб сформулювати обґрунтовані вимоги до системи безпеки. На основі цієї інформації розробляється технічне завдання на побудову системи безпеки, яке включає перелік необхідних засобів і заходів протидії.

Документ приділяє особливу увагу використанню засобів захисту інформації, які повинні бути перевірені або сертифіковані уповноваженим національним органом. Після реалізації всіх заходів і рішень ІТС сертифікується (або акредитується), що підтверджує відповідність вимогам КЗІ.

Таким чином, НД ТЗІ 2.5 є комплексною методологією створення надійного середовища технічного захисту, що має як стратегічний (організаційний, плановий), так і практичний (технічний) рівні реалізації.

Разом дві збірки документів НД ТЗІ 1.1 та НД ТЗІ 2.5 складають основу нормативної бази у сфері технічного захисту інформації. Ці документи визначають не тільки термінологію, якою користуються фахівці з інформаційної безпеки, а й конкретні процедури впровадження механізмів захисту в сучасних ІТ-системах з урахуванням актуальних ризиків і загроз. Дотримання цих документів є обов'язковим для організацій, що працюють з конфіденційною інформацією, і допомагає забезпечити стійкість інформаційної інфраструктури до внутрішніх і зовнішніх загроз.

На міжнародному рівні спеціалісти з кібербезпеки орієнтуються на серію стандартів ISO/IEC 27000, що є світовим бенчмарком у сфері захисту інформації: ISO/IEC 27001 визначає вимоги до ISMS, ISO/IEC 27002 описує практичні заходи

безпеки, ISO/IEC 27005 фокусується на управлінні ризиками, а ISO/IEC 27035 — на реагуванні на інциденти.

Американські стандарти NIST, зокрема NIST SP 800-53 (контроль безпеки та приватності), NIST SP 800-171 (захист контрольованої некласифікованої інформації) та NIST SP 800-88 (рекомендації з очищення носіїв), є корисними при розробленні політик безпеки та процедур в компаніях, що працюють у міжнародному середовищі [39].

Додатково, регламент GDPR формує вимоги до захисту персональних даних у ЄС, а фреймворки COBIT та ITIL допомагають вибудовувати управління IT та кібербезпекою в цілому [40].

Законодавство України (Закон «Про інформацію», Закон «Про захист інформації в ІТС», Закон «Про державну таємницю»), міжнародні стандарти (ISO/IEC 27001, GDPR, NIST SP 800-53 тощо) та спеціалізовані нормативні документи з технічного захисту інформації (НД ТЗІ 1.1-003-99 та 2.5-010-03), нормативна база безпосередньо формує вимоги до структури, функціонування та відповідності систем захисту інформації. Ці вимоги забезпечуються шляхом:

– юридичну узгодженість системи із внутрішнім і міжнародним правовим полем;

– методологічну чіткість при проєктуванні архітектури системи;

– стандартизацію термінів і процедур, що важливо для внутрішньої документації та аудиту;

– захист від юридичних ризиків, зокрема під час перевірок, ліцензування, сертифікації;

– готовність до інтеграції в корпоративну інфраструктуру, яка працює в багатонаціональному правовому середовищі.

## 1.4 Постановка задачі проєктування

Згідно проведеного аналізу предметної області, дослідження існуючих

систем протидії інформаційним витокам, а також нормативно-правової бази, що регулює питання захисту даних, було визначено основні напрями для розробки ефективної системи запобігання витокам інформації на комп'ютеризованому робочому місці. Було встановлено, що сучасні загрози включають як технічні, так і організаційні чинники: з одного боку, це вразливості програмного забезпечення, недостатній захист мереж, технічні канали витоку (акустичні, віброакустичні, оптичні, електромагнітні); з іншого боку, це людський фактор, недостатня обізнаність персоналу, відсутність чітких політик безпеки, слабкий контроль доступу та моніторингу. Окрім цього, важливу роль відіграють законодавчі вимоги як на національному рівні (зокрема закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», а також стандарти ДСТУ ISO/IEC 27001), так і на міжнародному рівні (стандарти ISO/IEC серії 27000, рекомендації NIST, європейський регламент GDPR), що задають рамки та стандарти для формування комплексної політики кіберзахисту.

Відповідно проєктування передбачає створення багаторівневої системи захисту інформації, яка включає організаційні, адміністративні та технічні заходи. Основні компоненти — багатофакторна автентифікація, контроль доступу, шифрування даних, моніторинг дій користувачів та виявлення аномалій.

Також передбачено блокування технічних каналів витоку, політика «чистого столу» та фізична безпека. Система має відповідати чинному законодавству та міжнародним стандартам. Впровадження методів планується на експериментальному робочому місці з подальшою інтеграцією у робочі процеси. Після реалізації буде проведено тестування за критеріями захищеності, швидкодії, зручності та відповідності вимогам користувачів. У результаті розроблять рекомендації щодо впровадження, оновлення та адаптації системи до нових кіберзагроз. Це дозволить мінімізувати ризики витоків і підвищити рівень інформаційної безпеки в цифровому середовищі.

Таким чином, для досягнення мети кваліфікаційної роботи буде вирішенно такі послідовні задачі:

– формування плану подальших дій, на основі знайдених та проаналізованих теоретичних відомостей за темою кваліфікаційної роботи;

– визначення найбільш загрозливих потенційних каналів витоку інформації;

– створення моделі загроз та моделі порушника типового комп’ютеризованого робочого місця;

– проєктування системи запобігання інформаційним витокам комп’ютеризованого робочого місця;

– імплементація спроєктованої системи в рамках експериментального робочого місця;

– тестування та апробація реалізованої системи;

– оцінка захищеності та оцінка затрат реалізації спроєктованої системи запобігання інформаційним витокам.

Послідовне виконання перелічених кроків дозволить в повній мірі досягнути мети кваліфікаційної роботи. Керуючись цим, можемо приступити до виконання поставлених задач.

## 1.5 Висновок

У цьому розділі було проведено глибокий аналіз предметної області, зосередившись на проблематиці інформаційних витоків, що є однією з найгостріших загроз у сучасній кібербезпеці. Було детально вивчено різні аспекти цієї загрози, її потенційні наслідки для організацій та вразливі місця, які можуть бути використані зловмисниками. Досліджено існуючі методи запобігання інформаційним витокам, зокрема системи DLP-класу, та визначено їхню ефективність і обмеження, особливо у контексті захисту окремого комп'ютеризованого робочого місця. Це дозволило виявити прогалини у поточних підходах, які потребують інноваційних рішень. Також, детально розглянуто нормативно-правову базу, що регулює безпеку даних, для

забезпечення відповідності майбутньої системи чинним стандартам та міжнародним вимогам. На основі отриманих результатів та виявлених потреб сформульовано ключові завдання для проєктування системи захисту інформації на комп'ютеризованому робочому місці та чітко поставлено задачу проектування. Це закладає міцний аналітичний фундамент для подальшої розробки та імплементації ефективного, економічно доцільного та адаптованого рішення, здатного протистояти сучасним викликам у сфері інформаційної безпеки та забезпечити надійний захист конфіденційних даних. Основними висновками є:

– інформаційні витоки залишаються однією з головних загроз для організацій, що підтверджується статистикою інцидентів та масштабами збитків;

– сучасні методи захисту включають багаторівневий контроль доступу, моніторинг дій користувачів, шифрування даних та впровадження політик інформаційної безпеки;

– для ефективного захисту необхідно розробити комплексну систему, яка включатиме як технічні, так і організаційні заходи;

– використання сучасних dlp-систем значно знижує ризики несанкціонованого витоку інформації. Таким чином, результати аналізу дозволили сформувати конкретні завдання для розробки системи захисту, яка відповідатиме актуальним викликам кібербезпеки.

# 2 ПРОЄКТУВАННЯ СИСТЕМИ ЗАПОБІГАННЯ ІНФОРМАЦІЙНИМ ВИТОКАМ КОМП'ЮТЕРИЗОВАНОГО РОБОЧОГО МІСЦЯ

## 2.1 Визначення найбільш загрозливих каналів витоку інформації в контексті окремого комп'ютеризованого робочого місця.

Одним із ключових кроків у створенні ефективної системи запобігання витоку інформації є визначення каналів, якими може відбуватися несанкціоноване поширення конфіденційних даних. У контексті конкретного комп'ютеризованого робочого місця особливо важливо визначити канали, які становлять найбільшу загрозу, з урахуванням особливостей середовища. У цьому підрозділі описано підхід до категоризації та оцінки загрози каналів витоку інформації, зокрема визначення критеріїв, за якими той чи інший канал вважається більш або менш небезпечним.

Одним із визначальних факторів при оцінці ризику витоку даних є не лише потенційна шкода, яку може завдати витік даних, але й імовірність того, що ця подія взагалі відбудеться. Канали, технічно здатні до витоку інформації, але які рідко використовуються або потребують високої кваліфікації, становлять меншу загрозу, ніж ті, що активно застосовуються персоналом (наприклад, електронна пошта, хмарні сервіси, знімні носії). Тому критерій потенціалу витоку є ключовим для правильного ранжування загроз і ефективного розподілу ресурсів безпеки. Ігнорування ймовірності використання каналів може призвести до неправильних пріоритетів у захисті. Водночас важливо враховувати людський фактор — доступність, простоту використання та необізнаність користувачів, що підвищує ризик. Застосування цього критерію забезпечує більш реалістичну та збалансовану оцінку загроз на комп'ютеризованих робочих місцях [41].

Оцінка ризиків витоку конфіденційної інформації повинна базуватись на низці ключових критеріїв. Один із них — обсяг інформації, що може бути переданий через певний канал. Навіть якщо канал використовується рідко, здатність швидко передавати великі обсяги даних (через хмарні сервіси, FTP або знімні носії) значно підвищує рівень загрози. Особливо небезпечні випадки

автоматичного витоку, що відбуваються без участі користувача — наприклад, через шкідливе програмне забезпечення або фонові процеси.

Важливим є також ступінь контрольованості каналу. Канали, які важко виявити або обмежити (наприклад, особисті мобільні пристрої, нестандартні протоколи чи зашифровані з'єднання), створюють вищий рівень ризику, ніж ті, що перебувають під постійним моніторингом, як-от внутрішня мережа або корпоративна електронна пошта. Якщо організація не має технічної чи організаційної можливості контролювати певний канал, його слід вважати потенційно небезпечним.

Ще один важливий фактор — цінність інформації, що може бути передана. Не всі дані однаково критичні: витік технічної або фінансової документації, персональних даних чи комерційної таємниці матиме значно серйозніші наслідки, ніж витік загальнодоступної інформації. Тому при оцінці ризику необхідно враховувати не лише технічні характеристики каналу, а й значущість інформації, з якою працює конкретне комп'ютеризоване робоче місце [42].

Швидкість виявлення витоку інформації є критично важливим чинником для мінімізації шкоди від інциденту. Навіть якщо через канал передається невеликий обсяг даних, витік, що залишається непоміченим протягом тривалого часу, може призвести до суттєвих наслідків. Чим швидше виявляється інцидент, тим більше шансів зупинити витік і зменшити ризики для організації.

Менш загрозливими вважаються канали, де витоки легко виявити — наприклад, завдяки системам журналювання, активному моніторингу чи прямому контролю керівництва. Натомість канали, що дозволяють передавати дані у фоновому режимі або автоматично (наприклад, через синхронізацію з хмарними сервісами, шкідливе ПЗ чи приховані процеси), є значно небезпечнішими через низьку ймовірність своєчасного виявлення.

Крім технічних засобів контролю, важливим є людський фактор. Недостатня обізнаність персоналу або відсутність відповідного інструктажу можуть призвести до затримки виявлення витоку. Тому швидкість виявлення слід розглядати як один із ключових показників загрози, а канали, де витоки

фіксуються лише постфактум, мають розглядатися як високоризикові [43].

Складність технічної реалізації витоку інформації є ключовим фактором при оцінці ризику використання певного каналу. Чим простіше організувати витік — тим вищою є ймовірність його реалізації. Канали, які не потребують спеціальних знань чи інструментів (наприклад, копіювання даних на USB-носій або надсилання через особисту пошту), мають високий пріоритет з точки зору загрози.

Натомість технічно складні методи витоку, як-от використання стеганографії, мережеве тунелювання чи модифікація системних компонентів, потребують значних зусиль і ресурсів. Такі канали вважаються менш імовірними для типових сценаріїв, особливо на звичайних робочих місцях, де працівники мають обмежений рівень технічної підготовки.

Врахування цього критерію дозволяє правильно розставити пріоритети в системі захисту: не слід у першу чергу захищатися від складних, малоймовірних атак, якщо лишаються відкритими прості та доступні способи витоку. Отже, технічна складність каналу напряму впливає на його ризиковість та доцільність впровадження відповідних заходів захисту [44].

Оцінка потенційних наслідків витоку інформації є критично важливим елементом системи управління інформаційними ризиками. Навіть незначний за обсягом витік через другорядний канал може мати катастрофічні наслідки, якщо йдеться про критично важливу або чутливу інформацію. Втрата персональних даних, комерційної таємниці або службової інформації може спричинити штрафи, судові позови, втрату довіри клієнтів і партнерів, а в окремих випадках — навіть загрожувати національній безпеці.

Особливо важливо враховувати довгостроковий ефект таких витоків. Зловмисник може використати викрадену інформацію не одразу, а з певною затримкою — для шантажу, фінансових махінацій чи конкурентної боротьби. Через це навіть одиничний інцидент може мати серйозні наслідки для репутації та стабільності організації.

Отже, оцінка загроз повинна базуватись не лише на технічних

характеристиках каналів, а й на масштабі потенційної шкоди. Це дозволяє адекватно розподіляти ресурси безпеки та захищати насамперед ті ділянки, де витік матиме найболючіші наслідки [45].

Таким чином ми будемо проводити оцінку каналів витоку інформації за таким списком критеріїв:

- ймовірність реалізації;
- обсяг даних;
- контрольованість;
- важливість інформації;
- швидкість виявлення;
- складність реалізації;
- потенційні наслідки.

Оцінку ми будемо проводити по десятибальній шкалі, де 1 – це меньший шанс для загрози, а 10 – це найвищий шанс для загрози.

Наступним етапом, для коректної оцінки критеріїв, розроблено таблиці до кожного каналу витоку інформації, в яких показано та пояснено надану оцінку.

Одним з каналів витоку інформації є оптичний, та в таблиці продемонстровано оцінки до кожних критеріїв та пояснення чому саме такі значення, табл. 2.1.

Таблиця 2.1 – Оцінювання критеріїв оптичні каналу витоку інформації.

| Критерії | Оцінка | Пояснення |
|---|---|---|
| 1 | 2 | 3 |
| Ймовірність реалізації | 3 | Оптичні канали вимагають специфічного обладнання, домовленостей та умов. У більшості середовищ потенціал для розгортання низький. |
| Обсяг даних | 2 | Кількість інформації, яку можна передати оптичними каналами, обмежена. |
| Контрольованість | 5 | Оптичні канали можуть бути утворені несподіваними елементами, що робить їх контроль дуже складним. |

Закінчення таблиці 2.1

| 1 | 2 | 3 |
|---|---|---|
| Важливість інформації | 9 | Якщо канал дозволяє зчитувати екран або клавіатуру, може бути розкрита важлива інформація, така як паролі, персональні дані або конфіденційні документи. |
| Швидкість виявлення | 2 | Оптичні канали важко виявити без цілеспрямованого аналізу. Вони зазвичай не виявляються технічними засобами захисту, а виявлення загроз займає багато часу. |
| Складність реалізації | 8 | Потрібні спеціальні знання, обладнання (наприклад, високочутливі камери та відповідні місця) і доступ до прямої видимості, що ускладнює реалізацію. |
| Потенційні наслідки | 6 | Хоча канал обмежений за обсягом, компрометація навіть малої кількості чутливої інформації (паролі, ключі) може мати серйозні наслідки. |

Відповідно до цієї таблиці ми бачимо, що найбільш критичним критерієм є обсяг даних, а найменш критичними критеріями контрольованість та швидкість виявлення.

Оцінка критичності акустичного каналу витоку інформації за вказаними критеріями буде відображена у таблиці, табл. 2.2.

Таблиця 2.2 – Оцінювання критичностні акустичного каналу витоку інформації.

| Критерії | Оцінка | Пояснення |
|---|---|---|
| 1 | 2 | 3 |
| Ймовірність реалізації | 5 | Витік звуку можливий лише в тому випадку, якщо зловмисник перебуває в межах видимості або має прихований записуючий пристрій. |
| Обсяг даних | 3 | Вона обмежується інформацією, яку можна озвучити, наприклад, усні переговори та фрагменти повідомлень. |

Закінчення таблиці 2.2

| 1 | 2 | 3 |
|---|---|---|
| Контрольованість | 10 | Один із найскладніших для контролю каналів. Люди розмовляють голосно, не усвідомлюючи ризиків, мікрофони приховані або вбудовані в невеликі пристрої. |
| Важливість інформації | 6 | Голосові повідомлення часто містять важливу, але не завжди повну інформацію, наприклад, номери телефонів, паролі та фрагменти розмов. У деяких ситуаціях це може мати велике значення. |
| Швидкість виявлення | 10 | Перехоплення зазвичай не залишає видимих слідів. Якщо не використовувати спеціальне обладнання,не проаналізувати технічне середовище, виявити прослуховування майже неможливо. |
| Складність реалізації | 9 | Достатньо смартфона або прихованого диктофона. |
| Потенційні наслідки | 5 | Якщо передається важлива інформація (наприклад, номери карток або паролі), наслідки можуть бути значними, тоді як для звичайних розмов вплив незначний. |

З даної таблиці видно, що найбільш критичним критерієм є контрольованість та швидкість виявлення, а найменш критичним - обсяг даних.

Оцінка критичності вібро-акустичного каналу витоку інформації за вказаними критеріями буде відображена у таблиці, табл. 2.3.

Таблиця 2.3 – Оцінювання вібро-акустичного каналу витоку інформації.

| Критерії | Оцінка | Пояснення |
|---|---|---|
| 1 | 2 | 3 |
| Ймовірність реалізації | 7 | Реалізація вимагає технічних знань і спеціалізованого підходу, але може бути здійснена зловмисниками з досвідом. |

Закінчення таблиці 2.3

| 1 | 2 | 3 |
|---|---|---|
| Обсяг даних | 4 | Обмежується текстовими даними і залежить від швидкості набору тексту та роботи пристрою. |
| Контрольованість | 9 | Традиційні методи захисту (екрани, політики безпеки) ускладнюють виявлення таких каналів, а для контролю потрібні спеціальні інструменти. |
| Важливість інформації | 7 | Через канал можуть бути перехоплені важливі дані, такі як логіни, паролі та внутрішні документи. |
| Швидкість виявлення | 8 | Без радіомоніторингу або ПЕМ-контролю важко виявити витоки. |
| Складність реалізації | 8 | Для виявлення та декодування сигналів потрібне спеціальне обладнання, яке важко реалізувати, але можливо. |
| Потенційні наслідки | 6 | Залежно від перехопленої інформації, це може мати серйозні наслідки, особливо якщо йдеться про доступ до критично важливих даних. |

У цій таблиці видно, що найбільш критичним критерієм є контрольованість, а найменш критичним критерієм є обсяг даних.

Оцінка критичності мережевого каналу витоку інформації за вказаними критеріями буде відображена у таблиці, табл. 2.4.

Таблиця 2.4 - Оцінювання критерій мережевих каналів витоку інформації.

| Критерії | Оцінка | Пояснення |
|---|---|---|
| 1 | 2 | 3 |
| Ймовірність реалізації | 8 | Реалізація можлива за наявності знань та обладнання, яке стає доступнішим. |
| Обсяг даних | 9 | Через ці канали можна перехоплювати великі обсяги даних, зокрема вміст екрана або натискання клавіш. |

Закінчення таблиці – 2.4

| 1 | 2 | 3 |
|---|---|---|
| Контрольованість | 4 | Контролювати складно через прихований характер і необхідність спеціального моніторингу. |
| Важливість інформації | 7 | Часто витікає важлива інформація — паролі, службові дані тощо. |
| Швидкість виявлення | 5 | Витік важко помітити, часто лишається невиявленим. |
| Складність реалізації | 7 | Потрібні технічні знання й обладнання, що дещо ускладнює атаку. |
| Потенційні наслідки | 8 | Успішний витік може призвести до значних втрат або компрометації системи. |

З даної таблиці видно, що найбільш критичним критерієм є обсяг даних та важливість інформації, а найменш критичними критеріями є контрольованість та швидкість виявлення.

Виконавши оцінювання кожного каналу витоку за критеріями до всіх, було створено загальну таблицю, для розрахунків, щоб визначити найзагрозливіші критерії, табл. 2.5.

Таблиця 2.5 – Загальна оцінка критичності типів каналів витоку інформації.

| Тип каналу | Ймовірність реалізації. | Обсяг даних | Контрольованість | Важливість інформації | Швидкість виявлення | Складність реалізації | Потенційні наслідки | Сума |
|---|---|---|---|---|---|---|---|---|
| Оптичні | 3 | 2 | 5 | 9 | 2 | 8 | 6 | 35 |
| Акустичні | 5 | 3 | 10 | 6 | 10 | 9 | 5 | 47 |
| Вібро-акустичні | 7 | 4 | 9 | 7 | 8 | 8 | 6 | 49 |
| Мережеві | 8 | 9 | 4 | 5 | 5 | 7 | 8 | 46 |

Для визначення найбільш небезпечних каналів витоку інформації, буде застосовано метод аналізу ієрархій для вибору альтернативи за багатьма критеріями. У ході обчислень за даним методом буде виконано попарне порівняння критеріїв між собою для визначення їх вагових коефіцієнтів, а також попарне порівняння каналу витоку, з урахуванням вагових коефіцієнтів критеріїв.

В попарному порівнянні застосовуються оцінки: «1», «3», «5» та «9», де «1» - це ідентичні альтернативи, «3» - це трішки краща альтернатива, «5» - це краще та «9» - це набагато краще. Гіршій альтернативі буде встановлена протилежна оцінка.

Виконаємо попарне порівняння критеріїв, табл. 2.6.

Таблиця 2.6 – Матриця парних порівнянь критеріїв.

| | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 |
|---|---|---|---|---|---|---|---|
| Q1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Q1 | 1 | 5 | 1/5 | 1 | 1/5 | 1/9 | 1/9 |
| Q2 | 1/5 | 1 | 5 | 1/3 | 3 | 1/5 | 5 |
| Q3 | 5 | 1/5 | 1 | 1/3 | 1/5 | 1 | 3 |
| Q4 | 1 | 3 | 3 | 1 | 1/5 | 3 | 1/3 |
| Q5 | 5 | 1/3 | 5 | 5 | 1 | 1/5 | 3 |
| Q6 | 9 | 5 | 1 | 1/3 | 5 | 1 | 3 |
| Q7 | 9 | 1/5 | 1/3 | 3 | 1/3 | 1/3 | 1 |

Після того як ми маємо дані попередньої матриці, ми переходимо до визначення середнього геометричного (формула 2.1) та оцінки векторів критеріїв (формула 2.2).

$$MG=\sqrt[n]{x_1 * x_2 * x_3 \dots * x_n} \quad (2.1)$$

$$w_i = \frac{GM_i}{\sum_{k=1}^{n} GM_k} \quad (2.2)$$

Таким чином, створюється нова таблиця, у якій буде додано також значення середнього геометричного та оцінки вектора, табл. 2.7.

Таблиця 2.7 – Матриця парних порівнянь критеріїв.

| | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | MG | w |
|---|---|---|---|---|---|---|---|---|---|
| Q1 | 1 | 5 | 1/5 | 1 | 1/5 | 1/9 | 1/9 | 0.407 | 0.052 |
| Q2 | 1/5 | 1 | 5 | 1/3 | 3 | 1/5 | 5 | 1 | 0.129 |
| Q3 | 5 | 1/5 | 1 | 1/3 | 1/5 | 1 | 3 | 0.785 | 0.101 |
| Q4 | 1 | 3 | 3 | 1 | 1/5 | 3 | 1/3 | 1.085 | 0.140 |
| Q5 | 5 | 1/3 | 5 | 5 | 1 | 1/5 | 3 | 1.583 | 0.204 |
| Q6 | 9 | 5 | 1 | 1/3 | 5 | 1 | 3 | 2.128 | 0.273 |
| Q7 | 9 | 1/5 | 1/3 | 3 | 1/3 | 1/3 | 1 | 0.785 | 0.101 |
| | | | | | | | Підсумок: | 7.773 | 1 |

З таблиці видно, що найбільш значущим є критерій Q6. Наступним пунктом є оцінка каналів за кожним критерієм. Далі було проведено попарне порівняння альтернатив за критерієм Q1, табл. 2.8.

Таблиця 2.8 – Оцінка каналів витоку інформації за критерієм ймовірність реалізації.

| Q1 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 3 | 5 | 9 | 3.400 | 0.581 |
| A2 | 1/3 | 1 | 3 | 5 | 1,495 | 0.255 |
| A3 | 1/5 | 1/3 | 1 | 3 | 0.669 | 0.114 |
| A4 | 1/9 | 1/5 | 1/3 | 1 | 0.294 | 0.050 |
| | | | | Підсумок: | 5.858 | 1 |

За цими результатами видно, за критерієм Q1, найвищу оцінку отримала альтернатива A1. Далі було проведено порівняння з критерієм Q2, табл. 2.9.

Таблиця 2.9 - Оцінка каналів витоку інформації за критерієм обсяг даних.

| Q2 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 3 | 5 | 9 | 3.400 | 0.557 |
| A2 | 1/3 | 1 | 3 | 9 | 1.732 | 0.283 |
| A3 | 1/5 | 1/3 | 1 | 5 | 0.760 | 0.124 |
| A4 | 1/9 | 1/9 | 1/5 | 1 | 0.222 | 0.036 |
| | | | | Підсумок: | 6.114 | 1 |

За цими проміжними результатами видно, що за критерієм Q2, найвищу оцінку отримала альтернатива А1. Наступне було проведено попарне порівняння альтернатив з критерієм Q2, табл. 2.10.

Таблиця 2.10 - Оцінка каналів витоку інформації за критерієм контрольованість.

| Q3 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 5 | 9 | 1/3 | 1.968 | 0.319 |
| A2 | 1/5 | 1 | 1/3 | 1/9 | 0.293 | 0.048 |
| A3 | 1/9 | 3 | 1 | 1/5 | 0.505 | 0.082 |
| A4 | 3 | 9 | 5 | 1 | 3.400 | 0.551 |
| | | | | Підсумок: | 6.166 | 1 |

Ці проміжні результати показують, що за критерієм Q3 найвищий бал отримала альтернатива А4. Далі наведено попарне порівняння альтернатив за критерієм Q3 у таблиці, табл. 2.11.

Таблиця 2.11 - Оцінка каналів витоку інформації за критерієм важливість інформації.

| Q4 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 1/5 | 1/3 | 1/9 | 0.293 | 0.050 |
| A2 | 5 | 1 | 3 | 1/3 | 1.495 | 0.255 |
| A3 | 3 | 1/3 | 1 | 1/5 | 0.669 | 0.114 |
| A4 | 9 | 3 | 5 | 1 | 3.400 | 0.581 |
| | | | | Підсумок: | 5.857 | 1 |

За цими результатами показано, що за критерієм Q4 - найвищий бал має А4. Далі наведено порівняння альтернатив за критерієм Q5 у таблиці, табл. 2.12.

Таблиця 2.12 - Оцінка каналів витоку інформації за критерієм швидкість виявлення.

| Q5 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

Закінчення таблиці 2.12.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| A1 | 1 | 9 | 5 | 3 | 3.400 | 0.551 |
| A2 | 1/9 | 1 | 1/3 | 1/5 | 0.294 | 0.048 |
| A3 | 1/5 | 3 | 1 | 1/9 | 0.507 | 0.082 |
| A4 | 1/3 | 5 | 9 | 1 | 1.968 | 0.319 |
| | | | | Підсумок: | 6.169 | 1 |

Ці проміжні результати показують, що за критерієм Q5 найвищий бал отримала альтернатива A1. Далі наведено попарне порівняння альтернатив за критерієм Q6 у таблиці, табл. 2.13.

Таблиця 2.13 - Оцінка каналів витоку інформації за критерієм складність реалізації.

| Q6 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 3 | 1 | 1/3 | 1 | 0.201 |
| A2 | 1/3 | 1 | 1/3 | 1/5 | 0.384 | 0.077 |
| A3 | 1 | 3 | 1 | 1/3 | 1 | 0.201 |
| A4 | 3 | 5 | 3 | 1 | 2.593 | 0.521 |
| | | | | Підсумок: | 4.977 | 1 |

Ці проміжні результати показують, що за критерієм Q6 найвищий бал отримала альтернатива A4, що свідчить про її перевагу за цим показником. Це дозволяє зробити попередній висновок про її ефективність у межах даного критерію. Далі для повноти аналізу розглянемо попарне порівняння альтернатив за критерієм Q7, яке наведено у таблиці 2.14.

Таблиця 2.14 - Оцінка каналів витоку інформації за критерієм потенційні наслідки.

| Q7 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| A1 | 1 | 1/3 | 1 | 5 | 1.139 | 0.220 |
| A2 | 3 | 1 | 3 | 5 | 2.593 | 0.502 |
| A3 | 1 | 1/3 | 1 | 5 | 1,139 | 0.220 |

Закінчення таблиці 2.14

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| A4 | 1/5 | 1/5 | 1/5 | 1 | 0.299 | 0.058 |
| | | | | Підсумок: | 5.170 | 1 |

Ці проміжні результати за останньою таблицею показують, що за критерієм Q7 найвищий бал отримала альтернатива А2.

Після проведення оцінювання кожного критерія, наступним кроком буде обчислення кількісного індикатора якості кожної альтернативи, для цього буде використано формулу 2.3. Вона дозволяє звести результати багатокритеріального аналізу до єдиного числового показника, який відображає узагальнену оцінку кожної альтернативи з урахуванням вагових коефіцієнтів критеріїв.

$$Q^{2Л}(a_j) = \sum_{i=1}^{N} w_j V_{ji} \quad (2.3)$$

Таким чином буде створено таблицю, де будуть відображені дані для обчислення кількісного індикатору критичності кожної альтернативи.

Таблиця 2.15 – Дані для обчислення кількісного індикатору критичності кожної альтернативи.

| | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | | U |
|---|---|---|---|---|---|---|---|---|---|
| A1 | 0.581 | 0.557 | 0.319 | 0.050 | 0.551 | 0.201 | 0.220 | | 0.052 |
| A2 | 0.255 | 0.283 | 0.048 | 0.255 | 0.048 | 0.077 | 0.502 | X | 0.129 |
| A3 | 0.114 | 0.124 | 0.082 | 0.114 | 0.082 | 0.201 | 0.220 | | 0.101 |
| A4 | 0.050 | 0.036 | 0.551 | 0.581 | 0.319 | 0.521 | 0.058 | | 0.140 |
| | | | | | | | | | 0.204 |
| | | | | | | | | | 0.273 |
| | | | | | | | | | 0.101 |

У таблиці були зазначені усі дані, за якими далі буде проведено розрахунки кожного значення. Для цього буде використано попередню формулу 2.3. Після,

для перевірки точності рішення усіх альтернатив, шукаємо їхню суму, що має дорівнювати одиниці за формулою 2.4 .

$$Q^{2Л}(a_1) + Q^{2Л}(a_2) + \cdots + Q^{2Л}(a_n) = 1 \quad (2.4)$$

Результати обчислення буде відображено у таблиці, табл. 2.16.

Таблиця 2.16 – Розрахунок кількісного індикатор якості кожної альтернативи.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0.030 | + | 0.071 | + | 0.032 | + | 0.007 | + | 0.112 | + | 0.055 | + | 0.022 | = | 0.329 |
| 0.013 | + | 0.037 | + | 0.005 | + | 0.036 | + | 0.010 | + | 0.021 | + | 0.051 | = | 0.173 |
| 0.006 | + | 0.016 | + | 0.008 | + | 0.016 | + | 0.017 | + | 0.055 | + | 0.022 | = | 0.140 |
| 0.003 | + | 0.005 | + | 0.056 | + | 0.081 | + | 0.065 | + | 0.142 | + | 0.006 | = | 0.358 |
| | | | | | | | | | | | Підсумок: | | | 1 |

Згідно з розрахунками, найбільш критичним каналом витоку інформації є мережевий канал, з відносним коефіцієнтом 0.36. Це пов'язано з важливістю інформації, що витікає через мережу, а не з обсягом та безпосереднім впливом витоку, а також з великою складністю впровадження захисних заходів та контролю за ними. На другому місці - оптичний канал витоку, з коефіцієнтом 0.33.

За результатами даної оцінки, було визначено найбільш критичні, разом з тим – найбільш пріоритетні до усунення, канали витоку інформації.

## 2.2 Побудова моделі загроз та моделі порушника типового комп’ютеризованого робочого місця.

Оскільки метою даної кваліфікаційної роботи не є повноцінна розробка КСЗІ, а лише проектування та створення системи протидії інформаційним витокам, модель загроз та модель порушника буде створена у спрощеному вигляді

з акцентом на технічні аспекти інформаційної безпеки. Створенні моделі будуть використанні надалі в ході проектування системи протидії інформаційним витокам.

Таким чином будуть враховані настанови та рекомендації із Закону України "Про національну безпеку України", а також НД ТЗІ 1.4 – 001 – 2000 «Типове положення про службу захисту інформації в автоматизованій системі». Також буде вказано рівень ризику кожної можливої загрози та позначено які саме складові інформаційної безпеки вони порушують. Три основні складові інформаційної безпеки, такі, як конфіденційність (К), цілісність (Ц), доступність (Д), а також спостереженість (С), табл 2.17.

Таблиця 2.17 – Модель загроз комп'ютеризованого робочого місця.

| № | Загроза | Канал витоку | Ймовірність | Рівень шкоди | К | Ц | Д | С |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | Прослуховування розмов через мікрофони ПК чи смартфонів або через людський фактор | Акустичний | Висока | Високий | + | | | + |
| 2 | Витік інформації через вібрації, що фіксуються акселерометрами | Вібро-акустичний | Низька | Середній | + | | | + |
| 3 | Витік інформації через незахищені протоколи передачі даних (HTTP, FTP) | Мережевий | Висока | Неприпустимо високий | + | + | | + |
| 4 | Зчитування інформації з екрана за допомогою спеціальних засобів (шпигунство) | Оптичний | Середня | Високий | + | | | + |
| 5 | Витік інформації через відбиття монітора на окулярах, вікнах тощо | Оптичний | Низька | Середній | + | | | + |

Закінчення таблиці 2.17

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| 6 | Перехоплення мережевого трафіку | Мережевий | Висока | Неприпустимо високий | + | + | | + |
| 7 | Несанкціонований доступ через незахищені порти чи Wi-Fi | Мережевий | Висока | Неприпустимо високий | + | + | + | + |
| 8 | Віруси/шпигунське ПЗ, що передає дані через мережу | Мережевий | Висока | Неприпустимо високий | + | + | + | + |
| 9 | Витік інформації через принтери, сканери з модулем Wi-Fi | Мережевий/ оптичний | Середня | Високий | + | + | | + |
| 10 | Спостереження за натисканнями клавіш за допомогою спецзасобів | Оптичний | Середня | Середній | + | | | + |
| 11 | Витік інформації через фішингові атаки (введення даних у підроблену форму) | Мережевий | Висока | Високий | + | + | | + |
| 12 | Витік інформації через відкриті мережеві порти служб (наприклад, RDP, SMB) | Мережевий | Висока | Неприпустимо високий | + | + | + | + |
| 13 | Витік інформації через ненадійні VPN чи проксі | Мережевий | Середня | Високий | + | + | | + |
| 14 | Витік інформації через публічні або скомпрометовані Wi-Fi мережі | Мережевий | Висока | Високий | + | + | + | + |
| 15 | Витік інформації через зловмисне розширення браузера | Мережевий | Середня | Високий | + | + | | + |
| 16 | Витік інформації через неправильне налаштування файрвола | Мережевий | Середня | Неприпустимо високий | + | + | + | + |

У попередній таблиці було додано можливі загрози, які можуть очікувати на даному робочому місці. Загрози мають різні джерела, але в цілому вони засновані на каналах витоку інформації, які були попередньо згадані. За кількісним індикатором якості альтернатив найбільш небезпечним є мережевий канал. Відповідно до таблиці моделі загроз, більшість ризиків також входять у даний канал витоку інформації.

Для пріоритезації зазначених загроз, буде створено підсумкову таблицю із градацією пріоритетів згідно співвідношення ймовірності виникнення та шкоди загроз, табл. 2.18.

Таблиця 2.18 - Градації пріоритетів згідно співвідношення ймовірності виникнення та шкоди загроз.

| Рівень шкоди / Ймовірність | Низька | Середня | Висока | Небезпечно висока |
|---|---|---|---|---|
| Низька | | 2 | | |
| Середня | | 1 | 4 | 1 |
| Висока | | | 3 | 5 |

Наступним кроком є розробка моделі порушника. Порушники будуть оцінені за різними критеріями зокрема: за категорією порушника, за мотивацією порушника, рівнем обізнаності та рівнем доступу до робочого місця. Опис даних критеріїв зведено в таблицю, табл. 2.19.

Таблиця 2.19 – Критерії оцінки порушника.

| Позначення | Визначення категорії | Рівень загроз |
|---|---|---|
| 1 | 2 | 3 |
| За категорією порушника | | |
| Внутрішні порушники | | |
| ВП 1 | Технічний персонал, (прибиральники, охоронці, електрики тощо) | 1 |
| ВП 2 | Користувачі комп'ютеризованого робочого місця | 2 |

Закінчення таблиці 2.19

| 1 | 2 | 3 |
|---|---|---|
| ВП 3 | Персонал, який обслуговує технічні засоби (адміністратор тощо) | 3 |
| Зовнішні порушники | | |
| ЗП 1 | Відвідувач | 1 |
| ЗП 2 | Хакери | 4 |
| За мотивацією порушника | | |
| М 1 | Безвідповідальність | 1 |
| М 2 | Самоствердження | 2 |
| М 3 | Корислива мета | 3 |
| М 4 | Професійний обов’язок | 4 |
| Рівні обізнаності | | |
| К 1 | Порушник володіє низьким рівнем знань, проте вміє працювати з технічними засобами комп’ютернізованого робочого місця | 1 |
| К 2 | Порушник володіє середнім рівнем знань та практичними навичками роботи з технічними засобами комп’ютернізованого робочого місця | 2 |
| К 3 | Порушник володіє високим рівнем знань у програмуванні та обчислювальної техніки, проєктування та експлуатації комп’ютернізованого робочого місця | 3 |
| К 4 | Порушник знає структуру, функції та механізми дії засобів захисту інформації в комп’ютернізованого робочого місця, їх недоліки та можливості | 4 |
| Доступність до АС | | |
| 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 |

Таблиця категорій порушників дозволяє визначити джерело загрози (внутрішні співробітники, зовнішні сторони, технічний персонал, звичайні користувачі). Це дозволяє зосередити заходи захисту на найбільш ймовірних сценаріях порушень. Таблиця мотивів вказує на те, що атаки можуть бути

мотивовані корисливими інтересами, помстою, ідеологією або недбалістю. Таблиці обізнаності дозволяють оцінити, наскільки добре зловмисник розуміє систему і може передбачити складність атаки. Таблиця доступності вказує на ймовірність фізичного або логічного доступу до об'єкта. Всі ці таблиці допомагають більш точно змоделювати ризики та визначити найкращі заходи захисту.

На основі зазначених критеріїв, побудуємо модель порушників із оцінкою загроз кожного порушника за кожним критерієм та обчисленням відповідної суми загроз, (табл. 2.20).

Таблиця 2.20 – Модель порушника.

| Посада | Категорія порушника | Мотив порушення | Рівень обізнаності | Доступність | Сума загроз |
|---|---|---|---|---|---|
| Користувач | ВП 2 | М 1, М 3 | К 3 | Д 4 | 13 |
| Системний адміністратор | ВП 3 | М 3 | К 4 | Д 4 | 14 |
| Електрик | ВП 1 | М 1 | К 2 | Д 2 | 6 |
| Прибиральник | ВП 1 | М 1 | К 1 | Д 2 | 5 |
| Охоронець | ВП 1 | М 3 | К 2 | Д 3 | 9 |
| Відвідувач | ЗП 1 | М 3 | К 2 | Д 1 | 7 |
| Хакер | ЗП 2 | М 4 | К 4 | Д 1 | 13 |

Згідно з аналізом моделі, найбільші загрози становлять системні адміністратори, користувачі та зовнішні зловмисники. Адміністратори та користувачі є потенційно небезпечними, оскільки мають законний доступ до внутрішніх систем і знання про них, особливо якщо вони мають фінансові мотиви. Зовнішні зловмисники не мають прямого доступу, але компенсують це високими технічними знаннями та мотивацією.

Загрози з боку персоналу з обмеженим доступом і низьким рівнем обізнаності, наприклад, прибиральників або електриків, менш значні. Водночас, навіть помірні загрози від охоронців або відвідувачів не слід повністю виключати, оскільки вони можуть мати фізичний доступ. Загалом, модель фокусується на

загрозах від привілейованих внутрішніх сторін та цілеспрямованих атак ззовні.

## 2.3 Проєктування системи запобігання інформаційним витокам.

У попередніх розділах було розглянуто канали витоку інформації, їх критичність та пріоритетність, а також було створено модель загроз та модель порушника із урахуванням багатьох критеріїв та їх загальної небезпеки. Відповідно до цього найбільш загрозливим до інформаційного витоку є мережевий канал витоку даних, наступним за ним йде оптичний. Відповідно до моделі порушника, найбільш небезпечними є системний адміністратор та користувач, із числа внутрішніх порушників, та зловмисник, із числа зовнішніх. На підставі цього, в ході проектування системи запобігання інформаційним витокам, в першу чергу будуть сплановані заходи щодо усунення найбільш пріоритетних загроз пов’язаних, із даними каналами витоку, із перспективи зазначених порушників. Згідно моделі загроз, критичними є:

– витік інформації через незахищені протоколи передачі даних (HTTP, FTP);

– перехоплення мережевого трафіку (sniffing);

– несанкціонований доступ через незахищені порти чи Wi-Fi;

– віруси/шпигунське ПЗ, що передає дані через мережу;

– витік інформації через відкриті мережеві порти служб (наприклад, RDP, SMB).

Для реалізації комплексного підходу до протидії інформаційним витокам окремо взятого комп’ютеризованого робочого місця, одним із найбільш ефективних засобів є використання режиму кіоску. Використання даного режиму обмежує користувача в діях та змінює загальну філософію роботи комп’ютера із «користувачу не можна робити тільки те, що явно заборонено» на «користувачу можна робити тільки те, що явно дозволено». Це поширена міжнародна практика інформаційної безпеки, що має назву «Заборона по замовчуванню».

Для часткової імплементації режиму кіоска, а також для можливості більш гнучкого налаштування безпекових політик на комп’ютеризованому робочому місці з операційною системою Windows, буде використаний український програмний комплекс ЛОЗА-1.

Система ЛОЗА-1 є програмним засобом захисту інформації від несанкціонованого доступу до автоматизованих систем класу 1 (як правило, автономних комп'ютерів). Система ЛОЗА-1 працює з операційними системами Windows 7/8/8.1/10/11/ Server 2008/2012/2016/. 2019 (32-розрядні та 64-розрядні версії). В системі ЛОЗА-1 реалізовані всі стандартні функції, необхідні для надійного захисту інформації від несанкціонованого доступу та створення комплексної системи захисту інформації. Система «ЛОЗА-1» підтверджена Експертним висновком № 1095, виданим Державною службою спеціального зв'язку та захисту інформації України 2 квітня 2020 року, що підтверджує можливість її застосування для захисту інформації, що становить державну таємницю. Термін дії експертного висновку продовжено до закінчення воєнного стану (лист Адміністрації Держспецзв'язку № 04/05/01-373/ВС1 від 07 лютого 2023 року) [46].

Також система протидії інформаційним витокам включатиме в себе компоненти, спрямовані на вирішення конкретних загроз із числа найбільш пріоритетних. Розглянемо конкретні заходи протидії витоку для даних загроз.

Загроза витоку інформації через незахищені протоколи передачі даних може бути вирішена за допомогою переходів на безпечні протоколи, такі як HTTPS, SFTP або SSH, або використання TLS, зменшує загрози, пов'язані з використанням незахищених протоколів передачі даних у мережевому каналі. Це гарантує, що дані, які передаються, зашифровані та захищені від перехоплення. Крім того, використання незахищених протоколів має бути заборонено на рівні політик доступу та конфігурації мережевого обладнання. Ефективним також може бути використання брандмауерів, систем виявлення атак і моніторингу мережевого трафіку для швидкого виявлення спроб несанкціонованої передачі даних. Важливим елементом є підвищення обізнаності персоналу про ризики,

пов'язані з передачею інформації у відкритому доступі, а також налаштування користувацьких політик на робочих станціях Windows, які обмежують використання незахищених сервісів і протоколів.

Загрозу витоку інформації через перехоплення мережевого трафіку можна зменшити, шифруючи всі дані, що передаються, за допомогою протоколів TLS, OpenVPN та IPsec. Це унеможливлює доступ до вмісту трафіку навіть у разі його перехоплення. Також важливо обмежити доступ до мережі авторизованим користувачам, використовувати сегментацію мережі та відстежувати трафік для виявлення підозрілої активності. На комп'ютеризованих робочих місцях слід додатково впровадити користувацькі політики Windows, що забороняють зміну мережевих налаштувань і підключення до незахищених мереж.

Для реалізації цих заходів можна використовувати такі програми:

– Wireshark для моніторингу та аналізу мережевого трафіку,(рис. 2.1);
– OpenVPN або Cisco AnyConnect для створення безпечних VPN-з'єднань;
– політику безпеки користувача Windows Group Policy;
– Snort або Suricata для виявлення та запобігання вторгнень (IDS/IPS).

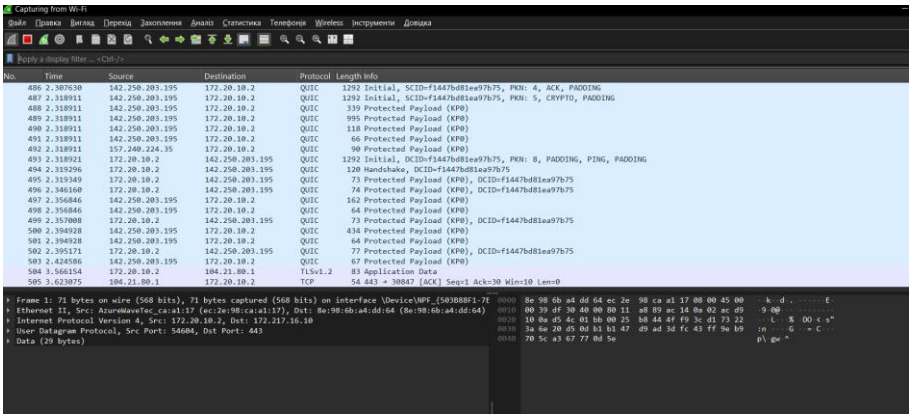



Рисунок 2.1 – Інтерфейс програми для моніторингу трафіку – Wireshark

На комп'ютеризованому робочому місці загрозу несанкціонованого доступу через незахищені порти або Wi-Fi можна зменшити, вимкнувши або заблокувавши всі невикористовувані порти в налаштуваннях операційної системи або за допомогою брандмауера. Також можна встановити покращений фаєрвол від довіреної комерційної компанії, наприклад Norton, який постачається із

вбудованим антивірусним захистом. Дані фаєрволи мають більш широкий функціонал блокування, створення правил та виключень у аналізі трафіку. Підключення до Wi-Fi слід дозволяти тільки в довірених мережах, захищених WPA2 або WPA3. Рекомендується приховувати SSID внутрішньої мережі, використовувати складні паролі доступу та налаштувати автентифікацію пристрою за MAC-адресою.

Для цього можна використовувати такі інструменти:

– брандмауер Windows Defender для контролю мережевих підключень,рис(2.1);

– редактор групової політики для запобігання підключенню до сторонніх Wi-Fi мереж;

– Nmap для виявлення відкритих портів;

– мережеві NetSetMan або Netsh для управління профілями.

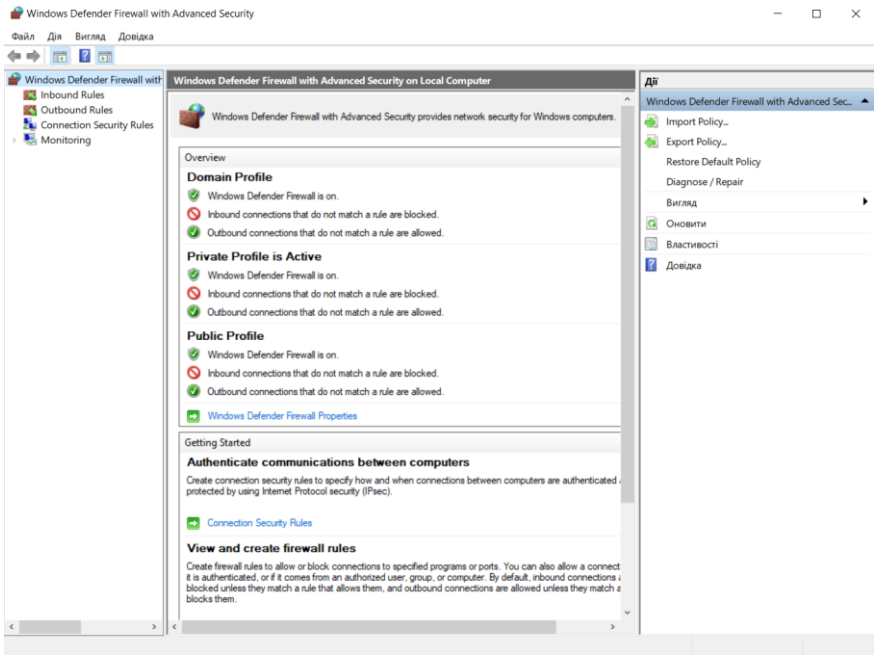



Рисунок 2.2 – Інтерфейс Windows брендмауера

Ці заходи можуть додатково захистити комп'ютеризовані робочі місця від зовнішнього втручання.

Щоб забезпечити захист комп'ютеризованого робочого місця від вірусів і шпигунських програм, які передають дані через мережу, необхідно вжити кілька

заходів. Для початку, слід встановити та регулярно оновлювати антивірусне програмне забезпечення, яке виявляє та блокує шкідливе програмне забезпечення та мережевий трафік. Також необхідно переконатися, що брандмауери налаштовані на моніторинг вхідного та вихідного трафіку для блокування підозрілих з'єднань. Необхідно встановити системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) для моніторингу та аналізу аномалій мережевого трафіку. Крім того, слід регулярно оновлювати операційні системи та програмне забезпечення для усунення відомих вразливостей. Важливо також обмежити права користувачів, щоб запобігти встановленню несанкціонованого програмного забезпечення. Зокрема можна використати готові комерційні програмні комплекси від міжнародних виробників із гарною безпековою репутацією, наприклад вище згаданий Norton.

Для запобігання витоку інформації через відкриті мережеві порти служб, таких як RDP та SMB, необхідно закрити всі непотрібні порти та служби на комп’ютеризованому робочому місці. Впровадити фільтрацію мережевого трафіку за допомогою міжмережевого екрану (брандмауера), налаштувавши його на блокування доступу до критичних портів ззовні. Використовувати засоби шифрування для захисту даних, які передаються через дозволені порти, та впровадити багатофакторну автентифікацію для доступу до служб віддаленого доступу. Регулярно перевіряти відкриті порти і оновлювати програмне забезпечення служб для усунення вразливостей. Заборонити використання небезпечних або застарілих протоколів, а також контролювати права доступу користувачів до мережевих служб. Це забезпечить мінімізацію ризиків несанкціонованого доступу та витоку інформації. У випадку, коли віддалений доступ, зокрема за протоколом RDP все ж необхідний, дані сервіси в жодному разі не повинні бути винесені у публічну зону (зовнішні порти). Дані сервіси повині працювати у локальній або віртуальній мережі комп’ютера, доступ до якої повинен здійснюватись виключно через захищені протоколи, такі як SSH, OpenVPN тощо.

Далі розглянемо загрози із високим пріоритетом, що використовують

мережевий канал витоку інформації. Згідно моделі загроз, такими загрозами є:

– витік інформації через принтери, сканери з модулем Wi-Fi;

– витік інформації через фішингові атаки (введення даних у підроблену форму);

– витік інформації через ненадійні VPN-сервіси чи проксі;

– витік інформації через публічні або скомпрометовані Wi-Fi мережі;

– витік інформації через зловмисне розширення браузера.

Щоб запобігти витоку інформації через мережі, зокрема через Wi-Fi принтери та сканери, бездротовий інтерфейс слід вимикати, коли він не використовується, або працювати лише в захищених та обмежених сегментах мережі. Рекомендується використовувати шифрування з'єднання, автентифікацію користувачів та обмежувати друк і сканування за правами доступу. Також слід вимкнути функцію прямого зовнішнього підключення та постійно оновлювати прошивку пристрою.

Для запобігання витоку інформації через фішингові атаки, такі як введення даних у підроблені форми, впроваджувати механізми фільтрації фішингових ресурсів на рівні шлюзу, використовувати багатофакторну автентифікацію та проводити регулярне навчання користувачів щодо виявлення підозрілих посилань та веб-сайтів. Також важливо використовувати сучасні браузери з увімкненою функцією виявлення фішингу та обмежити доступ до критично важливих ресурсів лише з довірених пристроїв.

Витік інформації через ненадійні VPN-сервіси та проксі-сервери можна усунути, заборонивши використання сторонніх інструментів тунелювання трафіку на комп'ютеризованих робочих місцях. Доступ до корпоративних ресурсів має надаватися лише через авторизовані внутрішні VPN з сучасними алгоритмами шифрування, аутентифікацією користувачів та веденням журналу сеансів. Політика безпеки повинна блокувати встановлення сторонніх VPN-клієнтів та проксі-розширень у браузерах. Вона також повинна відстежувати мережеву активність, яка намагається встановити з'єднання з відомими сервісами анонімізації.

Витік інформації через публічні або скомпрометовані мережі Wi-Fi є серйозним ризиком, і його слід мінімізувати, обмеживши підключення до незахищених бездротових мереж на рівні операційної системи. Доступ до корпоративних мереж повинен бути дозволений лише з довірених з'єднань або через VPN, що вимагають багатофакторної автентифікації. Співробітників не слід заохочувати до використання публічних хот-спотів для передачі конфіденційних даних та проінструктувати про ризики використання відкритого Wi-Fi у громадських місцях.

Витоку інформації через шкідливі розширення для браузерів можна запобігти, якщо централізовано керувати браузерами на комп'ютеризованих робочих станціях, дозволяючи встановлювати лише довірені розширення, схвалені IT-відділом, і не дозволяючи користувачам самостійно встановлювати інші розширення. Це можна зробити за допомогою групової політики (GPO), інструментів керування кінцевими точками (наприклад, Intune, MDM) та засобів керування сховищем розширень. Також важливо регулярно проводити аудит встановлених розширень і оновлювати браузери до останніх версій, щоб усунути відомі вразливості.

Враховуючи, що оптичний канал є другим за рівнем загрози після мережевого каналу витоку інформації, надалі буде розглянуто заходи з його ефективного захисту, спрямовані на запобігання несанкціонованому доступу та мінімізацію ризиків витоку даних через цей канал.

Також будуть сплановані заходи щодо усунення найбільш пріоритетних загроз пов’язаних, із даним каналом витоку, із перспективи зазначених порушників. Згідно моделі загроз, такими загрозами є:

– зчитування інформації з екрана за допомогою спеціальних засобів (шпигунство);

– витік інформації через відбиття монітора на окулярах, вікнах тощо;

– спостереження за натисканнями клавіш за допомогою спецзасобів.

Для усунення першої загрози необхідно забезпечити фізичну безпеку робочого місця, щоб запобігти несанкціонованому зчитуванню інформації з

екранів за допомогою технічних пристроїв моніторингу (наприклад, відеокамер, оптичних пристроїв). Екрани повинні бути встановлені таким чином, щоб їх не було видно з вікон, дверей або громадських місць. Слід використовувати екрани, що обмежують кут огляду дисплея. Крім того, робочі місця повинні знаходитися під наглядом, а доступ до приміщень повинен контролюватися.

Друга загроза витік інформації через відбиття монітора на окулярах, вікнах тощо. Цей шлях витоку є малопомітним, але технічно можливим. Щоб зменшити ризик, монітори не слід розміщувати перед вікнами або дзеркальними поверхнями. Якщо необхідно, вікна можна закрити жалюзі або заклеїти плівкою (рис. 2.3) [47] проти запотівання, щоб зменшити віддзеркалення. Співробітникам, які мають доступ до конфіденційної інформації, рекомендується уникати носіння блискучих окулярів з високим коефіцієнтом віддзеркалення. Також потрібно оглянути територію навколо робочого місця на предмет наявності небезпечних поверхонь, що відбивають світло.


Рисунок – 2.3 – Захисна плівка від шпіонажу

Остання загроза по оптичному каналу витоку інформації є спостереження за натисканнями клавіш за допомогою спецзасобів. Щоб захистити інформацію від візуального спостереження за натисканням клавіш (наприклад, камер і візуальних шпигунів), необхідно дотримуватися гігієни екрану. Потрібно тримати клавіатуру поза полем зору сторонніх осіб і камер та використовувати захисні

перегородки. У критичних випадках потрібно використовувати спеціальні клавіатури з нерозбірливою розкладкою клавіш або екранні клавіатури для введення паролів. Також варто запровадити політику «чистого столу» та обмежити встановлення зовнішніх камер спостереження лише тими місцями, де обробляється конфіденційна інформація.

Таким чином, було розглянуто основні заходи усунення найбільш пріоритетних загроз. Імплементація даних компонентів дозволить усунути усі найбільш ймовірні загрози із високим рівнем шкоди. На основі спланованих заходів надалі перейдемо до безпосередньої їх реалізації на реальному комп’ютеризованому робочому місці.

## 2.4 Висновок

У цьому розділі першим кроком було визначення найбільш загрозливих шляхів витоку інформації в контексті конкретного робочого місця. Для цього були застосовані такі критерії оцінки ризику, як потенційна шкода, ймовірність виконання, обсяг даних, контрольованість, важливість інформації, швидкість виявлення, складність виконання та потенційний вплив. Оцінка показала, що мережевий та оптичний канали витоку інформації є найбільш загрозливими і що їх захисту слід приділяти особливу увагу.

Далі було побудовано спрощену спеціалізовану моделі загроз та порушників для типового комп'ютеризованого робочого місця. Це дало змогу детально зрозуміти потенційні вектори атаки та мотивацію суб'єктів, які можуть вчинити витік даних. Модель загроз враховувала низку факторів, включаючи вразливість програмного забезпечення, недостатній рівень мережевої безпеки, технічні шляхи витоку (акустичні, віброакустичні, оптичні та електромагнітні), а також людські фактори, такі як недостатня обізнаність персоналу та відсутність чітких політик безпеки. Модель порушника визначила потенційних порушників та їхні можливості.

На основі виявлених загроз та визначених шляхів витоку було

запропоновано сестиматизовані заходи із протидії інформаційному витоку, згідно пріоритетів встановлених моделю загроз. Проект передбачає побудову комплексної системи протидії інформаційним витокам, з урахуванням їх ймовірності та критичності, що включає організаційні, адміністративні та технічні заходи. Основними компонентами є багатофакторна автентифікація, контроль доступу, шифрування даних, моніторинг поведінки користувачів та виявлення аномалій. Вона також передбачає блокування технічних шляхів витоку інформації, впровадження політики «чистого столу» та фізичну безпеку. Впровадження цієї системи планується на експериментальному робочому місці з подальшою інтеграцією у робочі процеси.

# 3 ІМПЛЕМЕНТАЦІЯ ТА АПРОБАЦІЯ СПРОЄКТОВАНОЇ СИСТЕМИ ЗАПОБІГАННЯ ІНФОРМАЦІЙНИМ ВИТОКАМ.

## 3.1 Імплементація системи запобігання інформаційним витокам на експериментальному робочому місці.

У цьому розділі детально описані практичні кроки з впровадження системи запобігання витоку інформації, включаючи специфічні налаштування міжмережевого екрану та використання спеціалізованих програмних засобів.

Впровадження рішень, призначених для запобігання витоку інформації на комп'ютеризованих лабораторних робочих місцях, ґрунтується на визначенні пріоритетів загроз, наведених у попередньому розділі. Імплементація запропонованих рішень відбуватиметься у визначеній послідовності, відповідно до їх пріоритезації.

Аналіз показує, що найбільшу загрозу витоку інформації становить мережевий канал, за яким слідує оптичний канал. Враховуючи модель зловмисника, де системні адміністратори, користувачі (внутрішні) та зловмисники (зовнішні) є найнебезпечнішими акторами. Заходи з мінімізації загроз плануються з метою протидії в першу чергу цим категоріям порушників, проте інші категорії порушників також будуть взяті до уваги, оскільки також ймовірно можуть становити загрозу.

Для початку будь-якої роботи спрямованої на захист робочого місця під операційною системою Windows необхідно правильно налаштувати локальні політики безпеки. Зокрема політику паролів, політику блокування облікових записів, політику прав користувачів тощо. Операційна система Windows має достатні можливості для гнучкого налаштування цих політик, (рис. 3.1).

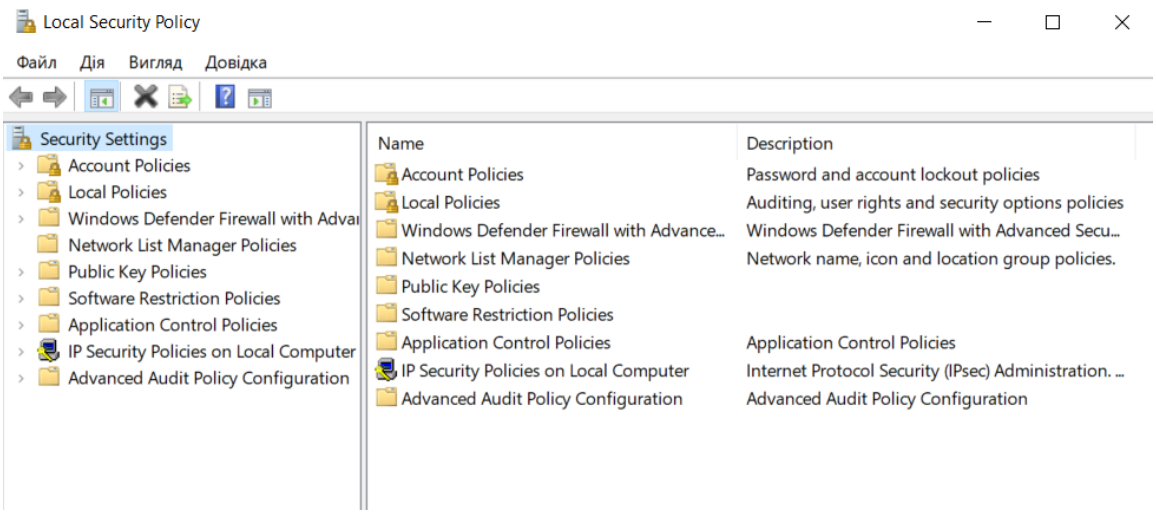



Рисунок 3.1 – Центр керування безпековими політиками ОС Windows

В цьому центрі безпекових політик зокрема можна налаштувати політику користувацьких паролів, політику блокування акаунтів, політики аудиту, зокрема системного логування,(рис 3.2).

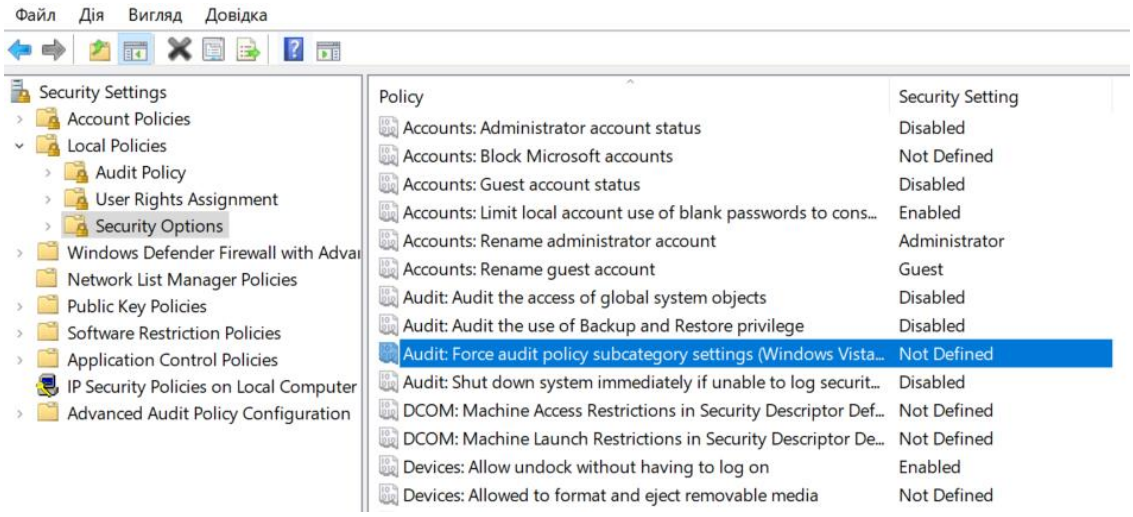



Рисунок 3.2 – Налаштування локальної політики аудиту

Таким чином налаштуємо базові вимоги до користувацьких паролів, що вже суттєво підвищить захищеність робочого місця, оскільки зобов'язуватиме користувача регулярно змінювати достатню захищені паролі. Загальні вимоги встановлено як: 10 символів – мінімальна довжина паролів, 30 днів – максимальний час життя паролю, пароль повинен містити символи різних регістрів цифри та спецсимволи, (рис 3.3).

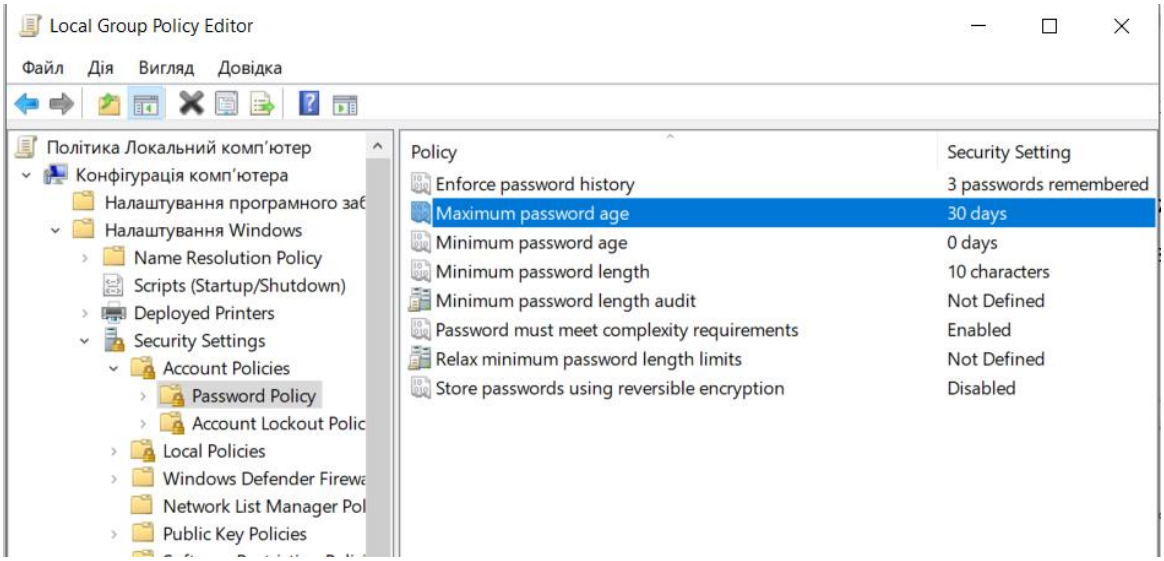



Рисунок 3.3 – Політика паролів робочого місця

В доповнення до стандартних системних налаштувань безпекових політик комп'ютера, буде застосовано програмний комплекс захисту інформації ЛОЗА-1, який доповнює та розширює стандарти налаштування. Часткове впровадження режиму кіоску та гнучкої політики безпеки на робочих місцях під управлінням Windows може бути досягнуто шляхом використання програмного комплексу захисту інформації ЛОЗА-1. Даний програмний комплекс є сертифікований, та підтверджений експертним висновком ДССЗЗІ України. Виконаємо інсталяцію ліцензованої копії програмного забезпечення ЛОЗА-1, на експериментальне робоче місце, (рис 3.4).

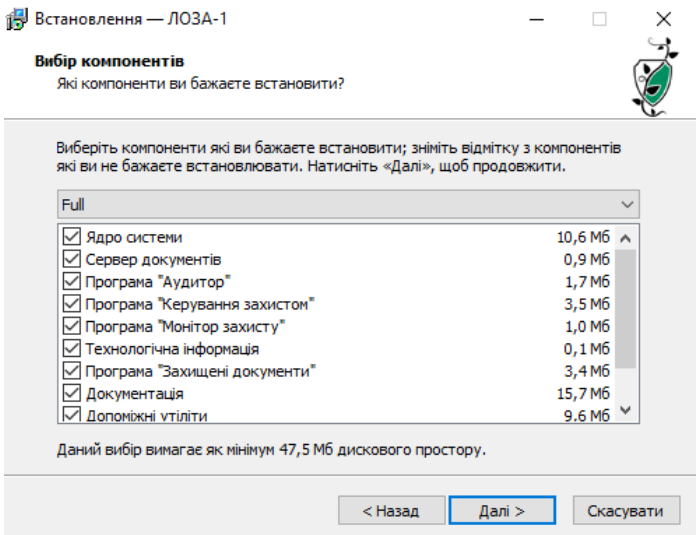



Рисунок 3.4 – Інтерфейс інсталяції програмного комплексу ЛОЗА-1

Після успішного встановлення програмного комплексу, з’являються на головному екрані додатки, для роботи.

Додаток Auditor призначений для роботи з журналами подій. Він формується з подіями аудиту, зафіксованих системою ЛОЗА-1, та подій, імпортованих з журналу Window. Файл журналу схожий на структуру журналу Windows. Аудитор також може працювати з резервною копією файлу журналу, (рис. 3.5)

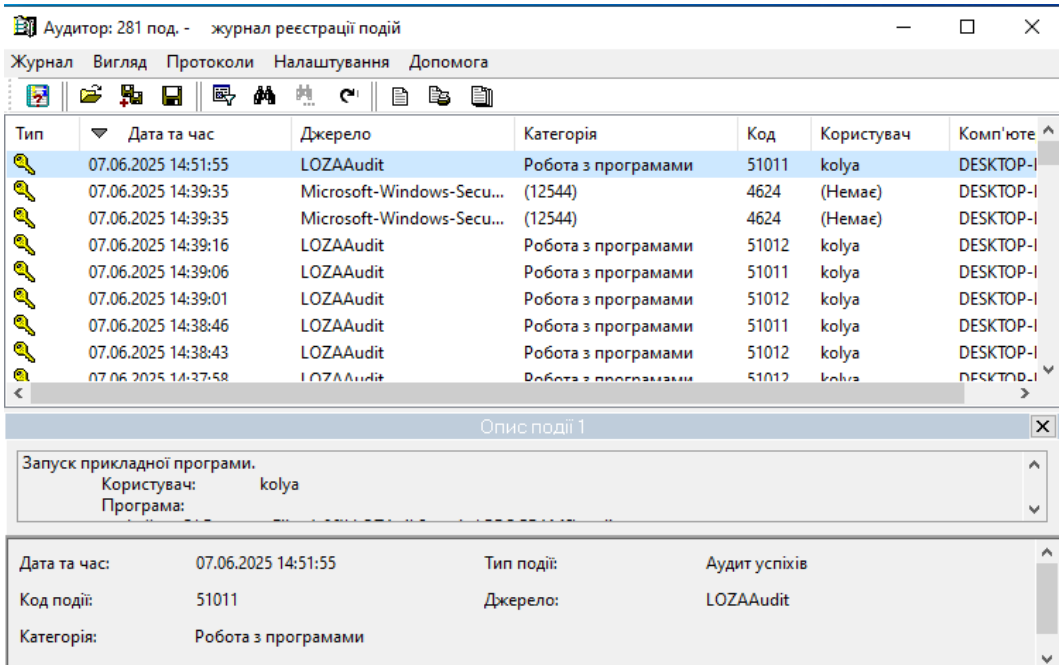



Рисунок 3.5 – Інтерфейс аудитора програмного комплексу ЛОЗА-1

«Монітор захисту» програмного комплексу ЛОЗА-1 є важливим компонентом для безперервного моніторингу та аналізу потоків даних на лабораторному майданчику. Його основна функція полягає у виявленні та запобіганні несанкціонованому розголошенню конфіденційної інформації різними каналами. Це включає моніторинг мережевого трафіку (веб, електронна пошта, месенджери), контроль використання знімних носіїв (USB, зовнішні диски), моніторинг друку та локальних операцій, таких як копіювання з буфера обміну. «Монітори захисту використовують заздалегідь визначені правила, ключові слова, регулярні вирази або цифрові відбитки пальців для аналізу вмісту даних. У разі виявлення конфіденційної інформації або спроб порушити політику

безпеки вони можуть блокувати передачу даних, попереджати користувачів, надсилати сповіщення адміністраторам і реєструвати всі події в системному журналі для подальшого аудиту. Таким чином, монітор захисту забезпечує активний контроль і швидке реагування на потенційні загрози витоку даних,(рис. 3.6).

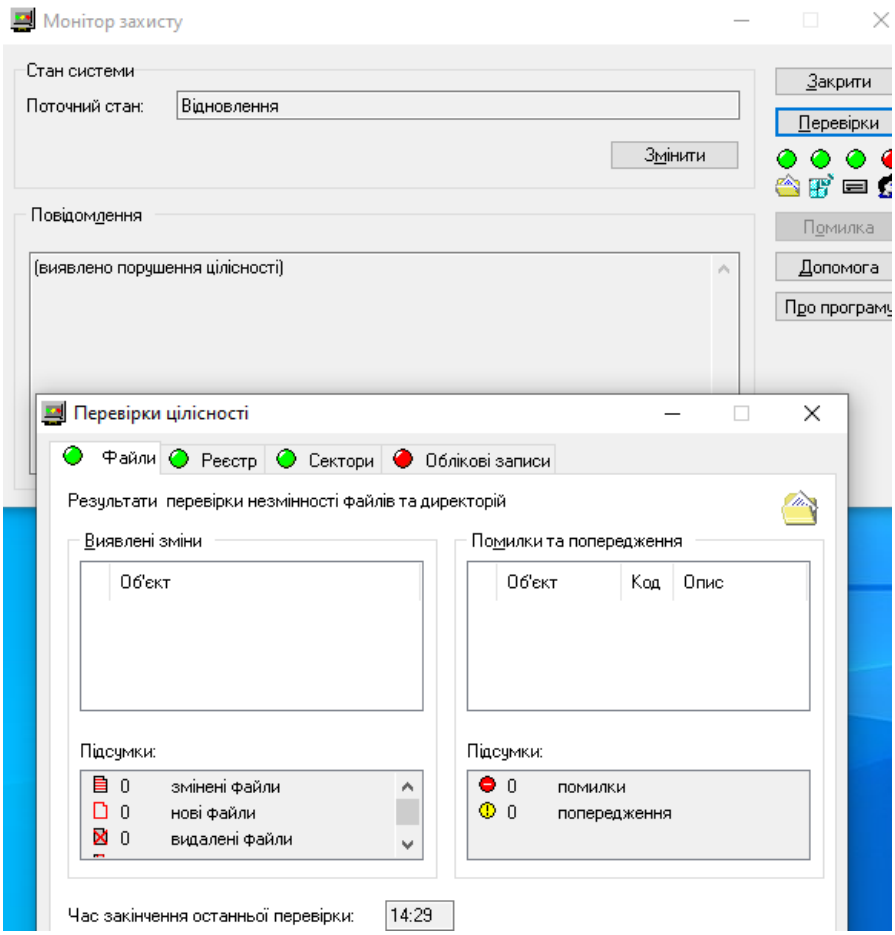



Рисунок 3.6 – Інтерфейс моніторингу захисту програмного комплексу ЛОЗА-1

Створивши базу документів, ми можемо налаштувати атрибути доступу як до самих файлів, так і до каталогу, в якому вони зберігаються. У системі ЛОЗА-1 для цього використовується механізм розмежування прав доступу, що дозволяє встановлювати обмеження за типами користувачів, рівнем секретності або наявністю відповідних повноважень. Наприклад, можна заборонити відкриття, копіювання, друк або пересилання файлів із даної папки для окремих ролей або груп. Це забезпечує багаторівневий контроль за доступом до конфіденційної інформації та мінімізує ризик її несанкціонованого витоку, (рис. 3.7).

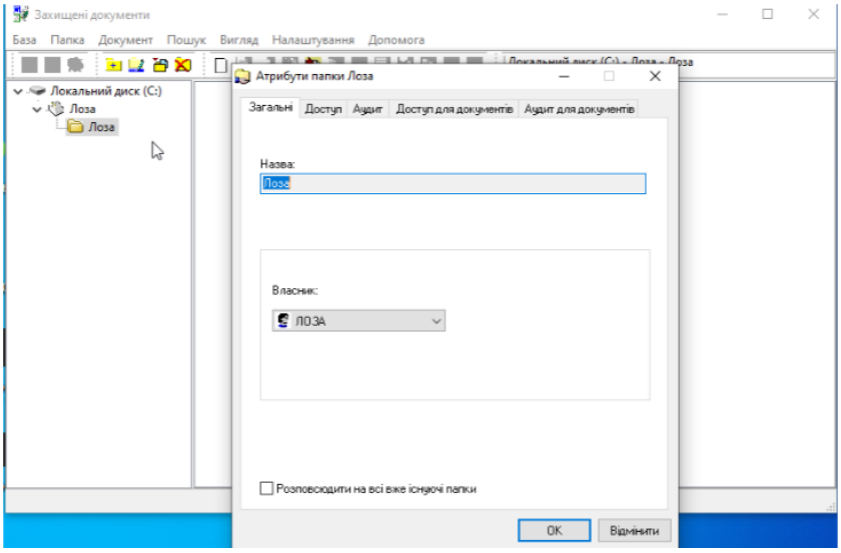



Рисунок 3.7 – Атрибути доступів до файлів

Контрзаходи проти витоку інформації через незахищені протоколи передачі даних (HTTP, FTP) та перехоплення мережевого трафіку (sniffing). Перехід на безпечні протоколи та заборона незахищених протоколів є ключовим фактором для забезпечення шифрування та захисту даних, що передаються, від перехоплення. Потрібно забезпечити, що до всіх вебресурсів, які використовуються, можна отримати доступ тільки через HTTPS. Цього можна досягнути за допомогою стандартного брендмауера Windows, який дозволяє створювати власні правила мережевих з'єднань. Зокрема, за допомогою брендмауера можна заборонити вихідні з'єднання за стандартними портами незахищених протоколів, (рис 3.8).

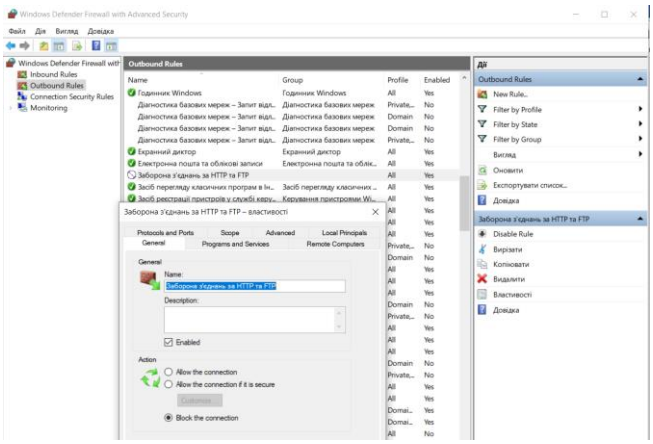



Рисунок 3.8 – Правило заборони вихідного трафіку за незахищеними протоколами

Окрім стандартного брендмауера Windows можна також використати інші спеціалізовані інструменти, що дають більш розширений функціонал. Це, як правило, комерційні рішення які потребують оплати у визначеній формі, проте надають значно більші можливості в налаштуванні безпеки, в тому числі і мережевої. Прикладом такого програмного забезпечення, програмний антивірусний комплекс Norton, який, на відмінну від стандартного брендмауера, потребує щорічної оплати у формі підписки, проте пропонує значно більш функціональні інструменти, щодо налаштування правил роботи у мережі, (рис. 3.9).

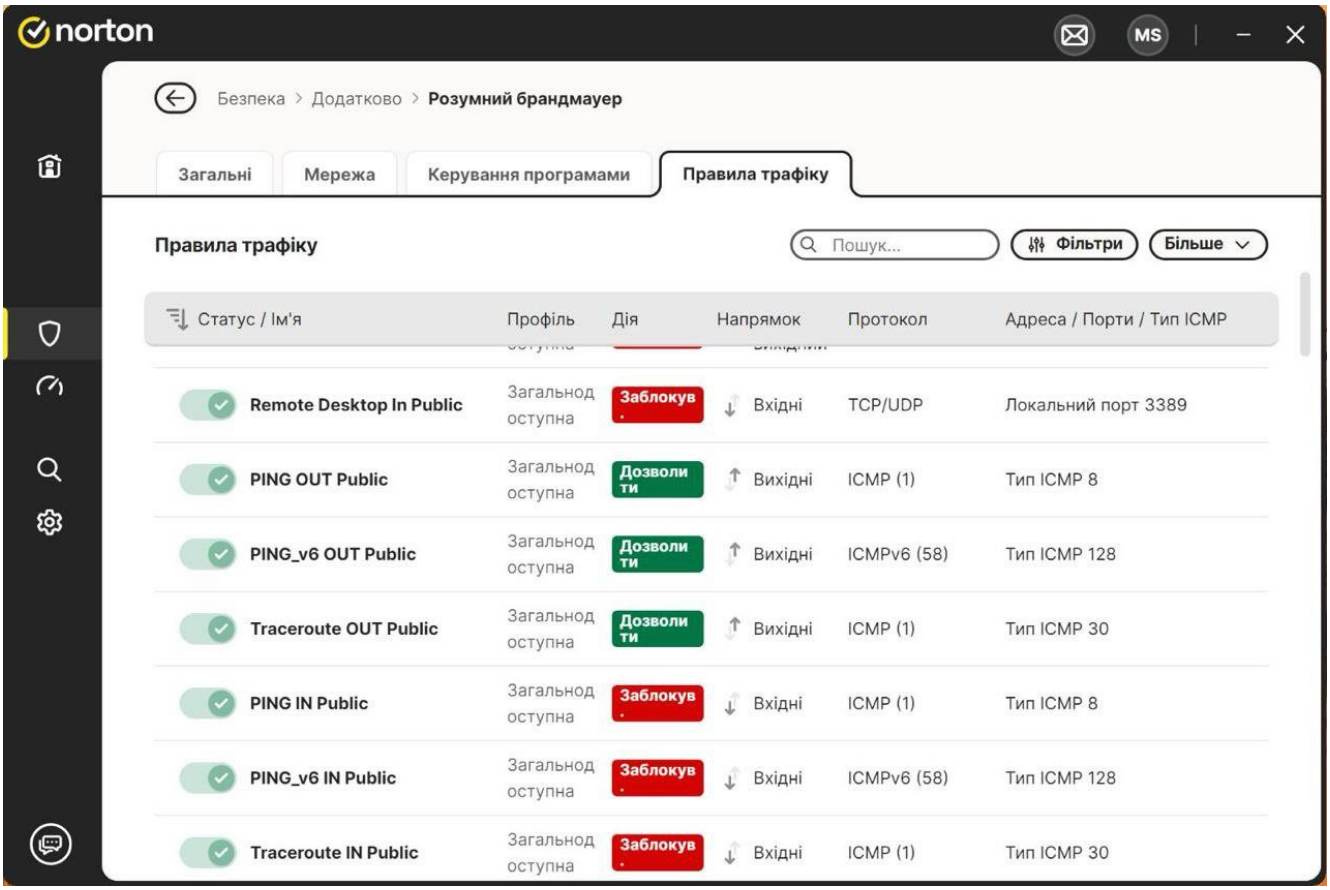



Рисунок 3.9 – Інтерфейс фаєрволу програмного комплексу Norton

Окрім цього, дане комерційне програмне забезпечення має власні, постійно оновлюванні, бази шкідливих сайтів, вразливостей трафіку, що дозволяє краще захищати робоче місце під час роботи у мережі, а також воно поєднує у собі антивірусний комплекс та інструменти боротьби зі спамом, (рис 3.10).

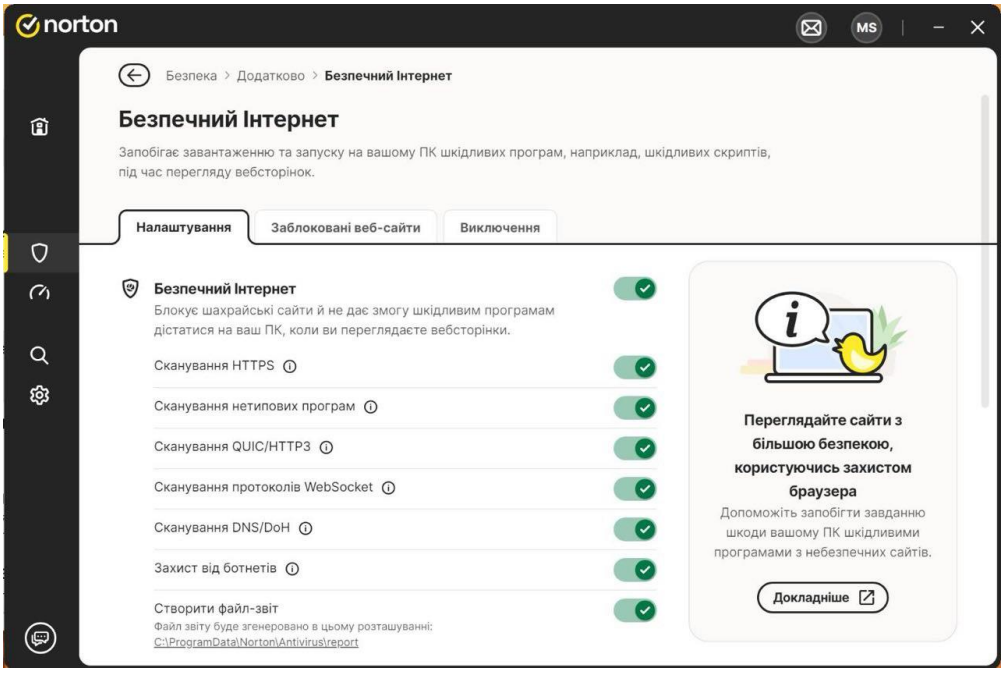



Рисунок 3.10 – Параметри логічного мережевого захисту програмного комплексу Norton

Таким чином, налаштування правил роботи у мережі може бути реалізовано за допомогою стандартних інструментів операційної системи Windows, наведених вище, проте для більш глибокого та комплексного захисту у якості основного інструменту на експереминтальному комп'ютеризованому робочому місці, буде використаний програмний комплекс Norton.

На комп'ютеризованому робочому місці також було встановлено програмний клієнт FileZilla, що підтримує, зокрема, захищений протокол sFTP, призначений для безпечного обміну файлами,(рис. 3.11).

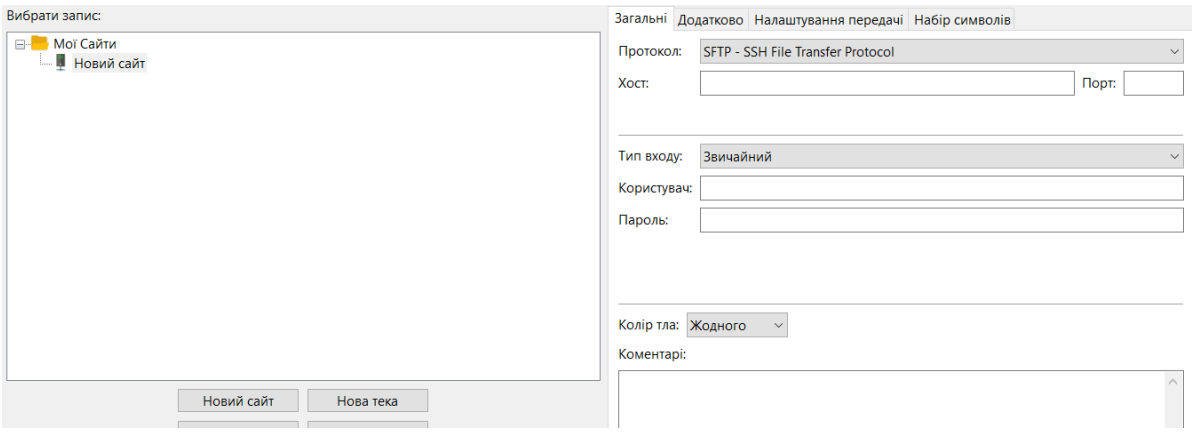



Рисунок 3.11 – Інтерфейс підключення sFTP з'єднання FileZilla

Віддалений доступ до комп'ютерів і мережевого обладнання повинен здійснюватися через SSH (Secure Shell), а не через Telnet. Для цього буде використано програмне забезпечення PuTTY, що дозволяє створювати SSH з’єднання, тунелі, зокрема з багатофактерною аутенфікацією. Запущену програму PuTTY відображено на рисунку, (рис. 3.12).

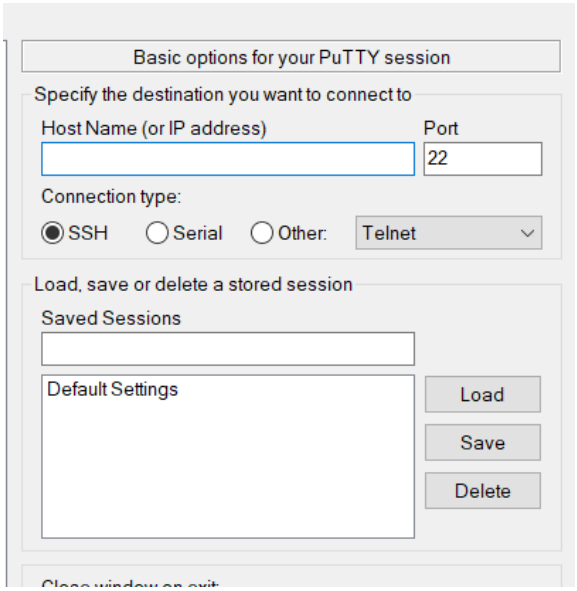



Рисунок 3.12 – Налаштування віддаленого доступу SSH

Навіть після переведення всіх комунікацій на захищені протоколи та ретельного налаштування брандмауерів, постійний моніторинг все одно був важливим. З цією метою в операційній системі буде увімкнено розширене логування та моніторинг, як із числа стандартних інструментів Windows, так і з інструментарію комлексу, (рис. 3.13).

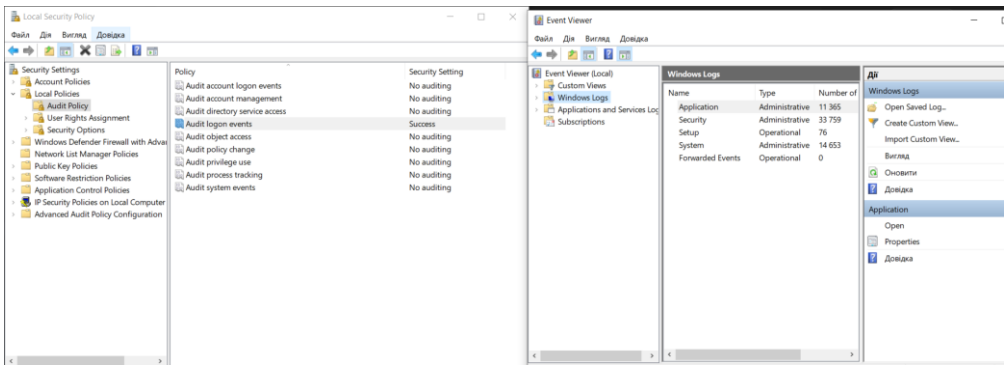


Рис 3.13 – Налаштування логування та моніторингу

Захист від несанкціонованого доступу через незахищені порти та Wi-Fi також розглядається як потенційна загроза. Ця загроза тісно пов'язана з попередньою, але зосереджена на контролі доступу до самої мережі та портів. Необхідно налаштувати брандмауери на блокування невикористовуваних портів, тобто було закрито всі непотрібні порти в конфігурації операційної системи та брандмауера. Це принцип «заборонити за замовчуванням». Блокування загальних вхідних портів для підвищення безпеки, особливо якщо робоча станція не працює як сервер, можна встановити загальне блокування всіх вхідних з'єднань і дозволити лише необхідні з'єднання.

За необхідності використання робочого місця віддалено, наприклад за допомогою протоколу RDP, з’єднання не повино бути прямим, на відкритий порт комп’ютера. Для реалізації подібних з’єднань повинно бути використано програмне забезпечення для тунелювання трафіку, таке як вже згадане PuTTY (через SSH тунель), або якийсь із захищених VPN протоколів, наприклад OpenVPN.

Щоб ефективно виявляти всі відкриті порти на комп'ютеризованому робочому місці, які можуть бути потенційними векторами атак, використовується інструмент сканування мережі Nmap. Цей інструмент дає актуальну картину мережевого доступу до мого комп'ютера, (рис. 3.14).

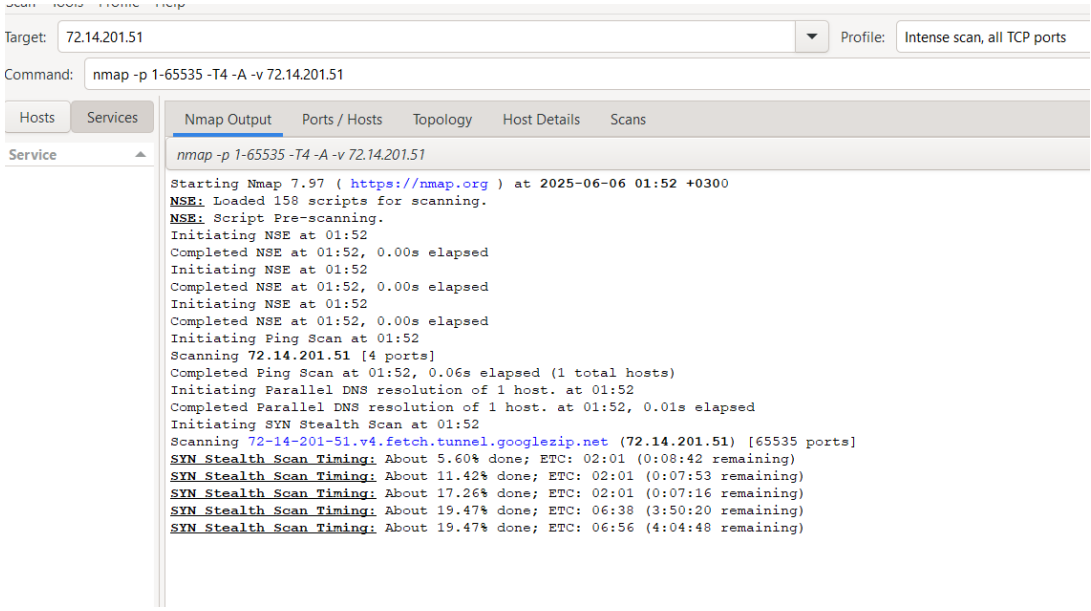



Рисунок 3.14 - Виявлення відкритих портів за допомогою Nmap.

Після завершення сканування Nmap виводить звіт про виявлені відкриті порти та служби, які на них працюють. Даний інструмент може використовуватись інженером з безпеки для періодичного моніторингу стану робочого місця.

Після налаштування брандмауера та перевірки відкритих портів на Nmap, зосереджуємо зусилля на посиленні безпеки Wi-Fi з'єднання. Це пов'язано з тим, що бездротові мережі можуть бути дуже вразливим шляхом для витоку інформації. На робочому місці потрібно заборонити підключатися до публічних або незахищених Wi-Fi мереж і завжди дозволяти доступ тільки до перевірених мереж, захищених новітніми протоколами шифрування WPA2 або WPA3. Це основне правило, яке потрібно дотримуватись. На рівні маршрутизатора внутрішньої мережі рекомендовано приховувати SSID (ім'я) мережі як додатковий рівень безпеки. Оскільки досвідчений зловмисник може виявити приховану мережу, але потрібно використовувати складні, надійні та унікальні паролі для доступу до Wi-Fi і регулярно їх змінюю. Потрібно використовувати комбінацію великих і малих літер, цифр і спеціальних символів у своїх паролях. Одним з найефективніших заходів, які можна використовува на роутері автентифікацію MAC-адреси.

Витік інформації через публічні або скомпрометовані мережі Wi-Fi є серйозним ризиком. Оскільки може бути важко контролювати ці з'єднання безпосередньо за допомогою розширених групових політик, зосередження на ручному налаштуванні операційної системи і посиленому контролі мережевого трафіку за допомогою брандмауерів. Стратегія полягає в тому, щоб переконатися, що комп'ютер підключається лише до мереж, до яких є довіра, і навіть тоді суворо контролювати весь трафік. Одним з принципів захисту є: «забути про всі ненадійні мережі»: це один із важливих і універсальних кроків, доступний у всіх версіях Windows. Вручну керуємо списком відомих мереж Wi-Fi, щоб комп'ютер не міг автоматично підключатися до небезпечних хот-спотів. Для не довірених мереж (наприклад, домашні мережі з надійними паролями або захищені мережі в офісі), потрібно їх «забути». Таким чином, комп'ютер не буде автоматично

підключатися до цих мереж в майбутньому.

Важливою частиною комплексного запобігання витоку інформації є заходи фізичної безпеки, а також програмне та апаратне забезпечення. На експериментальному робочому місці було вжито заходів для мінімізації ризику витоку візуальної інформації. Зокрема, монітори покриті захисною плівкою, яка обмежує кут огляду екрану і запобігає перегляду контенту сторонніми особами.

Це особливо важливо на робочих місцях з відкритим офісним простором або в місцях з високим ризиком стеження.

Ще одним аспектом є використання фізичних бар'єрів і процедур для запобігання неконтрольованому копіюванню та фотографуванню конфіденційних документів, щоб запобігти витоку інформації через друковані матеріали. Це включає в себе контроль доступу до друкарського обладнання, захищені зони для обробки документів та використання спеціального маркування на чутливих носіях документів.

Таким чином, було успішно виконано низку завдань з впровадження системи, призначеної для запобігання витоку інформації на експериментальному робочому місці. Це включало встановлення та первинне налаштування програмного комплексу «ЛОЗА-1», що дозволило контролювати та захищати основні шляхи потенційного витоку інформації, починаючи з фізичного та закінчуючи мережевим рівнем. Впроваджені заходи стали основою для подальшого тестування та валідації функціональності системи.

## 3.2 Апробація та тестування імплементованої системи та розробка настанов щодо її експлуатації

Апробація та тестування на експериментальних об'єктах є важливим етапом підтвердження ефективності та надійності встановленої системи запобігання витоку інформації. Одним з ключових моментів тестування є перевірка коректності функціонування механізму блокування шляхів витоку інформації

через мережеві порти. Для перевірки стану мережевих портів і забезпечення блокування несанкціонованого доступу та витоку інформації використовувався мережевий сканер Nmap.

В рамках тестування експериментальні робочі станції були просканованні ззовні та зсередини за допомогою Nmap. Сканування виконувалося з операційної системи Kali Linux, що дозволило повною мірою використати можливості Nmap для глибокого аналізу мережевої безпеки, (рис.3.16)

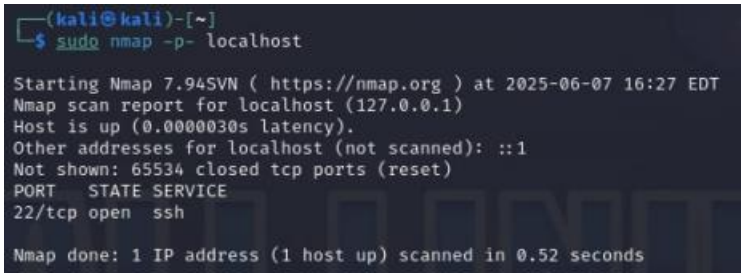



Рисунок 3.15 – Результат сканування портів через Nmap

Результати сканування Nmap чітко показують, що з 65535 просканованих портів 65534 порти перебувають у стані «фільтрації» і лише один TCP-порт 22 (SSH) - у стані «відкритий». Стан «фільтрації» вказує на те, що брандмауер успішно блокує пакети зондування Nmap, не дозволяючи визначити стан цих портів, що є ідеальним показником ефективного захисту. Це означає, що всі потенційні шляхи витоку через мережеві порти були успішно закриті. Однак порт SSH необхідний для віддаленого адміністрування і сам по собі не є шляхом витоку, якщо він належним чином авторизований. Цей результат є важливим свідченням ефективності впровадженої системи та підтверджує її здатність запобігати несанкціонованому доступу до мережі та потенційному витоку інформації через відкриті порти.

Окрім технічних аспектів тестування, важливим фактором успішної роботи системи запобігання витокам є розробка та впровадження процедур навчання співробітників. Людський фактор залишається одним з найбільш вразливих елементів в системах інформаційної безпеки, і без належної обізнаності користувачів навіть найнадійніші технічні засоби можуть виявитися

неефективними. Для забезпечення довгострокової ефективності встановлених систем розроблені комплексні процедури навчання. Це включає обов'язкове вступне навчання для нових співробітників щодо загальних принципів інформаційної безпеки та важливості запобігання витоку даних. Співробітники ретельно ознайомлюються з внутрішньою політикою використання інформаційних ресурсів, правилами поводження з конфіденційною інформацією та деталями встановлених контрольних функцій. Проводяться практичні вправи та демонстрації щодо правильного використання захищених робочих станцій, включаючи поводження з конфіденційними даними, електронною поштою та знімними носіями. Особлива увага приділяється навчанню алгоритмам реагування у разі виявлення підозрілої поведінки або інших інцидентів інформаційної безпеки, з акцентом на своєчасне інформування відповідальних осіб. Крім того, проводяться регулярні семінари та тренінги для оновлення знань співробітників про нові загрози, законодавчі зміни та оновлення системи безпеки, а також регулярні тести на знання для оцінки рівня засвоєння матеріалу.

Розробка та впровадження таких навчальних процедур може значно підвищити обізнаність та відповідальність працівників за інформаційну безпеку та суттєво знизити ризик витоку інформації через людський фактор.

## 3.3 Оцінка затрачених ресурсів та створення настанов щодо експлуатації системи

Після встановлення системи запобігання витоку інформації на комп'ютеризованому робочому місці було оцінено витрати, пов'язані з її впровадженням, налаштуванням та подальшою експлуатацією. Одноразові витрати включали придбання обладнання, такого як захисна плівка для моніторів, гарнітури з шумозаглушенням та периферійні пристрої з функціями фізичного захисту, загальною вартістю приблизно 2600 грн. ЛОЗА-1, ліцензії версії 4 коштували 9000 грн., ліцензія Norton Plus коштувала 1048 грн за одного

користувача на рік. Також оплата 5000 гривень за послуги фахівця з кібербезпеки для початкового налаштування системи.

Крім вартості системи безпеки, загальна вартість проекту включала оцінку вартості самого комп'ютеризованого робочого місця. Базова конфігурація включає системний блок середнього класу, монітор, клавіатуру, мишу та базове програмне забезпечення (ліцензійну операційну систему та офісний пакет), що оцінюється приблизно в 25000 гривень. Це забезпечує комфортну та стабільну роботу персоналу навіть в умовах підвищених вимог до інформаційної безпеки.

Загальні одноразові витрати на встановлення системи, включаючи робочі станції, обладнання, програмне забезпечення та професійні послуги, склали приблизно 42648 гривень. Щорічні витрати на обслуговування системи включають витрати на оновлення та підтримку програмного забезпечення, підписку на антивірусний захист та частину гонорарів, що сплачуються експертам за регулярний моніторинг та аудит системи безпеки. Середньорічні витрати становлять приблизно 28200 гривень. Вона також враховує можливість непередбачуваних витрат, таких як реагування на інциденти інформаційної безпеки, модернізація або заміна обладнання, придбання додаткових ліцензій та проведення розслідувань. Прогнозована сума таких витрат може становити до 10 000 грн на рік, залежно від частоти та серйозності інцидентів.

Для ефективної роботи системи потрібно регулярно оновлювати програмне забезпечення, щотижня контролювати журнали активності, щоквартально проводити аудит безпеки та регулярно проводити навчання персоналу. Такий підхід забезпечує стабільну роботу механізмів безпеки та своєчасне виявлення нових ризиків. Фінансові витрати на встановлену систему є помірними, що цілком виправдано з огляду на рівень захисту, який ця система забезпечує.

## 3.4 Висновки

У третьому розділі детально описано структуру програмно-апаратної

реалізації системи. Зокрема, подано опис апаратного середовища: експериментальне робоче місце з встановленими обмеженнями на фізичному рівні (вимкнені порти, відсутність доступу до зовнішніх носіїв, фізичне блокування роз'ємів). Операційна система була налаштована з використанням політик групової безпеки (GPO), що обмежують виконання сторонніх програм, доступ до налаштувань мережі та системних функцій. Встановлено додаткове ПЗ, яке моніторить активність користувача та контролює мережеву активність, що дозволяє виявляти потенційні спроби витоку інформації.

Особливу увагу було приділено реалізації обмежень на рівні користувача, зокрема — вимушене використання службових акаунтів без прав адміністратора, жорстке обмеження політик доступу та включення системного моніторингу активностей (включно з записом спроб доступу до мережевих ресурсів, USB-портів тощо). Було впроваджено також механізм контролю за активністю через PowerShell-скрипти, що дозволяють виконувати регулярні перевірки та створення журналів дій.

У наступному підпункті проведено апробацію реалізованої системи. Здійснено серію тестів для перевірки спроможності системи протидіяти спробам витоку даних через різні вектори: USB-накопичувачі, підключення мобільних пристроїв, спроби надсилання електронної пошти з вкладеннями, копіювання даних у буфер обміну, передачу через Telegram Web тощо. Для кожного сценарію було зафіксовано відповідну реакцію системи: або блокування операції, або її протоколювання з подальшим сповіщенням адміністратора.

Також оцінено ефективність DLP-механізмів, включаючи обмеження на друк документів, збереження файлів на локальні диски та заборону підключення несанкціонованих пристроїв. Зафіксовано, що система коректно блокує ці операції або виконує попереджувальні дії відповідно до налаштованих політик. Апробація показала високу стабільність роботи системи у штатних умовах — обмеження не перешкоджали виконанню службових обов'язків, при цьому несанкціоновані дії були унеможливлені.

Окремо варто відзначити реалізацію блокування мережевих каналів витоку:

заборонено передавання даних через сторонні VPN-клієнти, обмежено DNS-запити до неперевірених адрес, встановлено фільтрацію HTTP-запитів. Це дозволяє зменшити ризики витоку через інтернет-сервіси.

У останьому підпункті 3.3 проведено аналіз ресурсних витрат на реалізацію системи. Наведено детальну калькуляцію витрат часу на налаштування, інсталяцію, тестування та документацію. Також враховано вартість програмного забезпечення, якщо використовується комерційне (наприклад, DLP-система), витрати на ліцензії, а також час адміністратора на підтримку системи. Було виявлено, що більшість рішень можуть бути реалізовані з використанням безкоштовного ПЗ з відкритим кодом (OpenDLP, Snort, PowerShell-скрипти тощо), що значно знижує загальні витрати.

Загалом, реалізація проєкту продемонструвала, що навіть із обмеженими ресурсами можливо впровадити дієву багаторівневу систему захисту комп’ютеризованого робочого місця від інформаційних витоків. Система успішно пройшла апробацію, виявила стабільність та здатність протидіяти широкому спектру загроз. При цьому її структура залишається модульною та масштабованою — її можна адаптувати до реальних виробничих середовищ.

# ВИСНОВКИ

У межах кваліфікаційної роботи на тему «Система захисту комп’ютеризованого робочого місця від інформаційних витоків» було успішно виконано повний цикл дослідження, проєктування, впровадження та апробації системи кіберзахисту, що орієнтована на запобігання витоку конфіденційної інформації з комп’ютеризованого робочого середовища. У ході виконання роботи було досягнуто всі поставлені завдання, що засвідчує повноцінну реалізацію її мети.

Таким чином, у межах дипломної роботи виконано всі поставлені завдання:

- проведено аналіз предметної області та загроз;
- досліджено сучасні підходи та інструменти;
- сформовано нормативну основу;
- побудовано моделі загроз і каналів витоку;
- розроблено архітектуру системи;
- імплементовано експериментальну реалізацію;
- проведено апробацію і тестування;
- здійснено аналіз ресурсних витрат.

Проведено ґрунтовний аналіз предметної області, який охоплює специфіку сучасних інформаційних витоків, їх наслідки, типові вектори атак та проблематику забезпечення захисту. Виявлено основні джерела загроз — технічні, організаційні та людські чинники, а також проаналізовано найпоширеніші канали витоку: мережеві, акустичні, віброакустичні, оптичні та інші.

Досліджено існуючі системи запобігання витокам інформації, зокрема рішення класу DLP, та оцінено їх ефективність і обмеження. Аналіз показав, що більшість сучасних рішень недостатньо враховують специфіку окремих робочих місць, що потребує індивідуалізованого підходу при проєктуванні системи безпеки.

Третім важливим етапом стало вивчення нормативно-правової бази України

та міжнародних стандартів у сфері інформаційної безпеки. На основі цього сформульовано вимоги до системи, яка не лише технічно ефективна, але й юридично обґрунтована.

У другому розділі побудовано моделі загроз і порушників для типового комп'ютеризованого робочого місця. Було здійснено багатокритеріальне оцінювання каналів витоку за такими параметрами: ймовірність реалізації, обсяг даних, контрольованість, важливість інформації, швидкість виявлення, складність реалізації та потенційні наслідки. Це дозволило визначити найбільш критичні вектори — мережевий та оптичний — і пріоритезувати контрзаходи.

На основі цього проєктно-методологічного фундаменту було сформовано архітектуру захисної системи, що включає технічні, організаційні та адміністративні компоненти: багатофакторну автентифікацію, контроль доступу, шифрування, моніторинг дій користувача, політику «чистого столу», блокування технічних каналів витоку.

У третьому розділі реалізовано розроблену систему в експериментальному середовищі. Проведено налаштування апаратного й програмного середовища, встановлення обмежень на рівні користувача, застосування групових політик та скриптів PowerShell. Далі здійснено тестування функціонування системи під час спроб витоку інформації через USB-пристрої, хмарні сервіси, Telegram Web, буфер обміну, сторонні програми тощо. Усі загрози були успішно виявлені або заблоковані, що підтвердило практичну ефективність системи.

Також проведено економічну оцінку впровадження. Встановлено, що більшість рішень реалізуються з використанням безкоштовного або відкритого ПЗ, що робить систему доступною для організацій з обмеженими ресурсами.

Розроблена система підтвердила свою ефективність, масштабованість і здатність адаптуватися до реальних умов використання. Отримані результати можуть бути використані в корпоративних середовищах, установах та організаціях, де актуальним є захист конфіденційної інформації. Робота може слугувати основою для подальших наукових досліджень або практичної реалізації в галузі кібербезпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Bada, M., Sasse, A. & Nurse, J.R.C. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? // Computers & Security. – 2021. – Vol. 108. – https://doi.org/10.1016/j.cose.2021.102390

2. Chatterjee, S., Rana, N.P., Tamilmani, K. & Sharma, D.K. Security and privacy issues in digital transformation: a literature review. // Information Systems Frontiers. – 2020. – Vol. 22. – https://doi.org/10.1007/s10796-019-09902-7

3. Кібербезпека та управління ризиками в цифровому середовищі управління проєктами [Електронний ресурс] // ВНУЗ ЛДУБЖД. – 2023. – Режим доступу: https://virt.ldubgd.edu.ua/pluginfile.php/308970/mod_resource/content/2/Тема%206%20Кібербезпека%20та%20управління%20ризиками.pdf (дата звернення: 12.02.2025).

4. Конфіденційність, кібербезпека і ISO 27001: як вони пов'язані [Електронний ресурс]. – 2023. – Режим доступу: https://tic-ua.com/uk/statti/konfidenczijnist-kyberbezpeka-i-iso-27001-yak-vony-povyazani/ (дата звернення: 12.02.2025).

5. IBM. Cost of a Data Breach Report 2023 [Електронний ресурс]. – Режим доступу: https://www.ibm.com/reports/data-breach (дата звернення: 08.06.2025).

6. ENISA. Threat Landscape 2022. European Union Agency for Cybersecurity. – 2022. – Режим доступу: https://www.enisa.europa.eu/topics/csirt-cert-services/threat-landscape

7. Служба безпеки України. Рекомендації з кіберзахисту для підприємств критичної інфраструктури. – 2023. – Режим доступу: https://ssu.gov.ua/materials/kiberzakhyst-2023

8. Хто підпадає під вимоги GDPR і CCPA [Електронний ресурс] // Syrenis. – 2023. – Режим доступу: https://syrenis.com/resources/blog/who-is-affected-by-gdpr-and-ccpa-compliance/ (дата звернення: 12.02.2025).

9. Керівництво з відповідності GDPR та CCPA для маркетологів [Електронний ресурс] // CleverTap. – 2023. – Режим доступу:

https://clevertap.com/blog/gdpr-and-ccpa-compliance-a-guide-for-marketers/ (дата звернення: 12.02.2025).

10. Методичні матеріали з кібербезпеки / НТУУ "КПІ" [Електронний ресурс]. – 2022. – Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/d99a0045-e907-4d17-afc1-5431f67d2444/content (дата звернення: 12.02.2025).

11. Технічні заходи в інформаційній безпеці [Електронний ресурс]. – 2024. – Режим доступу: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/tehnichni-zahodi-v-informacijnij-bezpeci/ (дата звернення: 12.02.2025).

12. Витік даних: ризики та наслідки [Електронний ресурс] // Ukr.net. – 2024. – Режим доступу: https://www.ukr.net/news/details/technologies/104267003.html (дата звернення: 12.02.2025).

13. 10 загроз кібербезпеки для малого бізнесу та як їм запобігти [Електронний ресурс] // Itez. – 2023. – Режим доступу: https://itez.com.ua/blog/10-cybersecurity-threats-small-businesses-prevention.html (дата звернення: 12.02.2025).

14. Фішинг [Електронний ресурс] // Вікіпедія. – 2024. – Режим доступу: https://uk.wikipedia.org/wiki/Фішинг (дата звернення: 12.02.2025).

15. Кібербезпека: актуальні загрози та методи захисту [Електронний ресурс] // Lemon.school. – 2024. – Режим доступу: https://lemon.school/blog/kiberbezpeka-aktualni-zagrozy-ta-metody-zahystu (дата звернення: 12.02.2025).

16. Криптоджекінг [Електронний ресурс] // ESET. – 2024. – Режим доступу: https://help.eset.com/glossary/uk-UA/cryptojacking.html (дата звернення: 12.02.2025).

17. Microsoft Security. Cyber Signals Report 2024 [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/en-us/security/blog/ (дата звернення: 08.06.2025).

18. Mitrokotsa A., et al. Insider Threats and Detection Techniques

[Електронний ресурс] // Springer. – 2022. – Режим доступу: https://link.springer.com/chapter/10.1007/978-3-031-16516-0_7 (дата звернення: 12.02.2025).

19. Verizon. Data Breach Investigations Report 2023 [Електронний ресурс]. – Режим доступу: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 08.06.2025)

20. Що таке фішинг [Електронний ресурс] // Microsoft. – 2024. – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-phishing (дата звернення: 12.02.2025).

21. Багатофакторна автентифікація [Електронний ресурс] // ESET. – 2024. – Режим доступу: https://help.eset.com/glossary/uk-UA/multifactor_authentication.html (дата звернення: 12.02.2025).

22. Що таке шкідливе ПЗ [Електронний ресурс] // NordVPN. – 2024. – Режим доступу: https://nordvpn.com/uk/blog/shcho-take-shkidlyve-pz/ (дата звернення: 12.02.2025).

23. Як захиститися від шкідливого ПЗ [Електронний ресурс] // Cyber Star. – 2024. – Режим доступу: https://cyber-star.org/ua/cs-articles/how-to-protect-yourself-against-malware-ua/ (дата звернення: 12.02.2025).

24. Що таке DDoS-атака [Електронний ресурс] // Microsoft. – 2024. – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-ddos-attack (дата звернення: 12.02.2025).

25. Атака через порушення автентифікації [Електронний ресурс] // VPN Unlimited. – 2024. – Режим доступу: https://www.vpnunlimited.com/ua/help/cybersecurity/broken-authentication-attack (дата звернення: 12.02.2025)

26. DLP-системи для запобігання витоку інформації [Електронний ресурс] // SNT.ua. – 2023. – Режим доступу: https://www.snt.ua/portfolio/it-resheniya/informacionnaya-bezopasnost/predotvrashchenie-utechek-informacii-dlp (дата звернення: 12.02.2025).

27. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту

інформації в інформаційно-телекомунікаційних системах : навч. посіб. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

28. Брутфорс-атаки: суть, приклади, захист [Електронний ресурс] // Foxminded. – 2023. – Режим доступу: https://foxminded.ua/brute-force/ (дата звернення: 12.02.2025)

29. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

30. WannaCry [Електронний ресурс] // Вікіпедія. – 2024. – Режим доступу: https://uk.wikipedia.org/wiki/WannaCry (дата звернення: 12.02.2025).

31. DLP – системи запобігання витоку інформації [Електронний ресурс] // SNT.ua. – 2023. – Режим доступу: https://www.snt.ua/portfolio/it-resheniya/informacionnaya-bezopasnost/predotvrashchenie-utechek-informacii-dlp (дата звернення: 12.02.2025).

32. Чеботарьова Д. В., Пестєрєва С. Є. Аналіз технологій запобігання витоку інформації. – ФОП Петров В. В., 2021. – 524 с.

33. DLP – системи захисту даних від витоків [Електронний ресурс] // SNT.ua. – 2023. – Режим доступу: https://www.snt.ua/portfolio/it-resheniya/informacionnaya-bezopasnost/predotvrashchenie-utechek-informacii-dlp (дата звернення: 12.02.2025).

34. Захист інформації від витоку технічними каналами [Електронний ресурс] // TZI.com.ua. – 2024. – Режим доступу: https://tzi.com.ua/zaxist-nformacz-vd-vitoku-texnchnimi-kanalami.html (дата звернення: 12.02.2025).

35. Survey of Techniques on Data Leakage Protection and Methods to Address Insider Threats [Електронний ресурс] // Springer. – 2022. – Режим доступу: https://link.springer.com (дата звернення: 12.02.2025).

36. Prabakaran K., Ramachandran R. Optical Eavesdropping Channels and Protection Techniques in Secured Facilities // Optical and Quantum Electronics. – 2022.

37. Комплексні системи захисту інформації [Електронний ресурс] // ВНТУ. – 2022. – Режим доступу:

https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/rozdil1.html (дата звернення: 12.02.2025).

38. Орган із сертифікації систем менеджменту [Електронний ресурс] // CSI.cip.gov.ua. – 2024. – Режим доступу: https://csi.cip.gov.ua/en/pages/organ-z-sertifikaciyi-sistem-menedzhmentu (дата звернення: 12.02.2025).

39. NIST SP 800-53 Rev. 5 Update 1 [Електронний ресурс]. – 2023. – Режим доступу: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (дата звернення: 12.02.2025).

40. Політика конфіденційності ESRI згідно з GDPR [Електронний ресурс]. – 2023. – Режим доступу: https://www.esri.com/uk-ua/privacy/privacy-gdpr (дата звернення: 12.02.2025).

41. OWASP: Information Leakage – загрози інфраструктурної безпеки [Електронний ресурс]. – 2024. – Режим доступу: https://owasp.org/www-project-top-10-infrastructure-security-risks/docs/2024/ISR08_2024-Information_Leakage (дата звернення: 12.02.2025).

42. Найбільші ризики витоку даних [Електронний ресурс] // Metomic.io. – 2023. – Режим доступу: https://www.metomic.io/resource-centre/what-are-the-biggest-risks-of-data-leaks (дата звернення: 12.02.2025).

43. Data Leakage Detection: терміни і поняття [Електронний ресурс] // Cyberpedia by ReasonLabs. – 2024. – Режим доступу: https://cyberpedia.reasonlabs.com/EN/data%20leakage%20detection.html (дата звернення: 12.02.2025).

44. Хмарні обчислення в контексті інформаційної безпеки [Електронний ресурс] // CEUR Workshop Proceedings. – 2022. – Режим доступу: https://ceur-ws.org/Vol-3126/paper21.pdf (дата звернення: 12.02.2025).

45. Наслідки витоку даних для бізнесу [Електронний ресурс] // ZeroFox. – 2024. – Режим доступу: https://www.zerofox.com/blog/damaging-consequences-data-leakage/ (дата звернення: 12.02.2025).

46. Система захисту інформації ЛОЗА™ [Електронний ресурс] // Avtoprom.kiev.ua. – 2023. – Режим доступу:

http://avtoprom.kiev.ua/avtoprom/ua/content/Система-захисту-інформації-ЛОЗА-1-версія-4 (дата звернення: 12.02.2025).

47. 3M PF320W9B – фільтр приватації 32" [Електронний ресурс] // NET-S.pl. – Режим доступу: https://www.net-s.pl/produkt/3m-pf320w9b-filtr-prywatyzujacy-32-169-pf320w9b-398mm-x-708mm-1070711 (дата звернення: 08.06.2025).

Оцінювання критеріїв оптичні каналу витоку інформації.

| Критерії | Оцінка | Пояснення |
|---|---|---|
| Ймовірність реалізації | 3 | Оптичні канали вимагають специфічного обладнання, домовленостей та умов. У більшості середовищ потенціал для розгортання низький. |
| Обсяг даних | 2 | Кількість інформації, яку можна передати оптичними каналами, обмежена. |
| Контрольованість | 5 | Оптичні канали можуть бути утворені несподіваними елементами, що робить їх контроль дуже складним. |
| Важливість інформації | 9 | Якщо канал дозволяє зчитувати екран або клавіатуру, може бути розкрита важлива інформація, така як паролі, персональні дані або конфіденційні документи. |
| Швидкість виявлення | 2 | Оптичні канали важко виявити без цілеспрямованого аналізу. Вони зазвичай не виявляються технічними засобами захисту, а виявлення загроз займає багато часу. |
| Складність реалізації | 8 | Потрібні спеціальні знання, обладнання (наприклад, високочутливі камери та відповідні місця) і доступ до прямої видимості, що ускладнює реалізацію. |
| Потенційні наслідки | 6 | Хоча канал обмежений за обсягом, компрометація навіть малої кількості чутливої інформації (паролі, ключі) може мати серйозні наслідки. |

Оцінювання критеріїв мережевого каналу витоку інформації.

| Критерії | Оцінка | Пояснення |
|---|---|---|
| Ймовірність реалізації | 8 | Реалізація можлива за наявності знань та обладнання, яке стає доступнішим. |
| Обсяг даних | 9 | Через ці канали можна перехоплювати великі обсяги даних, зокрема вміст екрана або натискання клавіш. |
| Контрольованість | 4 | Контролювати складно через прихований характер і необхідність спеціального моніторингу. |
| Важливість інформації | 7 | Часто витікає важлива інформація — паролі, службові дані тощо. |
| Швидкість виявлення | 5 | Витік важко помітити, часто лишається невиявленим. |
| Складність реалізації | 7 | Потрібні технічні знання й обладнання, що дещо ускладнює атаку. |
| Потенційні наслідки | 8 | Успішний витік може призвести до значних втрат або компрометації системи. |

Оцінювання критеріїв акустичного каналу витоку інформації.

| Критерії | Оцінка | Пояснення |
|---|---|---|
| Ймовірність реалізації | 5 | Витік звуку можливий лише в тому випадку, якщо зловмисник перебуває в межах видимості або має прихований записуючий пристрій. |
| Обсяг даних | 3 | Вона обмежується інформацією, яку можна озвучити, наприклад, усні переговори та фрагменти повідомлень. |
| Контрольованість | 10 | Один із найскладніших для контролю каналів. Люди розмовляють голосно, не усвідомлюючи ризиків, мікрофони приховані або вбудовані в невеликі пристрої. |
| Важливість інформації | 6 | Голосові повідомлення часто містять важливу, але не завжди повну інформацію, наприклад, номери телефонів, паролі та фрагменти розмов. У деяких ситуаціях це може мати велике значення. |
| Швидкість виявлення | 10 | Перехоплення зазвичай не залишає видимих слідів. Якщо не використовувати спеціальне обладнання не проаналізувати технічне середовище, виявити прослуховування майже неможливо. |
| Складність реалізації | 9 | Достатньо смартфона або прихованого диктофона. |
| Потенційні наслідки | 5 | Якщо передається важлива інформація (наприклад, номери карток або паролі), наслідки можуть бути значними, тоді як для звичайних розмов вплив незначний. |

Оцінювання критеріїв вібро-акустичного каналу витоку інформації.

| Критерії | Оцінка | Пояснення |
|---|---|---|
| Ймовірність реалізації | 7 | Реалізація вимагає технічних знань і спеціалізованого підходу, але може бути здійснена зловмисниками з досвідом. |
| Обсяг даних | 4 | Обмежується текстовими даними і залежить від швидкості набору тексту та роботи пристрою. |
| Контрольованість | 9 | Традиційні методи захисту (екрани, політики безпеки) ускладнюють виявлення таких каналів, а для контролю потрібні спеціальні інструменти. |
| Важливість інформації | 7 | Через канал можуть бути перехоплені важливі дані, такі як логіни, паролі та внутрішні документи. |
| Швидкість виявлення | 8 | Без радіомоніторингу або ПЕМ-контролю важко виявити витоки. |
| Складність реалізації | 8 | Для виявлення та декодування сигналів потрібне спеціальне обладнання, яке важко реалізувати, але можливо. |
| Потенційні наслідки | 6 | Залежно від перехопленої інформації, це може мати серйозні наслідки, особливо якщо йдеться про доступ до критично важливих даних. |

ДОДАТОК А

Копії графічної частини

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | КРБКБ.2102150.21.02.13 Е8 | | |
| Змн. | Арк. | № докум. | Підпис | Дата | Система захисту комп'ютеризованого робочого місця від інформаційних витоків | Літера / Маса / Масштаб |
| Розроб. | | Коцюк М.М. | | | Таблиці оцінювання критичності оптичного, акустичного, вібро-акустичного та мережевого каналів витоку інформації | |
| Перевір. | | Чашун В.М. | | | | Аркуш 1 / Аркушів 12 |
| Т. Контр. | | | | | | |
| Н. Контр. | | Мостовий С.В. | | | | ХНУ, КБ-21-2 |
| Затверд. | | Кльоц Ю.П. | | | | |

Загальна оцінка критичності типів каналів витоку інформації

| Тип каналу | Ймовірність реалізації. | Обсяг даних | Контрольо-ваність | Важливість інформації | Швидкість виявлення | Складність реалізації | Потенційні наслідки | Сума |
|---|---|---|---|---|---|---|---|---|
| Оптичні | 3 | 2 | 5 | 9 | 2 | 8 | 6 | 35 |
| Акустичні | 5 | 3 | 10 | 6 | 10 | 9 | 5 | 47 |
| Вібро-акустичні | 7 | 4 | 9 | 7 | 8 | 8 | 6 | 49 |
| Мережеві | 8 | 9 | 4 | 5 | 5 | 7 | 8 | 46 |

Матриця парних порівнянь критеріїв

| | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | MG | w |
|---|---|---|---|---|---|---|---|---|---|
| Q1 | 1 | 5 | 1/5 | 1 | 1/5 | 1/9 | 1/9 | 0.407 | 0.052 |
| Q2 | 1/5 | 1 | 5 | 1/3 | 3 | 1/5 | 5 | 1 | 0.129 |
| Q3 | 5 | 1/5 | 1 | 1/3 | 1/5 | 1 | 3 | 0.785 | 0.101 |
| Q4 | 1 | 3 | 3 | 1 | 1/5 | 3 | 1/3 | 1.085 | 0.140 |
| Q5 | 5 | 1/3 | 5 | 5 | 1 | 1/5 | 3 | 1.583 | 0.204 |
| Q6 | 9 | 5 | 1 | 1/3 | 5 | 1 | 3 | 2.128 | 0.273 |
| Q7 | 9 | 1/5 | 1/3 | 3 | 1/3 | 1/3 | 1 | 0.785 | 0.101 |
| | | | | | | | Підсумок: | 7.773 | 1 |

Оцінка каналів витоку інформації за критерієм ймовірність реалізації

| Q1 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 3 | 5 | 9 | 3.400 | 0.581 |
| A2 | 1/3 | 1 | 3 | 5 | 1,495 | 0.255 |
| A3 | 1/5 | 1/3 | 1 | 3 | 0.669 | 0.114 |
| A4 | 1/9 | 1/5 | 1/3 | 1 | 0.294 | 0.050 |
| | | | | Підсумок: | 5.858 | 1 |

Оцінка каналів витоку інформації за критерієм обсяг даних

| Q2 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 3 | 5 | 9 | 3.400 | 0.557 |
| A2 | 1/3 | 1 | 3 | 9 | 1.732 | 0.283 |
| A3 | 1/5 | 1/3 | 1 | 5 | 0.760 | 0.124 |
| A4 | 1/9 | 1/9 | 1/5 | 1 | 0.222 | 0.036 |
| | | | | Підсумок: | 6.114 | 1 |

Оцінка каналів витоку інформації за критерієм контрольованість

| Q3 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 5 | 9 | 1/3 | 1.968 | 0.319 |
| A2 | 1/5 | 1 | 1/3 | 1/9 | 0.293 | 0.048 |
| A3 | 1/9 | 3 | 1 | 1/5 | 0.505 | 0.082 |
| A4 | 3 | 9 | 5 | 1 | 3.400 | 0.551 |
| | | | | Підсумок: | 6.166 | 1 |

Оцінка каналів витоку інформації за критерієм важливість інформації

| Q4 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 1/5 | 1/3 | 1/9 | 0.293 | 0.050 |
| A2 | 5 | 1 | 3 | 1/3 | 1.495 | 0.255 |
| A3 | 3 | 1/3 | 1 | 1/5 | 0.669 | 0.114 |
| A4 | 9 | 3 | 5 | 1 | 3.400 | 0.581 |
| | | | | Підсумок: | 5.857 | 1 |

Оцінка каналів витоку інформації за критерієм швидкість виявлення

| Q5 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 9 | 5 | 3 | 3.400 | 0.551 |
| A2 | 1/9 | 1 | 1/3 | 1/5 | 0.294 | 0.048 |
| A3 | 1/5 | 3 | 1 | 1/9 | 0.507 | 0.082 |
| A4 | 1/3 | 5 | 9 | 1 | 1.968 | 0.319 |
| | | | | Підсумок: | 6.169 | 1 |

Оцінка каналів витоку інформації за критерієм складність реалізації

| Q6 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 3 | 1 | 1/3 | 1 | 0.201 |
| A2 | 1/3 | 1 | 1/3 | 1/5 | 0.384 | 0.077 |
| A3 | 1 | 3 | 1 | 1/3 | 1 | 0.201 |
| A4 | 3 | 5 | 3 | 1 | 2.593 | 0.521 |
| | | | | Підсумок: | 4.977 | 1 |

Оцінка каналів витоку інформації за критерієм потенційні наслідки

| Q7 | A1 | A2 | A3 | A4 | MG | w |
|---|---|---|---|---|---|---|
| A1 | 1 | 1/3 | 1 | 5 | 1.139 | 0.220 |
| A2 | 3 | 1 | 3 | 5 | 2.593 | 0.502 |
| A3 | 1 | 1/3 | 1 | 5 | 1,139 | 0.220 |
| A4 | 1/5 | 1/5 | 1/5 | 1 | 0.299 | 0.058 |
| | | | | Підсумок: | 5.170 | 1 |

Дані для обчислення кількісного індикатору критичності кожної альтернативи

| | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 |
|---|---|---|---|---|---|---|---|
| A1 | 0.581 | 0.557 | 0.319 | 0.050 | 0.551 | 0.201 | 0.220 |
| A2 | 0.255 | 0.283 | 0.048 | 0.255 | 0.048 | 0.077 | 0.502 |
| A3 | 0.114 | 0.124 | 0.082 | 0.114 | 0.082 | 0.201 | 0.220 |
| A4 | 0.050 | 0.036 | 0.551 | 0.581 | 0.319 | 0.521 | 0.058 |

X

| U |
|---|
| 0.052 |
| 0.129 |
| 0.101 |
| 0.140 |
| 0.204 |
| 0.273 |
| 0.101 |

Розрахунок кількісного індикатор якості кожної альтернативи.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0.030 | + | 0.071 | + | 0.032 | + | 0.007 | + | 0.112 | + | 0.055 | + | 0.022 | = | 0.329 |
| 0.013 | + | 0.037 | + | 0.005 | + | 0.036 | + | 0.010 | + | 0.021 | + | 0.051 | = | 0.173 |
| 0.006 | + | 0.016 | + | 0.008 | + | 0.016 | + | 0.017 | + | 0.055 | + | 0.022 | = | 0.140 |
| 0.003 | + | 0.005 | + | 0.056 | + | 0.081 | + | 0.065 | + | 0.142 | + | 0.006 | = | 0.358 |
| | | | | | | | | | | | Підсумок: | | | 1 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | КРБКБ.2102150.21.02.13 Е8 | |
| | | | | | | Система захисту комп'ютеризованого робочого місця від інформаційних витоків. Таблиці визначення найбільш загрозливихканалів витоку інформації | Літера: — Маса: — Масштаб: — |
| Змін. | Арк. | № докум. | Підпис | Дата | | | Аркуш 2 / Аркушів 12 |
| Розроб. | | Коцюк М.М. | | | | | |
| Перевір. | | Чешун В.М. | | | | | |
| Т. Контр. | | | | | | | |
| Н. Контр. | | Мостовий С.В. | | | | | ХНУ, КБ-21-2 |
| Затверд. | | Кльоц Ю.П. | | | | | |

Модель загроз комп'ютеризованого робочого місця.

| № | Загроза | Канал витоку | Ймовірність | Рівень шкоди | К | Ц | Д | С |
|---|---|---|---|---|---|---|---|---|
| 1 | Прослуховування розмов через мікрофони ПК чи смартфонів або через людський фактор | Акустичний | Висока | Високий | + | | | + |
| 2 | Витік інформації через вібрації, що фіксуються акселерометрами | Вібро-акустичний | Низька | Середній | + | | | + |
| 3 | Витік інформації через незахищені протоколи передачі даних (HTTP, FTP) | Мережевий | Висока | Неприпустимо високий | + | + | | + |
| 4 | Зчитування інформації з екрана за допомогою спеціальних засобів (шпигунство) | Оптичний | Середня | Високий | + | | | + |
| 5 | Витік інформації через відбиття монітора на окулярах, вікнах тощо | Оптичний | Низька | Середній | + | | | + |
| 6 | Перехоплення мережевого трафіку | Мережевий | Висока | Неприпустимо високий | + | + | | + |
| 7 | Несанкціонований доступ через незахищені порти чи Wi-Fi | Мережевий | Висока | Неприпустимо високий | + | + | + | + |
| 8 | Віруси/шпигунське ПЗ, що передає дані через мережу | Мережевий | Висока | Неприпустимо високий | + | + | + | + |
| 9 | Витік інформації через принтери, сканери з модулем Wi-Fi | Мережевий/ оптичний | Середня | Високий | + | + | | + |
| 10 | Спостереження за натисканнями клавіш за допомогою спецзасобів | Оптичний | Середня | Середній | + | | | + |
| 11 | Витік інформації через фішингові атаки (введення даних у підроблену форму) | Мережевий | Висока | Високий | + | + | | + |
| 12 | Витік інформації через відкриті мережеві порти служб (наприклад, RDP, SMB) | Мережевий | Висока | Неприпустимо високий | + | + | + | + |
| 13 | Витік інформації через ненадійні VPN чи проксі | Мережевий | Середня | Високий | + | + | | + |
| 14 | Витік інформації через публічні або скомпрометовані Wi-Fi мережі | Мережевий | Висока | Високий | + | + | + | + |
| 15 | Витік інформації через зловмисне розширення браузера | Мережевий | Середня | Високий | + | + | | + |
| 16 | Витік інформації через неправильне налаштування файрвола | Мережевий | Середня | Неприпустимо високий | + | + | + | + |

Градації пріоритетів згідно співвідношення ймовірності виникнення та шкоди загроз.

| Ймовірність \ Рівень шкоди | Низька | Середня | Висока | Небезпечно висока |
|---|---|---|---|---|
| Низька | | 2 | | |
| Середня | | 1 | 4 | 1 |
| Висока | | | 3 | 5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | КРБКБ.2102150.21.02.13 Е8 | |
| Зм. | Арк. | № докум. | Підпис | Дата | Система захисту комп'ютеризованого робочого місця від інформаційних витоків | Літера / Маса / Масштаб |
| Розроб. | | Коцюк М.М. | | | | |
| Перевір. | | Чешун В.М. | | | Таблиця моделі загроз на комп'ютеризованому робочому місці | |
| Т. Контр. | | | | | | Аркуш 3 / Аркушів 12 |
| Н. Контр. | | Мостовий С.В. | | | | |
| Затверд. | | Кльоц Ю.П. | | | | ХНУ, КБ-21-2 |

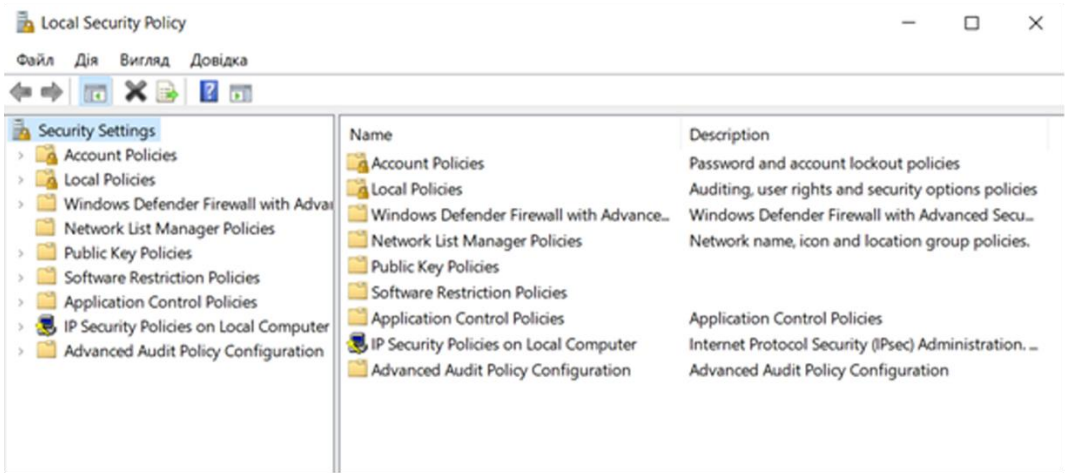
Критерії оцінки порушника.

| Позначення | Визначення категорії | Рівень загроз |
|---|---|---|
| За категорією порушника | | |
| Внутрішні порушники | | |
| ВП 1 | Технічний персонал, (прибиральники, охоронці, електрики тощо) | 1 |
| ВП 2 | Користувачі комп'ютеризованого робочого місця | 2 |
| ВП 3 | Персонал, який обслуговує технічні засоби (адміністратор тощо) | 3 |
| Зовнішні порушники | | |
| ЗП 1 | Відвідувач | 1 |
| ЗП 2 | Хакери | 4 |
| За мотивацією порушника | | |
| М 1 | Безвідповідальність | 1 |
| М 2 | Самоствердження | 2 |
| М 3 | Корислива мета | 3 |
| М 4 | Професійний обов’язок | 4 |
| Рівні обізнаності | | |
| К 1 | Порушник володіє низьким рівнем знань, проте вміє працювати з технічними засобами комп’ютернізованого робочого місця | 1 |
| К 2 | Порушник володіє середнім рівнем знань та практичними навичками роботи з технічними засобами комп’ютернізованого робочого місця | 2 |
| К 3 | Порушник володіє високим рівнем знань у програмуванні та обчислювальної техніки, проєктування та експлуатації комп’ютернізованого робочого місця | 3 |
| К 4 | Порушник знає структуру, функції та механізми дії засобів захисту інформації в комп’ютернізованого робочого місця, їх недоліки та можливості | 4 |
| Доступність до АС | | |
| 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 |

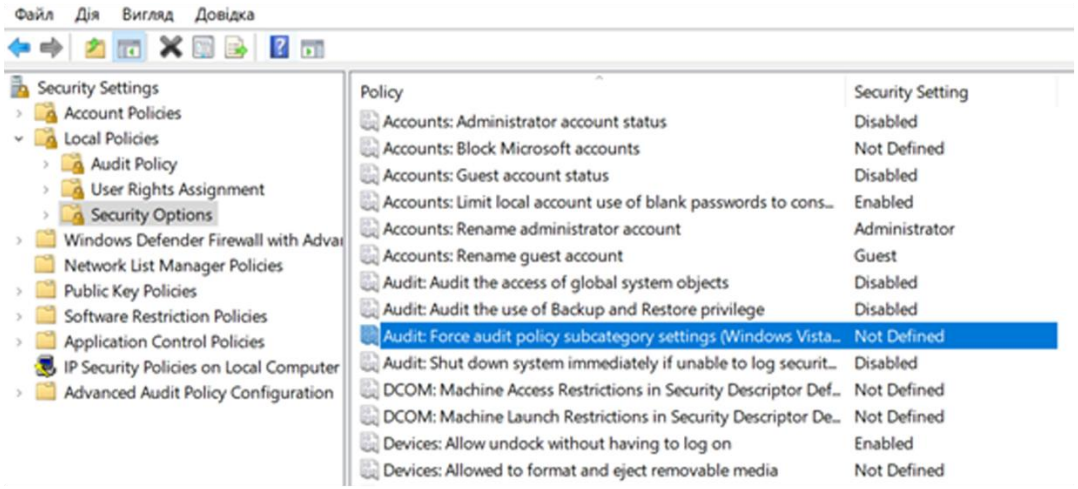
Модель порушника

| Посада | Категорія порушника | Мотив порушення | Рівень обізнаності | Доступність | Сума загроз |
|---|---|---|---|---|---|
| Користувач | ВП 2 | М 1, М 3 | К 3 | Д 4 | 13 |
| Системний адміністратор | ВП 3 | М 3 | К 4 | Д 4 | 14 |
| Електрик | ВП 1 | М 1 | К 2 | Д 2 | 6 |
| Прибиральник | ВП 1 | М 1 | К 1 | Д 2 | 5 |
| Охоронець | ВП 1 | М 3 | К 2 | Д 3 | 9 |
| Відвідувач | ЗП 1 | М 3 | К 2 | Д 1 | 7 |
| Хакер | ЗП 2 | М 4 | К 4 | Д 1 | 13 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | КРБКБ.2102150.21.02.13 Е8 | |
| Змн. | Арк. | № докум. | Підпис | Дата | Система захисту комп'ютеризованого робочого місця від інформаційних витоків | Літера | Маса | Масштаб |
| Розроб. | | Коцюк М.М. | | | Таблиця моделі порушника на комп'ютеризованому робочому місці | | | |
| Перевір. | | Чешун В.М. | | | | Аркуш 4 | Аркушів 12 | |
| Т. Контр. | | | | | | | | |
| Н. Контр. | | Мостовий С.В. | | | | ХНУ, КБ-21-2 | | |
| Затверд. | | Кльоц Ю.П. | | | | | | |

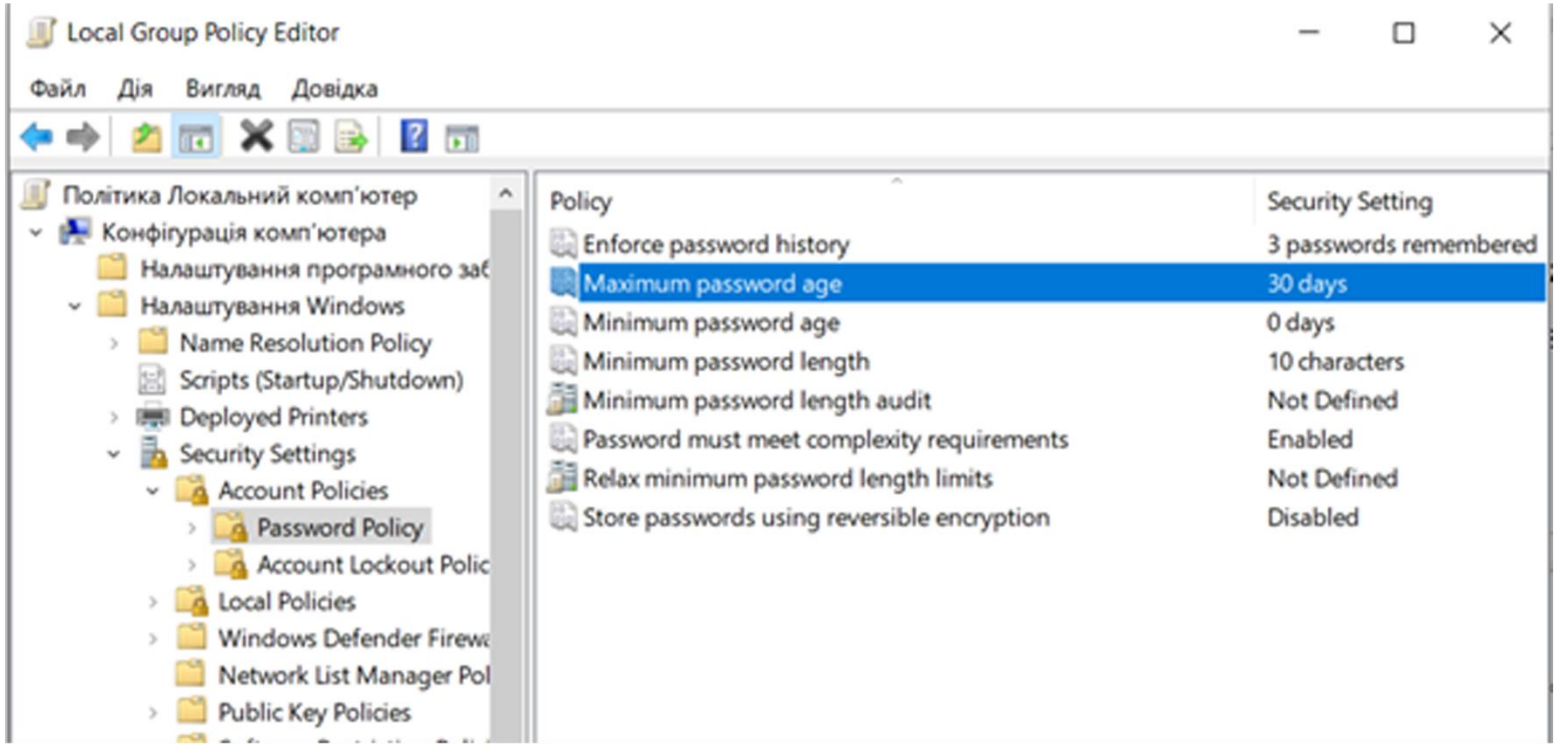



Центр керування безпековими політиками ОС Windows



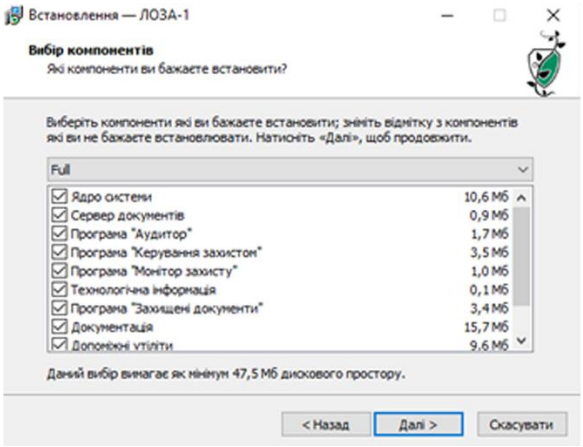

Налаштування локальної політики аудиту

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | КРБКБ.2102150.21.02.13 Е8 | | |
| Зм. | Арк. | № докум. | Підпис | Дата | Система захисту комп'ютеризованого робочого місця від інформаційних витоків<br>Налаштування політик безпеки ОС Windows | Літера | Маса | Масштаб |
| Розроб. | | Кощук М.М. | | | | | | |
| Перевір. | | Чешун В.М. | | | | | | |
| Т. Контр. | | | | | | Аркуш 5 | Аркушів 12 | |
| Н. Контр. | | Мостовий С.В. | | | | | | |
| Затверд. | | Кльоц Ю.П. | | | | ХНУ, КБ-21-2 | | |

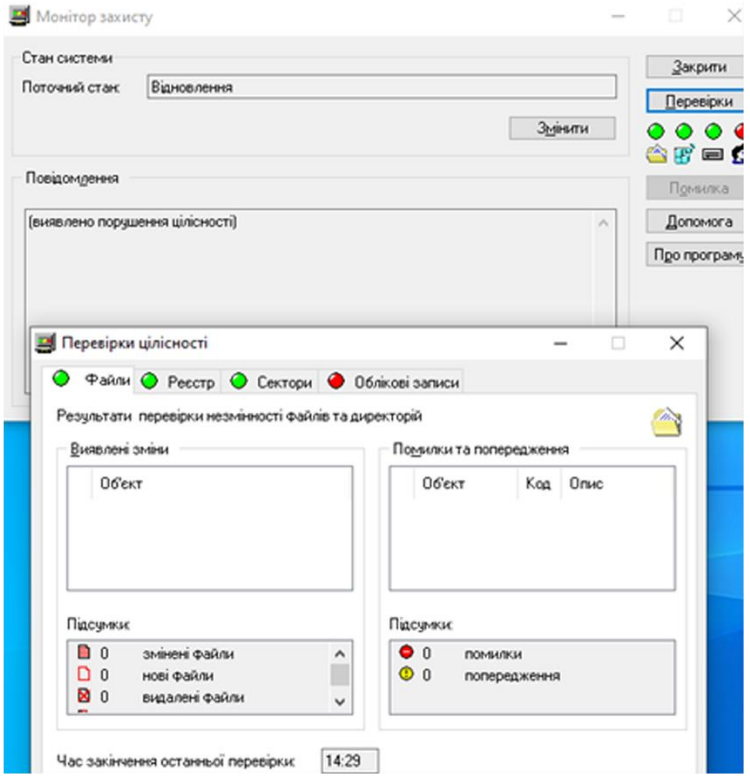



Політика паролів коип'ютеризованого робочого місця

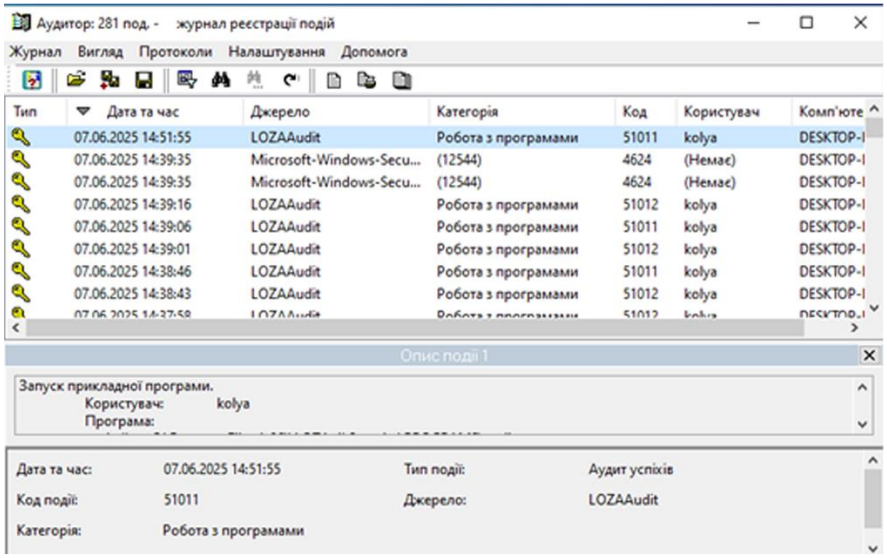
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | КРБКБ.2102150.21.02.13 Е8 | | |
| Зм. | Арк. | № докум. | Підпис | Дата | Система захисту комп'ютеризованого робочого місця від інформаційних витоків | Літера | Маса | Масштаб |
| Розроб. | | Коцюк М.М. | | | Політика паролів комп'ютеризованого робочого місця | | | |
| Перевір. | | Чешун В.М. | | | | Аркуш 6 | Аркушів 12 | |
| Т. Контр. | | | | | | | | |
| Н. Контр. | | Мостовий С.В. | | | | ХНУ, КБ-21-2 | | |
| Затверд. | | Кльоц Ю.П. | | | | | | |




Інтерфейс інсталяції
програмного комплексу ЛОЗА-1

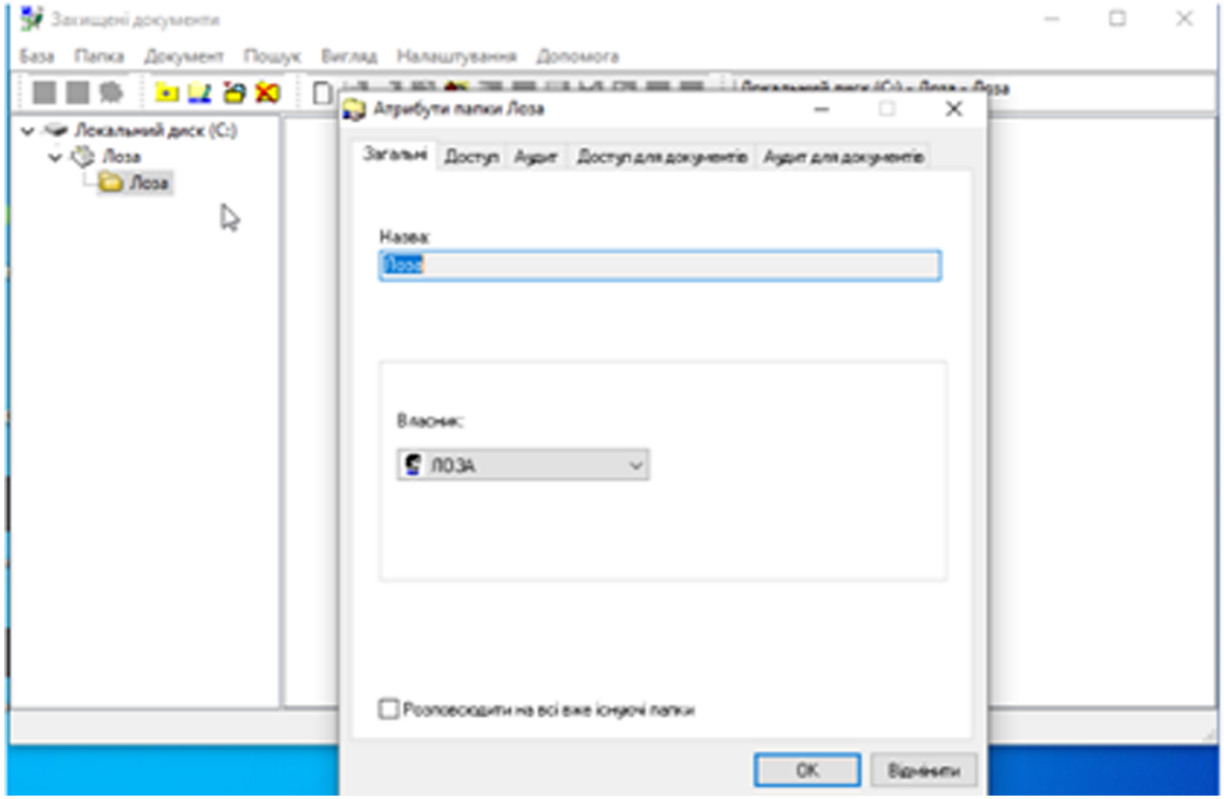



Інтерфейс моніторингу захисту
програмного комплексу ЛОЗА-1



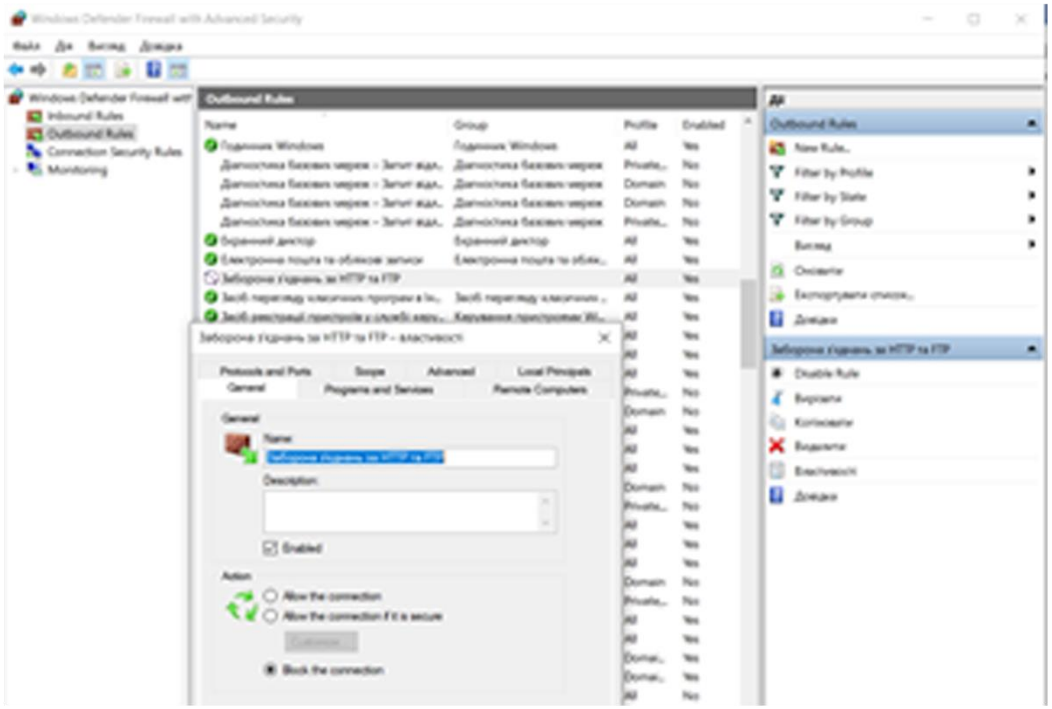

Інтерфейс аудитора
програмного комплексу ЛОЗА-1

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | КРБКБ.2102150.21.02.13 Е8 | | |
| Зм. | Арк. | № докум. | Підпис | Дата | Система захисту комп'ютеризованого робочого місця від інформаційних витоків. Робота у програмному комплексі ЛОЗА-1 | Літера | Маса | Масштаб |
| Розроб. | | Коцюк М.М. | | | | | | |
| Перевір. | | Чешун В.М. | | | | Аркуш 7 | Аркушів 12 | |
| Т. Контр. | | | | | | | | |
| Н. Контр. | | Мостовий С.В. | | | | ХНУ, КБ-21-2 | | |
| Затверд. | | Кльоц Ю.П. | | | | | | |



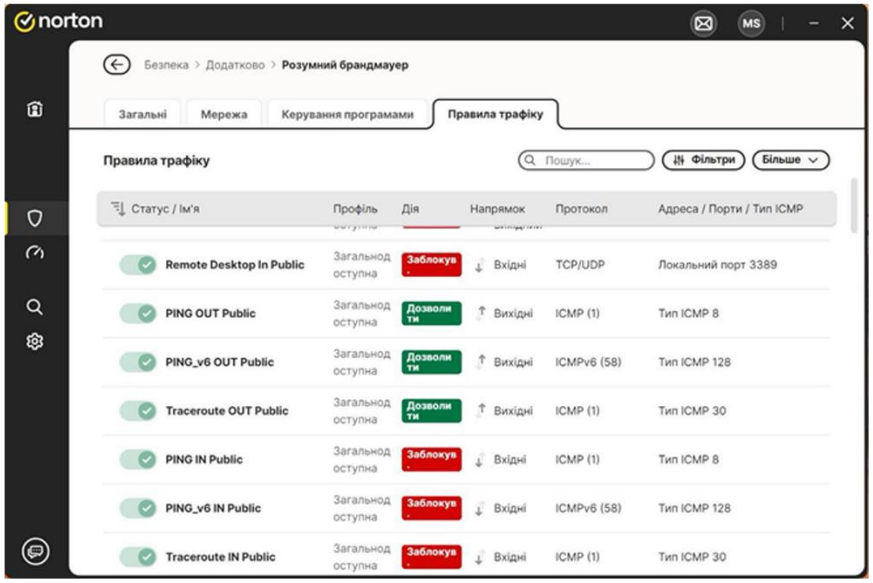

Атрибути доступів до файлів

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | КРБКБ.2102150.21.02.13 Е8 | |
| | | | | | | Система захисту комп'ютеризованого робочого місця від інформаційних витоків<br>Атрибути доступів до файлів | Літера / Маса / Масштаб |
| Змін. | Арк. | № докум. | Підпис | Дата | | | |
| Розроб. | | Коцюк М.М. | | | | | Аркуш 8 / Аркушів 12 |
| Перевір. | | Чешун В.М. | | | | | |
| Т. Контр. | | | | | | | |
| Н. Контр. | | Мостовий С.В. | | | | | ХНУ, КБ-21-2 |
| Затверд. | | Кльоц Ю.П. | | | | | |

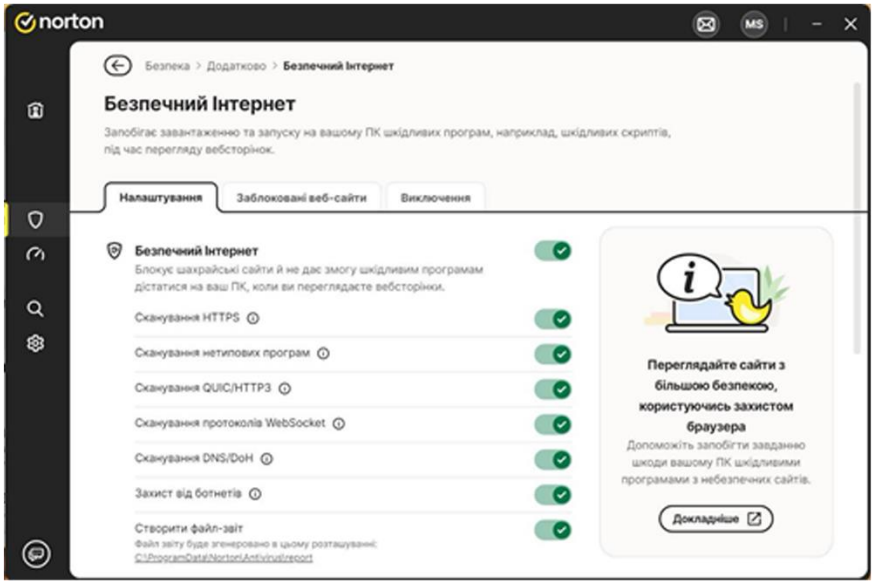



Правило заборони вихідного трафіку за незахищеними протоколами

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | КРБКБ.2102150.21.02.13 Е8 | | |
| Змн. | Арк. | № докум. | Підпис | Дата | Система захисту комп'ютеризованого робочого місця від інформаційних витоків<br>Правило заборони вихідного трафіку за незахищеними протоколами | Літера | Маса | Масштаб |
| Розроб. | | Коцюк М.М. | | | | | | |
| Перевір. | | Четчун В.М. | | | | | | |
| Т. Контр. | | | | | | Аркуш 9 | Аркушів 12 | |
| Н. Контр. | | Мостовий С.В. | | | | ХНУ, КБ-21-2 | | |
| Затверд. | | Кльоц Ю.П. | | | | | | |

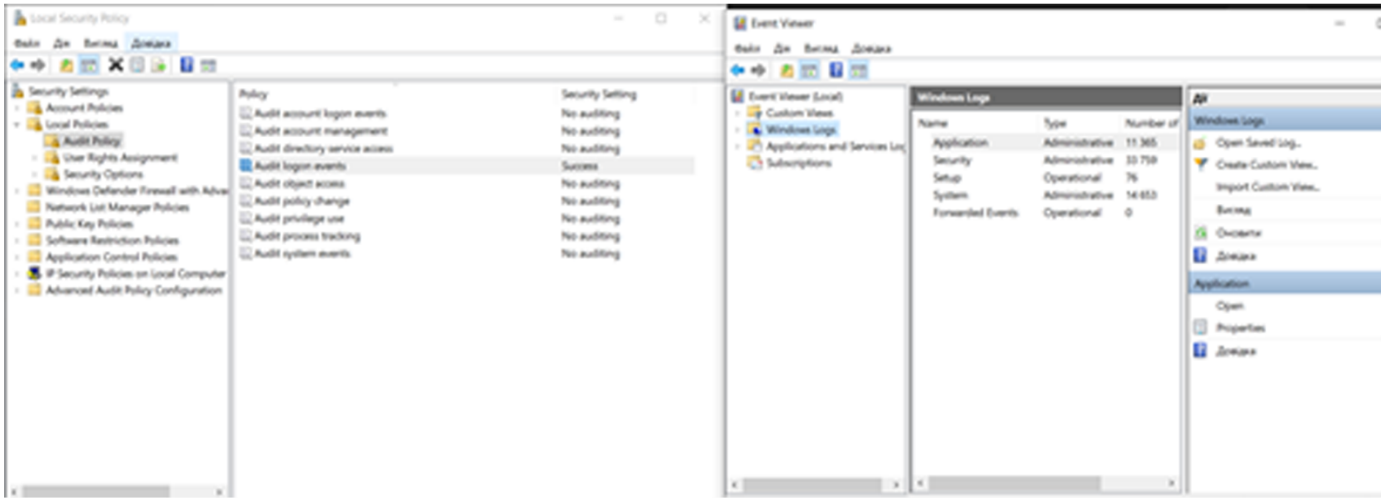



– Інтерфейс фаєрволу програмного комплексу Norton



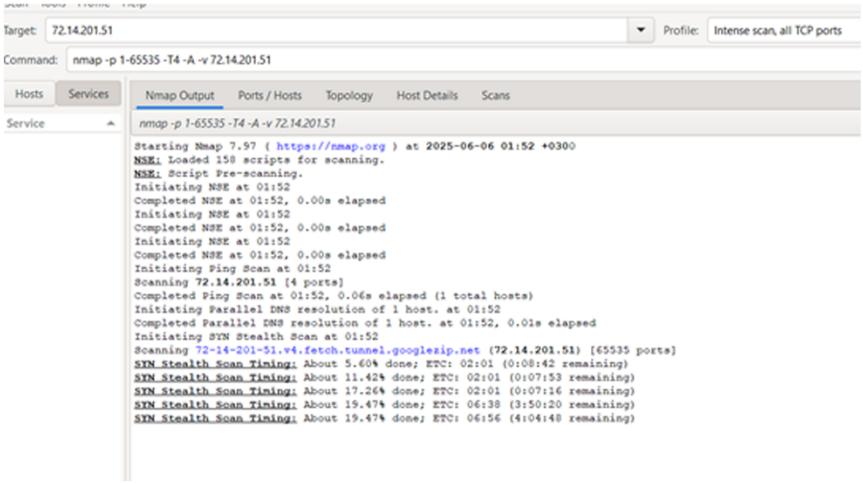

Параметри логічного мережевого захисту програмного комплексу Norton

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | КРБКБ.2102150.21.02.13 Е8 | |
| Змін. | Арк. | № докум. | Підпис | Дата | Система захисту комп'ютеризованого робочого місця від інформаційних витоків. Робота у програмному комплексі Norton | Літера | Маса | Масштаб |
| Розроб. | | Коцюк М.М. | | | | | | |
| Перевір. | | Чешун В.М. | | | | | | |
| Т. Контр. | | | | | | Аркуш 10 | Аркушів 12 | |
| Н. Контр. | | Мостовий С.В. | | | | ХНУ, КБ-21-2 | | |
| Затверд. | | Кльоц Ю.Л. | | | | | | |

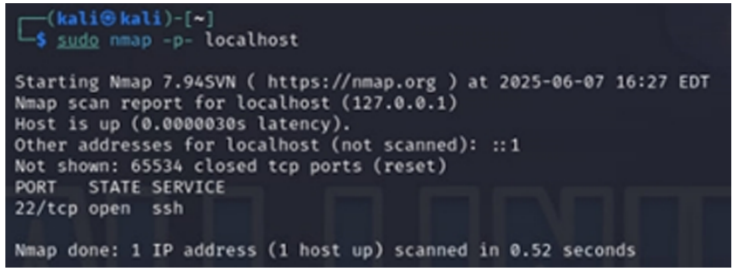



Налаштування логування та моніторингу

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | КРБКБ.2102150.21.02.13 Е8 | | |
| М. | Арк. | № докум. | Підпис | Дата | Система захисту комп'ютеризованого робочого місця від інформаційних витоків<br>Налаштування логування та моніторингу | Літера | Маса | Масштаб |
| Розроб. | | Коцюк М.М. | | | | | | |
| Перевір. | | Чешун В.М. | | | | | | |
| Т. Контр. | | | | | | Аркуш 11 | Аркушів 12 | |
| Н. Контр. | | Мостовий С.В. | | | | ХНУ, КБ-21-2 | | |
| Затверд. | | Кльоц Ю.П. | | | | | | |




Виявлення відкритих портів за допомогою Nmap




Результат сканування портів через Nmap

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | КРБКБ.2102150.21.02.13 Е8 | |
| Змін. | Арк. | № докум. | Підпис | Дата | Система захисту комп'ютеризованого робочого місця від інформаційних витоків<br>Робота з портами за допомогою Nmap | Літера / Маса / Масштаб |
| Розроб. | | Коцюк М.М. | | | | |
| Перевір. | | Чегшун В.М. | | | | |
| Т. Контр. | | | | | | Аркуш 12 / Аркушів 12 |
| Н. Контр. | | Мостовий С.В. | | | | ХНУ, КБ-21-2 |
| Затверд. | | Ключ Ю.П. | | | | |

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Коцюка Миколи Миколайовича
Студента ФІТ, 4 курсу, групи КБ-21-2

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений та надаю свою згоду на обробку й збереження університетом моєї роботи в інституційному репозитарії Хмельницького національного університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-обчислювального комплексу StrikePlagiarism та/або програмнотехнічного засобу Anti-Plagiarism) і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення текстових збігів в роботах.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

05.06.25
дата

підпис

**Протокол аналізу звіту подібності науковим керівником**

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

**Автор:** Коцюк Микола Миколайович

**Співавтор:**

**Назва:** Система захисту комп'ютеризованого робочого місця від інформаційних витоків

**Науковий керівник:**

**Підрозділ:** Кафедра кібербезпеки

**Коефіцієнт подібності 1:**3%

**Коефіцієнт подібності 2:**0%

**Мікропробіли:** 0

**Заміна букв:** 0

**Інтервали:** 0

**Білі знаки:** 0

**Дата створення звіту:** 2025-06-09 19:38:33.0

**Після аналізу Звіту подібності констатую наступне:**

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

10.06.2025р.

# Anti-Plagiarism (UA) v-15.281 Educational

**The maximum coincidence with one document 0.0%**

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 8%**

| ID: 244283<br>Title: Система захисту комп'ютеризованого робочого місця від інформаційних витоків<br>Added in a DB: 2025-06-09<br>Authors: Коцюк Микола Миколайович<br>Heads: Чешун В.М.<br>Consultants:<br>Opponents: | Document | | Sum coincidence on the DB | |
|---|---|---|---|---|
| | Symbols | Lexemes | Symbols | Lexemes |
| | 98028 | 738 | 886 (1%) | 12 (2%) |

Plagiarism sources

| ID | Description | Plagiarism presence in the document | |
|---|---|---|---|
| | | Symbols | Lexemes |

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система захисту комп'ютеризованого робочого місця від інформаційних витоків

Автор: Коцюк Микола Миколайович

Спеціальність: 125 – Кібербезпека

Освітня програма:Кібербезпека

Науковий керівник:Віктор ЧЕШУН, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

| № | Висновок | Позначка про відповідність |
|---|---|---|
| 1 | Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту. | відповідає |
| 2 | Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи. | |
| 3 | Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат. | |
| 4 | Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту. | |
| 5 | Інше: | |

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих методів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 3%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Віктор ЧЕШУН

Завідувач кафедри КБ _____ Юрій КЛЬОЦ

Гарант ОП _____ Віктор ЧЕШУН

Дата:

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

# РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Коцюк Микола Миколайович

Тема Система захисту комп'ютеризованого робочого місця від інформаційних витоків

Спеціальність 125 – Кібербезпека

**Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:**

кількість листів креслень 12; кількість сторінок записки 81.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі була розроблена система захисту комп'ютеризованог робочого місця від інформаційних витоків. У межах дослідження проаналізовано різні канали витоку інформації та методи їх протидії, включаючи нормативно-правову базу і закони України. Визначено найбільш критичні канали витоку інформації, а також загрози і модель порушникаю Розроблено систему запобігання витокам інформації через кожен канал, імплементацію та апробацію системи запобігання інформаційним витокам. Протестовано імплементовану систему та надано настанови що до ії експлуатації. Оцінено затрачені ресурси.

2. Висновок про відповідність кваліфікаційної роботи завданню У роботі повністю виконано поставлені завдання, визначені темою та завданням на кваліфікаційну роботу, як у теоретичній, так і в практичній частинах. Розроблено систему захисту типового комп'ютеризованого робочого місця від інформаційних витоків

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовано актуальність теми, сформульовано мету та завдання, описано методи дослідження. У першому розділі було проаналізовано предметну область, досліджено існуючі системи протидії і державної та міжнародної нормативно - правової бази. У другому розділі визначено найбільш загрозливіші канали витоку інформації, побудовано модель загроз та модель загроз, а токож спроектовано систему запобігань інформаційним витокам. У третьому розділі розроблено імплементацію та апробацію системи запобігання інформаційним витокам. Протестовано імлементовану систему та оцінено використані ресурси.

4. Позитивні сторони Робота має високу практичну цінність, оскільки спрямована на проєктування та реалізацію системи запобігання інформаційним витокам з комп'ютеризованого робочого місця. Запропонована система враховує актуальні загрози (мережеві, оптичні, акустичні, віброакустичні канали) технічний, адміністративний і нормативно-правовий. Рішення відзначається модульністю, можливістю масштабування та адаптації до різних середовищ, у тому числі з обмеженими ресурсами. Експериментальна апробація показала стабільну роботу системи, її здатність блокувати або виявляти спроби витоку через основні вектори атак.

5. Негативні сторони роботи Впровадження системи може потребувати значних зусиль на етапі початкової конфігурації та адміністрування, особливо в умовах багатокористувацького середовища. Для ефективної роботи в реальному масштабі часу, зокрема при постійному моніторингу дій користувачів та аналізі мережевого трафіку, система може потребувати достатнього обсягу обчислювальних ресурсів або розгортання в гібридному середовищі. Крім того, ефективність моніторингу й виявлення порушень значною мірою залежить від коректності налаштувань, оновлення політик безпеки та навчання користувачів. Іншою проблемою є необхідність постійного супроводження системи з боку фахівця, що може бути складно реалізувати в умовах невеликих підприємств або за обмеженого бюджету.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень для досягнення мети.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Пивовар Олег Сергійович,
Кандидат технічних наук, доцент, доцент кафедри телекомунікацій, медійних та інтелектуальних технологій

«9» червня 2025

Пивовар О.С.