**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**
**КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**
**КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Підвищення ефективності захисту мережевих каналів передачі інформації об'єкту інформаційної діяльності від несанкціонованого витоку даних»

на здобуття освітнього ступеня магістра
зі спеціальності __125 _Кібербезпека та захист інформації»_____
*(код, найменування спеціальності)*
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

*Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*
_____ Євген БАКУМ

Виконав: здобувач вищої освіти групи СЗДМ 61
Євген БАКУМ

Керівник: __НІМЧЕНКО Тетяна_____
*к.т.н., доцент* (ПРІЗВИЩЕ, Ім'я)

Рецензент: __
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

Кафедра Технічних систем кіберзахисту
Ступінь вищої освіти магістр
Спеціальність Кібербезпека та захист інформації
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

**ЗАТВЕРДЖУЮ**
Завідувач кафедри СІКЗ
_____Олександр Туровський

«____» _____ 2025 р.

**ЗАВДАННЯ**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Бакуму Євгену Андрійовичу
*(прізвище, ім'я, по батькові здобувача)*

1. Тема кваліфікаційної роботи:
«Підвищення ефективності захисту мережевих каналів передачі інформації об'єкту інформаційної діяльності від несанкціонованого витоку даних»
керівник кваліфікаційної роботи Тетяна НІМЧЕНКО к.т.н., доцент
*(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)*
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: об'єкт критичної інфраструктури, технічні канал витоку інформації, вимоги до захисту інформації з обмеженим доступом, персонал організаційно-штатних структур державних органів управління.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Провести огляд процесу обробки персональних даних в локальних ком'ютерних мережах, каналів та способів несанкціонованого доступу до них;
4.2. Проаналізувати методи захисту інформації в локальній ком'ютерній мережі від несанкціонованого доступу до персональних даних;
4.3. Розробити практичні рекомендацій що до застосування програмних застосунків для захисту персональних даних, що оброляються в локальній комп'ютерній мережі.

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах.

6. Дата видачі завдання 15.10.2025

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Підбір науково-технічної літератури | | |
| 2 | Написання першого розділу роботи | | |
| 3 | Написання другого розділу роботи | | |
| 4 | Написання третього розділу роботи | | |
| 5 | Написання висновків по роботі | | |
| 6 | Підготовка демонстраційних матеріалів | | |
| 7 | Підготовка доповіді | | |

Здобувач вищої освіти _____ Євген БАКУМ
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Тетяна НІМЧЕНГКО
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

# РЕФЕРАТ

Текстова частина кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 64 сторінок, має 11 рисунків, 6 таблиць. Список використаних джерел містить 33 найменування і займає 4 сторінки.

**Метою кваліфікаційної** роботи є підвищення рівня захищеності локальної комп'ютерної мережі від несанкціонованого доступу до персональних даних шляхом застосування прогамного за стосунку.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести огляд процесу обробки персональних даних в локальних ком'ютерних мережах, каналів та способів несанкціонованого доступу до них;

– проаналізувати методи захисту інформації в локальній ком'ютерній мережі від несанкціонованого доступу до персональних даних;

- розробити практичні рекомендацій що до застосування програмних застосунків для захисту персональних даних, що оброляються в локальній комп'ютерній мережі.

**Апробація:**

**Є.В. Бакум, Є.М. Шиньковий, Є.І. Нагаєв.** Типи та механізми кібератак на мережеві канали передачі даних об'єктів інформаційної діяльності. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.34-35. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: ЛОКАЛЬНА КОМ'ЮТЕРНА МЕРЕЖА, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ЗАХИСТ ІНФОРМАЦІЇ, ЗАГРОЗИ, УПРАВЛЯННЯ ДОСТУПОМ, ІДЕНИФІКАЦІЯ, АУТЕНТИФІКАЦІЯ.

# ABSTRACT

The text part of the qualification work consists of an introduction, three sections, general conclusions, a list of sources used, the total volume of the work is 64 pages, has 11 figures, 6 tables. The list of sources used contains 33 names and takes up 4 pages.

**The purpose of the qualification work** is to increase the level of protection of a local computer network from unauthorized access to personal data by using software for this purpose.

To achieve the set goal, it is necessary to solve the following tasks:

– to conduct a review of the process of processing personal data in local computer networks, channels and methods of unauthorized access to them;

– to analyze methods of protecting information in a local computer network from unauthorized access to personal data;

- to develop practical recommendations for the use of software applications to protect personal data processed in a local computer network.

**Approbation:**

E.V. Bakum, E.M. Shynkovy, E.I. Nagayev. Types and mechanisms of cyberattacks on network data transmission channels of information activity objects. All-Ukrainian scientific and practical conference: Current problems of information and telecommunication systems security. Kyiv, November 05, 2025, Kyiv: DUIKT Research and Development Center. – 2025. P.83-84. https://duikt.edu.ua/uploads/p_2661_93669247.pdf

**Keywords:** LOCAL COMPUTER NETWORK, UNAUTHORIZED ACCESS, INFORMATION PROTECTION, THREATS, ACCESS MANAGEMENT, IDENTIFICATION, AUTHENTICATION.

# ЗМІСТ

## ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

| | | |
|---|---|---|
| ЛКМ | – | Локальна комп’ютерна мережа |
| БСМ | – | Бездротова сенсорна мережа |
| ПЗ | – | Програмне забеспечення |
| СЗІ | – | Система захисту інформації |
| ПК | – | Персональний комп’ютер |
| АС | – | Автоматизована система |
| СКЗІ | – | Система комплексного захисту інформації |
| НСД | – | Несанкціонований доступ |

# ВСТУП

Питання захисту інформації від несанкціонованого доступу набуло актуальності відколи людство навчил писемності. З тих пір існувала інформація, яка має бути доступною не для всіх. Ті хто володів такою інформацію, вдавалися до різних способів її захисту. Нині в епоху комп'ютеризації, контроль та управління різними об'єктами, благополуччя та навіть життя багатьох, залежить від забезпечення інформаційної безпеки, комп'ютерних систем обробки інформації. Для нормального та безпечного функціонування цих систем необхідно підтримувати їх безпеку та цілісність, тобто задіяти так званий «спеціальний захист» даних.

Проблеми захисту у локальних обчислювальних мережах (далі – ЛКМ) постійно перебувають у центрі уваги як фахівців із розробки та використання цих систем, а й широкого кола користувачів.

Забезпечення захисту інформації є актуальним завданням при використанні інформаційно-комунікаційних технологій.

**Метою кваліфікаційної** роботи є підвищення рівня захищеності локальної комп’ютерної мережі від несанкціонованого доступу до персональних даних шляхом застосування прогамного за стосунку.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести огляд процесу обробки персональних даних в локальних ком’ютерних мережах, каналів та способів несанкціонованого доступу до них;

– проаналізувати методи захисту інформації в локальній ком’ютерній мережі від несанкціонованого доступу до персональних даних;

- розробити практичні рекомендацій що до застосування програмних застосунків для захисту персональних даних, що оброляються в локальній комп’ютерній мережі.

**Об'єктом дослідження** є процес обробки персональних даних в локальній комп’ютерній мережі комерційного підприємства иємства..

**Предмет дослідження** – захист персональних даних в локальній комп’ютерній мережі.

# Розділ 1
# ОГЛЯД ПРОЦЕСУ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ В ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ ТА СПОСОБІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО НИХ

## 1.1 Персональні дані

Термін «персональні дані» є відправною точкою для застосування Загального регламенту про захист даних (GDPR). GDPR застосовується лише тоді, коли обробка даних стосується персональних даних. Термін визначено у Розділі 4, пункті 1 GDPR. Персональні дані означають будь-яку інформацію, що стосується ідентифікованої або ідентифікованої фізичної особи [1].

Суб'єкт даних вважається ідентифікованим, якщо його можна ідентифікувати прямо чи опосередковано, зокрема за допомогою ідентифікатора, такого як ім'я, номер посвідчення особи, дані про місцезнаходження, онлайн-ідентифікатор або за певним фактором, що стосується фізичної, фізіологічної, генетичної, психічної, комерційної, культурної чи соціальної ідентичності цієї фізичної особи.[2] На практиці це також включає всі дані, які належать фізичній особі або можуть бути віднесені до неї будь-яким чином. Наприклад, номери телефонів, номери кредитних карток або персональні ідентифікаційні номери, інформація про особу, реєстраційні номери транспортних засобів, фізичні характеристики, номери клієнтів або адреси – все це є персональними даними.

Оскільки визначення містить «будь-яку інформацію», слід вважати, що термін «персональні дані» слід тлумачити якомога ширше. Судова практика Європейського Суду також підтримує цю точку зору, класифікуючи менш точну інформацію, таку як записи про робочий час, включаючи години відпочинку працівників, періоди відпочинку та неробочі години, як персональні дані, включаючи письмові відповіді кандидата під час іспиту та

будь-які коментарі екзаменатора щодо цих відповідей також вважаються «персональними даними». Те саме стосується IP-адрес.

Якщо контролер даних має законне право вимагати від постачальників послуг надання додаткової інформації, яка може ідентифікувати користувача за його IP-адресою, ця інформація також вважається персональними даними. Важливо також зазначити, що персональні дані не обов'язково мають бути об'єктивними. Суб'єктивна інформація, така як думки, судження чи оцінки, також може бути персональними даними. Наприклад, оцінки кредитоспроможності особи або оцінка роботи роботодавця[2].

Нарешті, закон передбачає, що інформація в особових справах повинна стосуватися фізичної особи. Іншими словами, захист даних не поширюється на інформацію юридичних осіб (таких як компанії, фонди та установи). Для фізичних осіб захист даних починається і закінчується їхньою правоздатністю. Зазвичай, особа набуває правоздатності при народженні та втрачає її після смерті. Тому, щоб вважатися персональними даними, дані повинні бути пов’язані з ідентифікованою або такою, що може бути ідентифікована, живою фізичною особою[3].

Окрім загальних персональних даних, слід в першу чергу розглянути спеціальні категорії персональних даних (також відомі як конфіденційні персональні дані), оскільки вони дуже важливі, оскільки підлягають вищому рівню захисту. Ці дані включають генетичні дані, біометричні дані та дані про стан здоров'я, а також персональні дані, що розкривають расове чи етнічне походження, політичні погляди, релігійні чи ідеологічні переконання, або членство в профспілці.[3]

### 1.2 Визначення локальної обчислювальної мережі

Інститут інженерів з електротехніки та електроніки (IEEE) визначає локальну обчислювальну мережу (LAN) як «систему передачі даних, яка дозволяє кільком незалежним пристроям безпосередньо спілкуватися один з

одним на помірних швидкостях через фізичний канал зв'язку в межах відповідного географічного району».[4] Як правило, локальна мережа з'єднує сервери, робочі станції, принтери та пристрої масового зберігання даних через спільну мережеву операційну систему, що дозволяє користувачам спільно використовувати ресурси та функції, що надаються локальною мережею.[4]

## 1.3. Проблема безпеки локальної мережі

### 1.3.1 Несанкціонований доступ (НС)

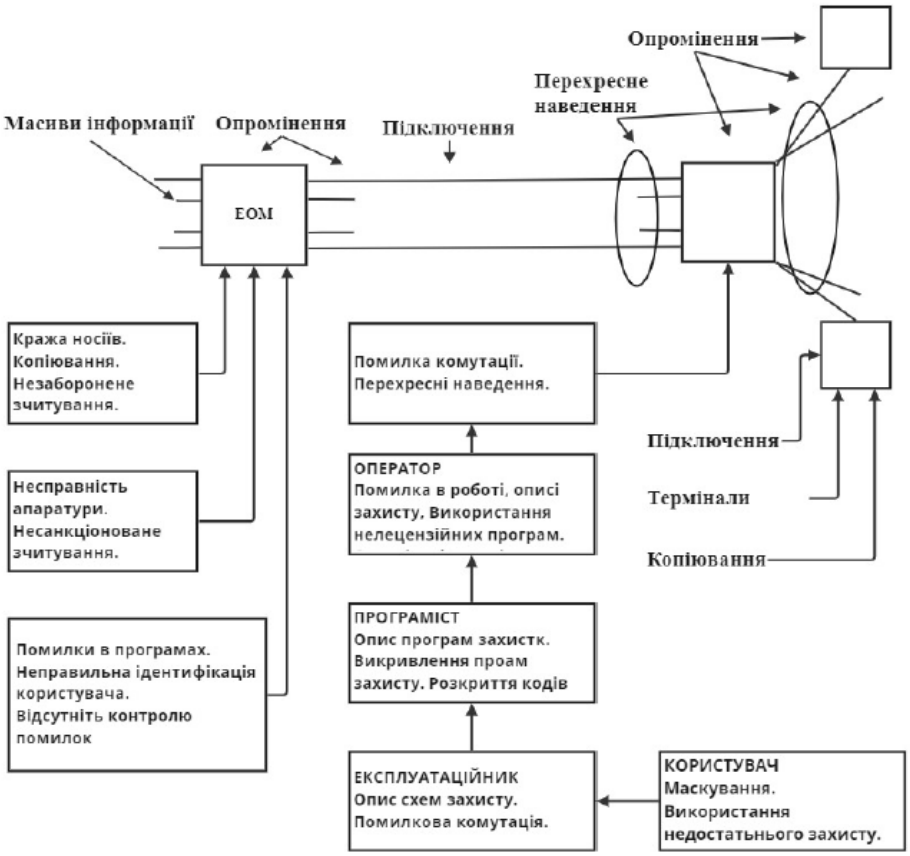


Рис.1.1 Шляхи несанкціонованого отримання інформації

Архітектура та експлуатаційні характеристики LCM дозволяють зловмисникам знаходити або спеціально створювати вразливості для отримання прихованого доступу до інформації. Враховуючи різноманітні відомі злочинні дії, це говорить про те, що таких вразливостей може існувати більше [4]. Методи несанкціонованого доступу до інформації (Рисунок 1.1)

Несанкціонований доступ до інформації в LCM включає:

– Прямий доступ – (вимагає фізичного контакту з компонентами LCM).

– Непрямий доступ – (не вимагає фізичного контакту з компонентами LCM).

Несанкціонований доступ до інформації (канали витоку інформації) включає: [3,5,6]

– Запис акустичних каналів за допомогою пристроїв;

– Перехоплення електромагнітного випромінювання;

– Дистанційна фото- та відеозйомка;

– Втрата носіїв інформації та крадіжка виробничих відходів;

– Зчитування даних інших користувачів;

– Копіювання та зчитування носіїв інформації;

– Несанкціоноване проникнення в термінал керування;

– Вхід у систему як зареєстрований користувач.

– Отримання захищених даних через серію авторизованих запитів;

– Використання вразливостей у мовах програмування та операційних системах;

– Навмисне вбудовування спеціальних блоків коду типу «троянський кінь» у бібліотеки програм;

– Зловмисне відключення механізмів захисту.

Канали витоку інформації складаються з джерела інформації, фізичного носія або середовища поширення сигналу, що містить інформацію, та методів вилучення інформації з сигналу або носія [4,6] (рис. 1.2).


Рис. 1.2 Основні канали витоку інформації під час її обробки на ПК

### 1.3.2 Використання програмних засобів для НС

Клас шкідливих ПЗ (далі – віруси) складають розроблені комп'ютерні віруси, троянські коні (закладки) та засоби проникнення у віддалені системи через локальні та глобальні мережі [5], (Рис. 1.3).


Рис. 1.3 Типи руйнівних програмних засобів

Залежно від джерела зараження, файлові віруси можна класифікувати на файлові віруси, завантажувальні віруси, гібридні (віруси завантаження файлів), пакетні віруси та мережеві віруси. Файлові віруси зазвичай заражають файли з розширеннями .com та .exe. Однак деякі варіанти можуть також заражати інші типи файлів (наприклад, .dll, .sys, .ovl, .prg, .bat, .mnu), але зазвичай втрачають здатність до самовідтворення [5]. Залежно від джерела зараження, файлові віруси також можна класифікувати на резидентні віруси та нерезидентні віруси. Останні стають активними лише під час запуску зараженого файлу та залишаються активними протягом обмеженого часу [5]. Резидентні віруси встановлюють свою копію в пам'ять, перехоплюючи доступ операційної системи до різних об'єктів та заражаючи їх. Деякі віруси можуть перехоплювати кілька різних функцій переривання, тому файли можуть бути заражені під час перейменування, копіювання, видалення, зміни атрибутів, перегляду каталогів, виконання, відкриття файлів та інших операцій. Резидентні віруси залишаються активними до вимкнення комп'ютера. Макровіруси – це відносно новий тип вірусів, які використовують

функціональність макромови, вбудовану в програмне забезпечення, таке як текстові редактори та електронні таблиці. Макровіруси наразі широко поширені в Microsoft Word та Excel. Вони перехоплюють певні функції файлів, коли заражений документ відкривається або закривається, згодом заражаючи інші файли, до яких програма отримує доступ. У певному сенсі ці віруси можна назвати резидентними вірусами, оскільки вони працюють лише в межах свого середовища виконання (тобто відповідної програми) [5].

Ще однією категорією файлових вірусів є сімейство вірусів DIR, які не впроваджуються у файли, а натомість реструктуризують файлову систему таким чином, що керування передається вірусу щоразу, коли відкривається будь-який файл.

Завантажувальні віруси відрізняються від резидентних вірусів тим, що вони поширюються між системами через завантажувальний сектор. Комп'ютер заражається, коли намагається завантажитися із зараженого диска або під час читання вмісту дискети [5].

Комбіновані віруси можуть поширюватися як через завантажувальний сектор, так і через файли.

Пакетні віруси – це відносно прості та старіші типи вірусів, написані з використанням мови керування завданнями операційної системи.

Мережеві віруси («черв’яки») поширюються комп’ютерними мережами, зменшуючи пропускну здатність мережі, уповільнюючи роботу серверів тощо. Вони є одними з найшвидше поширюваних вірусів. Найвідомішим з них є так званий «черв’як Морріса». Найновіші «черв’яки» вбудовані в різні стиснуті файли (arj, zip тощо) і займають місце на диску[5].

За ступенем пошкодження віруси можна класифікувати на такі категорії:

• Відносно безпечні та нешкідливі — їхній вплив обмежується зайняттям доступної пам’яті та впливом на графіку чи звукові ефекти. Варто зазначити, що використання пам’яті в деяких випадках може призвести до збоїв системи, і ці ефекти можуть відволікати користувачів, що призводить до помилок користувача;

• Небезпечний тип – віруси, які можуть спричинити збій системи;

• Дуже небезпечний тип – віруси, поведінка яких може призвести до втрати програм, пошкодження даних або стирання інформації системної області.

Через велику різноманітність вірусів їх важко класифікувати на основі алгоритмічних характеристик. Ми можемо розрізнити найпростіші «звичайні» віруси, які написані в одному блоці коду та можуть бути ідентифіковані з тексту програми-носія; та «фрагментовані» віруси, які розділені на, здавалося б, не пов'язані частини, але містять інструкції щодо того, як комп'ютер збирає їх у ціле та реплікує вірус [5].

З точки зору методів маскування, віруси можна розділити на стелс-віруси (приховані віруси) та поліморфні віруси. Перші перехоплюють функції операційної системи, відповідальні за обробку файлів, та підробляють результати запитів.

Ці віруси використовують різні механізми «прихованого» доступу, але можна узагальнити кілька спільних принципів [3,5]:

• Щоб приховати збільшення довжини заражених файлів, вірус надсилає менше значення довжини файлу програмі перегляду каталогів;

• Щоб запобігти виявленню коду вірусу користувачами під час перегляду файлів, вірус шифрує файл під час його відкриття та повторно заражає його під час закриття;

• Щоб приховати свою присутність у пам'яті комп'ютера, вірус стежить за активністю монітора резидентної пам'яті; якщо робиться спроба переглянути код вірусу, система аварійно завершує роботу.

Віруси, які використовують кілька методів для шифрування власних файлів, називаються поліморфними вірусами. Алгоритм шифрування змінюється випадковим чином під час зараження інших файлів. У цьому випадку важко ідентифікувати характерні послідовності байтів коду вірусу [5].

Несанкціоновані зміни даних та програмного забезпечення можуть відбуватися через такі типи вразливостей [3,5]:

• Користувачам з правами лише на читання надаються права на запис;

• До програмного забезпечення вносяться непомічені зміни, включаючи додавання коду, що використовується для створення троянських програм;

• Конфіденційні дані не мають контрольних сум шифрування;

• Відсутність методів захисту від вірусів та їх виявлення.

### 1.4 Висновок по розділу

1. Досліджено концепції локальних мереж та персональних даних.

2. Досліджено канали витоку інформації та технічні засоби, які можуть призвести до несанкціонованого доступу до локальної мережі підприємства.

3. Уточнено цілі впровадження системи інформаційної безпеки:

- Збереження конфіденційності даних під час зберігання, обробки або передачі даних у локальній мережі;

- Збереження цілісності даних під час зберігання, обробки або передачі даних у локальній мережі;

- Збереження доступності даних, що зберігаються в локальній мережі, а також можливості своєчасної обробки та передачі даних.

# РОЗДІЛ 2.
# АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ЛОКАЛЬНІЙ КОМ'ЮТЕРНІЙ МЕРЕЖІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

## 2.1 Способи захисту інформації

Система захисту інформації (СЗІ) – це комплекс організаційних та інженерних заходів, програмного та апаратного забезпечення, призначених для забезпечення інформаційної безпеки в інформаційній системі (ІС). СЗІ включає заходи та інструменти, що реалізують різні методи та механізми захисту інформації від несанкціонованих операцій та доступу. Ці операції та доступи можуть здійснюватися шляхом підключення пристроїв та ліній зв'язку, видавання себе за зареєстрованих користувачів, обходу заходів захисту для використання або підробки інформації, використання вбудованих пристроїв або програм, або використання комп'ютерних вірусів. [6]

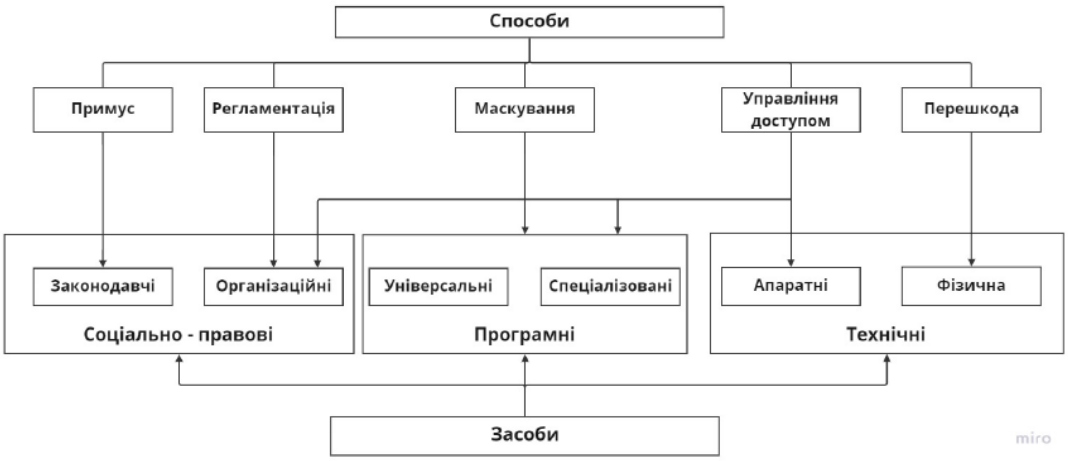


Рис. 2.1 Способи та засоби захисту інформації в ЛВС Способи

Методи захисту інформації в LCM включають усі наступні елементи (Рисунок 2.1):

1. Бар'єри — фізичні бар'єри, що захищають носії інформації від вторгнення [6].

2. Контроль доступу — система захисту інформації, яка використовує всі ресурси підприємства [6].

Вона включає такі захисні функції:

- ідентифікація інформації та персоналу за допомогою паролів, карток, біометрії, програмних інструментів тощо;

- перевірка журналів системи реєстрації персоналу для розуміння робочих призначень, дозволів та прав доступу до інформації;

- створення та організація роботи в рамках нормативної бази;

- система є відмовостійкою під час несанкціонованих спроб (затримки роботи, відмови, зупинки, тривоги).

3. Маскування — використання шифрувальних перетворень для захисту даних у LCM. Шифрування є найважливішим методом захисту, коли інформація передається по незашифрованих лініях зв'язку [6].

4. Регламент — документування правил, що визначають обов'язки персоналу та процедури обробки конфіденційної інформації [6].

5. Обов'язковість — Користувачі та персонал інформаційної системи зобов'язані дотримуватися правил обробки та використання захищеної інформації, інакше їм загрожує матеріальна, адміністративна або кримінальна відповідальність [6]. Розглянуті заходи захисту інформації реалізуються за допомогою різноманітних заходів, які можна розділити на технічні заходи, програмні заходи, організаційні заходи, законодавчі заходи та морально-етичні заходи [7].

6. Організаційні заходи захисту стосуються організаційно-правових заходів, що регулюють створення та функціонування інформаційних систем.

- Організаційні заходи охоплюють усі структурні елементи всіх етапів інформаційної системи: будівництво об'єкта, проектування системи, встановлення та введення в експлуатацію обладнання, тестування та перевірку, а також експлуатацію.

- Законодавчі заходи захисту включають закони та нормативні акти, розроблені державою для регулювання використання та обробки інформації з обмеженим доступом та для визначення заходів відповідальності за порушення цих правил.

- Морально-етичні правила включають правила, які традиційно сформувалися в певній країні чи суспільстві або розвинулися з поширенням обчислювальних ресурсів. Ці правила здебільшого є обов'язковими та належать до законодавчих заходів, але порушення цих правил зазвичай призводить до втрати авторитету та престижу для окремих осіб або груп [7].

## 2.2 Заходи захисту інформації в ЛКМ

Захист інформації на персональних комп'ютерах стосується організації різних методів та засобів для зменшення можливості каналів витоку інформації та можливості спотворення інформації під час зберігання та обробки на персональних комп'ютерах[8]. 1. Організаційні заходи захисту стосуються загальних заходів, які ускладнюють доступ неавторизованого персоналу до важливої інформації, незалежно від конкретних обставин методу обробки інформації та каналу витоку інформації [8]. Організаційні заходи включають:

– Обмеження доступу до місць, де обробляється конфіденційна інформація.

– Дозвіл виконувати завдання на персональних комп'ютерах, що використовуються для обробки конфіденційної інформації, лише перевіреному персоналу. Посадовці розробили процедури виконання операцій на

персональних комп'ютерах. Носії інформації зберігалися в щільно закритих, міцних шафах.[8]

* Визначали один або кілька персональних комп'ютерів для обробки важливої інформації, і подальша робота могла виконуватися лише на цих комп'ютерах.

* Встановлювали монітори, клавіатури та принтери таким чином, щоб запобігти перегляду вмісту інформації, що обробляється, сторонніми особами.

* Постійно контролювали роботу принтерів та інших пристроїв, що виводять важливу інформацію на носії інформації.

* Знищували барвники або інші матеріали, що містять фрагменти важливої інформації.

* Забороняли персоналу, який брав участь в обробці секретної інформації, вести переговори щодо безпосереднього змісту секретної інформації.

2. Організаційно-технічні заходи захисту — заходи, пов'язані з конкретними обставинами каналів витоку та методів обробки інформації, але не вимагають впровадження нестандартних технологій та/або обладнання.[9] Організаційно-технічні заходи включали:

* Обмеження доступу до корпусів персональних комп'ютерів шляхом встановлення механічних блокувальних пристроїв.

* Знищення всієї інформації на жорсткому диску комп'ютера за допомогою засобів низькорівневого форматування для можливості її відправлення на ремонт.

- Блоки живлення комп'ютерів повинні бути незалежними або підключеними до загального (мережевого) джерела живлення через регулятор напруги (мережевий фільтр).

- Використовуйте РК- або плазмовий дисплей для відображення інформації та струменевий або лазерний принтер для друку.

Монітор, хост, клавіатуру та принтер слід розміщувати на відстані щонайменше 2,5-3,0 метрів від освітлювального обладнання, кондиціонерів, комунікаційного обладнання (телефону), металевих труб, телевізійного та радіообладнання, а також інших комп'ютерів, що не використовуються для обробки конфіденційної інформації.[10]

## 2.3. Основні сервіси безпеки

### 2.3.1 Ідентифікація та автентифікація

Першим кроком у захисті ресурсів локальної мережі є перевірка особи користувача. Процес підтвердження особи користувача називається автентифікацією.[11] Автентифікація є основою ефективності інших засобів контролю в локальній мережі. Наприклад, механізми реєстрації можуть надавати інформацію про використання на основі ідентифікаторів користувачів. Механізми контролю доступу дозволяють доступ до ресурсів локальної мережі на основі ідентифікаторів користувачів. Обидва ці засоби контролю ефективні лише в тому випадку, якщо запитувач служби локальної мережі є дійсним користувачем, призначеним цьому конкретному ідентифікатору користувача.[12] Автентифікація вимагає, щоб локальна мережа певним чином ідентифікувала користувачів. Зазвичай це базується на призначеному ідентифікаторі користувача. Однак без автентифікації локальна мережа (LAN) не може довіряти особі користувача. Автентифікація досягається шляхом надання користувачеві інформації, якою володіє лише він (наприклад, токен), інформації, яку знає лише користувач (наприклад, пароль), або іншої інформації. Відбитки пальців та інші ознаки можуть зробити особу користувача унікальною. Чим більше ознак має надати користувач, тим менший ризик видавати себе за законного користувача. [12]

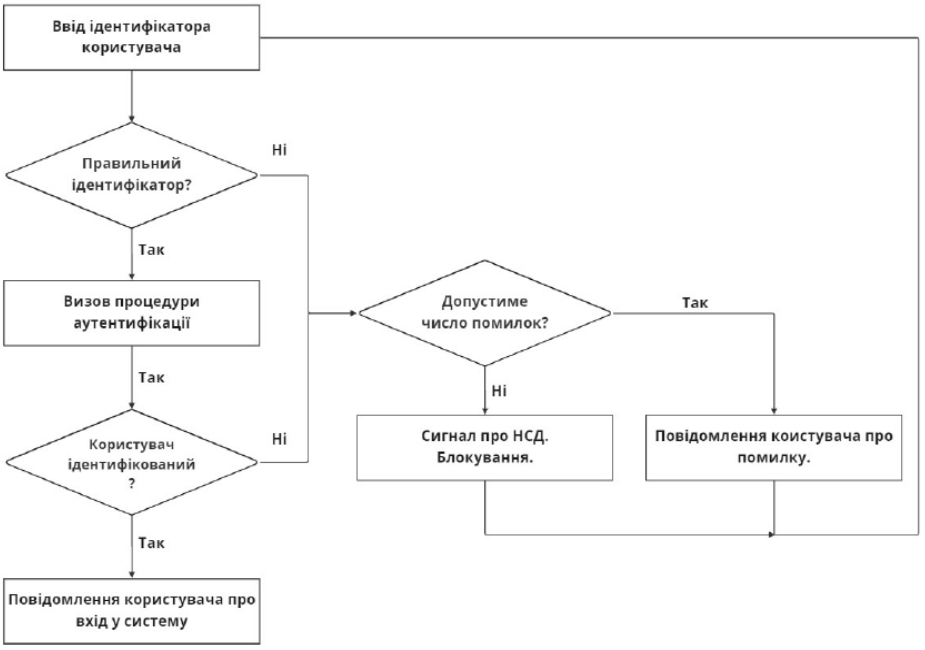


Рис 2.2 Класична процедура ідентифікації та аутентифікації

На рисунку 2.2 показано загальний процес ідентифікації та верифікації, коли користувач отримує доступ до AS. Якщо особа користувача підтверджена під час процесу автентифікації, система безпеки повинна визначити його дозволи (набір дозволів). Це важливо для подальшого контролю та обмеження доступу до ресурсів [13].

Коли користувач (або інша особа) стверджує, що є фізичною особою, це називається ідентифікацією. Ідентифікація може здійснюватися за допомогою імені користувача, ідентифікатора процесу, смарт-картки або будь-якої іншої інформації, яка може однозначно ідентифікувати користувача чи особу. Системи безпеки використовують цей метод ідентифікації, щоб визначити, чи має хтось право доступу до об'єкта [13].

Ідентифікація означає знання того, хто є хтось, навіть якщо він відмовляється співпрацювати.

Системи відеоспостереження, відбитки пальців та зразки ДНК – це деякі з ресурсів, які можна використовувати для ідентифікації осіб. З іншого боку, цифровий світ використовує відбитки пальців пристроїв або інші біометричні дані для досягнення тієї ж мети. Особи також можна ідентифікувати в

Інтернеті за стилем письма, натисканнями клавіш або тим, як вони грають у комп'ютерні ігри [14].

Акт визначення особи людини зазвичай називається ідентифікацією.

Чому важлива ідентифікація користувача?

Персональна ідентифікація – це процес пов’язування конкретної особи з певною ідентичністю. Вона важлива, оскільки відповідає на певні питання про людей, такі як «Чи є ця особа тією особою, за яку вона себе видає?», «Чи була ця особа тут раніше?» або «Чи слід дозволити цій особі доступ до нашої системи?»

Ідентифікація корисна для організацій, оскільки вона:

– Може бути легко інтегрована в різні системи

– Є недорогою

– Може ефективно стримувати самозванців

Види ідентифікації

Для ідентифікації особи можна використовувати документи, що посвідчують особу (посвідчення особи, національне посвідчення особи, картку громадянина) або паспорт (якщо паспорт має формат невеликої стандартної кредитної картки). Деякі країни також видають офіційні документи, що посвідчують особу, такі як національні посвідчення особи, які можуть бути обов’язковими або необов’язковими; тоді як інші країни можуть покладатися на регіональні документи, що посвідчують особу, або неофіційні документи для підтвердження особи. [14] Деякі інші прийнятні методи ідентифікації включають:

Інформацію, відому особі: паролі, PIN-коди, дівоче прізвище матері або коди замків дверей. Використання інформації, відомої особі, для автентифікації може бути найпростішим варіантом, але також найменш безпечним.

Речі, що належать особі: ключі, картки, картки доступу або бейджі тощо. Цей метод зазвичай використовується для отримання доступу до таких місць, як банки та офіси, але його також можна використовувати для входу в конфіденційні місця або перевірки облікових даних системи. Це простий варіант, але ці предмети легко вкрасти.

Щодо фізичних осіб: Біометричні дані фізичної особи повністю належать цій особі та не можуть бути втрачені чи викрадені. Використання біометричних даних для ідентифікації є найточнішим та найбезпечнішим варіантом.

Автентифікація – це процес перевірки особи, який відбувається, коли суб'єкт надає відповідні облікові дані. Наприклад, коли користувач вводить правильне ім'я користувача та пароль, пароль підтверджує, що користувач є власником цього імені користувача. Коротше кажучи, автентифікація використовується для перевірки дійсності заявленої особи [15].

У системах, захищених іменем користувача та паролем, користувачі повинні надати дійсні облікові дані для доступу до системи. Це не лише допомагає захистити систему від атак невідомих третіх осіб, але й допомагає захистити конфіденційність користувачів, оскільки порушення конфіденційності користувачів можуть призвести до юридичних проблем [15].

Виходячи з кількості елементів ідентифікації або автентифікації, наданих користувачем, процес автентифікації можна розділити на такі рівні:

– Однофакторна автентифікація

– Двофакторна автентифікація

– Багатофакторна автентифікація

Автентифікація допомагає організаціям захищати безпеку своєї мережі, дозволяючи лише автентифікованим користувачам (або процесам) доступ до захищених ресурсів, таких як комп'ютерні системи, мережі, бази даних, веб-

сайти та інші веб-додатки або сервіси [15]. Автентифікація користувачів пропонує кілька переваг:

Запобігання крадіжкам: Основною метою систем контролю доступу є обмеження доступу для захисту персональних даних користувачів від крадіжки або несанкціонованого втручання. Багато веб-сайтів, які вимагають особистої інформації для надання послуг, особливо ті, які вимагають від користувачів надання інформації про кредитні картки або номери соціального страхування, зобов'язані згідно із законом або нормативними актами мати механізми контролю доступу.[15]

Рівень безпеки: Сучасні системи контролю постійно розвиваються разом із технологічним прогресом. Користувачі, які хочуть захистити свою інформаційну безпеку, мають більше можливостей, ніж просто чотиризначні PIN-коди та паролі. Наприклад, біометричні сканувальні замки тепер можна встановлювати біля входів до будинків та офісів.[16] Методи автентифікації

Кіберзлочинці постійно вдосконалюють свої методи атаки на системи. Як наслідок, команди безпеки стикаються з численними та постійно мінливими проблемами автентифікації. Як наслідок, підприємства починають впроваджувати більш складні рішення безпеки, що включають автентифікацію.[16]

Деякі з найпоширеніших методів автентифікації, що використовуються для захисту сучасних систем, включають:

Автентифікація за паролем: Найпоширенішим методом автентифікації є ім'я користувача та пароль. Комбінації літер, цифр та спеціальних символів можуть створювати надійні паролі, але їх все одно можна зламати або вкрасти.

Двофакторна автентифікація (2FA): 2FA вимагає від користувачів автентифікації двома або більше різними способами. Коди підтвердження, тести кодів підтвердження або інші додаткові фактори, що генеруються смартфоном користувача, можуть забезпечити додатковий захист на додаток до імен користувачів та паролів. Однак, викраденого телефону або ноутбука може бути достатньо для обходу таких заходів безпеки. Біометрична

багатофакторна автентифікація (MFA): Біометрична автентифікація спирається на унікальні біометричні характеристики людини та наразі є найбезпечнішим методом перевірки особи. За допомогою технології біометричної MFA авторизовані характеристики, що зберігаються в базі даних, можна швидко порівняти з біометричними характеристиками. При встановленні в системах контролю доступу біометрична автентифікація може бути використана для контролю дозволів на фізичний доступ. [16].

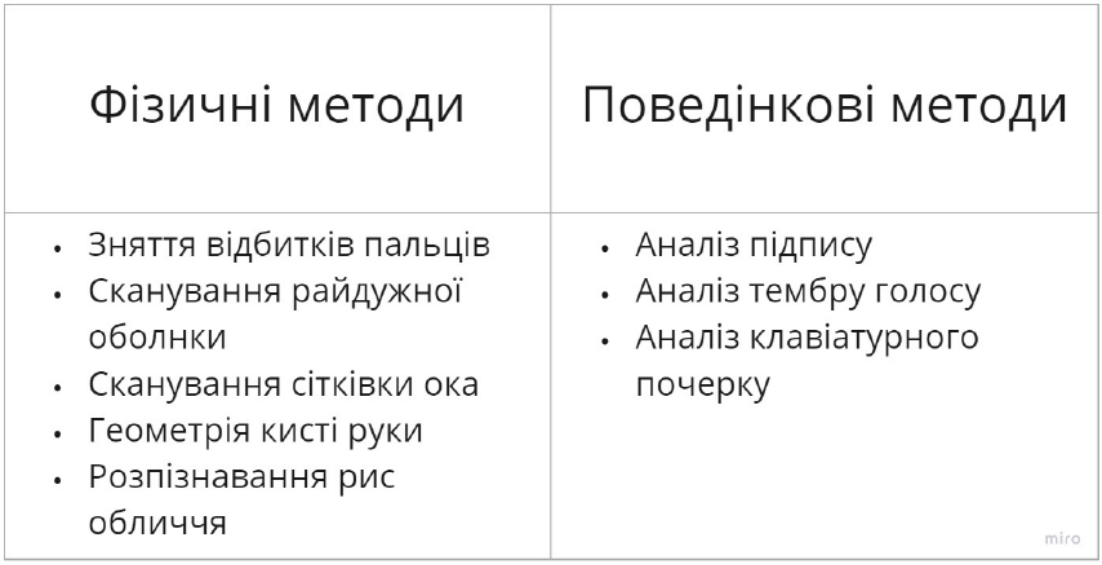


Рис 2.3 Приклади методів біометрії

Авторизація – це технологія безпеки, яка використовується для визначення дозволів користувача на виконання певних завдань у системі. Процес авторизації визначає дозволи на основі ролей, які користувач може мати в системі після автентифікації. [17] Важливо зазначити, що авторизацію неможливо здійснити без ідентифікації та автентифікації. Тому що, якщо всі входять, використовуючи один і той самий обліковий запис, їм буде надано або заборонено доступ до ресурсів. Якщо всі використовують один і той самий обліковий запис, ви не зможете розрізнити користувачів. Однак, після того, як ви ідентифікуєте та автентифікуєте користувачів за допомогою певних облікових даних, ви можете надати їм доступ до певних ресурсів на основі їхніх ролей або рівнів доступу. Авторизація визначає, що користувачі можуть

робити та бачити у вашому приміщенні, мережі чи системі. Отже, які переваги авторизації для вас? – Забезпечення того, щоб користувачі не могли отримати доступ до облікових записів інших людей

– Запобігання доступу відвідувачів та співробітників до захищених зон

– Забезпечення того, щоб безкоштовні облікові записи не могли використовувати всі функції

– Забезпечення того, щоб внутрішні облікові записи мали доступ лише до необхідної їм інформації

Методи авторизації:

Ключі інтерфейсу прикладного програмування (API): Щоб використовувати більшість API, спочатку потрібно зареєструватися, щоб отримати ключ API. Ключ API — це довгий рядок, який зазвичай міститься в URL-адресі або заголовку запиту, і який в основному використовується для ідентифікації особи, яка здійснює виклик API (API використовує автентифікацію). Ключі API можуть бути пов'язані з певною програмою, для якої зареєструвався користувач.[18]

Базова автентифікація: Базова автентифікація — це ще один метод авторизації, який вимагає від відправника ввести ім'я користувача та пароль у заголовок запиту. Base64 — це техніка кодування, яка перетворює ім'я користувача та пароль у рядок із 64 символів для забезпечення безпечної передачі.

HMAC: HMAC розшифровується як Hash-Based Message Authorization Code (код авторизації повідомлення на основі хешування), більш безпечний метод автентифікації, який зазвичай зустрічається у фінансових API. Як відправник, так і одержувач мають унікальний для них ключ. Відправник створює повідомлення, використовуючи системні властивості, такі як позначка часу запиту та ідентифікатор облікового запису. Ключ використовується для

шифрування повідомлення, яке потім шифрується за допомогою безпечного алгоритму хешування.[19]

Коли сервер API отримує запит, він використовує ті самі системні властивості та генерує той самий рядок, використовуючи ключ та безпечний алгоритм хешування (SHA). Якщо рядок відповідає підпису в заголовку запиту, запит приймається. Якщо воно не збігається, запит відхиляється. 2.3.2 Реєстрація та аудит

Реєстрація стосується збору та запису інформації про події, що відбуваються в інформаційній системі підприємства. Кожна служба має свій власний набір подій, але ці події загалом можна розділити на зовнішні та внутрішні. Проблеми внутрішньої безпеки можна розділити на три типи: проблеми безпеки, спричинені поведінкою інших сервісів, проблеми безпеки, спричинені власною поведінкою сервісу, та проблеми безпеки, спричинені поведінкою користувачів та адміністраторів [20].

Аудит включає аналіз накопиченої інформації та може виконуватися оперативно, майже в режимі реального часу або періодично.

Впровадження журналювання та аудиту спрямоване на досягнення таких цілей:

- Забезпечення підзвітності користувачів та адміністраторів;
- Забезпечення можливості реконструкції послідовностей подій;
- Виявлення спроб порушення інформаційної безпеки;
- Надання інформації для виявлення та аналізу проблем.

Забезпечення підзвітності є, перш за все, стримуючим фактором. Якщо користувачі та адміністратори знають, що всі їхні дії реєструються, вони можуть уникнути несанкціонованих дій. Якщо є підстави підозрювати користувача в нечесній поведінці, його дії можна реєструвати дуже детально, навіть до кожного натискання клавіші. Це дозволяє не лише розслідувати порушення безпеки, але й скасовувати помилкові зміни. Таким чином, забезпечується цілісність інформації [20].

Реконструкція послідовностей подій може допомогти виявити слабкі місця в захисті послуг, знайти порушників, оцінити ступінь пошкодження та відновити нормальну роботу.

Виявлення та аналіз проблем допомагають покращити параметри безпеки, такі як доступність. Після виявлення вузького місця можна спробувати переналаштувати або налаштувати систему, виміряти продуктивність тощо [20].

### 2.3.3 Криптографія

Криптографія забезпечує безпечний зв'язок у присутності зловмисної третьої сторони (так званого зловмисника). Шифрування використовує алгоритм і ключ для перетворення вхідних даних (тобто відкритого тексту) у зашифрований вихід (тобто шифротекст). За певного алгоритму той самий відкритий текст завжди буде перетворено на той самий шифротекст, якщо використовується той самий ключ. Алгоритм вважається безпечним, якщо зловмисник не може визначити жодної властивості відкритого тексту або ключа з шифротексту. Враховуючи велику кількість комбінацій відкритого тексту/шифротексту, що використовуються для створення ключа, зловмисник не повинен мати змоги визначити жодної інформації про ключ [21]. У чому різниця між симетричною та асиметричною криптографією?

У симетричній криптографії шифрування та дешифрування використовують один і той самий ключ. Відправник і одержувач повинні мати спільний ключ, відомий обом сторонам заздалегідь. Розподіл ключів є складною проблемою, саме тому була розроблена асиметрична криптографія.

В асиметричній криптографії шифрування та дешифрування використовують два різні ключі. Кожен користувач в асиметричній криптосистемі має відкритий ключ і закритий ключ. Закритий ключ завжди зберігається в секреті, тоді як відкритий ключ може вільно поширюватися [21]. Дані, зашифровані відкритим ключем, можна розшифрувати лише за допомогою відповідного закритого ключа. Отже, щоб надіслати повідомлення

Джону, його потрібно зашифрувати за допомогою відкритого ключа Джона. Тільки Джон може розшифрувати повідомлення, оскільки тільки Джон має свій закритий ключ. Будь-які дані, зашифровані закритим ключем, можна розшифрувати лише за допомогою відповідного відкритого ключа. Аналогічно, Джейн може цифровим підписом підписати повідомлення, використовуючи свій закритий ключ, і будь-хто, хто має відкритий ключ Джейн, може розшифрувати підписане повідомлення та перевірити, чи дійсно повідомлення було надіслано Джейн. [21] Симетричне шифрування, як правило, дуже швидке та добре підходить для шифрування великих обсягів даних, таких як цілі розділи диска або бази даних. Асиметричне шифрування набагато повільніше та може шифрувати лише блоки даних, менші за розмір ключа (зазвичай 2048 біт або менше). Тому асиметричне шифрування часто використовується для шифрування симетричних ключів шифрування, а потім використання цих ключів для шифрування більших блоків даних. Для цифрових підписів асиметричне шифрування часто використовується для шифрування хешу повідомлення, а не всього повідомлення. [22] Криптографічні системи забезпечують управління ключами шифрування, включаючи генерацію ключів, обмін, зберігання, використання, скасування та заміну. Які проблеми вирішує криптографія? Безпечна система повинна забезпечувати численні гарантії, такі як конфіденційність, цілісність та доступність даних, а також автентичність та невідмовність відмов. Правильне використання криптографії допомагає забезпечити ці запобіжні заходи. Криптографія може забезпечити конфіденційність та цілісність даних під час передачі та даних у стані спокою. Вона також може перевірити особу відправника та одержувача та запобігти атакам типу «відмова в обслуговуванні».

Програмні системи зазвичай мають кілька кінцевих точок, зазвичай кілька клієнтів та один або кілька серверів. Ці клієнт-серверні зв'язки відбуваються в ненадійних мережах. Зв'язок може відбуватися у відкритих

загальнодоступних мережах (таких як Інтернет) або в приватних мережах, які можуть бути скомпрометовані зовнішніми зловмисниками або порушниками.

Він може захищати зв'язок, що передається через ненадійні мережі. Зловмисники можуть запускати два основні типи атак на мережу. Пасивні атаки стосуються зловмисників, які прослуховують сегменти мережі та намагаються зчитати конфіденційну інформацію під час передачі. Пасивні атаки можуть бути онлайн (зловмисники зчитують трафік у режимі реального часу) або офлайн (зловмисники захоплюють трафік у режимі реального часу та переглядають його пізніше, що може зайняти деякий час для розшифрування). Активні атаки стосуються зловмисників, які видають себе за клієнтів або сервери, перехоплюють зв'язок під час передачі та переглядають та/або змінюють (або видаляють) контент перед його пересиланням до цільового місця. [23] Захист конфіденційності та цілісності, що забезпечується протоколами шифрування, такими як SSL/TLS, може запобігти прослуховуванню та підробці зв'язку. Автентифікація гарантує, що користувачі дійсно спілкуються із системою належним чином.

### 2.3.4 Системи виявлення вторгнень

Системи виявлення вторгнень (IDS) контролюють мережевий трафік, виявляють аномальну або підозрілу активність та надсилають сповіщення адміністраторам. Виявлення аномальної активності та повідомлення мережевих адміністраторів є їхньою основною функцією; Однак деякі програми систем виявлення вторгнень (IDS) також можуть вживати заходів на основі правил, коли виявляється шкідлива активність, наприклад, блокувати певний вхідний трафік. [24]

Типи систем виявлення вторгнень

Системи виявлення вторгнень загалом класифікуються на дві категорії (які будуть детально розглянуті далі в цьому посібнику):

- Системи виявлення вторгнень на базі хоста (HIDS) – ці системи досліджують події на комп’ютерах у мережі, а не трафік, що проходить через систему.

- Мережеві системи виявлення вторгнень (NIDS) – ці системи досліджують трафік у мережі.

Програмне забезпечення та системи виявлення вторгнень у мережі зараз є важливими для безпеки мережі. На щастя, ці системи дуже прості у використанні, і більшість найкращих доступних IDS є безкоштовними. У цьому огляді ви дізнаєтеся про десять найкращих систем виявлення вторгнень, які ви можете встановити одразу, щоб захистити свою мережу від атак. Ми розглянемо інструменти, доступні для Windows, Linux та Mac. Системи виявлення вторгнень на основі хоста (HIDS), також відомі як системи виявлення вторгнень на основі хоста або IDS на основі хоста, перевіряють події на комп’ютерах у мережі, а не трафік, що проходить через систему. Цей тип системи виявлення вторгнень, який часто називають просто HIDS, працює переважно шляхом перевірки даних у файлах адміністратора на захищеному комп’ютері. Ці файли включають файли журналів та файли конфігурації. [25] HIDS створить резервну копію ваших файлів конфігурації, щоб ви могли відновити свої налаштування, якщо шкідливі віруси послаблять безпеку вашої системи, змінивши налаштування комп’ютера. Ще одним важливим фактором, від якого слід захищатися, є root-доступ на Unix-подібних платформах або зміни в реєстрі на системах Windows. Системи виявлення вторгнень хоста (HIDS) не можуть запобігти цим змінам, але повинні мати можливість повідомляти вас про будь-який такий доступ.

Програмне забезпечення має бути встановлено на кожному хості, який контролюється HIDS. Ви можете налаштувати HIDS для моніторингу лише одного комп'ютера. Однак більш поширеною практикою є встановлення HIDS на кожному пристрої в мережі. Це тому, що ви не хочете пропустити жодних змін конфігурації обладнання. Звичайно, якщо у вашій мережі є кілька хостів HIDS, вам не потрібно входити на кожен хост для отримання зворотного

зв'язку. Тому розподілена система HIDS повинна містити централізований модуль управління. Шукайте системи, які можуть шифрувати зв'язок між агентами хоста та центральним монітором.

Системи виявлення вторгнень мережі (NIDS), також відомі як системи виявлення вторгнень мережі або мережеві IDS, використовуються для перевірки мережевого трафіку. Тому типова NIDS повинна містити аналізатор пакетів для збору мережевого трафіку для аналізу.

Механізм аналізу системи виявлення вторгнень мережі (NIDS) зазвичай базується на правилах і може бути змінений шляхом додавання користувацьких правил. Багато постачальників систем NIDS або спільнот користувачів пропонують правила, які можна імпортувати безпосередньо у вашу систему. Щойно ви ознайомитеся з синтаксисом правил обраної вами NIDS, ви зможете створювати власні правила. [26]

Повертаючись до збору трафіку, ви точно не хочете експортувати весь трафік у файли або обробляти всі дані через панель інструментів, оскільки ви просто не можете проаналізувати їх усі. Тому правила, що керують аналізом NIDS, також вибірково збиратимуть дані. Наприклад, якщо у вас є правило, спрямоване на певний тип підозрілого HTTP-трафіку, то ваш NIDS повинен фіксувати та зберігати лише HTTP-пакети, які мають ці характеристики.

Зазвичай NIDS встановлюється на спеціалізованому обладнанні. Високоякісні платні рішення корпоративного рівня часто пропонуються як частина попередньо встановленого мережевого пакету програмного забезпечення. Однак вам не потрібно витрачати багато грошей на спеціалізоване обладнання. Система виявлення вторгнень у мережу (NIDS) потребує сенсорного модуля для збору мережевого трафіку, тому ви можете завантажити його в локальний мережевий аналізатор або використовувати спеціалізований комп'ютер для виконання цього завдання. Однак переконайтеся, що обране вами обладнання має достатню тактову частоту, щоб уникнути уповільнення вашої мережі. Методи виявлення: системи виявлення вторгнень на основі сигнатур або аномалій

Незалежно від того, чи потрібна вам система виявлення вторгнень на основі хоста, чи мережі, всі системи виявлення вторгнень використовують два режими роботи — деякі можуть використовувати лише один, але більшість використовують обидва.

- Система виявлення вторгнень на основі сигнатур
- Система виявлення вторгнень на основі аномалій
- Система виявлення вторгнень на основі сигнатур

Методи на основі сигнатур перевіряють контрольні суми та виконують автентифікацію повідомлень. Методи виявлення на основі сигнатур можуть використовуватися в системах виявлення мережевих вторгнень (NIDS) та системах виявлення вторгнень хоста (HIDS). HIDS перевіряє журнали та файли конфігурації на наявність будь-яких неочікуваних перезаписів, тоді як NIDS перевіряє контрольні суми в захоплених пакетах та цілісність систем автентифікації повідомлень (таких як SHA1).

NIDS може містити базу даних, що зберігає сигнатури, що переносяться відомими шкідливими пакетами. На щастя, хакери не сидять перед комп'ютером, шалено друкуючи, щоб зламати паролі або отримати root-доступ. Натомість вони використовують автоматизовані програми, що надаються відомими хакерськими інструментами. Ці інструменти, як правило, генерують однакові сигнатури трафіку щоразу, оскільки комп'ютерна програма повторює одні й ті ж інструкції знову і знову, а не вводить випадкові варіації. [27]

Системи виявлення вторгнень на основі аномалій (IDS)

Виявлення на основі аномалій спрямоване на пошук неочікуваних або незвичайних моделей поведінки. Таке виявлення також може бути досягнуто за допомогою систем виявлення вторгнень на основі хоста або мережі. Для HIDS аномалії можуть проявлятися як повторювані невдалі спроби входу або

незвичайна активність на портах пристрою, що може свідчити про сканування портів. Для систем виявлення мережевих вторгнень (NIDS) методи виявлення аномалій вимагають встановлення базової поведінкової лінії для створення стандартного сценарію та порівняння з нею поточних шаблонів трафіку. Система встановлює прийнятний діапазон для шаблонів трафіку та запускає сповіщення про аномалію, коли поточний трафік у реальному часі перевищує цей діапазон.

Вибір підходу до системи виявлення вторгнень (IDS)

Розширені NIDS можуть створювати стандартні журнали поведінки та коригувати їхні межі з часом. Як правило, використання програмного забезпечення Системи виявлення вторгнень хоста (HIDS) для аналізу сигнатур та аналізу аномалій є зручнішим, ніж NIDS.

Методи на основі сигнатур швидші, ніж виявлення аномалій. Повністю комплексний механізм виявлення аномалій вимагає штучного інтелекту, розробка якого може бути дуже дорогою. Однак методи на основі сигнатур спрощуються до порівняння числових значень. Фактично, для HIDS зіставлення шаблонів з версіями файлів може бути дуже простим завданням.

Користувачі можуть виконувати цю операцію самостійно, використовуючи інструменти командного рядка з регулярними виразами. Тому вартість їх розробки низька, і вони, ймовірно, будуть застосовані до безкоштовних систем виявлення вторгнень [28].

Комплексна система виявлення вторгнень вимагає методів виявлення як на основі сигнатур, так і на основі аномалій.

## 2.4 Висновки по другому розділу

1. Пояснюється сутність та основні концепції запобігання несанкціонованому розголошенню інформації в галузі захисту інформації підприємства.

2. Обговорюються заходи захисту, що використовуються на підприємствах.

3. Вводиться склад та опис методів розпізнавання та автентифікації ідентифікації локальної мережі підприємства, ведення журналу та аудиту, захисту шифруванням та систем виявлення вторгнень.

# РОЗДІЛ 3
# ДОСЛІДЖЕННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ ПРОГРАМНОГО ЗАХИСТУ ПІДПРИЄСМТВА ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ПЕРСНОЛЬНИХ ДАНИХ В ЛОКАЛЬНІЙ МЕРЕЖІ

## 3.1 Склад інформації, що підлягає захисту

Захищені інформаційні ресурси в інфраструктурі ТОВ «СХІД» такі:

1. Цільова інформація: Комерційна таємниця ТОВ «СХІД»; персональні дані співробітників ТОВ «СХІД» та персональні дані іншого персоналу, який має доступ до ТОВ «СХІД» у процесі своєї роботи.

2. Технічна інформація: Дані конфігурації та інша інформація про технології, програмне та апаратне забезпечення, що використовуються для збору, зберігання, обробки, передачі та захисту інформації; службова інформація про засоби безпеки (ідентифікатори, паролі, таблиці обмежень доступу, ключі шифрування, інформація журналу аудиту безпеки тощо).

3. Програмне забезпечення: Програмні інформаційні ресурси інформаційної інфраструктури ТОВ «СХІД», включаючи програмне забезпечення загального та спеціалізованого призначення, резервні копії програмного забезпечення та програмне забезпечення засобів захисту інформації.

Інфраструктура ТОВ «СХІД» включає такі інформаційні ресурси:

Інформація, що стосується комерційної таємниці:

* Договори з постачальниками та покупцями;
* Трудові договори;
* Особисті справи співробітників;
* Особисті картки співробітників;
* Інформація на веб-сайті компанії та в брошурах;
* Установчі документи та організаційні документи;

### 3.2 Мережеве та програмне забезпечення підприємства

Локальна комп'ютерна мережа ТОВ «СХІД» побудована на стандартному мережевому рішенні. Локальна мережа ТОВ «ТОР» включає:

* Серверне обладнання, розташоване в незалежних стійках (шафах);

* Автоматизовані робочі місця користувачів;

* Комутаційне обладнання загального призначення та структуровану кабельну систему.

Обмін даними ТОВ «СХІД» з податковими органами, пенсійними фондами та ощадними банками здійснюється через зовнішні мережі.

ТОВ «схід» використовує сертифіковане, ліцензоване та вільно розповсюджуване програмне забезпечення (Таблиця 3.1).

Таблица 3.1

Сертифіковане ПЗ

| **№ п/п** | **Найменування продукту** | **Кількість** | **Термін дії** |
|---|---|---|---|
| 1 | Microsoft Windows 10 Professional | 20 | Бестроково |
| 2 | Microsoft Office 2016 | 20 | 1 рік |
| 3 | Microsoft Windows Server 2016 R2 EE | 3 | Бестроково |
| 4 | Правова база даних "LIGA 360" | 2 | Бестроково |
| 5 | Інформаційна система ALMEXOFT | 4 | Бестроково |
| 4 | 1С-Бухгалтерія 8 | 2 | Бестроково |

Тому в інформаційній інфраструктурі ТОВ «СХІД» було впроваджено багатокористувацьку модель обробки інформації з розподілом контролю доступу. Ця модель регулюється чинним законодавством України, документацією ТОВ «СХІД» та виконується відповідно до опису робіт.

## 3.3 Аналіз уразливості підприємства

### 3.3.1 Можливі способи реалізації загроз НСД у ТОВ «СХІД»

Під час аналізу інформаційної безпеки підприємства «TOR» було виявлено такі потенційні загрози несанкціонованого доступу. У таблиці 3.2 перелічені загрози, з якими наразі стикається інфраструктура ТОВ «TOR», виявлені під час аналізу загроз несанкціонованого доступу.

Таблиця 3.2

Загрози

| № п/п | Загроза | Оцінка ймовірності | Оцінка тяжкості наслідків | Рекомендації | Рівень ризику |
|---|---|---|---|---|---|
| 1 | Крадіжка паролів | 4 | 7 | Інструкція користувача, облік паролів. | 28 |
| 2 | Крадіжки, модифікації, знищення інформації. | 6 | 10 | Налаштування систем захисту, політика безпеки. | 60 |
| 3 | Несанкціоноване відключення засобів захисту | 2 | 5 | Налаштування засобів захисту | 10 |
| 4 | Дії шкідливих програм (вірусів) | 6 | 7 | Антивірусне ПЗ | 42 |
| 5 | Недекларовані можливості ПЗ | 2 | 8 | Сертифікація | 16 |
| 6 | Установка ПЗ не пов'язаного з виконанням обов'язків | 7 | 7 | Налаштування засобів захисту. Політика безпеки. | 49 |
| 7 | Ненавмисна модифікація (знищення) інформації співробітниками | 2 | 5 | Налаштування політика безпекии. Іструкція користувача. | 10 |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Розголошення інформації,модифікація, знищення співробітником | 3 | 4 | Налаштування політика безпеки. Інструкція користувача. | 12 |
| 9 | Загрози віддаленого запуску додатків. | 5 | 8 | Міжмережевий екран, Антивірусне ПЗ | 40 |
| 10 | Перехоплення в межах контрольованої зони | 6 | 10 | Засоби криптографічної захисту | 60 |

Після аналізу матриці оцінки ризиків (рис. 3.1) ми виявили, що рівень ризику визначається формулою F*G. Тут F представляє значення оцінки ймовірності витоку, втрати або підробки інформації внаслідок конкретного ризику, яке варіюється від 1 (найнижча ймовірність) до 10 (найвища ймовірність); G представляє ступінь негативних наслідків, яких може зазнати підприємство у разі витоку, втрати або підробки інформації внаслідок конкретного ризику. Доповнюємо дані в таблиці 3.2, де ≥50 вказує на загрозу високого ризику, а ≥25 – на загрозу середнього ризику.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 10 | 20 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 |
| 9 | 9 | 18 | 27 | 36 | 45 | 54 | 63 | 72 | 81 | 90 |
| 8 | 8 | 16 | 24 | 32 | 40 | 48 | 56 | 64 | 72 | 80 |
| 7 | 7 | 14 | 21 | 28 | 35 | 42 | 49 | 56 | 63 | 70 |
| 6 | 6 | 12 | 18 | 24 | 30 | 36 | 42 | 48 | 54 | 60 |
| 5 | 5 | 10 | 15 | 20 | 25 | 30 | 35 | 40 | 45 | 50 |
| 4 | 4 | 8 | 12 | 16 | 20 | 24 | 28 | 32 | 36 | 40 |
| 3 | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 24 | 27 | 30 |
| 2 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

Рис 3.1 Матриця оцінки ризиків

В таблиці 3.2. виділимо по групам ризики, для подальшого використання.

Таблиця 3.3

Відношення ризиків по рівню

| **Описання** | **Рівень ризику** | **Кількість** | **Доля ризиків даного рівня** |
|---|---|---|---|
| Низький рівень | <= 25 | 4 | 40 % |
| Середній | <= 50 | 4 | 40% |
| Високий | <= 75 | 2 | 20% |
| Критичний | 100 | 0 | 0% |

Використовуючи дані з таблиць 3.2 та 3.3, ми побудуємо карту розподілу ризиків (рисунок 3.2) та матрицю ризиків для нашої компанії (рисунок 3.3).

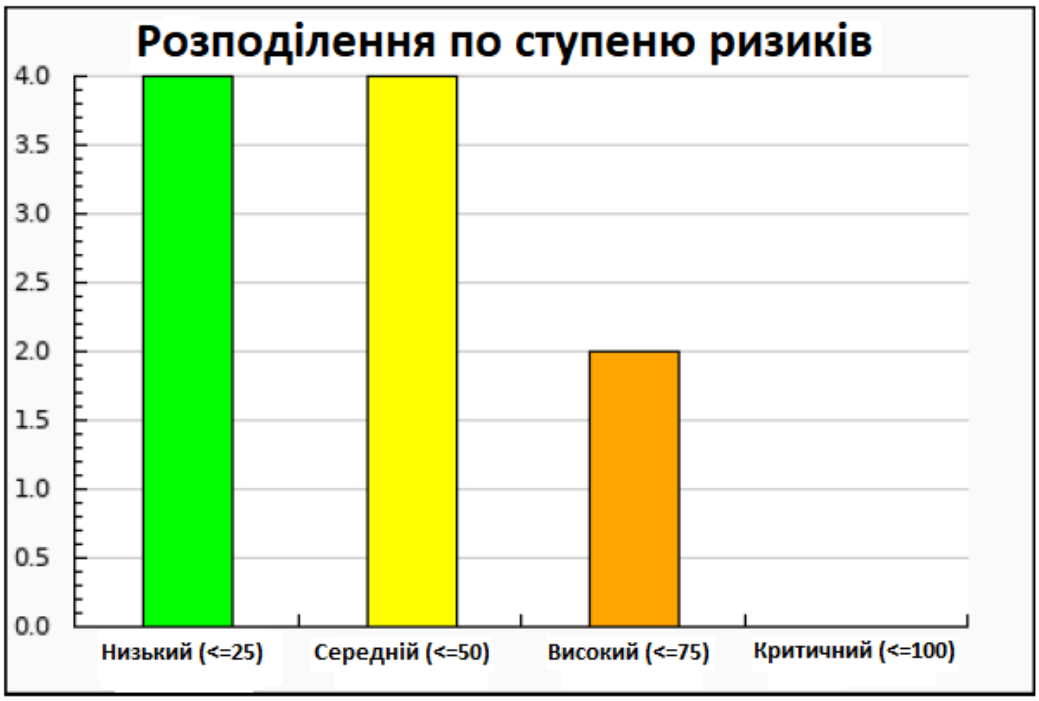


Рис. 3.2 Графік розподілення по ступеню ризику

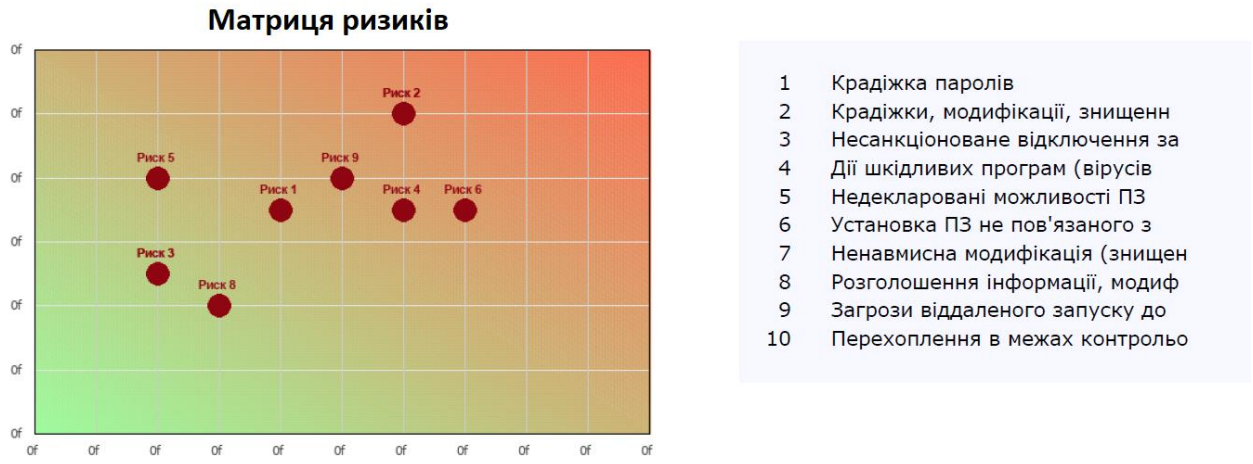


Рис. 3.3 Матриця ризиків

Проаналізувавши всі вхідні дані, ми дійшли висновку, що необхідно вдосконалити апаратно-програмну комбінацію засобів захисту комп'ютерної інформації в таких аспектах:

– Вибір методів шифрування захисту від витоку даних мережевої безпеки (NSD);

– Забезпечення безпеки периметра мережі та вибір брандмауера;

– Визначення засобів виявлення вторгнень та антивірусних засобів.

## 3.4 Рекомендації щодо програмно-апаратних засобів захисту інформації

### 3.4.1 Встановлення брандмауера

Під час аналізу захисту даних ТОВ «СХІД» однією з наших перших рекомендацій було встановлення брандмауера для забезпечення зовнішнього захисту від NSD.

Основне призначення брандмауера — захист комп'ютерної мережі або окремого вузла від зовнішніх атак. Брандмауери можуть фільтрувати вхідний та вихідний трафік через систему. Для корпоративних мереж ми обрали програмний брандмауер UserGate Proxy & Firewall 6.5, який є ефективною альтернативою економічно ефективним апаратним та програмним

брандмауерам та маршрутизаторам для захисту конфіденційної інформації та даних у захищених системах [29].

Цей продукт використовує комплексний підхід до забезпечення безпеки локальної мережі та використовує сучасні технології для боротьби з інтернет-загрозами, прагнучи організувати безпечну інтернет-взаємодію, статистику трафіку та захистити локальну мережу організації від зовнішніх загроз. Цей продукт є сертифікованим засобом захисту брандмауера, який забезпечує безпечний доступ до Інтернету для захищених систем.

Це комплексне рішення UserGate Proxy підтримує:

- Підключення VPN-серверів до VPN-клієнтів локальної мережі через протоколи PPTP та L2TP, а також подальшу публікацію мережевих ресурсів для віддаленого використання;

Визначення політик доступу до Інтернету та забезпечення комплексного контролю над використанням внутрішнього інтернет-трафіку за допомогою детальної статистики;

Створення правил для контролю швидкості передачі даних між локальною мережею та Інтернетом, а також встановлення обмежень часу використання трафіку та мережі для користувачів та груп користувачів;

Спрощення управління мережею;

Налаштування дозволів доступу співробітників до програмного забезпечення для обробки, шифрування та передачі даних;

Налаштування безпечного доступу до Інтернету для програмного забезпечення.

На рисунках 3.4–3.7 наведено приклади роботи UserGate Proxy та брандмауерів.

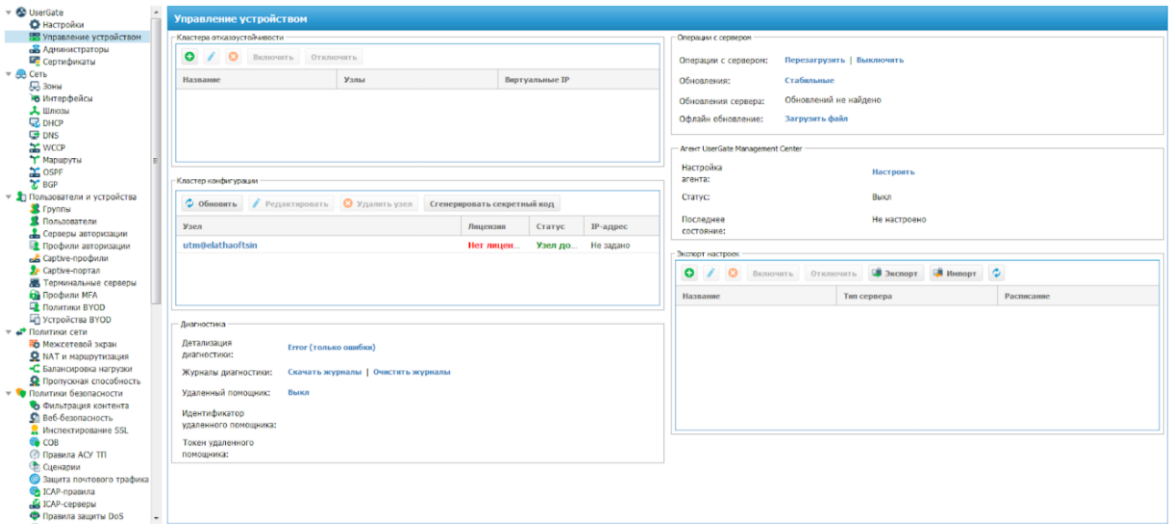


Рис. 3.4 Управління пристроями

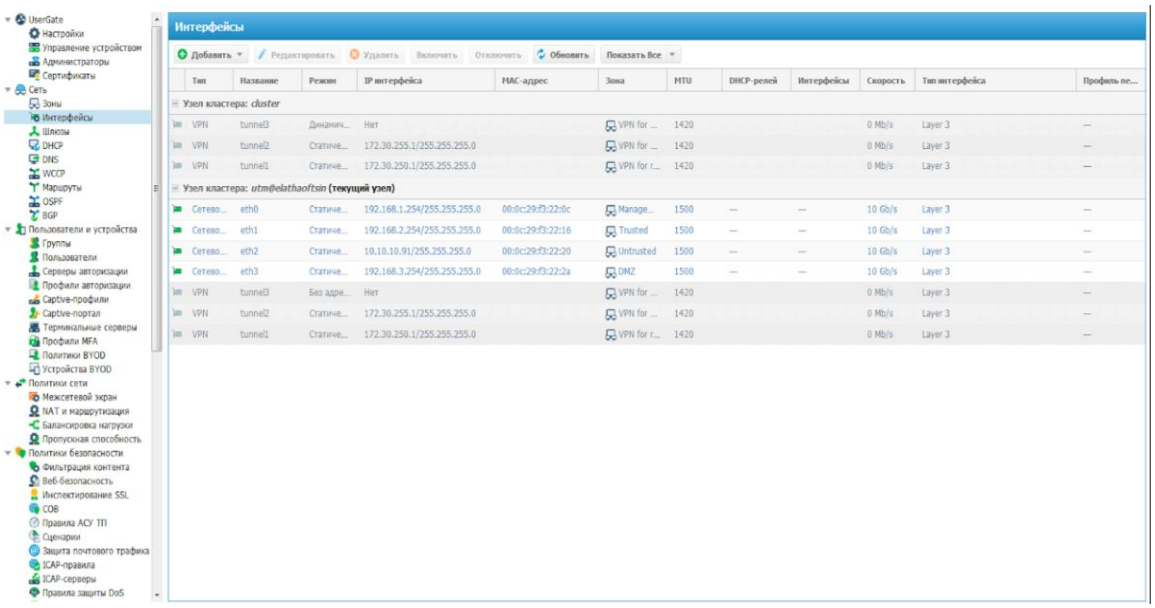


Рис. 3.5 Інтерфейси підключення

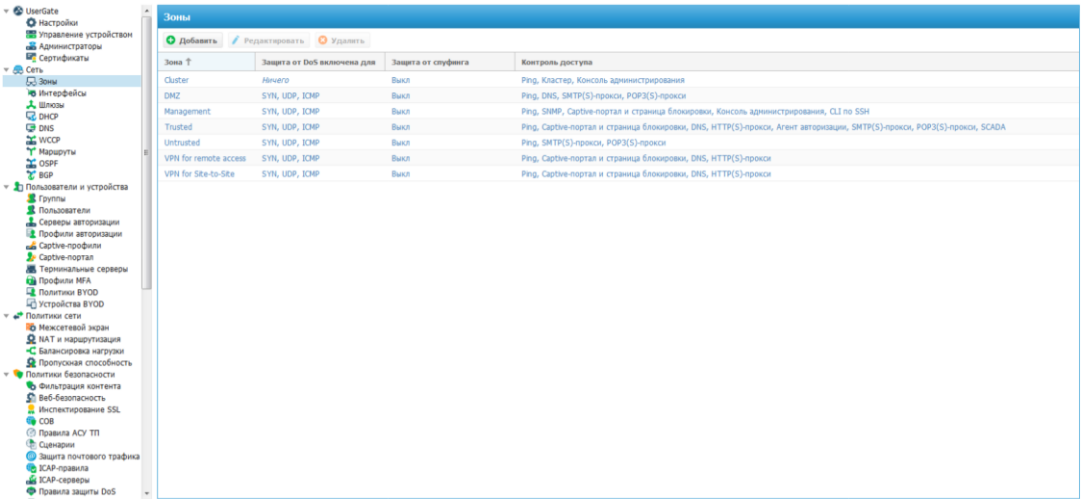


Рис 3.6 Налаштування зон мережі

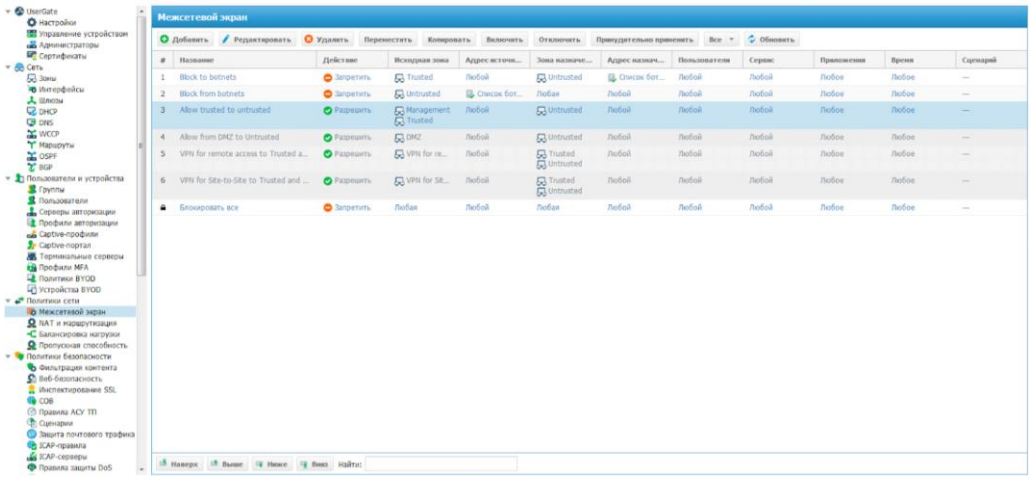


Рис. 3.7 Налаштування міжмережевих екранів

3.4.2 Встановлення постачальників шифрування в системах захисту даних

Заходи захисту шифрування, що використовуються для запобігання НСР, повинні відповідати наступним криптографічним вимогам Національного стандарту ДСТУ:

– Національний стандарт ДСТУ 4145-2002 "Інформаційні технології. Захист інформації шифруванням. Цифрові підписи на основі еліптичних кривих. Генерація та перевірка [30]"

– Національний стандарт ДСТУ 7624:2014 "Інформаційні технології. Захист інформації шифруванням. Алгоритм симетричного перетворення блоків [31]"

– Національний стандарт ДСТУ 7564:2014 "Інформаційні технології. Захист інформації шифруванням. Хеш-функції [32]"

Особливої уваги заслуговує захід захисту шифрування інформації "ІІТ ЦСК-1", який:

– Використовується для генерації ключів шифрування та ключів електронного підпису для досягнення шифрування та захисту даних, забезпечення цілісності та автентичності інформації.

Забезпечує зберігання та обробку персональних даних, конфіденційної інформації, службової інформації, комерційної інформації тощо (за винятком інформації, що становить державну таємницю), а також гарантує юридичну обґрунтованість обміну такою інформацією та потоку електронних документів. Обмін електронною інформацією відбувається між державними органами, органами місцевого самоврядування, організаціями та громадянами (фізичними особами) та всередині них.

ІІТ ЦСК-1 ІЦЗІ застосовується не лише до програмного забезпечення ІІТ ЦСК-1, що виробляється ПрАТ «Інститут інформаційних технологій», але й може бути інтегрований у прикладне програмне забезпечення інших виробників та надаватися кінцевим користувачам. Його функції включають:

– Створення ключів електронного підпису відповідно до Наказу Міністерства юстиції України та Державної служби спеціального зв'язку України від 30 вересня 2020 року № 140/614 «Вимоги до технічних засобів, процедур створення, використання та експлуатації у складі інформаційно-телекомунікаційної системи при наданні кваліфікованих електронних довірчих послуг», який зареєстровано в Міністерстві юстиції України 22 жовтня 2020 року за реєстраційним номером 1093/35322[33];

– Виконання обробки хешування даних за алгоритмом ДСТУ 7564:2014 [32];

– Виконання шифрування даних та захисту від шпигунського програмного забезпечення за алгоритмом ДСТУ 28147-2009. Генерація випадкових та псевдовипадкових чисел, а також ключів шифрування сеансу [34];

– Використання протоколу SSL/TLS для автентифікації під час передачі даних та генерації ключів сеансу. Зберігання сертифікатів відкритих ключів безпосередньо в контейнері ключів;

– Підтримка різних пристроїв зберігання ключів (eToken, Shipka тощо).

Для виконання шифрування та перевірки цифрового підпису постачальник шифрування «ІІТ CSK-1» використовує відкритий ключ у сертифікаті одержувача зашифрованого документа або користувача, який отримує документ із цифровим підписом. Для розшифрування та створення цифрового підпису постачальник шифрування використовує закритий ключ (ключ, вказаний користувачем) користувача, який виконує ці операції. Наведена нижче діаграма ілюструє процес надсилання конфіденційного електронного листа Outlook (рис. 3.8).

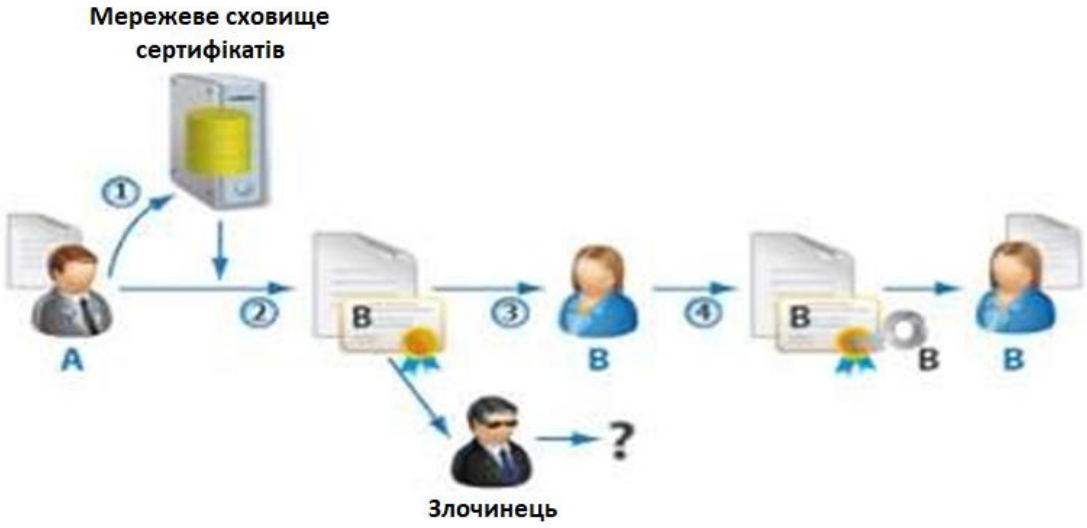


Рис. 3.8 Схема обміну захищеними документами

Користувачу А потрібно надіслати конфіденційний електронний лист Outlook користувачу В:

- Користувач А запитує сертифікат відкритого ключа з мережевого сховища та зіставляє його з контактом користувача В в Outlook.

- А шифрує документ за допомогою відкритого ключа в сертифікаті В.

- А надсилає зашифрований електронний лист користувачу В.

- Користувач В розшифровує документ за допомогою свого закритого ключа.

- Таким чином, користувач В отримує конфіденційний електронний лист від користувача А.

Якщо електронний лист перехопить зловмисник, він не зможе прочитати його вміст, оскільки у нього немає закритого ключа користувача В. Якщо користувач В не може розшифрувати електронний лист, отриманий від А, це означає, що електронний лист був підроблений третьою стороною або пошкоджений під час передачі. У цьому випадку користувач В може попросити користувача А повторно надіслати електронний лист.

Процес створення та перевірки цифрового підпису показано на рисунку 3.9.

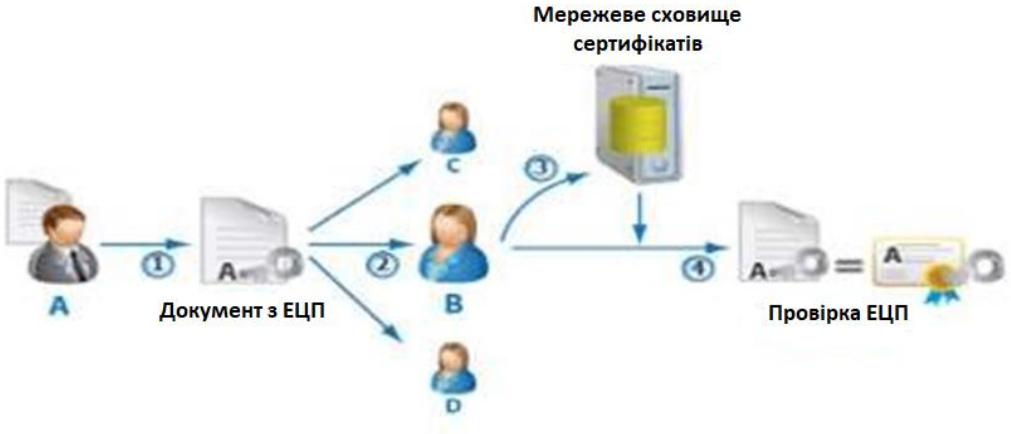


Рис. 3.9 Процес формування та перевірки підпису документа

Користувач А повинен автентифікувати документ (наприклад, електронний лист Outlook) за допомогою цифрового підпису, щоб запобігти

його зміні іншими користувачами та забезпечити, щоб кожен міг перевірити, що користувач А є автором документа;

– Користувач А підписує документ, використовуючи свій закритий ключ

– А надсилає цей документ усім відповідним сторонам (користувачам B, C та D) або робить його загальнодоступним.

– Користувач В запитує сертифікат для відкритого ключа А зі сховища сертифікатів.

– Перевіряє документ, використовуючи відкритий ключ А зі свого сертифіката.

SKZI «ІІТ CSK-1» призначений для комп'ютерів (настільних, портативних або мобільних) з такими рекомендованими конфігураціями: процесор архітектури x86 або x86-64; щонайменше 512 МБ пам'яті; щонайменше 100 МБ доступного місця на жорсткому диску.

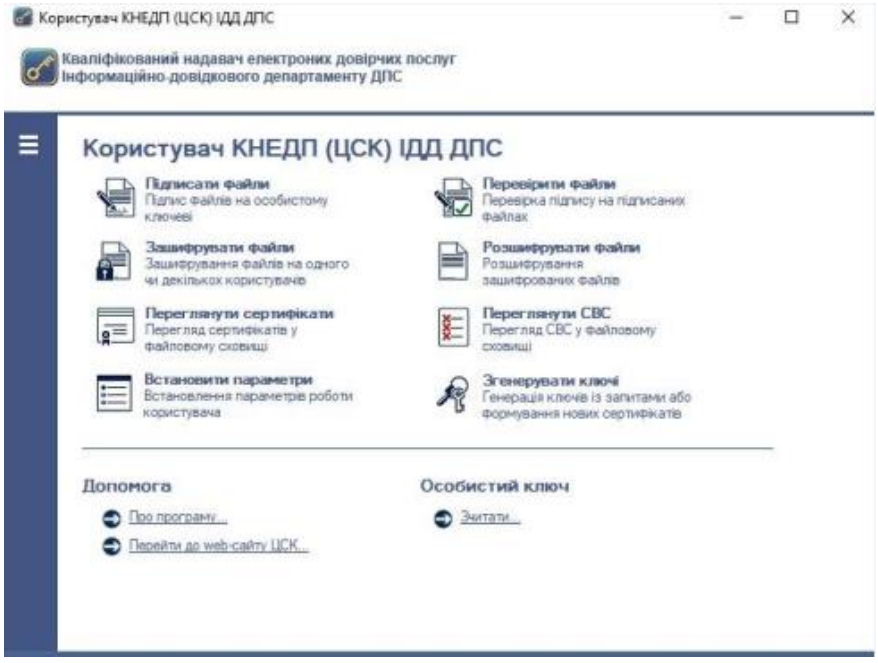


Рис. 3.10 Інтерфейс ІІТ ЦСК-1

### 3.4.3 Встановлення засобу виявлення вторгнень та антивірусу

ManageEngine EventLog Analyzer

ManageEngine є провідним виробником рішень для моніторингу та управління мережевою інфраструктурою IT. EventLog Analyzer є частиною портфоліо продуктів безпеки компанії. Це система виявлення вторгнень хоста (HIDS), орієнтована на керування та аналіз файлів журналів, що генеруються стандартними програмами та операційними системами. Цей інструмент можна встановити на системах Windows Server або Linux. Він може збирати дані не лише з цих операційних систем, але й із систем Mac OS, IBM AIX, HP UX та Solaris. Джерелами журналів для систем Windows є Windows Server, Windows Vista та пізніші версії, а також сервери Windows DHCP.

Основні характеристики:

– Керування та аналіз файлів журналів

– Аудит відповідності вимогам захисту даних

ManageEngine EventLog Analyzer фіксує, агрегує та зберігає повідомлення журналів з різних частин системи. Потім він шукає ці записи на наявність ознак злому або шкідливого програмного забезпечення. Пакет включає модуль звітності про відповідність.

На додаток до операційних систем, сервіс також може збирати та агрегувати журнали з баз даних Microsoft SQL Server та Oracle. Він також може пересилати сповіщення від кількох антивірусних систем, включаючи Microsoft Anti-malware, ESET, Sophos, Norton, FireEye, Malwarebytes, McAfee та Symantec. Він збирає журнали з веб-серверів, брандмауерів, гіпервізорів, маршрутизаторів, комутаторів та сканерів мережевих вразливостей.

EventLog Analyzer збирає повідомлення журналів та діє як сервер файлів журналів, організовуючи повідомлення у файли та каталоги за джерелом та датою. Екстрені сповіщення також пересилаються на панель керування EventLog Analyzer і можуть бути переслані як заявки до системи служби

підтримки для негайної технічної підтримки. Вбудований модуль аналізу загроз пакета визначає, які події можуть являти собою вразливості безпеки.

Сервіс включає автоматичний пошук у журналах та можливості кореляції подій, що дозволяє регулярно генерувати звіти про безпеку. Ці звіти включають формат моніторингу та аудиту привілейованих користувачів (PUMA) та різні формати, необхідні для демонстрації відповідності таким нормам, як PCI DSS, FISMA, ISO 27001, GLBA, HIPAA, SOX та GDPR.

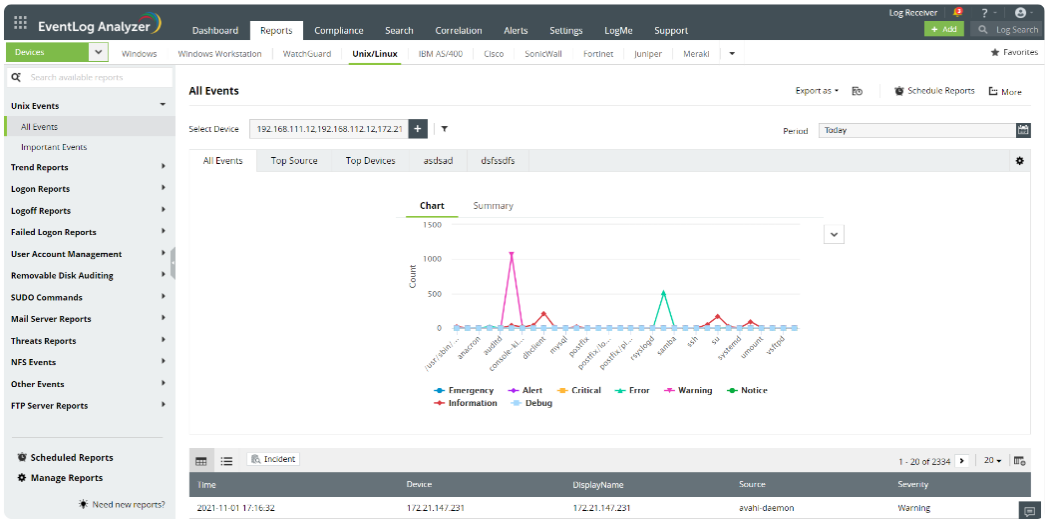


Рис. 3.11 Інтерфейс ManageEngine EventLog Analyzer

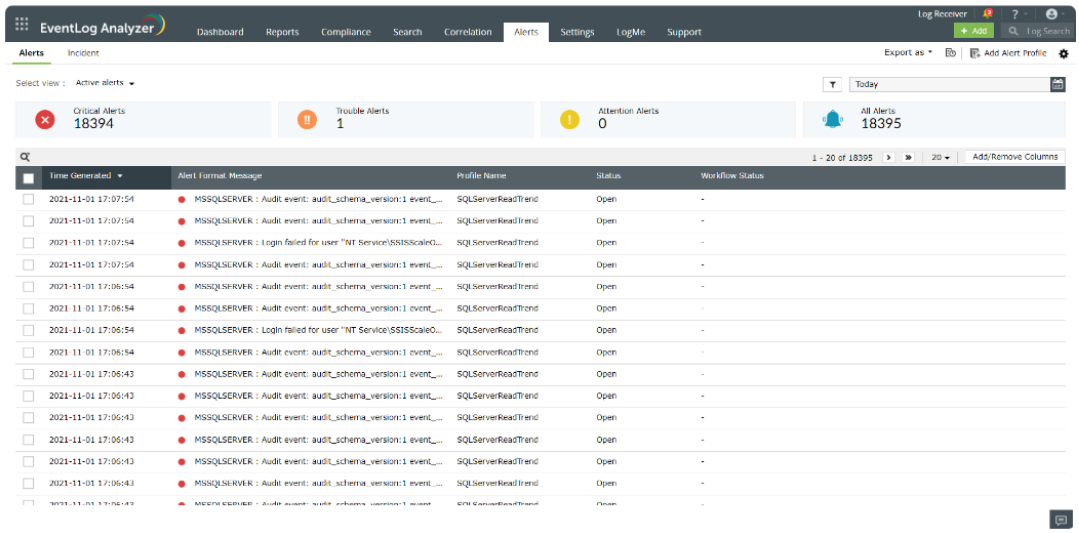


Рис. 3.12 Інтерфейс ManageEngine EventLog Analyzer

ESET Internet Security

Список функцій ESET Internet Security:

* **Антивірусне та антишпигунське програмне забезпечення;**

* **Брандмауер.** Запобігає несанкціонованому доступу до вашого комп’ютера та використанню ваших особистих даних. Антивірусне та антишпигунське програмне забезпечення:** Швидкий та ефективний сканер, який поєднує антивірусні та антишпигунські функції для виявлення та видалення шкідливих програм.

* **Перехоплювач експлойтів.** Блокує атаки, спеціально розроблені для обходу антивірусного програмного забезпечення, захищаючи веббраузери та програми для читання PDF-файлів від атак.

* **Сканування під час завантаження файлів;**

* **Керування пристроями.** Запобігає несанкціонованому копіюванню ваших даних. Дозволяє блокувати CD-ROM, DVD-ROM, USB-накопичувачі та дисководи, а також пристрої, підключені через Bluetooth.

* **Антиспам електронної пошти.**

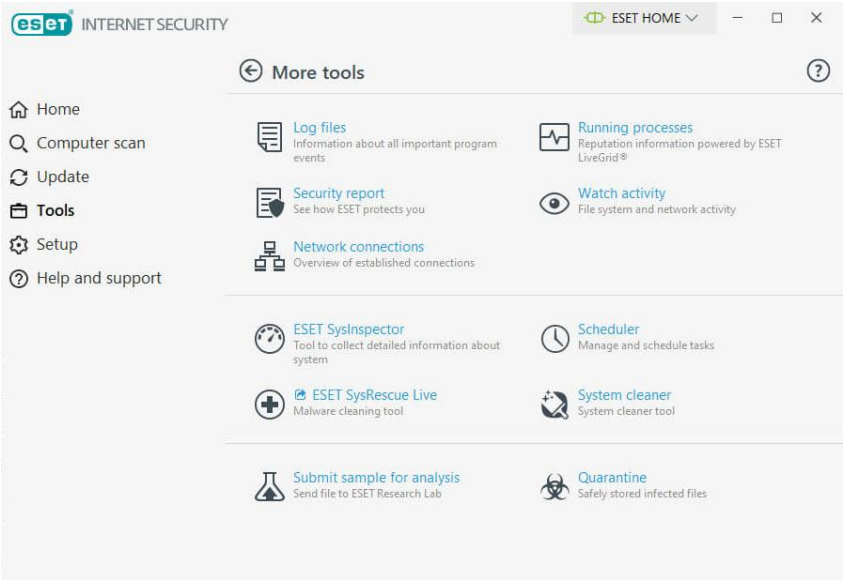


Рис. 3.13 Інтерфейс Eset Internet Security

Таблиця 3.4

Рекомендаційне ПЗ

| № | Загроза | Рекомендаційне ПЗ |
|---|---|---|
| 1 | Крадіжка паролів | UserGate Proxy |
| 2 | Крадіжки, модифікації, знищення інформації. | UserGate Proxy<br>«ІІТ ЦСК-1» |
| 3 | Несанкціоноване відключення засобів захисту | UserGate Proxy |
| 4 | Дії шкідливих програм (вірусів) | ManageEngine EventLog Analyzer |
| 5 | Недекларовані можливості ПЗ | Сетрифіковане ПЗ |
| 6 | Установка ПЗ не пов'язаного з виконанням обов'язків | Windows |
| 7 | Ненавмисна модифікація (знищення) інформації співробітниками | UserGate Proxy<br>«ІІТ ЦСК-1» |
| 8 | Розголошення інформації, модифікація, знищення співробітником | «ІІТ ЦСК-1» |
| 9 | Загрози віддаленого запуску додатків. | - UserGate Proxy<br>- ManageEngine EventLog Analyzer |
| 10 | Перехоплення в межах контрольованої зони | «ІІТ ЦСК-1» |

### 3.5 Аналіз ризиків після встановлення рекомендованого ПЗ.

Проведемо оцінку ймовірності і тяжкості наслідків, при умові виконання всіх рекомендації що до встановлення ПЗ для захисту інформації, і зберемо дані.

Таблиця 3.5

Загрози

| № п/п | Загроза | Оцінка ймовірності | Оцінка тяжкості наслідків | Рекомендації | Рівень ризику |
|---|---|---|---|---|---|
| 1 | Крадіжка паролів | 2 | 5 | Інструкція користувача, облік паролів. | 10 |
| 2 | Крадіжки, модифікації, знищення інформації. | 3 | 10 | Налаштування систем захисту, політика безпеки. | 30 |
| 3 | Несанкціоноване відключення засобів захисту | 1 | 5 | Налаштування засобів захисту | 5 |
| 4 | Дії шкідливих програм (вірусів) | 3 | 7 | Антивірусне ПЗ | 21 |
| 5 | Недекларовані можливості ПЗ | 2 | 8 | Сертифікація | 16 |
| 6 | Установка ПЗ не пов'язаного з виконанням обов'язків | 2 | 6 | Налаштування засобів захисту. Політика безпеки. | 12 |
| 7 | Ненавмисна модифікація (знищення) інформації співробітниками | 2 | 5 | Налаштування політика безпекии. Іструкція користувача. | 10 |
| 8 | Розголошення інформації,модифікація, знищення співробітником | 2 | 4 | Налаштування політика безпеки. Інструкція користувача. | 8 |
| 9 | Загрози віддаленого запуску додатків. | 2 | 8 | Міжмережевий екран, Антивірусне ПЗ | 16 |
| 10 | Перехоплення в межах контрольованої зони | 3 | 10 | Засоби криптографічної захисту | 30 |

По даним з таблиці 3.5. виділимов ризик по групам, і побудуємо графік розподілення(рис. 3.14) і матрицю ризиків(рис. 3.15).

Таблиця 3.6

Відношення ризиків по рівню

| **Описання** | **Рівень ризику** | **Кількість** | **Доля ризиків даного рівня** |
|---|---|---|---|
| Низький рівень | <= 25 | 8 | 80 % |
| Середній | <= 50 | 2 | 20% |
| Високий | <= 75 | 2 | 20% |
| Критичний | 100 | 0 | 0% |

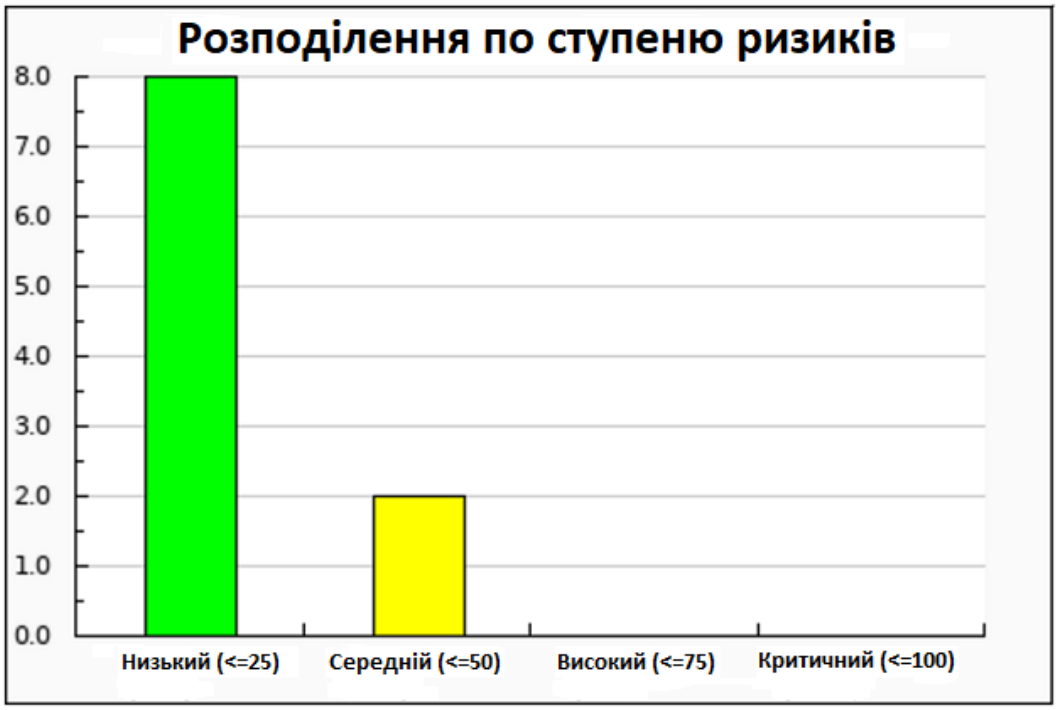


Рис. 3.14 Графік розподілення по ступеню ризику


Рис. 3.15 Матриця ризиків

Для більш наочної демонстрації результатів скористаємося наступною формулою для порівняння та аналізу ризиків до та після впровадження системи захисту інформації.

$$\left(\frac{\text{Н}}{x}\cdot 0.25\right)+\left(\frac{\text{С}}{x}\cdot 0.5\right)+\left(\frac{\text{В}}{x}\cdot 0.75\right)+\left(\frac{\text{К}}{x}\right)$$

Де:

Н – кількість ризиків низького рівня.

С – кількість ризиків середнього рівня

В – кількість ризиків високого рівня

К – кількість критичного низького рівня

х – загальна кількість ризиків.

Результатом є індекс від 0,25 до 1, де 0,25 означає найнижчу ймовірність витоку інформації через відомі ризики та їх вплив на підприємство, а 1 – найвищий ризик.

Перш ніж представити список рекомендованого програмного забезпечення, давайте розрахуємо цей індекс для підприємства.

$$\left(\frac{4}{10}\cdot 0.25\right)+\left(\frac{4}{10}\cdot 0.5\right)+\left(\frac{2}{10}\cdot 0.75\right)+\left(\frac{0}{10}\right)=(0.4\cdot 0.25)+(0.4\cdot 0.5)+(0.2\cdot 0.75)=0.45$$

Після введеня в роботу ПЗ захисту інформації.

$$\left(\frac{8}{10}\cdot 0.25\right)+\left(\frac{2}{10}\cdot 0.5\right)+\left(\frac{0}{10}\cdot 0.75\right)+\left(\frac{0}{10}\right)=(0.8\cdot 0.25)+(0.2\cdot 0.5)=0.3$$

На основі встановлення рекомендованого апаратного та програмного забезпечення (тобто:

- Брандмауер UserGate Proxy & Firewall 6.5
- Постачальник шифрування ІІТ CSK-1
- Засіб виявлення вторгнень ManageEngine EventLog Analyzer
- Антивірусне програмне забезпечення ESET Internet Security

Нам вдалося успішно знизити ймовірність втрати, витоку або несанкціонованого доступу до інформації з 0,45 до 0,3, що на 15 відсоткових пунктів, або на 33% менше, ніж початкове значення.

### 3.6 Висновки по третьому розділу

1. Було проаналізовано склад захищеної інформації в локальній комп'ютерній мережі та можливі канали витоку. Було оцінено серйозність цих загроз.

3. Було розглянуто та проаналізовано апаратні та програмні засоби захисту для запобігання несанкціонованому доступу.

4. Було розроблено перелік рекомендованих апаратних та програмних засобів для захисту персональних даних у локальній мережі підприємства від витоку, шахрайства або несанкціонованого доступу.

5. Було проаналізовано рівень захисту локальної мережі після впровадження рекомендованих програмних та апаратних засобів.

# ВИСНОВОК

Під час підготовки до кваліфікаційного огляду було виконано такі завдання:

- Розглянуто процес обробки персональних даних у локальній комп'ютерній мережі.

- Проаналізовано методи захисту персональних даних у локальній комп'ютерній мережі від несанкціонованого доступу.

- Надано практичні рекомендації щодо використання програмних додатків для захисту під час обробки персональних даних у локальній комп'ютерній мережі.

- Надано практичні рекомендації щодо використання програмних додатків для захисту під час обробки персональних даних у локальній комп'ютерній мережі.

1. У першій частині кваліфікаційного огляду було досліджено питання захисту персональних даних у локальній мережі від несанкціонованого крадіжки, розголошення або втручання. Було проаналізовано методи несанкціонованого доступу до інформації та основні канали витоку під час обробки інформації. Було визначено типи шкідливих програм, які можуть бути використані для несанкціонованого доступу до інформації.

2. У другій частині було проаналізовано систему захисту інформації та її заходи щодо запобігання несанкціонованому доступу. Було розглянуто методи ідентифікації та автентифікації, що використовуються для фізичного та програмного захисту даних у локальній мережі підприємства. У цій роботі представлено програмні методи виявлення мережевих вторгнень в інформаційні системи підприємства, а також функції ведення журналу та аудиту. Ці функції допомагають реконструювати послідовність подій вторгнення, ідентифікувати порушника, оцінити ступінь пошкодження та відновити нормальну роботу.

3. У третій частині аналізується інформація підприємства та перелічується інформація, яка потребує захисту, а також загрози, які можуть призвести до витоку або втрати даних. Крім того, оцінюються рівні ризику цих загроз.

На основі виявлених загроз у межах підприємства в цій статті розробляється рекомендований перелік програмних засобів для захисту персональних даних. Після впровадження цих рекомендацій у систему захисту в цій статті аналізується рівень захисту локальної мережі.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Council of Europe Convention on Access to Official Documents, Tromso, 2009 / / CETS № 205.

2. Charter of the United [Електронний ресурс]. — Режим доступу: http://www.un.orglen/documents/charter/.].

3. Sullivan, G. (2011). «The Bribery Act 2010 : Part One: an overview». Criminal Law Review. 2011 (2). ISSN 0011-135X. С. 46

5. Андреев В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є Основи кібербезпеки / За ред. проф. В.О. Хорошка. вид., доп. і перероб. — К. : Вид. ДУІКТ, 2009. — 292 с.

6. Максименко Ю.Є. Теоретико-правові засади забезпечення кібербезпеки України : дис.… канд. юрид. наук :12.00.01 / Ю.Є. Максименко. — К., 2007. — 186 с.

7. Марущак А.І. Кібербезпека як об’єкт дослідження правової науки / А.І. Марущак // Актуальні проблеми управління кібербезпекою держави : зб. матер. наук.- прак. конф., 17 березня 2010 року м. Київ. — К. : Наук. вид. відділ НА СБ України, 2010. — С. 36−41

8. Марущак А.І. Інформаційне право : Доступ до інформації : Навч. посіб. / А. І. Марущак. — К., 2007. — 280 с.

9. Марущак, А. І. Інформаційне право: регулювання інформаційної діяльності : Навчальний посібник. К. : Видавничий дім «Скіф», КНТ, 2008. — 344 с

10. Арістова, І.В. Державна інформаційна політика : організаційно-правові аспекти : Монографія / І.В. Арістова. —
Х. : Вид-во ун-ту внутр. справ, 2000. — 368 с.

11. Hells U., Karras A., Scherer K.R. Multichannel communication of emotion: synthetic signal production // Facets of
Emotion. Recent research / Ed. K.R.Scherer/ — Hillsdate,
N.J. — 1988. — P. 162

12. Sullivan, G. (2011). «The Bribery Act 2010 : Part One: an overview». Criminal Law Review. 2011 (2). ISSN 0011-135X. C. 46

13. Charter of the United [Електронний ресурс]. — Режим доступу: http://www.un.orglen/documents/charter/.].

14. Шутов, Р. Глиняний фундамент кібербезпеки — [Електронний ресурс] — Режим доступу: http://osvita.mediasapiens.ua/media_law/law/koli_sosud_napivporozhniy_scho _robiti_z_kontseptsieyu_informatsiynoi_bezpeki/.

15. Цимбалюк В.С. Сутність кібербезпеки в умовах входження України до глобальної кіберцивілізації / В. Цимбалюк // Науковий вісник академії ДПС України. —2007. — № 4. — С. 174–178.

16. Цимбалюк В.С. Інформаційне право (основи теорії і практики) / В.С. Цимбалюк. Монографія. — К. : «Освіта України», 2010. — 388 с.

17. What is Authorization? [Електронний ресурс] // auth0 bu Okta. – 2022. – Режим доступу до ресурсу: https://auth0.com/intro-to-iam/what-is-authorization.

18. API Reference [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://stripe.com/docs/api/errors.

19. Krawczyk H. HMAC: Keyed-Hashing for Message Authentication [Електронний ресурс] / H. Krawczyk, M. Bellare // IBM. – 1997. – Режим доступу до ресурсу: https://www.rfc-editor.org/rfc/rfc2104.

20. Лужецький В. А. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця: ВНТУ, 2009. – 268 с.

21. Аліпов Ілля Миколайович. Методи захисту інформації при її передаванні : Автореф. дис... канд. техн. наук: 05.13.08 / Харківський держ. технічний ун-т радіоелектроніки. - Х., 1997. - 22с

22. Богуш Володимир Михайлович, Мухачов Владислав Андрійович. Криптографічні застосування елементарної теорії чисел : Навч. посібник / Державний ун-т інформаційно-комунікаційних технологій. - К. : ДУІКТ, 2006. – 126 с.

23. Ємець Володимир, Мельник Анатолій, Попович Роман. Сучасна криптографія: Основні поняття . - Л. : БаК, 2003. - 144с. : рис., табл. - (Захист інформації в комп'ютерних та телекомунікаційних мережах). - Бібліогр.: с. 128.

24. Hung-JenLiao. Intrusion detection system: A comprehensive review / Hung-JenLiao, Kuang-YuanTunga. // Journal of Network and Computer Applications. – 2013. – №36. – С. 16–24.

25. Snort IDS and IPS Toolkit [Електронний ресурс]. – 2007. – Режим доступу до ресурсу: https://www.amazon.com/Snort-Toolkit-Beales-SourceSecurity/dp/1597490997.

26. Polymorphic Blending Attacks [Електронний ресурс]. – 2006. – Режим доступу до ресурсу: https://www.usenix.org/legacy/event/sec06/tech/full_papers/fogla/fogla.pdf.

27. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

28. Економічний ризик : методи оцінки та управління : навч. посіб. / за ред. Т. А. Васильєвої. Суми : ДВНЗ «УАБС НБУ», 2015. 208 с.

29. Traffic Inspector Next Generation [Електронний ресурс] // Smart-Soft. – 2014. – Режим доступу до ресурсу: https://www.evraas.com/upload/iblock/ead/eadf098bb265b5bce1e4ebd0db73c51b.pdf.

30. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння [Електронний ресурс]. – 2002. – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=68769.

31. ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Поправка [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page?id_doc=65314.

32. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування. З поправкою [Електронний ресурс]. – 2014. –

Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66229.

33. Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z2227-13#Text.

# ДОДАТКИ