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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захисту додатків від несанкціонованого доступу Positive Technologies Application Firewall»

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
_____ Руслан САД

Виконав: здобувач вищої освіти групи СЗДМ 61
Руслан САД

Керівник: ДРОБИК Олександр
к.т.н., професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2025

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

Кафедра Технічних систем кіберзахисту
Ступінь вищої освіти магістр
Спеціальність 125-Кібербезпека та захист інформації
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСК
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Саду Руслану Миколайовичу

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система захисту додатків від несанкціонованого доступу Positive Technologies Application Firewall»

керівник кваліфікаційної роботи ДРОБИК Олександр, к.т.н., професор

затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 20.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи: об'єкт інформаційної діяльності, мережеві канали витоку інформації, вимоги до захисту конфіденційної інформації, програмно-апаратні комплекси захисту інфомації в локальних комп'ютерних мережах.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Провести огляд процесу обробки конфіденційних даних в локальних комп'ютерних мережах, каналів та способів несанкціонованого доступу до них;
4.2. Проаналізувати методи захисту інформації в локальній комп'ютерній мережі від несанкціонованого доступу до конфіденційних даних;
4.3. Розробити практичні рекомендацій що до застосування програмних застосунків для захисту конфіденційних даних, що оброляються в локальній комп'ютерній мережі.

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах.

6. Дата видачі завдання 20.10.2024

КАЛЕНДАРНИЙ ПЛАН

/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
	Підбір науково-технічної літератури		
	Написання першого розділу роботи		
	Написання другого розділу роботи		
	Написання третього розділу роботи		
	Написання висновків по роботі		
	Підготовка демонстраційних матеріалів		
	Підготовка доповіді		

Здобувач вищої освіти _____ Руслан САД
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олександр ДРОБИК
(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 конфіденційних даних шляхом застосування програмних застосунків.

Для досягнення поставленої мети необхідно вирішити такі завдання:

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

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

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

Об'єктом дослідження є процес обробки конфіденційних даних в локальній комп'ютерній мережі комерційного підприємства.

Предмет дослідження – захист конфіденційних даних в локальній комп'ютерній мережі.

Апробація:

1. Р.С. Хворостяний, **Р.М. Сад**, П.В. Верещак. Аналіз процесу обробки персональних даних в локальних комп'ютерних мережах та способів несанкціонованого доступу до них. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.81-83. https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Ключові слова: ЛОКАЛЬНА КОМ'ЮТЕРНА МЕРЕЖА, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАННИХ, ПРОГРАМНІ ЗАСТОСУНКИ ЗАХИСТУ ІНФОРМАЦІЇ.

ABSTRACT

The textual part of the qualification work consists of an introduction, four sections, general conclusions, a list of sources used, the total volume of work is 59 pages, has 21 figures, 6 tables. The list of sources used contains 39 names and occupies 4 pages.

The purpose of qualification is to increase the level of protection of the local computer network from unauthorized access to personal data by applying promptly.

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

- to conduct an inspection of the process of processing confidential data in local communication networks, channels and methods of unauthorized access to them;

- to analyze the methods of information protection in the local communication network from unauthorized access to confidential data;

- to develop practical recommendations that the use of software applications to protect confidential data that is sprouting in the local computer network.

The object of research is the process of processing confidential data in the local computer network of the commercial enterprise of the Imy.

The subject of the study is the protection of confidential data in the local computer network.

LOCAL COMPUTER NETWORK, UNAUTHORIZED ACCESS, PROTECTION OF CONFIDENTIAL DATA, INFORMATION PROTECTION SOFTWARE APPLICATIONS.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ……. ...8
ВСТУП …… ...9
Розділ 1. ОГЛЯД ПРОЦЕСУ ОБРОБКИ КОНФІДЕНЦІЙНИХ ДАНИХ В ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ ТА СПОСОБІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО НИХ ……... .10
1.1 Процеси обробки конфіденційних даних в локальних комп'ютерних мережах об'єкту інформаційної діяльності ……. ..8
1.2 Принципи побудови та функціонування локальної комп'ютерної мережі об'єкту інформаційної діяльності ……..……. .12
1.3 Проблеми забезпечення кібербезпеки локальної комп'ютерної мережі. 12
1.3.1 Несанкціонований доступ до конфіденційних даних в локальній комп'ютерній мережі ……. 12
1.3.2 Використання програмних засобів для НС……... .14
1.4 Висновик до першого розідлу……. 17

Розділ 2. АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ЛОКАЛЬНІЙ КОМ'ЮТЕРНІЙ МЕРЕЖІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ …. .18
2.1 Способи захисту інформації…… .18
2.2 Заходи захисту інформації в ЛКМ…….. .20
2.3 Основні сервіси безпеки…….. .21
2.3.1 Ідентифікація та автентифікація……...…… 20
2.3.2 Протоколування та аудит……...……... 28
2.3.3 Криптографія……...……... 29
2.3.4 Система виявлення вторгнень……..…… 32
2.4 Висновки до другого розділу…….. 35

Розділ 3. ДОСЛІДЖЕННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ ПРОГРАМНОГО ЗАХИСТУ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ДАНИХ …. .36
3.1 Склад інформації, що підлягає захисту……..…….…… .36
3.2 Мережеве та програмне забезпечення процесів захисту інформації …….. .37
3.3 Аналіз уразливості мережевих каналів об'єкту інформаційної діяльності. .38
3.3.1 Можливі способи реалізації мережевих загроз в комп'ютерних мережах об'єкту інформаційної діяльності …….. .36
3.4 Рекомендації по застосуванню програмно-апаратних засобів захисту інформації Positive technologies application firewall ..... .41
3.4.1 Застосування міжмережевого екрану…….……..... 41
3.4.2 Встановлення криптопровайдера в системі захисту даних…… .42
3.4.3 Встановлення засобу виявлення вторгнень та антивірусу ManageEngine EventLog Analyzer ……... .49
3.5 Аналіз ризиків після впровадження рекомендованих програмно-апаратних комплексів ……. .52
3.6 Висновки по третього розділу…….. .56

ВИСНОВКИ …… .57
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ……. .59
ДОДАТКИ ……... .63

СПИСОК 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 прогамних застосунків.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– провести огляд процесу обробки конфіденційних 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 конфіденційних даних;

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

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

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

Розділ 1
ОГЛЯД ПРОЦЕСУ ОБРОБКИ КОНФІДЕНЦІЙНИХ ДАНИХ В ЛОКАЛЬНИХ КОМ'ЮТЕРНИХ МЕРЕЖАХ ТА СПОСОБІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО НИХ

1.1 Процеси обробки конфіденційних даних в локальних комп'ютерних мережах об'єкту інформаційної діяльності

Термін «персональні дані» є вхідним початком застосування рагального регламенту захисту даних (GDPR). Лише якщо обробка даних стосується персональних даних, застосовується Загальний регламент захисту даних. Термін визначено ст. 4 (1) (GDPR). Персональні дані - це будь-яка інформація, яка стосується ідентифікованої або ідентифікованої фізичної особи[1].

Суб'єкти даних можна ідентифікувати, якщо їх можна прямо чи опосередковано ідентифікувати, особливо за допомогою ідентифікатора, такого як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор або одна з кількох спеціальних характеристик, які виражають фізичні, фізіологічні, генетичні ментальна, комерційна, культурна чи соціальна ідентичність цих фізичних осіб[2]. На практиці сюди також входять усі дані, які будь-яким чином належать або можуть бути присвоєні особі. Наприклад, номер телефону, номер кредитної картки або персональний номер особи, облікові дані, номерний знак, зовнішній вигляд, номер клієнта або адреса – все це персональні дані.

Оскільки визначення включає «будь-яку інформацію», слід виходити з того, що термін «персональні дані» слід тлумачити якомога ширше. Це також пропонується в прецедентному праві Європейського суду, який також розглядає менш чітку інформацію, таку як записи робочого часу, які включають інформацію про час, коли працівник починає та закінчує свій робочий день, а також про перерви або час, коли не входять в робочий час, так як персональні дані[2].

Також «персональними даними» є письмові відповіді кандидата під час тестування та будь-які зауваження екзаменатора щодо цих відповідей, якщо кандидата можна теоретично ідентифікувати. Те ж саме стосується і IP-адрес.

Якщо контролер має законну можливість зобов'язати постачальника надати додаткову інформацію, яка дозволяє йому ідентифікувати користувача за IP-адресою, це також особисті дані. Крім того, слід зазначити, що персональні дані не обов'язково повинні бути об'єктивними. Суб'єктивна інформація, така як думки, судження чи оцінки, може бути особистими даними. Таким чином, сюди входить оцінка кредитоспроможності особи або оцінка роботи роботодавцем[2].

Не в останню чергу в законі зазначено, що відомості для кадрової довідки мають стосуватися фізичної особи. Іншими словами, захист даних не поширюється на інформацію про юридичних осіб, таких як корпорації, фонди та установи. Для фізичних осіб, з іншого боку, захист починається і припиняється з правоздатністю. В основному, людина отримує цю здатність з народженням і втрачає її після смерті. Тому дані повинні бути присвоєні ідентифікованим або ідентифікованим живим особам, щоб вважатися особистими[3].

На додаток до загальних персональних даних, перш за все, слід враховувати спеціальні категорії персональних даних (також відомі як конфіденційні персональні дані), які є дуже актуальними, оскільки підлягають вищому рівню захисту. Ці дані включають генетичні, біометричні дані та дані про стан здоров'я, а також особисті дані, що розкривають расове та етнічне походження, політичні погляди, релігійні чи ідеологічні переконання чи членство в профспілках[3].

1.2 Принципи побудови та функціонування локальної комп'ютерної мережі об'єкту інформаційної діяльності

Інститут інженерів з електротехніки та електроніки (IEEE) визначив локальну мережу як «систему передачі даних, яка дозволяє кільком незалежним пристроям безпосередньо спілкуватися один з одним у межах географічної області помірного розміру через фізичний канал зв'язку з помірними швидкостями»[4].

Зазвичай локальна мережа через загальну мережеву операційну систему з'єднує сервери, робочі станції, принтери та пристрої масової пам'яті, дозволяючи користувачам спільно використовувати ресурси та функції, які надає локальна мережа[4].

1.3 Проблеми забезпечення кібербезпеки локальної комп'ютерної мережі

1.3.1 Несанкціонований доступ до конфіденційних даних в локальній комп'ютерній мережі

Архітектура ЛКМ та специфіка її роботи надає змогу зловмиснику знаходити або спеціально створювати прогалини для прихованого доступу до інформації, враховуючи різноманітність відомих на даний момент зафіксовних злочинних дій, наштовхує на думку що даних лазівок існує ми може бути створено набагато більше[4]. Шляхи несанкціонованого отримання інформації (Рис. 1.1)

Несанкціонований доступ до інформації, що знаходиться в ЛКМ буває:

– прямим – (з фізичним доступом до елементів ЛКМ).

– непрямим – (без фізичного доступу до елементів ЛКМ);

Існують наступні шляхи несанкціонованого отримання інформації (канали витоку інформації):

– застосування апаратури для зняття акустичних каналів;

– перехоплення електромагнітного випромінюванння;

– дистанційна фото-відео зйомка;

– втрата носіїв інформації та розкрадання виробничих відходів;

– зчитування даних у масивах інших користувачів;

– копіювання та зчитування носіїв інформації;

– несанкціоноване вторгнення в термінали упаравління;

– вхід в систему під зареєстрованим користувачем.

– отримання захищених даних за допомогою серії дозволених запитів;

– використання недоліків мов програмування та операційних систем;

– умисне включення в бібліотеки програм спеціальних блоків типу "троянських коней";

– зловмисне виведення з ладу механізмів захисту.

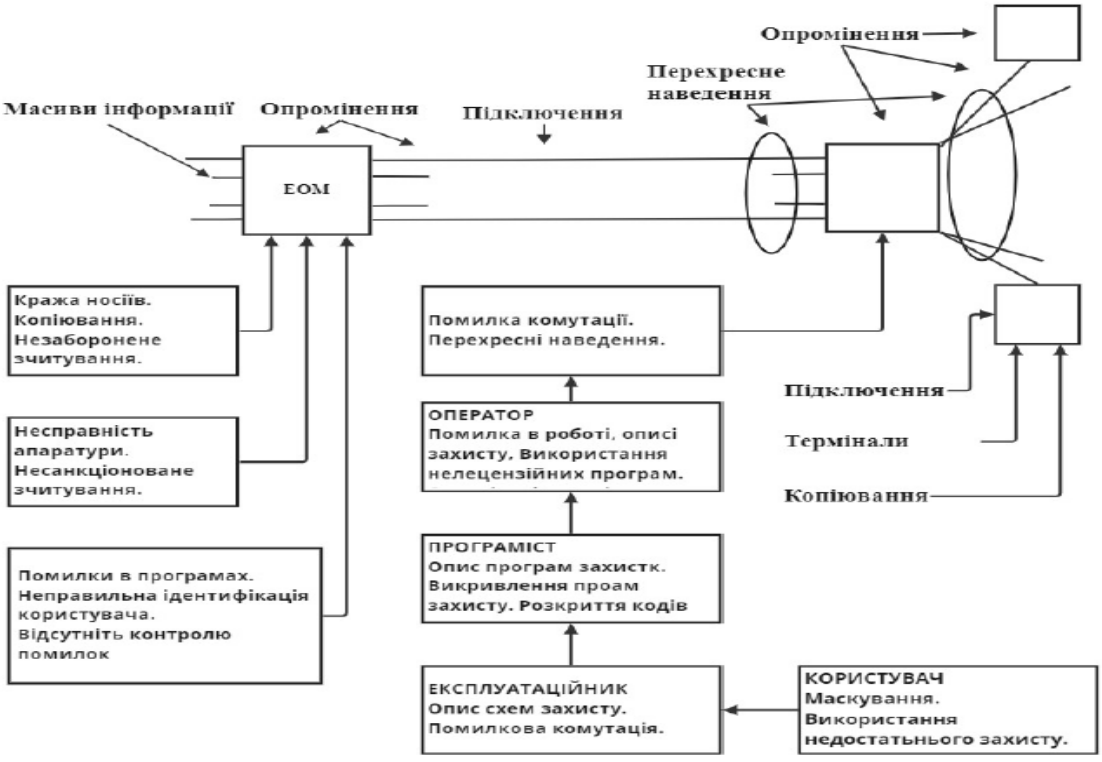


Рис.1.1 Шляхи несанкціонованого отримання інформації

Канал витоку інформації – сукупність інформаційних джерел, матеріального носія або середовища поширення сигналу, що несе цю інформацію, і засоби виділення інформації з сигналу або носія[4], (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

За середовищем існування розрізняють **файлові, завантажувальні, комбіновані (файловозавантажувальні), пакетні та мережні віруси**. Файлові віруси звичайно заражають файли з розширеннями .comта .exe. Однак, деякі їх різновиди можуть інфікувати файли й інших типів (.dll, .sys, .ovl, .prg, .bat, .mnu), при цьому вони, як правило, втрачають здатність до розмноження[5].

У свою чергу, за способом зараження середовища існування файлові віруси поділяють на **резидентні** та **нерезидентні**. Останні починають діяти тільки під час запуску зараженого файла на виконання і залишаються активними обмежений час[5].

Резидентні віруси інсталюють свою копію в оперативній пам'яті, перехоплюють звертання операційної системи до різних об'єктів і заражають їх. Деякі віруси здатні перехоплювати досить багато різних функцій переривань, у результаті чого файли можуть заражатись у процесі перейменування, копіювання, знищення, змінювання атрибутів, перегляду каталогів, виконання, відкривання та здійснення інших операцій. Резидентні віруси зберігають активність весь час до вимикання комп'ютера. Порівняно новою групою можна назвати макровіруси, які використовують можливості макромов, вбудованих у текстові редактори, електронні таблиці і т. ін. Нині поширені макровіруси у Microsoft Word і Excel. Вони перехоплюють деякі файлові функції в разі відкриття чи закриття зараженого документа і згодом інфікують решту файлів, до яких звертається програма. У певному сенсі такі віруси можна назвати резидентними, оскільки вони активні тільки у своєму середовищі відповідному додатку[5].

Окрему категорію файлових вірусів становлять віруси сім'ї DIR, які не впроваджуються у файли, а виконують реорганізацію файлової системи так, що під час запуску будь-якого файла управління передається вірусу.

Завантажувальні віруси відрізняються від файлових резидентних вірусів тим, що вони переносяться із системи в систему через завантажувальні сектори. Комп'ютер заражається таким з вірусом після спроби завантаження системи з інфікованого диска, а дискета — при читанні її «змісту»[5].

Комбіновані віруси можуть поширюватись як через завантажувальні сектори, так і черезфайли.

Пакетні віруси — це порівняно прості і старі віруси, написані мовою управління завданнями операційної системи.

Мережні віруси («черв'яки») розмножуються по комп'ютерній мережі, зменшуючи тим самим її пропускну здатність, уповільнюючи роботу серверів і т. ін. Вони посідають перше місце за швидкістю поширення. Найбільш відомим є так званий «черв'як Морріса». Останні моделі «черв'яків» упроваджуються у різні архіви (arj, zipта ін.) і зменшують вільний простір на диску[5].

За ступенем деструктивності віруси можна поділити на такі групи:

• порівняно безпечні, нешкідливі — їх вплив обмежується зменшенням вільної пам'яті і графічними або звуковими ефектами. Варто зазначити, що зменшення пам'яті в деяких випадках може призвести до збою системи, а ефекти — відволікти користувача, у результаті чого він припуститься помилки;

• небезпечні — віруси, які можуть призводити до збійних ситуацій;

• дуже небезпечні — дії вірусів можуть призвести до втрати програм, знищення даних, стирання інформації в системних областях тощо.

За особливостями алгоритму віруси важко класифікувати через їх різноманітність. Можна виокремити найпростіші, «вульгарні» віруси, написані єдиним блоком, який можна розпізнати в тексті програми-носія, та віруси «роздроблені» — поділені на частини, що нібито не мають між собою зв'язку, але містять інструкції комп'ютерові, як їх зібрати в єдине ціле і розмножити вірус[5].

З погляду прийомів маскування розрізняють віруси-невидимки (стелс-віруси, stealth) та поліморфні віруси. Перші перехоплюють функції операційної системи, відповідальні за роботу з файлами, і коригують результати звернень.

Механізм **«невидимості»** в кожному з цих вірусів реалізується по-своєму, однак можна виокремити кілька загальних принципів:

• для приховування збільшення довжини заражених файлів вірус передає програмі перегляду каталогів зменшене значення їхньої довжини;

• для того щоб користувач не виявив код вірусу під час перегляду файла, вірус виліковує його в момент відкриття і заново заражає у процесі закриття;
• для того щоб замаскувати свою присутність у пам'яті комп'ютера, вірус стежить за діями резидентних моніторів пам'яті, у разі спроби перегляду коду вірусу система зависає.

Поліморфними називають віруси, які застосовують різноманітні способи шифрування власного тіла. У разі зараження чергового файла алгоритм шифрування змінюється випадковим чином. При цьому дуже важко виділити сигнатуру — характерну послідовність байтів у коді вірусу[5].

Несанкціонована модифікація даних і програмного забезпечення може статися за допомогою таких типів вразливості:

- дозвіл на запис, наданий користувачам, яким для доступу потрібен лише дозвіл на читання,
- непомічені зміни, внесені до програмного забезпечення, включаючи додавання коду для створення програми- трояна,
- відсутність криптографічної контрольної суми конфіденційних даних,
- відсутність засобів захисту та виявлення вірусів.

1.4 Висновки до першого розділу

1. Розглянули поняття локальна мережа та персональні дані.

2. Розглянули шляхи та технічні канили витоку інформації що можуть бути причиною несанкціонованого доступу в локальну мережу підприєства.

3. Вияснили цілі впровадження системи безепеки інформації:

- Зберігання конфіденційність даних під час їх зберігання, обробки або передачі в локальній мережі;

- Підтримування цілісністі даних під час їх зберігання, обробки або передачі в локальній мережі;

- Підтримку доступність даних, що зберігаються в локальній мережі, а також здатність своєчасно обробляти та передавати дані.

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

2.1 Способи захисту інформації

Система захисту інформації (СЗІ) — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІС.До складу СЗІ входять заходи та засоби, які реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін[6].

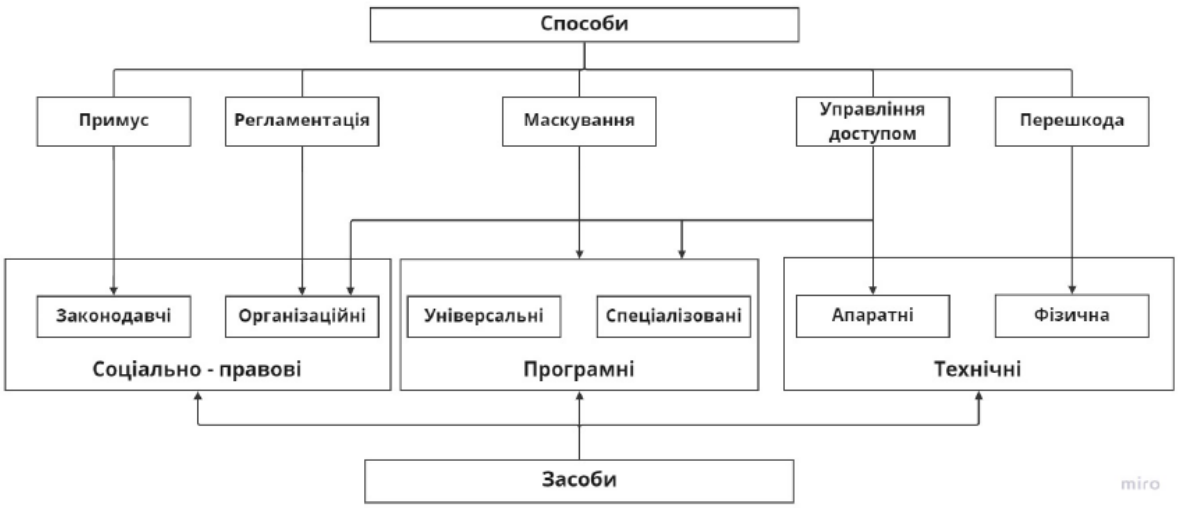


Рис. 2.1 Способи та засоби захисту інформації в ЛВС Способи

Способи захисту інформації в ЛКМ включають всі наступні елементи(Рис 2.1):

1. **Перешкода** – фізична перешкода що захищає носії інформації від зловнмисників[6].

2. **Управління доступом** – система захист інформації при якому використвуються всі ресурси підприємства[6].

Включає такі функції захисту:

- Ідентифікація інформації, персоналу з допомогою паролевих, карткових, біометричних, програмних засобів і. тп.;
- Перевірка системних журналів реєстру персоналу відносно робочого графіку, повноважень, доступів до інформації;
- Створення і організація роботи в межах регламенту ;
- Відмовостійкість систем (затримка робіт, відмова, відключення, сигналізація) під час спроб несанкціонованих дій.

3. **Маскування** – захист даних в ЛКМ шляхом використання криптографічних перетвіорень перетворення. При передачі інформації незахищеними лініями зв'язку, криптографічний захист є найголовнішим методом її захисту[6].

4. **Регламентація** – розроблення документації в які прописані посадові інструкції персоналу та правила робити з конфеденційною інформацією[6].

5. **Примус** – користувачі та персонал ЛКМ змушені дотримуватися правил обробки та використання інформації, що захищається під загрозою матеріальної, адміністративної чи кримінальної відповідальності[6].

Розглянуті засоби захисту інформації реалізуються застосуванням різних засобів захисту, причому, розрізняють технічні, програмні, організаційні, законодавчі і морально-етичні засоби[7].

1. Організаційними засобами захисту називаються організаційно- правові заходи які регулюють процес створення та експлуатації ЛКМ.

- Організаційні заходи охоплюють усі структурні елементи ЛКМ на всіх етапах: будівництво приміщень, проектування системи, монтаж та налагодження обладнання, випробування та перевірки, експлуатація.

- До законодавчих засобів захисту відносяться законодавчі акти країни, якими регламентуються правила використання та опрацювання інформації обмеженого доступу та встановлюються заходи відповідальності за порушення

цих правил.

- До морально-етичних відносять правила які формуються традиційно або складаються в міру поширення обчислювальних засобів у цій країні чи суспільстві. Ці норми здебільшого є обов'язковими, як законодавчі заходи, проте недотримання їх веде зазвичай до втрати авторитету, престижу людини чи групи осіб[7].

2.2 Заходи захисту інформації в ЛКМ

Захист інформації в ПК це - організація методів і засобів зо знижують можливість появи каналів витоку інформації, її спотворення при зберігані і оброрбці на ПК[8].

1. Організаційні заходи захисту – заходи загального характеру, утрудняють доступом до цінної інформації стороннім особам, незалежно від особливостей способу обробки інформації та каналів витоку інформації[8]. Організаційні заходи передбачають:

– Обмеження доступу до приміщень, де відбувається обробка конфіденційної інформації.

– Допуск до вирішення завдань на ПК із обробки секретної, конфіденційної інформації перевірених посадових осіб, визначення порядку проведення робіт на ПК. Зберігання носіїв інформації у ретельно закритих міцних шафах[8].

– Призначення однієї або кількох ПК для обробки цінної інформації та подальша робота тільки на цих ПК.

– Встановлення дисплея, клавіатури та принтера таким чином, щоб унеможливити перегляд сторонніми особами змісту інформації, що обробляється.

– Постійне спостереження за роботою принтера та інших пристроїв виведення на матеріальний носій цінної інформації.

– Знищення барвників або інших матеріалів, що містять фрагменти

цінної інформації.

– Заборона ведення переговорів щодо безпосереднього змісту конфіденційної інформації особам, які зайняті її обробкою.

2. Організаційно-технічні заходи захисту – заходи, пов'язані зі специфікою каналів витоку та методу обробки інформації, але не потребують реалізації нестандартних прийомів і/або устаткування[9]. Організаційно-технічні заходи передбачають:

– Обмеження доступу до корпусу ПК шляхом встановлення механічних запірних пристроїв.

– Знищення всієї інформації на вінчестері ПК під час її відправлення в ремонт із використанням засобів низькорівневого форматування.

– Організацію живлення ПК від окремого джерела живлення або загальної (міської) електромережі через стабілізатор напруги (мережевий фільтр).

– Використання для відображення інформації рідкокристалічних або плазмових дисплеїв, а для друку – струменевих чи лазерних принтерів.

Розміщення дисплея, системного блоку, клавіатури та принтера на відстані не менше 2,5-3,0 метрів від пристроїв освітлення, кондиціювання повітря, зв'язку (телефону), металевих труб, телевізійної та радіоапаратури, а також інших ПК, що не використовуються для обробки конфіденційної інформації[10].

2.3 . Основні сервіси безпеки

2.3.1 Ідентифікація та автентифікація

Першим кроком до захисту ресурсів локальної мережі є можливість перевірки ідентичності користувачів. Процес підтвердження особи користувача називається автентифікацією[11]. Автентифікація забезпечує основу для ефективності інших елементів керування, що використовуються в локальній мережі. Наприклад, механізм журналювання надає інформацію про

використання на основі ідентифікатора користувача. Механізм контролю доступу дозволяє доступ до ресурсів локальної мережі на основі ідентифікатора користувача. Обидва ці елементи керування ефективні лише за умови, що запитувач служби локальної мережі є дійсним користувачем, призначеним цьому конкретному ідентифікатору користувача[12].

Ідентифікація вимагає, щоб користувач був певним чином відомий локальній мережі. Зазвичай це базується на призначеному ідентифікаторі користувача. Однак локальна мережа не може довіряти достовірності того, що користувач насправді є тим, за кого себе видає, без аутентифікації.

Автентифікація здійснюється шляхом надання користувачеві чогось, що є лише у нього, наприклад маркера, чогось, що знає лише користувач, наприклад пароля, або чогось, що робить користувача унікальним, наприклад відбитка пальця. Чим більше їх має надати користувач, тим менший ризик для того, хто маскується під законного користувача[12].

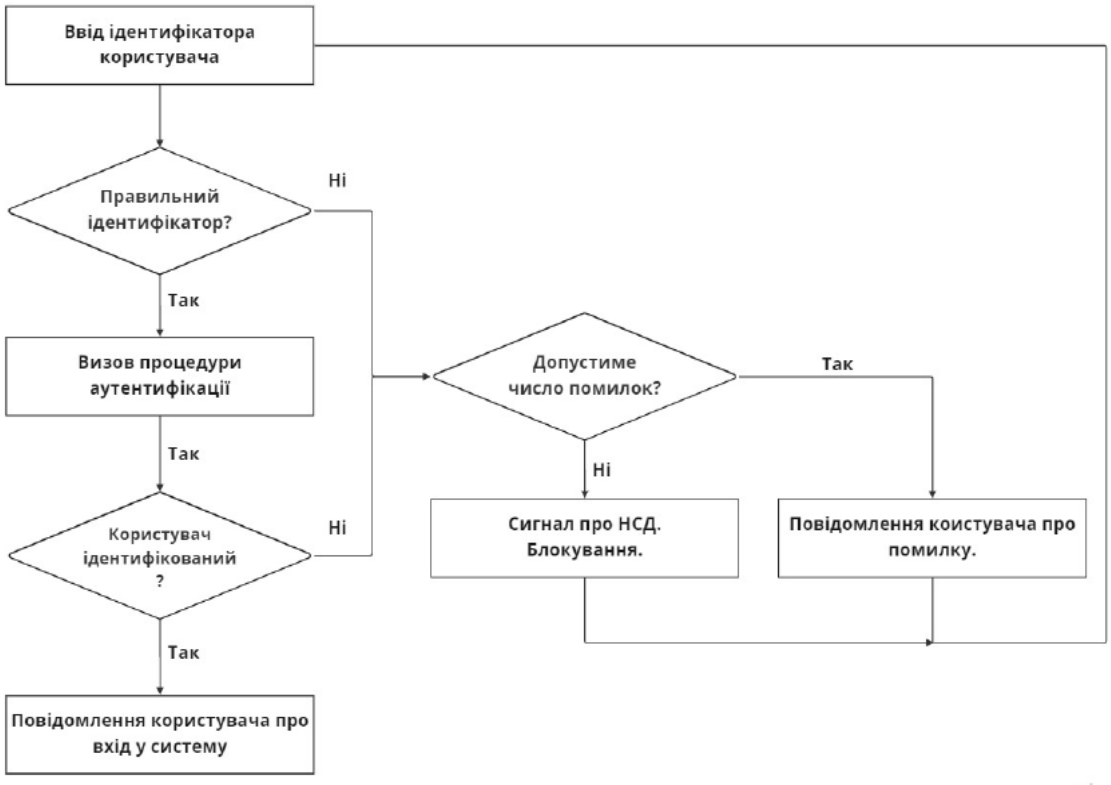


Рис 2.2 Класична процедура ідентифікації та аутентифікації

Загальна процедура ідентифікації та аутентифікації користувача при його

доступі до АС(Рис 2.2). Якщо в процесі аутентифікації справжність суб'єкта встановлено, то система захисту має визначити його повноваження (сукупність прав). Це необхідно для подальшого контролю та розмежування доступу до ресурсів[13].

Коли користувач (або інша особа) претендує на особу, це називається ідентифікацією. Для ідентифікації можна використовувати ім’я користувача, ідентифікатор процесу, смарт-картку чи будь-що інше, що може однозначно ідентифікувати суб’єкта чи особу. Системи безпеки використовують цей метод ідентифікації, щоб визначити, чи має особа дозвіл на доступ до об’єкта[13].

Ідентифікація означає знати, ким є хтось, навіть якщо він відмовляється співпрацювати.

Системи відеоспостереження, відбитки пальців і зразки ДНК – це деякі з ресурсів, за допомогою яких можна ідентифікувати особу. З іншого боку, цифровий світ використовує відбитки пальців пристрою або інші біометричні дані з тією ж метою. Індивідів також можна ідентифікувати в Інтернеті за стилем написання, натисканням клавіш або тим, як вони грають у комп’ютерні ігри[14].

Загалом акт визначення чиєїсь особи відомий як ідентифікація.

Чому ідентифікація користувача важлива?

Персональна ідентифікація стосується процесу асоціації конкретної особи з конкретною ідентичністю. Це вважається важливим процесом, оскільки він вирішує певні проблеми щодо особи, такі як «Чи є особа, за яку він/вона себе видає?», «Чи була ця особа тут раніше?» або «Чи слід надати цій особі доступ до наша система?»

Ідентифікація корисна для організацій, оскільки вона:

– Можна легко інтегрувати в різні системи
– Коштує недорого
– Служить стримуючим фактором для самозванців

Види ідентифікації

Щоб ідентифікувати особу, можна використовувати документ, що посвідчує особу (ідентифікаційний код, ідентифікаційна картка, картка громадянина) або паспорт (якщо він виданий у невеликому стандартному форматі кредитної картки). Деякі країни також видають офіційні документи, що посвідчують особу, наприклад національні посвідчення особи, які можуть бути обов'язковими або необов'язковими, тоді як інші можуть покладатися на регіональні ідентифікаційні документи або неофіційні документи для підтвердження особи[14].

Деякі інші прийнятні форми ідентифікації включають:

Щось, що людина знає: пароль, PIN-код, дівоче прізвище матері або комбінацію замка. Автентифікація особи за допомогою того, що вона вже знає, є, мабуть, найпростішим варіантом, але одним із найменш безпечних.

Щось, що є у людини: ключ, картка, картка доступу або бейдж – це приклади речей, якими може володіти людина. Цей метод зазвичай використовується для отримання доступу до таких об'єктів, як банки та офіси, але його також можна використовувати для отримання доступу до конфіденційних місць або перевірки облікових даних системи. Це також простий варіант, але ці предмети легко вкрасти.

Щось із особи: біометричні дані особи належать їй виключно, і їх не можна втратити чи вкрасти. Використання біометричних даних для ідентифікації особи є найбільш точним і безпечним варіантом.

Автентифікація — це процес підтвердження особи, який відбувається, коли суб'єкти надають відповідні облікові дані для цього. Коли користувач вводить правильний пароль разом із іменем користувача, наприклад, пароль підтверджує, що користувач є власником імені користувача. У двох словах, автентифікація встановлює дійсність заявленої особи[15].

У системі, захищеній іменем користувача та паролем, користувач повинен надати дійсні облікові дані, щоб отримати доступ до системи. Це не тільки допомагає захистити систему від атак невідомих сторонніх розробників, але й допомагає зберегти конфіденційність користувачів, порушення якої може

призвести до юридичних проблем[15].

Залежно від кількості елементів ідентифікації або автентифікації, які надає користувач, процедуру автентифікації можна класифікувати на такі рівні:

- Однофакторна автентифікація
- Двофакторна автентифікація
- Багатофакторна автентифікація

Автентифікація допомагає організаціям у захисті їхніх мереж, дозволяючи лише автентифікованим користувачам (або процесам) отримувати доступ до захищених ресурсів, таких як комп'ютерні системи, мережі, бази даних, веб-сайти та інші мережеві програми чи служби[15].

Автентифікація користувача надає кілька переваг:

Запобігання крадіжкам: Основна мета системи контролю доступу — обмежити доступ, щоб захистити особисті дані користувачів від викрадення або зміни. Багато веб-сайтів, які вимагають персональної інформації для своїх послуг, особливо ті, які вимагають інформацію про кредитну картку або номер соціального страхування особи, відповідно до закону чи нормативних актів повинні мати механізм контролю доступу[15].

Рівні безпеки: Сучасні системи контролю розвивалися разом із технологічним прогресом. Людина, яка хоче зберегти інформацію в безпеці, має більше можливостей, ніж просто чотиризначний PIN-код і пароль. Замки з біометричним скануванням, наприклад, тепер можуть бути встановлені на домашніх і офісних пунктах входу[16].

Методи автентифікації

Кіберзлочинці постійно вдосконалюють свої системні атаки. У результаті групи безпеки мають справу з безліччю проблем автентифікації, що постійно змінюються. Ось чому підприємства починають розгортати більш складні плани, які включають автентифікацію[16].

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

Автентифікація за паролем: найпоширенішим методом автентифікації є

імена користувачів і паролі. Поєднання букв, цифр і спеціальних символів створює надійний пароль, але його все одно можна зламати або вкрасти.

Двофакторна автентифікація (2FA): 2FA вимагає ідентифікації користувача двома або більше різними способами. Коди, згенеровані смартфоном користувача, тести Captcha або інші додаткові фактори, крім імені користувача та пароля, забезпечують додатковий рівень безпеки. Але викрадений мобільний телефон або ноутбук може бути всім, що потрібно, щоб обійти цей підхід.

Біометрична багатофакторна автентифікація (MFA): біометрична автентифікація спирається на унікальні біологічні особливості людини та є найбезпечнішим методом автентифікації особи. Завдяки біометричним технологіям MFA авторизовані характеристики, які зберігаються в базі даних, можна швидко порівняти з біологічними ознаками. При встановленні на воротах і дверях біометричну автентифікацію можна використовувати для регулювання фізичного доступу[16].

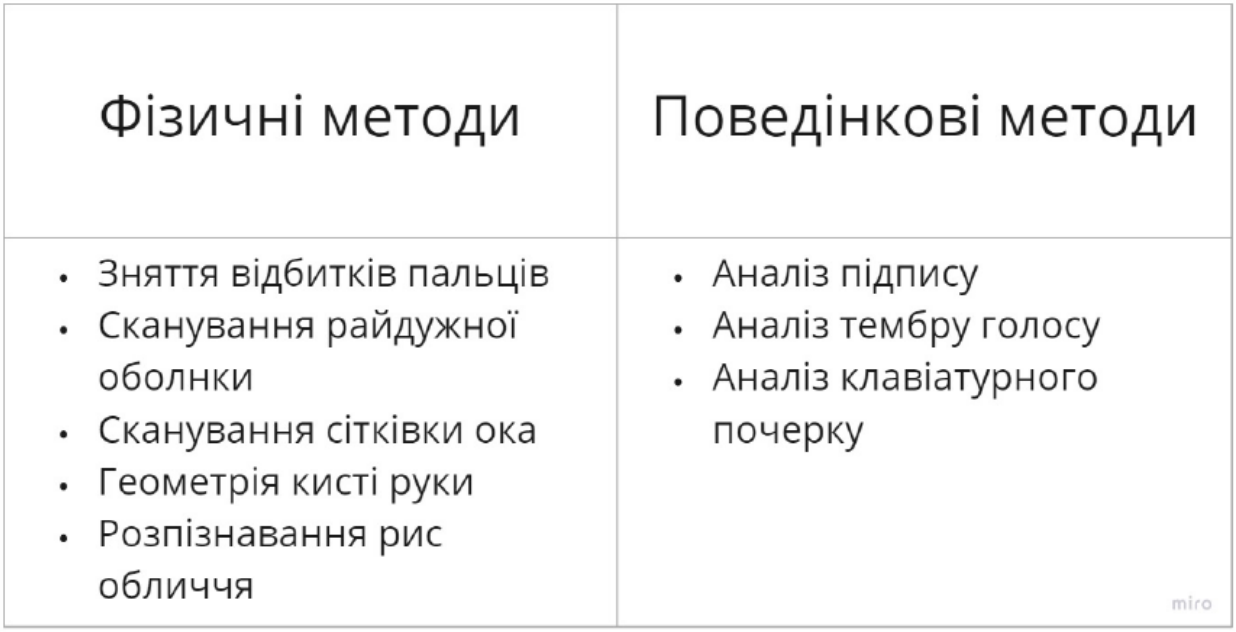


Рис 2.3 Приклади методів біометрії

Авторизація — це техніка безпеки для визначення привілеїв або права користувача на виконання певних завдань у системі. Процедура авторизації визначає рольові повноваження, які користувач може мати в системі після того,

як його було автентифіковано як прийнятного кандидата[17].

Важливо відзначити, що авторизація неможлива без ідентифікації та автентифікації. Бо якщо всі ввійдуть під одним обліковим записом, їм буде надано або заборонено доступ до ресурсів.-

Якщо всі користуються одним обліковим записом, ви не зможете розрізняти користувачів. Однак після того, як ви визначили та автентифікували їх за допомогою певних облікових даних, ви можете надати їм доступ до окремих ресурсів на основі їхніх ролей або рівнів доступу.?

Авторизація визначає, що користувач може робити та бачити у ваших приміщеннях, мережах або системах. Отже, яку користь вам принесе авторизація?

- Переконується, що користувачі не мають доступу до чужого облікового запису
- Запобігає доступу відвідувачів і співробітників до безпечних зон
- Гарантує, що всі функції недоступні для безкоштовних облікових записів
- Гарантує, що внутрішні облікові записи мають доступ лише до необхідної інформації

Методи авторизації:

Ключі інтерфейсу прикладного програмування (API): щоб використовувати більшість API, ви повинні спочатку зареєструватися для отримання ключа API, який є довгим рядком, який зазвичай міститься в URL-адресі або заголовку запиту. і в основному використовується для ідентифікації особи, яка виконує виклик API (аутентифікація для використання API). Ключ API потенційно може бути пов’язаний із певним додатком, у якому зареєструвалася особа[18].

Базова автентифікація: базова автентифікація — це інший тип авторизації, коли відправнику потрібно ввести ім’я користувача та пароль у заголовку запиту. Base64 — це техніка кодування, яка перетворює логін і пароль на набір із 64 символів для забезпечення безпечної доставки.

HMAC: HMAC означає код авторизації повідомлень на основі хешу та є більш безпечною формою автентифікації, яка зазвичай зустрічається у

фінансових API. І відправник, і одержувач мають доступ до секретного ключа, якого ніхто інший не має. Відправник створює повідомлення, використовуючи системні атрибути (наприклад, мітку часу запиту та ідентифікатор облікового запису). Секретний ключ використовується для шифрування повідомлення, яке потім надсилається через безпечний процес хешування[19].

Коли API-сервер отримує запит, він використовує ідентичні властивості системи та генерує ідентичний рядок за допомогою секретного ключа та безпечного хеш-алгоритму (SHA). Він приймає запит, якщо рядок збігається з підписом у заголовку запиту. Якщо рядки не збігаються, запит відхиляється.

2.3.2 Протоколування та аудит

Під протоколюванням розуміється збирання та накопичення інформації про події, що відбуваються в інформаційній системі підприємства. У кожного сервісу свій набір можливих подій, але в будь-якому випадку їх можна поділити на зовнішні - викликані діями інших сервісів, внутрішні - викликані діями самого сервісу та клієнтські – викликані діями користувачів та адміністраторів[20].

Аудит – це аналіз накопиченої інформації, проведений оперативно, майже реальному часі, чи періодично.

Реалізація протоколювання та аудиту переслідує такі цілі:

- забезпечення підзвітності користувачів та адміністраторів;
- забезпечення можливості реконструкції послідовності подій;
- виявлення спроб порушень інформаційної безпеки;
- надання інформації для виявлення та аналізу проблем.

Забезпечення підзвітності важливе насамперед як засіб стримування. Якщо користувачі та адміністратори знають, що всі їхні дії фіксуються, вони, можливо, утримаються від незаконних операцій. Якщо є підстави підозрювати будь-якого користувача в нечесності, можна реєструвати його дії особливо детально, аж до кожного натискання клавіші. У цьому забезпечується як можливість розслідування випадків порушення режиму безпеки, а й відкат

некоректних змін. Тим самим було забезпечується цілісність інформації[20].

Реконструкція послідовності подій дозволяє виявити слабкості у захисті сервісів, знайти винуватця вторгнення, оцінити масштаби завданих збитків та повернутися до нормальної роботи.

Виявлення та аналіз проблем дозволяють допомогти покращити такий параметр безпеки, як доступність. Виявивши вузькі місця, можна спробувати переконфігурувати або переналаштувати систему, виміряти продуктивність і т.д[20].

2.3.3 Криптографія

Криптографія забезпечує безпечний зв’язок у присутності зловмисних третіх сторін, відомих як противники. Шифрування використовує алгоритм і ключ для перетворення вхідних даних (тобто відкритого тексту) у зашифрований вихід (тобто зашифрований текст). Даний алгоритм завжди перетворюватиме той самий відкритий текст у той самий зашифрований текст, якщо використовується той самий ключ. Алгоритми вважаються безпечними, якщо зловмисник не може визначити будь-які властивості відкритого тексту або ключа з урахуванням зашифрованого тексту. Зловмисник не повинен мати змоги нічого визначити про ключ, враховуючи велику кількість комбінацій відкритого тексту/зашифрованого тексту, які використовували ключ[21].

Яка різниця між симетричною та асиметричною криптографією?

У симетричній криптографії той самий ключ використовується як для шифрування, так і для дешифрування. Відправник і одержувач повинні вже мати спільний ключ, відомий обом. Розподіл ключів є складною проблемою, що послужило поштовхом для розвитку асиметричної криптографії.

При асиметричному шифруванні для шифрування та дешифрування використовуються два різні ключі. Кожен користувач асиметричної криптосистеми має як відкритий, так і закритий ключ. Приватний ключ завжди зберігається в секреті, але відкритий ключ може вільно поширюватися[21].

Дані, зашифровані за допомогою відкритого ключа, можна розшифрувати

лише за допомогою відповідного закритого ключа. Отже, щоб надіслати повідомлення Джону, потрібно зашифрувати це повідомлення відкритим ключем Джона. Лише Джон може розшифрувати повідомлення, оскільки лише Джон має свій закритий ключ. Будь-які дані, зашифровані за допомогою закритого ключа, можна розшифрувати лише за допомогою відповідного відкритого ключа. Подібним чином Джейн могла цифрово підписати повідомлення своїм закритим ключем, і будь-хто, маючи відкритий ключ Джейн, міг розшифрувати підписане повідомлення та переконатися, що це справді Джейн надіслала його[21].

Симетричнйи, як правило, дуже швидкий і ідеально підходить для шифрування великих обсягів даних (наприклад, цілого розділу диска або бази даних). Асиметричний набагато повільніший і може шифрувати лише фрагменти даних, які менші за розмір ключа (зазвичай 2048 біт або менше). Таким чином, асиметричне шифрування зазвичай використовується для шифрування симетричних ключів шифрування, які потім використовуються для шифрування набагато більших блоків даних. Для цифрових підписів асиметричне шифрування зазвичай використовується для шифрування хешів повідомлень, а не цілих повідомлень[22].

Криптосистема забезпечує керування криптографічними ключами, включаючи генерацію, обмін, зберігання, використання, відкликання та заміну ключів.

Які проблеми вирішує криптографія?

Захищена система повинна забезпечувати кілька гарантій, таких як конфіденційність, цілісність і доступність даних, а також автентичність і неспростовність. При правильному використанні криптовалюта допомагає забезпечити ці гарантії. Криптографія може забезпечити конфіденційність і цілісність як даних у дорозі, так і даних у стані спокою. Він також може автентифікувати відправників і одержувачів один перед одним і захистити від відмови.

Системи програмного забезпечення часто мають кілька кінцевих точок, як

правило, кілька клієнтів і один або кілька серверів. Ці зв’язки клієнт/сервер відбуваються через мережі, яким не можна довіряти. Зв’язок відбувається через відкриті публічні мережі, такі як Інтернет, або приватні мережі, які можуть бути скомпрометовані зовнішніми зловмисниками або зловмисниками.

Він може захистити комунікації, які проходять через ненадійні мережі. Існує два основних типи атак, які зловмисник може спробувати здійснити в мережі. Пасивні атаки передбачають, що зловмисник просто прослуховує сегмент мережі та намагається прочитати конфіденційну інформацію під час її переміщення. Пасивні атаки можуть бути онлайн (під час яких зловмисник зчитує трафік у режимі реального часу) або офлайн (під час якого зловмисник просто захоплює трафік у режимі реального часу та переглядає його пізніше — можливо, витративши деякий час на його розшифровку). Активні атаки передбачають, що зловмисник видає себе за клієнта або сервер, перехоплює комунікації під час передачі та переглядає та/або змінює вміст перед тим, як передати його за призначенням (або повністю видалити)[23].

Захист конфіденційності та цілісності, який пропонують такі криптографічні протоколи, як SSL/TLS, може захистити зв’язок від зловмисного підслуховування та втручання. Захист автентичності забезпечує впевненість у тому, що користувачі справді спілкуються із системами належним чином.

2.3.4 Система виявлення вторгнень

Система виявлення вторгнень (IDS) відстежує мережевий трафік на предмет незвичних або підозрілих дій і надсилає сповіщення адміністратору. Виявлення аномальної активності та повідомлення про це адміністратору мережі є основною функцією; однак деякі програми IDS можуть вживати заходів на основі правил у разі виявлення зловмисної активності, наприклад, блокувати певний вхідний трафік[24].

Типи систем виявлення вторгнень

Існує два основних типи систем виявлення вторгнень (обидва більш детально пояснюються далі в цьому посібнику):

- **Система виявлення вторгнень на основі хоста (HIDS)** – ця система перевірятиме події на комп’ютері у вашій мережі, а не трафік, який проходить системою.
- **Мережева система виявлення вторгнень (NIDS)** – ця система перевірятиме трафік у вашій мережі.

Програмне забезпечення та системи виявлення вторгнень у мережу тепер необхідні для безпеки мережі. На щастя, ці системи дуже прості у використанні, і більшість найкращих IDS на ринку є безкоштовними для використання . У цьому огляді ви прочитаєте про десять найкращих систем виявлення вторгнень, які ви можете встановити зараз, щоб розпочати захист своєї мережі від атак. Ми розглядаємо інструменти для Windows, Linux і Mac.

Системи виявлення вторгнень на основі хоста (HIDS) , також відомі як системи виявлення вторгнення на хост або IDS на основі хосту , перевіряють події на комп’ютері у вашій мережі, а не трафік, що проходить системою. Цей тип системи виявлення вторгнень скорочено називається HIDS і в основному працює шляхом перегляду даних у файлах адміністратора на комп’ютері, який вона захищає. Ці файли включають файли журналу та файли конфігурації[25].

HIDS зробить резервну копію ваших файлів конфігурації, щоб ви могли відновити налаштування, якщо шкідливий вірус послабить безпеку вашої системи, змінивши налаштування комп’ютера. Інший важливий елемент, від якого варто захиститися, — це root-доступ на Unix-подібних платформах або зміни реєстру в системах Windows. HIDS не зможе заблокувати ці зміни, але він повинен мати можливість сповістити вас про будь-який такий доступ .

На кожному хості, який відстежує HIDS, має бути інстальоване програмне забезпечення. Ви можете просто отримати свій HIDS для моніторингу одного комп’ютера. Однак більш типовим є встановлення HIDS на кожному пристрої у вашій мережі . Це тому, що ви не хочете ігнорувати зміни конфігурації будь-якого обладнання. Природно, якщо у вашій мережі є більше ніж один хост HIDS, вам не потрібно входити на кожен з них, щоб отримати відгук. Отже, розподілена система HIDS повинна містити модуль централізованого керування

. Шукайте систему, яка шифрує зв’язок між хост-агентами та центральним монітором.

Мережеві системи виявлення вторгнень (NIDS), також відоме як мережева система виявлення вторгнень або мережева IDS, перевіряє трафік у вашій мережі. Таким чином, типовий NIDS має включати аналізатор пакетів для збору мережевого трафіку для аналізу.

Механізм аналізу NIDS зазвичай базується на правилах і може бути змінений шляхом додавання власних правил. З багатьма NIDS постачальник системи або спільнота користувачів надасть вам доступ до правил, і ви можете просто імпортувати їх у свою реалізацію. Ознайомившись із синтаксисом правил обраного вами NIDS, ви зможете створювати власні правила[26].

Повертаючись до збору трафіку, ви не хочете скидати весь свій трафік у файли або запускати весь його масив через інформаційну панель , оскільки ви просто не зможете проаналізувати всі ці дані. Отже, правила, які керують аналізом у NIDS, також створюють вибірковий збір даних. Наприклад, якщо у вас є правило для певного типу тривожного HTTP-трафіку, ваш NIDS має отримувати та зберігати лише ті HTTP-пакети, які відображають ці характеристики.

Як правило, NIDS встановлюється на спеціальному апаратному забезпеченні. Високоякісні платні корпоративні рішення постачаються як частина мережевого комплекту з попередньо завантаженим програмним забезпеченням. Однак вам не потрібно платити великі гроші за спеціалізоване обладнання . Для NIDS потрібен сенсорний модуль для збору трафіку, тому ви можете завантажити його в аналізатор локальної мережі або ви можете виділити комп’ютер для виконання завдання. Однак переконайтеся, що частина обладнання, яке ви обираєте для завдання, має достатню тактову частоту, щоб не сповільнити вашу мережу.

Методи виявлення: IDS на основі сигнатури або на основі аномалії

Незалежно від того, чи потрібна вам система виявлення вторгнень на хост або мережева система виявлення вторгнень, усі IDS використовують два

режими роботи — деякі можуть використовувати лише один або інший, але більшість використовує обидва.

- IDS на основі підписів
- IDS на основі аномалій
- IDS на основі підписів

Метод на основі підписів розглядає контрольні суми та автентифікацію повідомлень. Методи виявлення на основі сигнатур можна застосовувати як NIDS, так і HIDS . HIDS переглядатиме файли журналу та конфігурації на предмет будь-яких неочікуваних перезаписів, тоді як NIDS переглядатиме контрольні суми в захоплених пакетах і цілісність автентифікації повідомлень систем, таких як SHA1.

NIDS може включати базу даних сигнатур, які несуть пакети, відомі як джерела шкідливих дій. На щастя, хакери не сидять за комп'ютером і не друкують, як люті, щоб зламати пароль або отримати доступ до користувача root. Замість цього вони використовують автоматизовані процедури, які надають відомі хакерські інструменти. Ці інструменти, як правило, щоразу генерують однакові сигнатури трафіку, оскільки комп'ютерні програми повторюють ті самі інструкції знову і знову, а не вводять випадкові варіації[27].

IDS на основі аномалій

Виявлення на основі аномалій шукає несподівані або незвичайні моделі дій. Ця категорія також може бути реалізована системою виявлення вторгнень як на хості, так і на основі мережі. У випадку HIDS аномалією можуть бути повторні невдалі спроби входу або незвичайна активність на портах пристрою, що означає сканування портів.

У випадку NIDS аномальний підхід вимагає встановлення базової лінії поведінки для створення стандартної ситуації, з якою можна порівняти поточні моделі трафіку. Діапазон моделей трафіку вважається прийнятним, і коли поточний трафік у реальному часі виходить за межі цього діапазону, провокується сповіщення про аномалію.

Вибір методу IDS

Складні NIDS можуть створювати записи стандартної поведінки та коригувати свої межі в міру продовження терміну служби. Загалом і аналіз сигнатур, і аналіз аномалій є набагато простішим у роботі та легшим у налаштуванні за допомогою програмного забезпечення HIDS, ніж за допомогою NIDS.

Методи на основі сигнатур набагато швидші, ніж виявлення аномалій. Повністю комплексний механізм аномалій стосується методології штучного інтелекту та може коштувати багато грошей на розробку. Однак сигнатурні методи зводяться до порівняння значень. Дійсно, у випадку HIDS зіставлення шаблонів із версіями файлів може бути дуже простим завданням, яке будь-хто може виконати самостійно за допомогою утиліт командного рядка з регулярними виразами. Таким чином, їх розробка коштує не так багато, і, швидше за все, вони будуть реалізовані у безкоштовних системах виявлення вторгнень[28].

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

2.4 Висновки по розділу

1. Розкрито сутність та основні поняття у сфері захисту інформації підприємства від несанкціонованого витоку конфіденційних даних.

2. Розглянули заходи захисту які використовуються на підприємствах.

3. Подано склад та опис, способів ідентифікації та аутентифікації, протокоювання та аудиту, криптографічного захисту, та систем виявлення вторгнень в локальну комп’ютерну мережу об’єкту інформаційної діяльності.

Розділ 3
ДОСЛІДЖЕННЯ НАПРЯМКІВ УДОСКОНАЛЕННЯ ПРОГРАМНОГО ЗАХИСТУ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ДАНИХ

3.1 Склад інформації, що підлягає захисту

Інформаційними ресурсами інфраструктури ТОВ «REEP», що підялгають захисту є наступні:

1. Цільова інформація: комерційна таємниця ТОВ "REEP"; персональні дані працівників ТОВ «REEP» та інших фізичних осіб, яким стають відомі ТОВ «REEP» під час здійснення своєї діяльності.
2. Технологічна інформація: конфігураційні дані та інша інформація щодо технологій, програмних та технічних засобів, що використовуються для накопичення, зберігання, обробки, передачі та захисту інформації; службова інформація засобів захисту (ідентифікатори, паролі, таблиці розмежування доступу, криптографічні ключі, інформація журналів аудиту безпеки та інших.).
3. Програмне забезпечення: програмні інформаційні ресурси інформаційної інфраструктури ТОВ «REEP», що містять загальне та спеціальне програмне забезпечення, резервні копії програмного забезпечення, програмне забезпечення засобів захисту інформації.

Інфраструктура ТОВ «REEP» містить такі інформаційні ресурси:
інформація, що стосується комерційної таємниці:

- договори з постачальниками та покупцями;
- трудові договори;
- особисті справи працівників;
- особисті картки працівників;
- інформація на web-сайті фірми та буклети;
- статут та установчий документ;

3.2 Мережеве та програмне забезпечення процесів захисту інформації

Локальні обчислювальні мережі ТОВ "REEP" побудовані на базі стандартних мережевих рішень. До складу ЛОМ ТОВ «REEP» входить:

- серверне обладнання, розташоване в окремій стійці (шафі);
- автоматизовані робочі місця користувачів;
- загальне комутаційне обладнання та структурована кабельна система.

Обмін даними між ТОВ «REEP» та податковою службою, пенсійним фондом, ощадбанком здійснюється через зовнішні мережі.

У ТОВ «REEP» використовується: сертифіковане, ліцензійне та вільно розповсюджуване ПЗ(Табл 3.1).

Таблиця 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	1 рік
5	Інформаційна система ALMEXOFT	4	Підписка
6	1С-Бухгалтерія 8	3	Безстрокова

Отже, в інформаційній інфраструктурі ТОВ «REEP» реалізовано розрахований на багато користувачів режим обробки інформації з розмежуванням прав доступу, який регламентується чинним законодавством України, документами ТОВ «REEP» і здійснюється відповідно до посадових інструкцій.

3.3 Аналіз уразливості підприємства

3.3.1 Можливі способи реалізації мережевих загроз в комп'ютерних мережах об'єкту інформаційної діяльності

При проведенні аналізу захищеності інформації на підприємстві «REEP», було встановлено, що є ймовірність реалізації наступних загроз несанкціонованого доступу. У таблиці 3.2 наведено перелік актуальних загроз інфраструктури ТОВ «REEP», виявлений під час аналізу загроз несанкціонованого доступу до інформації.

Таблиця 3.2

Загрози

№ п/п	Загроза	Оцінка ймовірності	Оцінка тяжкості	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

Проаналізувавши матрицю оцінки ризиків(рис. 3.1), рівень якої визначаєтья за формулою **F*G.** Де **F** – оцінка ймовірності, витоку, втраті, модифікаці, інформації через вказаний ризик від 1 найменш ймовірно, до 10 найбільш; **G** - величина негативних наслідків для підприємства, при втряті крадіжці, втраті, модифікації, через вказані ризики. Доповнимо Таблицю 3.2., даними де >=50 - вискокий рівень загрози ризику, >=25 - середній рівень загрози 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%

Використочуючі дані з Таблиці 3.2. і Таблиці 3.3, побудумо графік розподілення по ступеню ризику(рис. 3.2), а також матрицю ризиків для нашого підприємтсва(рис. 3.3).

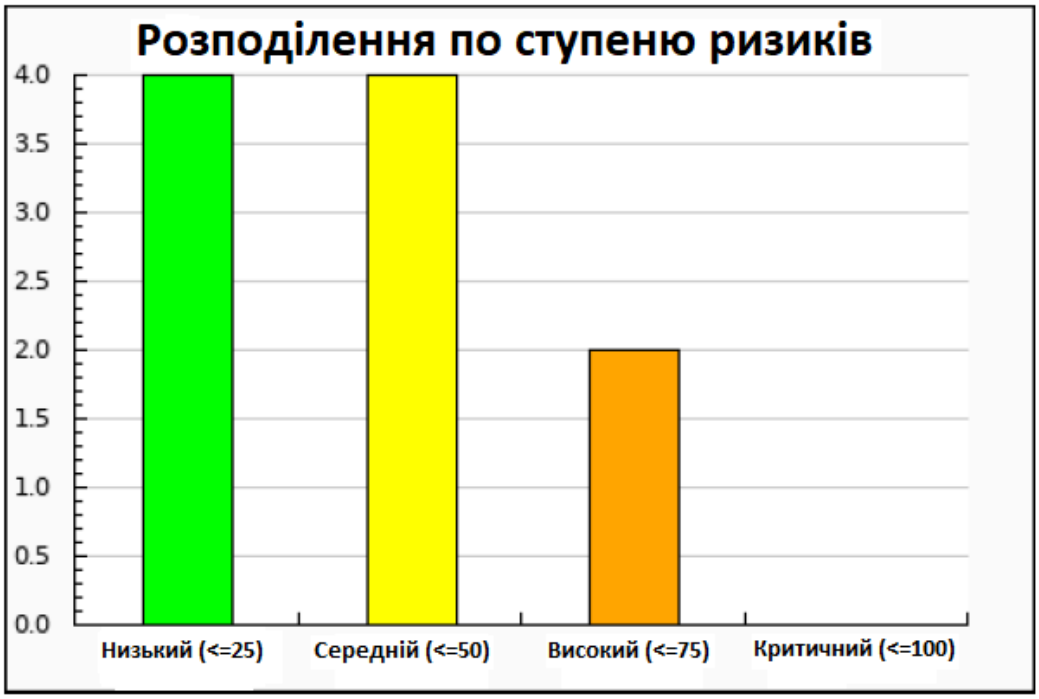


Рис. 3.2 Графік розподілення по ступеню ризику

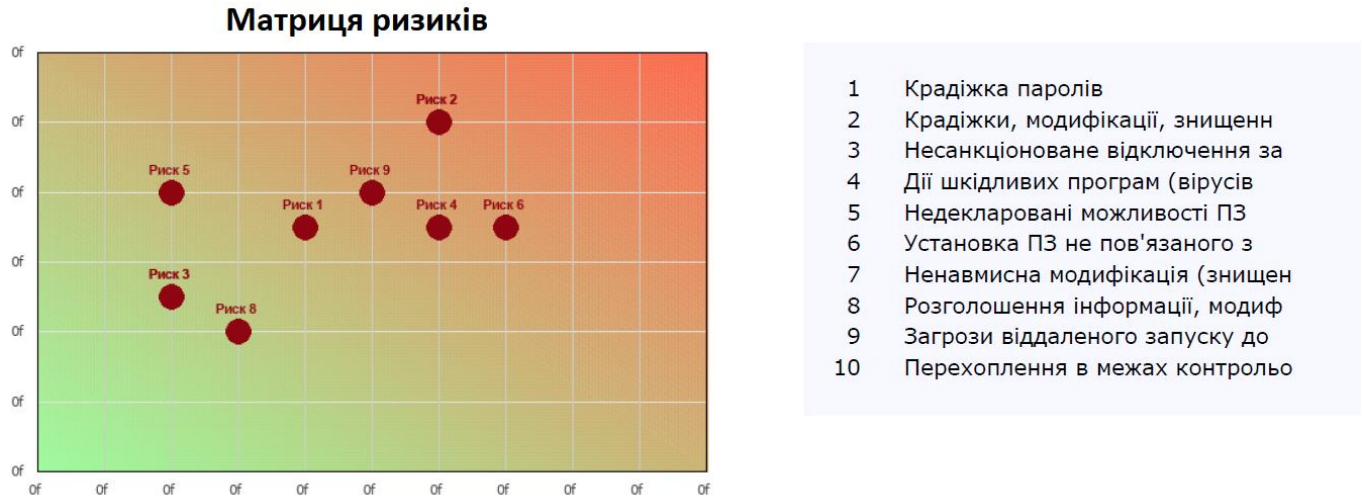


Рис. 3.3 Матриця ризиків

Проаналізувавщи всі вхідні дані, ми дійшли висновків що потрбіно доопрацьовувати програмно-апаратний комплекс засобів захисту комп'ютерної інформації за напрямами:

- вибрати криптографічні засоби захисту від НСД;
- забезпечити захист мережевого периметра та вибрати міжмережевий екран;
- визначити засоби виявлення вторгнень та антивірусу.

3.4 Рекомендації по застосуванню програмно-апаратних засобів захисту інформації Positive technologies application firewall

3.4.1 Застосування міжмережевого екрану

Однією з перших рекомендацій у ході аналізу захисту даних ТОВ «REEP» є установка міжмережевого екрану, яка є зовнішнім захистом від НСД.

Міжмережні екрани призначені в першу чергу для захисту комп'ютерних мереж або окремих вузлів від зовнішніх атак Міжмережевий екран уможливлює фільтрацію вхідного та вихідного трафіку, що йде через систему. Для корпоративної мережі фірми було обрано програмний міжмережевий екран UserGate Proxy & Firewall 6.5, який є ефективною альтернативою дорогим програмним та апаратним міжмережевим екранам та маршрутизаторам, які

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

Продукт використовує комплексний підхід до забезпечення безпеки локальної мережі та сучасні методи боротьби з Інтернет-загрозами, призначений для організації безпечної міжмережевої взаємодії, обліку трафіку та захисту локальної мережі організації від зовнішніх загроз та є сертифікованим засобом міжмережевого екранування та безпечного доступу до Інтернету для захищених систем.

Дане комплексне рішення UserGate Proxy дозволяє:

– підтримувати передачу трафіку через протоколи PPTP та L2TP для з'єднання VPN-сервера з VPN-клієнтами локальної мережі з подальшою публікацією мережевих ресурсів з метою віддаленого використання;

– визначати політику доступу до Інтернету та здійснювати повний контроль за використанням Інтернет-трафіку в компанії з веденням докладної статистики;

– створювати правила для контролю швидкості передачі даних між локальною мережею та Інтернетом з обмеженням обсягу трафіку та часу перебування в мережі для користувачів та груп;

– спростити мережеве адміністрування;

– налашутванн рівня доступу співробітників до програмного забезпечння оообробки, шифрування і передачі дани.

– налаштування доступу до мережі Інтернет для програмного забнзпечення.

На рис. 3.4 – 3.7 наведено приклади функціонування UserGate Proxy & Firewall.

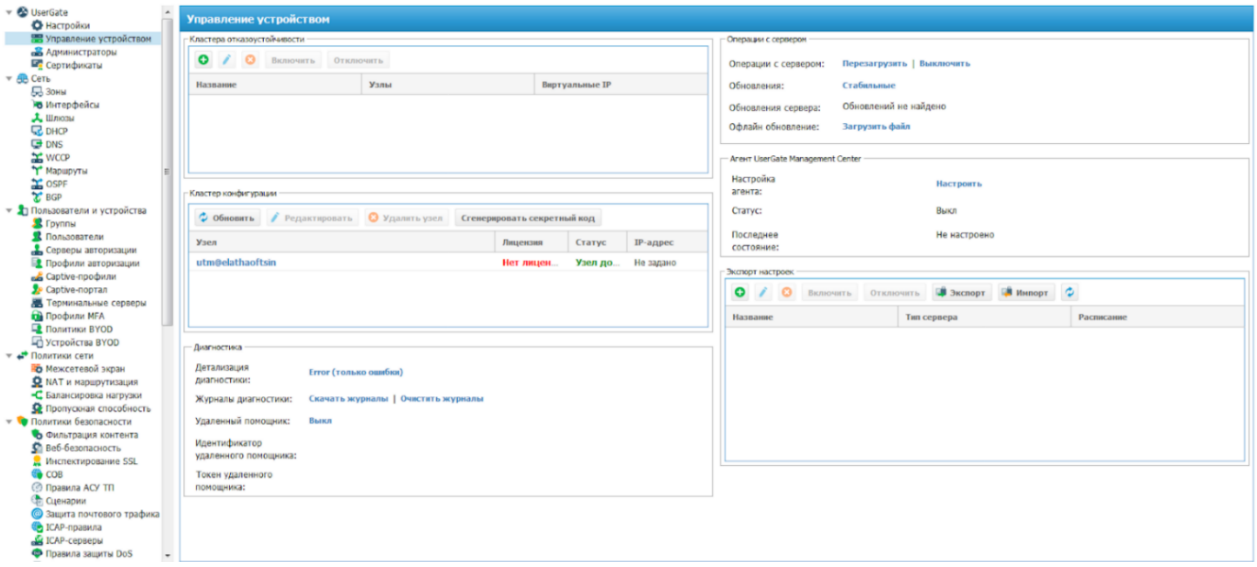


Рис. 3.4 Управління пристроями

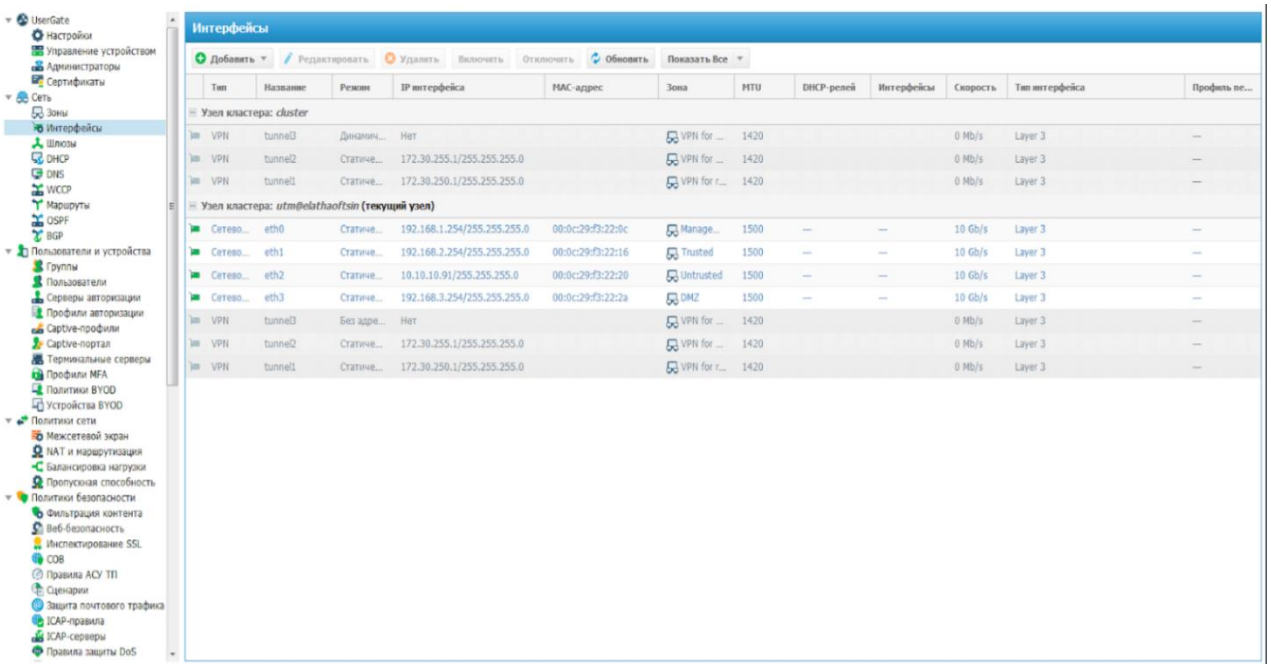


Рис. 3.5 Інтерфейси підключення

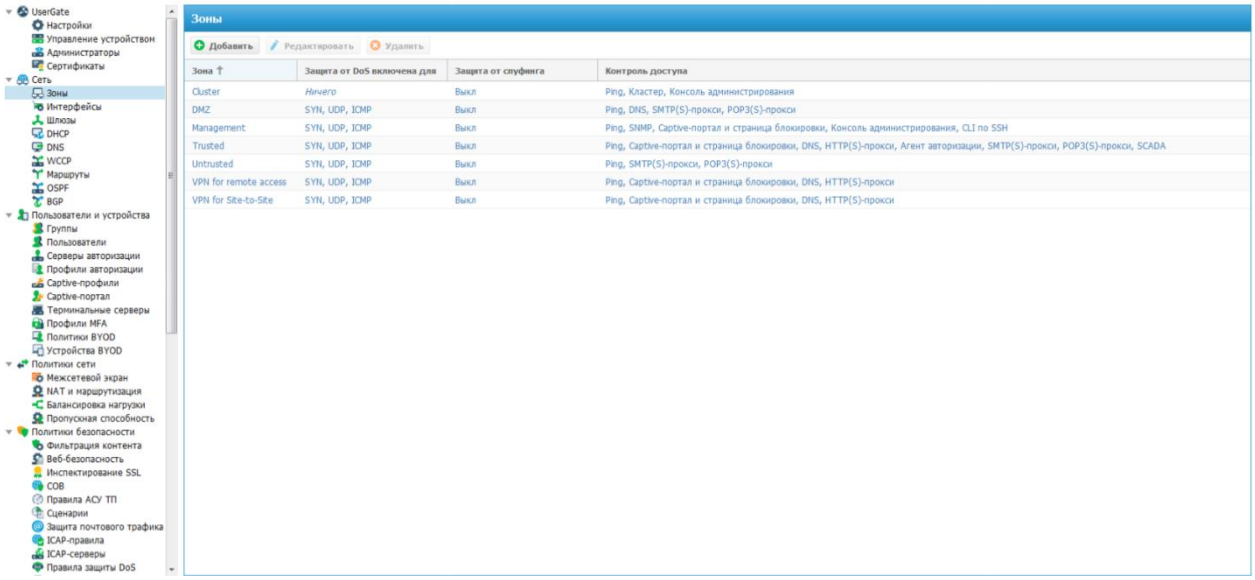


Рис 3.6 Налаштування зон мережі

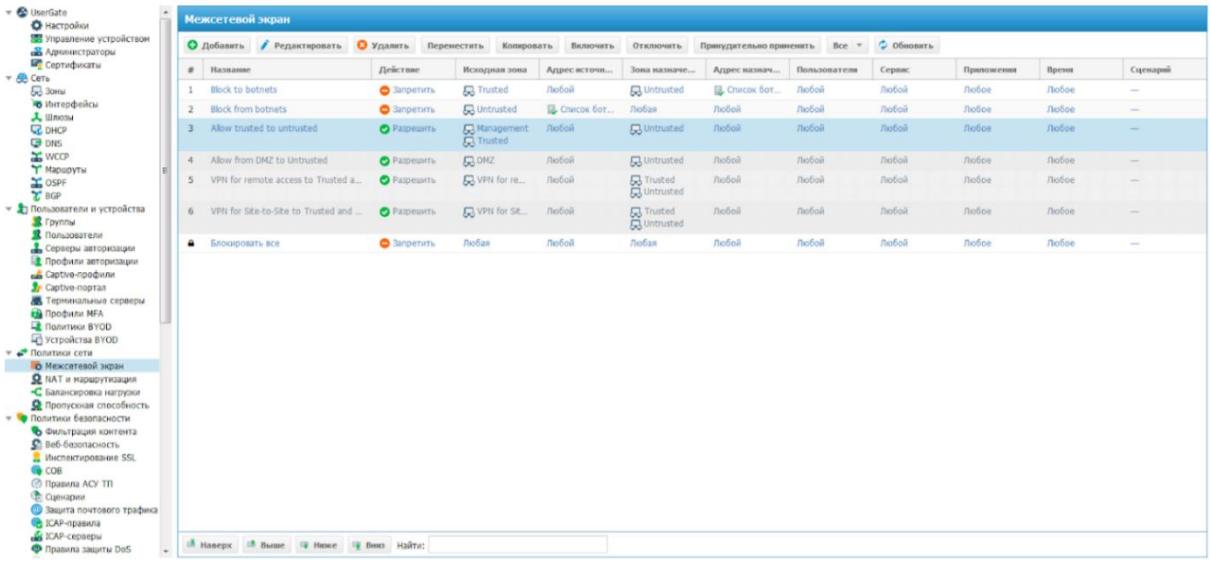


Рис. 3.7 Налаштування міжмережевих екранів

3.4.2 Встановлення криптопровайдера в системі захисту даних

Криптографічні засоби захисту від НСД повинні відповідати наступним ДСТУ з криптографії:

– Національний стандарт ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння[30]"

– Національний стандарт ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового

перетворення[31]"

– Національний стандарт ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування[32]".

Особливий інтерес представляє засіб криптографічного захисту інформації «ІІТ ЦСК-1» яке:

– призначено для формування ключів шифрування та ключів електронного підпису, шифрування та імітозахисту даних, забезпечення цілісності та справжності інформації.

– забезпечує зберігання та обробку персональних даних, конфіденційної, службової, комерційної та ін. інформації, що не містить відомостей, що становлять державну таємницю, а також забезпечує обмін такою інформацією та юридичну значущість електронного документообігу.

Обмін інформацією в електронній формі здійснюється всередині та між державними органами, органами місцевого самоврядування, організаціями, а також громадянами (фізичними особами).

СКЗІ «ІІТ ЦСК-1» призначено не тільки для використання у програмному забезпеченні «ІІТ ЦСК-1» t виробництва ПрАТ «Інститут інформаційних технологій», але й для вбудовування в прикладне програмне забезпечення інших виробників та для постачання кінцевим користувачам та забезпечує:

– Створення ключів електронного підпису за Наказ Міністерства юстиції України та Адміністрації Держспецзв'язку від 30.09.2020 № 140/614 " Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання кваліфікованих електронних довірчих послуг", зареєстрований в Міністерстві юстиції України 22 жовтня 2020 року за № 1093/35322[33];

– Хешування даних відповідно до алгоритму ДСТУ 7564:2014[32];

– Шифрування та імітозахист даних відповідно до алгоритму ДСТУ 28147-2009. Генерацію випадкових та псевдовипадкових чисел, сесійних ключів шифрування[34];

– Аутентифікацію та вироблення сесійного ключа під час передачі даних за протоколами SSL/TLS. Зберігання сертифікатів відкритих ключів безпосередньо у контейнері ключів;

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

Для здійснення функцій шифрування та перевірки електронного підпису криптопровайдер «ІІТ ЦСК-1» використовує відкритий ключ, який знаходиться в сертифікаті того користувача, якому адресовано зашифрований документ або від якого надійшов документ з електронним підписом. Для розшифрування та формування електронного підпису криптопровайдер використовує закритий ключ користувача, який здійснює дані операції (той ключ, який буде вказано самим користувачем). Процес передачі конфіденційного повідомлення Outlook схематично представлений нижче (рис 3.8).

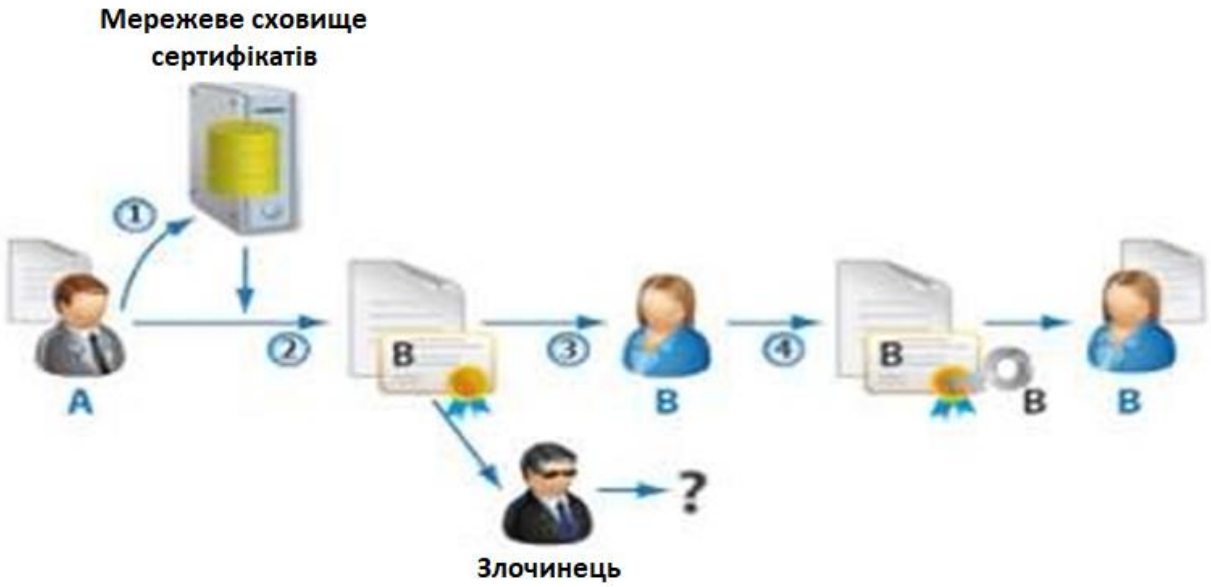


Рис. 3.8 Схема обміну захищеними документами

Користувачеві А необхідно передати користувачеві У конфіденційне повідомлення Outlook:

– Користувач А запитує з мережевого сховища сертифікат відкритого ключа користувача і зіставляє його з контактом В у програмі Outlook.

– А зашифровує документ із використанням відкритого ключа із

сертифіката В.

– А відправляє користувачеві до зашифрованого повідомлення.

– Розшифровує документ за допомогою свого закритого ключа.

– Таким чином користувач отримує конфіденційне повідомлення від користувача А.

Якщо повідомлення перехопить зловмисник, прочитати листа йому не вдасться, оскільки у нього немає закритого ключа користувача В. Якщо користувач В не зможе розшифрувати повідомлення, що надійшло від А, це означає, що лист був змінений сторонніми особами або пошкоджено в процесі пересилання. У цьому випадку може запросити у користувача А повторне відправлення повідомлення.

Процес формування та перевірки електронного підпису наведено на рис. 3.9.

Рис. 3.9 Процес формування та перевірки підпису документа

Користувачеві А необхідно завірити документ (наприклад, повідомлення Outlook) електронним підписом, щоб інші користувачі не змогли внести до нього зміни і кожен міг переконатися, що автор цього документа – користувач А;

– Користувач А підписує документ своїм закритим ключем

– А надсилає даний документ усім зацікавленим особам(Користувачі B, C і D) або викладає для загального доступу.

– Користувач B запитує в сховищі сертифікатів сертифікат відкритого ключа A.

– Перевіряє документ за допомогою відкритого ключа A,
котрий знаходиться у його сертифікаті.

СКЗІ «ІІТ ЦСК-1» призначено для роботи на комп'ютерах (стаціонарних, переносних або мобільних) з наступною конфігурацією, що рекомендується: процесор з архітектурою x86 або x86-64; ОЗУ – не менше 512 Мбайт; вільне місце на жорсткому диску – не менше ніж 100 Мбайт.

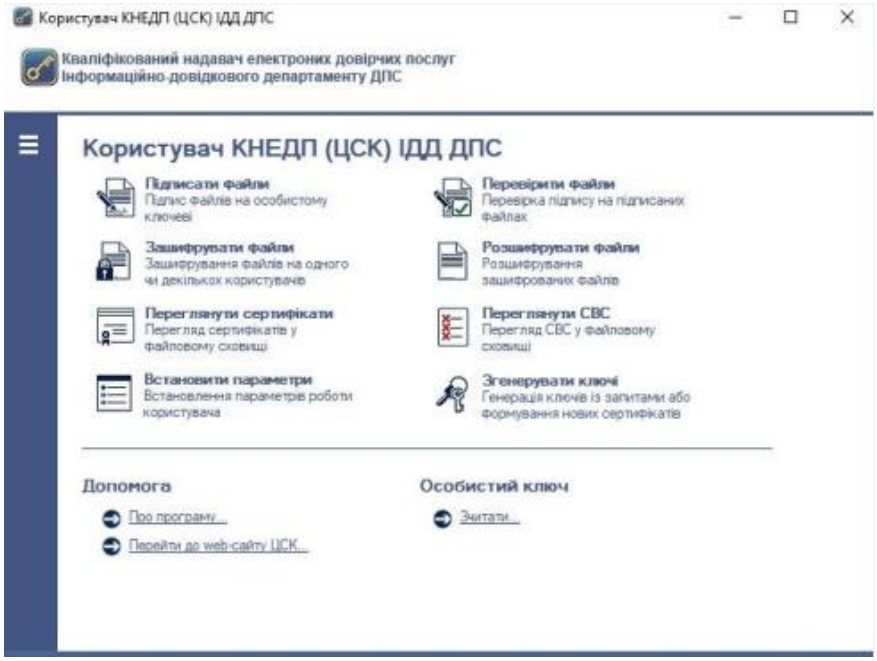


Рис. 3.10 Інтерфейс ІІТ ЦСК-1

3.4.3 Встановлення засобу виявлення вторгнень та антивірусу ManageEngine EventLog Analyzer

ManageEngine є провідним виробником рішень для моніторингу та управління IT-мережевою інфраструктурою. EventLog Analyzer є частиною продуктів безпеки компанії. Це HIDS , який зосереджений на управлінні та аналізі файлів журналів, створених стандартними програмами та операційними системами. Інструмент встановлюється на Windows Server або Linux . Він збирає дані з цих операційних систем, а також із систем Mac OS , IBM AIX , HP UX і Solaris . Журнали з систем Windows включають джерела з Windows Server Windows Vista і новіших версій і Windows DHCP Server.

Ключові риси:

– Керує та аналізує файли журналів

– Аудит на відповідність стандартам захисту даних

ManageEngine EventLog Analyzer фіксує, консолідує та зберігає повідомлення журналу з усіх частин вашої системи. Потім він шукає в цих записах ознаки хакерської діяльності або зловмисного програмного забезпечення. Пакет містить модуль звітності про відповідність.

Окрім операційних систем, сервіс збирає та консолідує журнали з баз даних Microsoft SQL Server і Oracle . Він також може передавати сповіщення від ряду антивірусних систем, зокрема Microsoft Anti-malware , ESET , Sophos , Norton , FireEye , Malwarebytes , McAfee та Symantec . Він збиратиме журнали з веб-серверів, брандмауерів, гіпервізорів, маршрутизаторів, комутаторів і сканерів мережевих вразливостей .

EventLog Analyzer збирає повідомлення журналу та працює як файл-сервер журналу, упорядковуючи повідомлення у файли та каталоги за джерелом повідомлення та датою. Термінові попередження також пересилаються на інформаційну панель EventLog Analyzer і можуть бути передані в системи служби підтримки як квитки, щоб викликати негайну увагу техніків. Рішення про те, які події є потенційним порушенням безпеки, приймається модулем аналізу загроз , вбудованим у пакет.

Послуга включає автоматичний пошук журналів і кореляцію подій для складання регулярних звітів про безпеку. Серед цих звітів є формат моніторингу та аудиту привілейованих користувачів (PUMA) і різноманітні формати, необхідні для демонстрації відповідності стандартам PCI DSS , FISMA , ISO 27001 , GLBA , HIPAA , SOX і GDPR

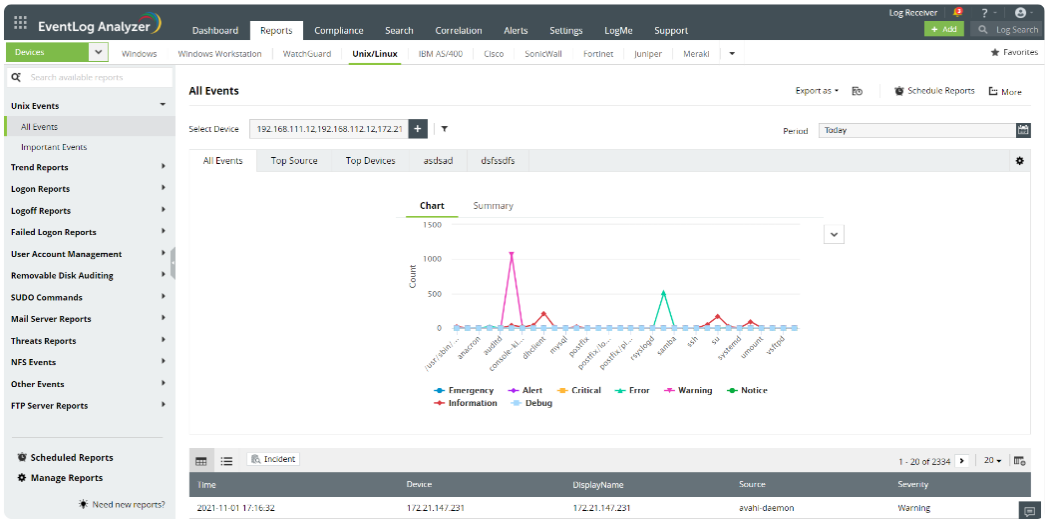


Рис. 3.11 Інтерфейс ManageEngine EventLog Analyzer

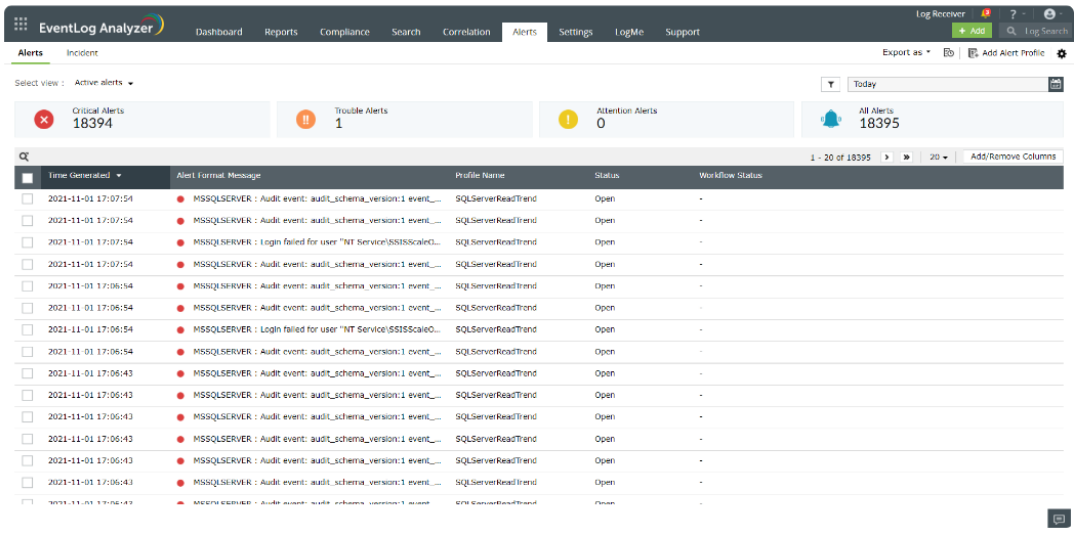


Рис. 3.12 Інтерфейс ManageEngine EventLog Analyzer

ESET Internet Security

Список можливсотей ESET Internet Security:

– Антивірус та антишпигунське ПЗ;

– Брандмауер.Запобігає несанкціонованого доступу до вашого комп'ютера і ми використання вашого особисті дані. Антивірус та антишпигун.

Швидкий та ефективний сканер, що поєднує антивірус та антишпигун, виявляє та знешкоджує шкідливе програмне забезпечення.

– Блокувальник експлойтів. Блокує атаки, спеціально розроблені для обходу антивірусної, захищає від атак на веб-браузери, програми для читання PDF;

– Сканувати під час завантаження файлів;

– Керування пристроями. Запобігає несанкціонованому копіюванню ваших даних. Дозволяє блокувати пристрої зчитування компакт-дисків, DVD-дисків, USB-накопичувачів та дискових накопичувачів, а також пристрої що підключається через Bluetooth;

– Антиспам електронної пошти.

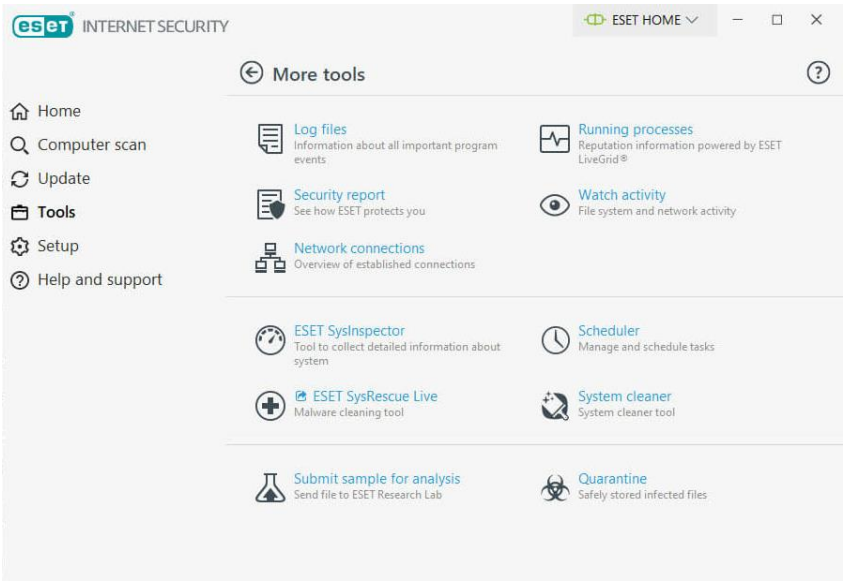


Рис. 3.13 Інтерфейс Eset Internet Security

3.5 Аналіз ризиків після встановлення рекомендованого ПЗ

Таблиця 3.4

Рекомендаційне ПЗ

№	Загроза	Рекомендаційне ПЗ
1	Крадіжка паролів	UserGate Proxy
2	Крадіжки, модифікації, знищення інформації.	UserGate Proxy «ІІТ ЦСК-1»
3	Несанкціоноване відключення засобів захисту	UserGate Proxy
4	Дії шкідливих програм (вірусів)	ManageEngine EventLog Analyzer
5	Недекларовані можливості ПЗ	Сетрифіковане ПЗ

Прожовження Таблиця 3.4

6	Установка ПЗ не пов'язаного з виконанням обов'язків	Windows
7	Ненавмисна модифікація (знищення) інформації співробітниками	UserGate Proxy «ІІТ ЦСК-1»
8	Розголошення інформації, модифікація, знищення співробітником	«ІІТ ЦСК-1»
9	Загрози віддаленого запуску додатків.	- UserGate Proxy - ManageEngine EventLog Analyzer
10	Перехоплення в межах контрольованої зони	«ІІТ ЦСК-1»

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	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%

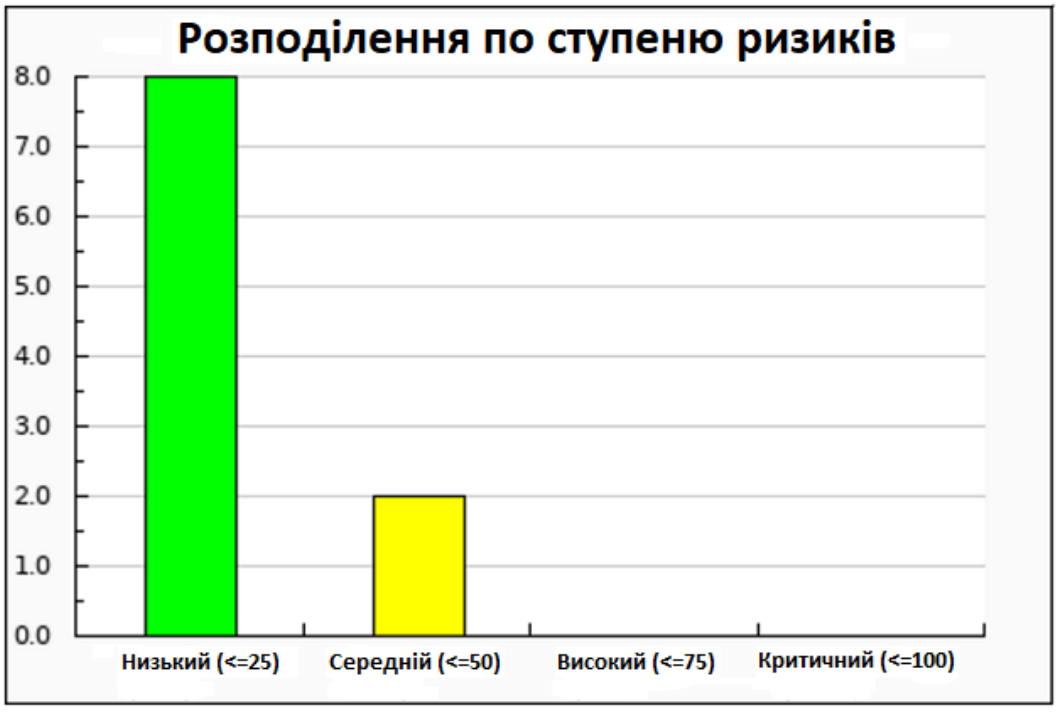


Рис. 3.14 Графік розподілення по ступеню ризику

Рис. 3.15 Матриця ризиків

Для нагляднішої результуту проведеної роботи, виконаємо порівняльний аналіз ризиків до провадження системи захисту інформації і після, за формулою.

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

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 якого є показник від 0.25 де 1, де 0.25 мінімальний можливий рівень ймовірності витоку інформації через відомі ризики і її наслідки для підприємства, а 1 максимальний критичний рівень.

Розрахуємо показник для підприємства до введення переліку рекомендаційного ПЗ.

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

Після введеня в роботу ПЗ захисту інформації.

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

Виходячи з розрахунків при встановлені рекомендованих програмно-апаратних засобів, а саме:

- Міжмережевого екрану UserGate Proxy & Firewall 6.5
- Криптопровайдера «ІІТ ЦСК-1»
- Засобу виявлення вторгнень ManageEngine EventLog Analyzer
- Анттивірус ESET Internet Security

Ми змогли зменшили показник рівня можливості втрати, витоку, ябо модифікації інформації на 15 пунктів з 0.45 до 0.3, тобто на 33 % відносно початкових показників.

3.6 Висновки по третього розділу

1. Проаналізовано склад інформації що підлягає захисту в локальній комп’.терній мережі, а також можливі канали її витоку. Проведено оцінку рівня критичності даних загроз.

3. Розглянуто і проаналізовано програмно-апаратні засоби захисту від несанкціонованого доступу.

3. Розроблено рекомендаційний список програмно-апаратних засобів для захисту персональних даних ввід витоку, кардіжки або мржифікації в локальній мережі підприємства.

4. Проведено аналіз рівню захисту локальної мережі, після впровадження рекомендаційних програмно - апаратних засобів.

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи були виконані наступні задачі:

- Проведено огляд процесу обробки конфіденційних даних в локальних комп'ютерних мережах.

- Проаналізовано методи захисту інформації в локальній комп'ютерній мережі від несанкціонованого доступу до конфіденційних даних.

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

1. У першому розділі кваліфікаційної роботи розглянуто проблеми захисту конфіденційних даних в локальній мережі від несанкціонованого викрадення, витоку або модифікації. Проведено аналіз шляхів несанкціонованого доступу до інформації, а також основні канали витоку інформації під час її обробки. Визначено види шкідливо програмного забезпечення яке може бути використано для несанкціонованого доступу до інформації.

2. У другому розділ проведено аналіз системи захисту інформації, та заходів від несанкціоновано доступу до неї. Розглянуто способи ідентифікація та автентифікація які використвуються для фізичного і програмного захисту даних, в локальній мережі підприємства. Подано способи програмного виявлення мережевих вторгення в інформаційню систему підприємства, і також протоколювання та аудит, що допомагають реконструювати послідовності подій під час вторгнення, знайти винуватця вторгнення, оцінити масштаби завданих збитків та повернутися до нормальної роботи.

3. У третьому розіділі проведено аналіз та сформований список інформації на підприємтсві що підлягає захисту, а також загрози які можуть спричинити витік або втрату даних. Проведено оцінку рівня ризику для даних загроз.

Розроблено рекомендаційний список програмних засобів для захисту конфіденційних даних, відносно загроз які були виявлені на підприємстві. Проведено аналіз рівню захисту локальної мережі, після впровадження в систему захисту рекомендаційних програм.

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. C. 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-ediREEP.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 InspecREEP 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.

34. ДСТУ ГОСТ 28147:2009 Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89 [Електронний ресурс]. – 2008. – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=55943.Білявський Г. О., Падун М. М., Фурдуй Р. С. Основи загальної екології. — К.: Либідь. 1995 — 368 с.

35. Білявський Г. О., Фурдуй Р. С. Практикум із загальної екології. // Навч. посібн.— К.:Либідь, 1997.—160с.

36. Волошин І. М. Методика дослідження проблем природокористування. — Львів: ЛДУ, 1994. — 160 с.

37. Екологічний словник: Навч. посібник /В.В.Прежко та ін. – Харків: ХДАМГ, 1999. – 416 с.

38. Екологія і закон: Екологічне законодавство України. У 2-х кн./ Відповідальний редактор док. юрид. наук, професор, акад. Андрейцев В. А. — К.: Юрінком їнтер, 1997. — 704 с.

39. Злобін Ю.А. Основи екології.- К.: Лібра, 1998. – 249.

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

Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»

СИСТЕМА ЗАХИСТУ ДОДАТКІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ POSITIVE TECHNOLOGIES APPLICATION FIREWALL

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Руслан САД

Керівник: к.т.н., проф. Олександр ДРОБИК

Київ - 2025

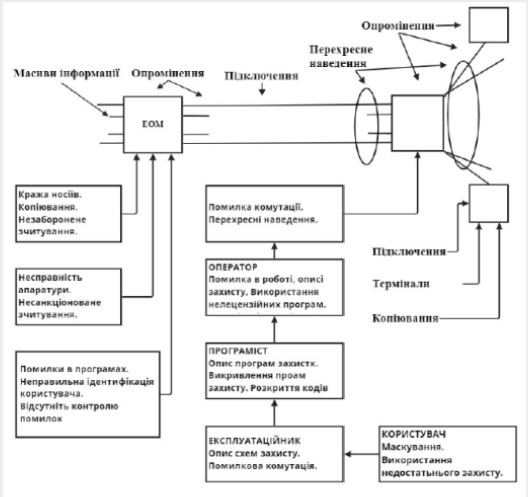
АКТУАЛЬНІСТЬ, МЕТА, ОБ’ЄКТ І ПРЕДМЕТ ДОСЛІДЖЕННЯ

- Актуальність теми визначається необхідністю захисту локальної комп’ютерної мережі від несанкціонованого доступу до конфіденційних і персональних даних.
- Мета роботи - підвищення рівня захищеності локальної комп’ютерної мережі шляхом застосування програмних застосунків і програмно-апаратних засобів захисту.
- Об’єкт дослідження - процес обробки конфіденційних даних у локальній комп’ютерній мережі комерційного підприємства.
- Предмет дослідження - захист конфіденційних даних у локальній комп’ютерній мережі.
- Основний акцент зроблено на практичних рекомендаціях щодо використання Positive Technologies Application Firewall та супутніх засобів захисту.

ОСНОВНІ ЗАВДАННЯ ТА СТРУКТУРА РОБОТИ

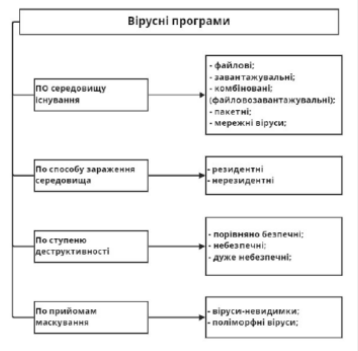
- Провести огляд процесу обробки конфіденційних даних у локальних комп’ютерних мережах та визначити канали несанкціонованого доступу.
- Проаналізувати способи, заходи та сервіси захисту інформації в локальній мережі.
- Дослідити склад інформації, що підлягає захисту на підприємстві, та оцінити актуальні ризики.
- Обґрунтувати перелік програмно-апаратних засобів: міжмережевий екран, криптопровайдер, засіб виявлення вторгнень і антивірус.
- Порівняти рівень ризиків до та після впровадження рекомендованих засобів.

ПРОЦЕС ОБРОБКИ КОНФІДЕНЦІЙНИХ ДАНИХ У ЛКМ



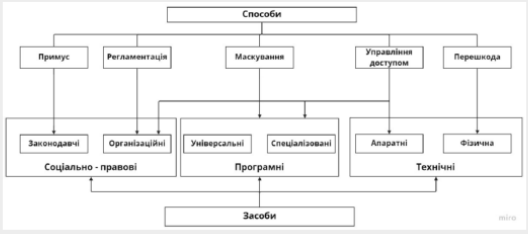
- Локальна комп’ютерна мережа використовується для зберігання, обробки та передавання персональних і службових даних підприємства.
- Несанкціонований доступ може бути прямим - із фізичним доступом до елементів мережі, або непрямим - через мережеві канали та програмні вразливості.
- До загроз належать перехоплення електромагнітних випромінювань, копіювання носіїв, вхід під зареєстрованим користувачем, використання недоліків ОС і програм.
- Захист повинен забезпечувати конфіденційність, цілісність і доступність даних.

КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ ТА РУЙНІВНІ ПРОГРАМНІ ЗАСОБИ



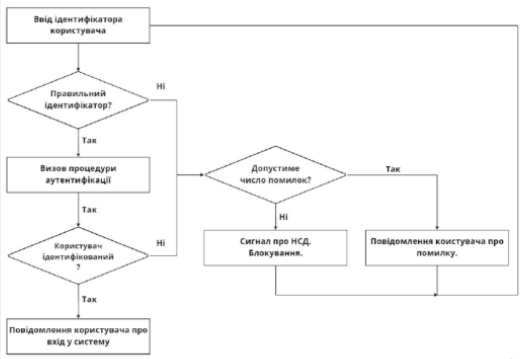
- У роботі виокремлено акустичні, матеріально-речові, візуально-оптичні, електромагнітні, електричні та індукційні канали витоку інформації.
- Окрему загрозу становлять віруси, троянські програми, мережеві черв’яки та засоби проникнення у віддалені системи.
- Застосування програмних засобів для НСД потребує обов’язкового антивірусного контролю, журналювання подій і виявлення аномальної активності.
- Протидія повинна поєднувати організаційні, технічні та програмні заходи.

СПОСОБИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ЛКМ



- Система захисту інформації включає організаційні, інженерні, програмні та апаратні засоби, спрямовані на запобігання НСД.
- Основні способи захисту: перешкода, управління доступом, маскування, регламентація та примус.
- Криптографічні перетворення застосовуються для захисту інформації під час передавання незахищеними каналами зв’язку.
- Організаційні заходи охоплюють режим доступу, посадові інструкції, порядок роботи з конфіденційною інформацією та відповідальність персоналу.

ІДЕНТИФІКАЦІЯ, АВТЕНТИФІКАЦІЯ ТА АВТОРИЗАЦІЯ



- Першим кроком захисту ресурсів локальної мережі є перевірка ідентичності користувача.
- Автентифікація підтверджує, що користувач є саме тим суб’єктом, за якого себе видає.
- Після автентифікації система визначає повноваження користувача та виконує контроль доступу до ресурсів.
- Для підвищення безпеки доцільне застосування двофакторної або багатофакторної автентифікації.

ОЦІНКА РИЗИКІВ ДО ВПРОВАДЖЕННЯ ЗАСОБІВ ЗАХИСТУ

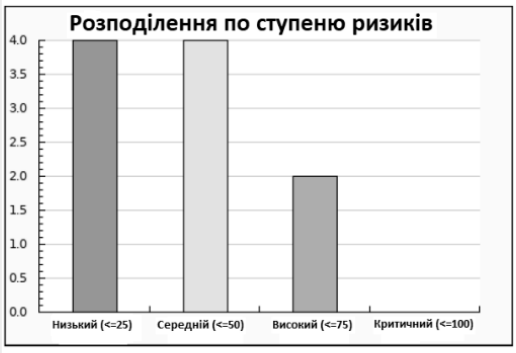
Початковий стан

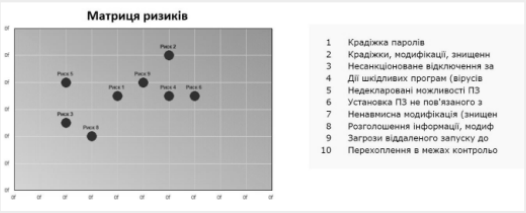
- Крадіжка паролів - рівень ризику 28.
- Крадіжка, модифікація або знищення інформації - 60.
- Дії шкідливих програм - 42.
- Перехоплення в межах контрольованої зони - 60.

Висновки аналізу

- 40 % ризиків мають низький рівень.
- 40 % ризиків мають середній рівень.
- 20 % ризиків мають високий рівень.
- Необхідне доопрацювання периметрового, криптографічного та антивірусного захисту.

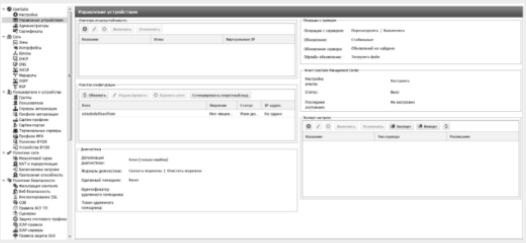
ВІЗУАЛІЗАЦІЯ ПОЧАТКОВОГО РІВНЯ РИЗИКІВ





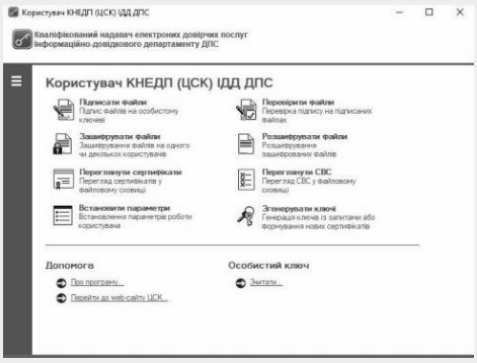
- Побудована діаграма показує розподіл ризиків за рівнями критичності до впровадження рекомендованих засобів.
- Матриця ризиків демонструє наявність загроз у середній та високій зонах, що потребує додаткових заходів захисту.
- Першочерговими напрямами визначено захист мережевого периметра, криптографічний захист та контроль шкідливої активності.
- Оцінка ризиків використана як основа для підбору програмно-апаратних комплексів.

ЗАСТОСУВАННЯ МІЖМЕРЕЖЕВОГО ЕКРАНУ USERGATE PROXY & FIREWALL



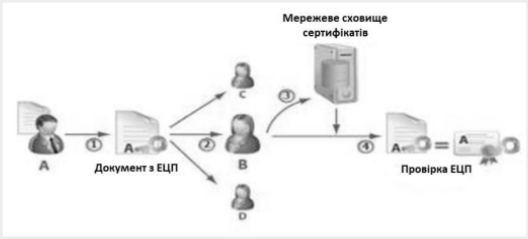
- Міжмережевий екран призначено для фільтрації вхідного та вихідного трафіку, захисту периметра і контролю доступу до мережевих ресурсів.
- UserGate Proxy & Firewall забезпечує облік трафіку, політики доступу до Інтернету, контроль швидкості та обмеження мережевої активності користувачів.
- Засіб дозволяє налаштовувати мережеві зони, правила фільтрації, VPN-доступ і параметри безпечної міжмережевої взаємодії.
- Впровадження міжмережевого екрану знижує ризики віддаленого запуску додатків, несанкціонованих підключень та нецільового використання мережі.

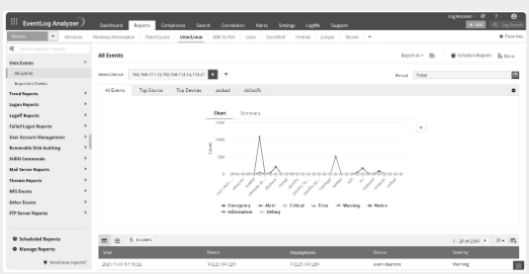
КРИПТОГРАФІЧНИЙ ЗАХИСТ ДАНИХ І КРИПТОПРОВАЙДЕР ІІТ ЦСК-1



- Криптографічний захист застосовується для забезпечення конфіденційності, цілісності та справжності інформації під час її зберігання і передавання.
- Криптопровайдер ІІТ ЦСК-1 підтримує формування ключів електронного підпису, шифрування, імітозахист і роботу з сертифікатами відкритих ключів.
- Засіб може використовуватись для захисту персональних, службових і комерційних даних, що не становлять державної таємниці.
- Схема обміну захищеними документами забезпечує можливість передавання конфіденційних повідомлень між користувачами.

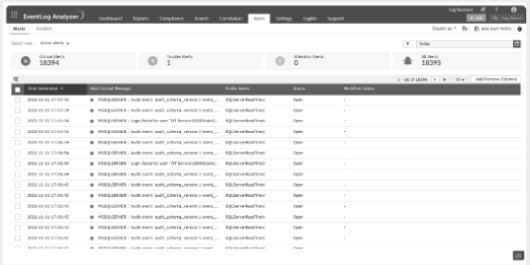
ПІДПИС ДОКУМЕНТІВ, ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА ЖУРНАЛЮВАННЯ

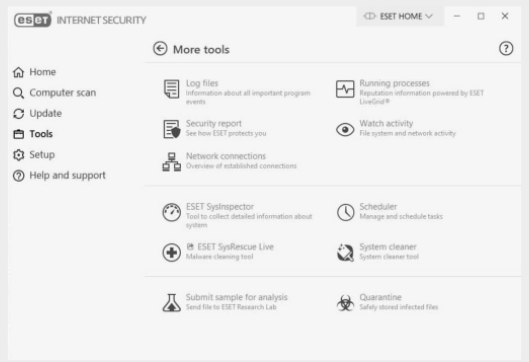




- Електронний підпис дозволяє підтвердити авторство документа та виявити несанкціоновані зміни після підписання.
- ManageEngine EventLog Analyzer виконує збір, консолідацію та аналіз журналів подій із серверів, робочих станцій, мережевого обладнання та систем безпеки.
- Система забезпечує аудит, кореляцію подій, формування звітів і оперативне виявлення ознак інцидентів інформаційної безпеки.
- Поєднання журналювання, аналізу подій і електронного підпису підвищує контрольованість процесів обробки конфіденційних даних.

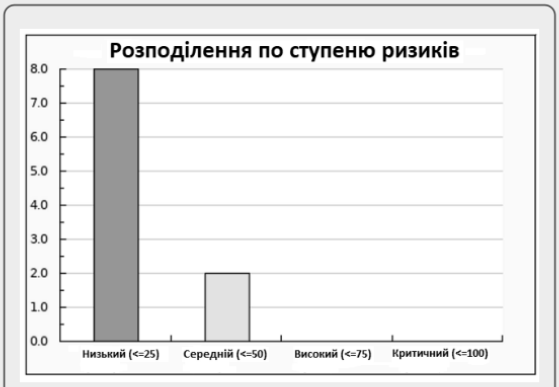
АНТИВІРУСНИЙ ЗАХИСТ ТА КОНТРОЛЬ КІНЦЕВИХ ПРИСТРОЇВ

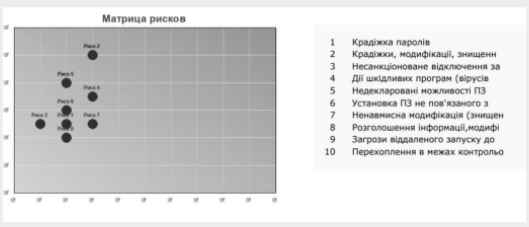




- ESET Internet Security забезпечує антивірусний і антишпигунський захист, роботу брандмауера, блокування експлойтів та контроль підключених пристроїв.
- Антивірусне ПЗ знижує ризик зараження шкідливими програмами та несанкціонованого копіювання конфіденційних даних.
- Журнали подій і сповіщення безпеки дозволяють відстежувати активність кінцевих пристроїв і швидко реагувати на відхилення.
- Комплексне застосування ESET і EventLog Analyzer забезпечує додатковий рівень захисту локальної мережі.

РЕЗУЛЬТАТИ АНАЛІЗУ РИЗИКІВ ПІСЛЯ ВПРОВАДЖЕННЯ ЗАХИСТУ





- Після впровадження рекомендованих засобів більшість ризиків перемістилася до низького рівня.
- За підсумками розрахунків частка низьких ризиків збільшилася до 80 %, а високі ризики були мінімізовані.
- Рівень можливості втрати, витоку або модифікації інформації зменшено з 0,45 до 0,30.
- Загальне зниження інтегрального показника ризику становить приблизно 33 % відносно початкового рівня.

ВИСНОВКИ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

- Проведено огляд процесу обробки конфіденційних даних у локальних комп’ютерних мережах та визначено основні канали НСД.
- Проаналізовано методи захисту інформації: управління доступом, ідентифікація, автентифікація, протоколювання, криптографія та IDS.
- Для підприємства ТОВ «REEP» сформовано перелік інформації, що підлягає захисту, та проведено оцінку актуальних ризиків.
- Рекомендовано впровадити UserGate Proxy & Firewall 6.5, криптопровайдер ІІТ ЦСК-1, ManageEngine EventLog Analyzer та ESET Internet Security.
- Розроблений комплекс заходів підвищує рівень захищеності локальної мережі та знижує ризики витоку, втрати або модифікації інформації.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Руслан САД

Тема: «Система захисту додатків від несанкціонованого доступу»

Київ - 2025