Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система комплексного антивірусного захисту локальної обчислювальної мережі філії "Ощадбанку" м. Хмельницький
Назва теми

КРКБ 190105.19.01.06 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 125 «Кібербезпека»
Шифр, назва

Освітня програма «Кібербезпека»
Назва

Виконав: студент IV курсу, група КБ-19-1 КБм 07.06.23 Б.В. Кальчун
Підпис Ініціали, прізвище

Керівник 7.06.2023 В.М. Джулій
Підпис, дата Ініціали, прізвище

Нормоконтролер 7.06.23 С.В. Мостовий
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки Ю.П. Кльоц
Підпис Ініціали, прізвище

«7» 06 2023 р.

Хмельницький 2023

Форма	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1	КРКБ.190105.19.01.06 ПЗ	Система комплексного	62	
				антивірусного захисту		
				локальної		
				обчислювальної мережі		
				філії «Ощадбанку»		
				м.Хмельницький		
				Пояснювальна записка		
А4		2	КРКБ. 190105.19.01.06 Е8	Схема алгоритму	1	
				спрацьовування антивірусу		
				на небезпечне ПЗ		
А4		3	КРКБ. 190105.19.01.06 Е8	Логічна топологія	1	
				локальної мережі банку		
А4		4	КРКБ. 190105.19.01.06 Е8	Загальна схема принципу	1	
				роботи системи		
				комплексного		
				антивірусного захисту		

Зм.	Арк.	№ Докум.	Підп.	Дата	КРКБ.190105.19.01.06 ВП		
Розробив		Кальчун Б.В.		7.06.23	Система комплексного антивірусного захисту локальної обчислювальної мережі філії “Ощадбанку” м.Хмельницький Відомість проєкту	Літера	Аркуш	Аркушів
Перев.		Джулій В.М.		7.06.23		н	1	1
Н. контр.		Мостовий С.В.		7.06.23		ХНУ, КБ-19-1		
Затв.		Кльоц Ю.П.		7.06.23				

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"1" 03 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кальчун Б.В.

Прізвище, ім'я, по батькові студента

Тема роботи Система комплексного антивірусного захисту локальної обчислювальної мережі філії "Ощадбанку" м. Хмельницький

Керівник роботи к.т.н., доц. Джулій В.М.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 01 березня 2023р. №5

2. Строк подання студентом роботи на кафедру 01 червня 2023р.

3. Вихідні дані до проекту (роботи) спроектувати та реалізувати комплексну систему антивірусного захисту локальної обчислювальної мережі. Передбачити захист від можливих вірусних загроз. Вдосконалити існуючі системи антивірусного захисту. Вибрати програмне забезпечення (обґрунтувати вибір програмного забезпечення за критеріями забезпечення безпеки в тих чи інших сферах) для захисту локальної мережі від вірусного програмного забезпечення. Створити комплексну антивірусну з урахуванням особливостей філії «Ощадбанку» м.Хмельницький

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз предметної області антивірусного захисту. Тестування актуальних засобів антивірусного захисту. Реалізація системи комплексного антивірусного захисту локальної обчислювальної мережі. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень): «Схема алгоритму спрацьовування антивірусу на небезпечне ПЗ», «Логічна топологія локальної мережі банку», «Загальна схема принципу роботи системи комплексного антивірусного захисту».

6. Консультанти розділів курсового проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання

7. Дата видачі завдання 01 березня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів проекту (роботи)	П
1	Аналіз предметної області	Січень	-
2	Пошук теоретичної інформації про антивірусний захист	Січень	-
3	Дослідження існуючих вірусних загроз та методів захисту від них	Лютий	-
4	Постановка задачі	Лютий	-
5	Аналіз теоретичної інформації про антивірусний захист та сучасні методи забезпечення антивірусної безпеки	Березень	-
6	Початок тестування та аналізу сучасного антивірусного програмного забезпечення	Квітень	-
7	Завершення створення системи комплексного антивірусного захисту	Квітень\Травень	-
8	Оформлення пояснювальної записки згідно вимог	Травень	-
9	Оформлення графічної частини	Червень	-
10	Захист КР	09.06.2023	

Студент _____ Кальчук Б.В.
Підпис Ініціали, прізвищ

Керівник проекту (роботи) _____ Джуні
Підпис Ініціали, прізвищ

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система комплексного антивірусного захисту локальної обчислювальної мережі філії “Ощадбанку” м. Хмельницький».

Автор роботи: Кальчун Богдан Володимирович.

Керівник роботи: Джулій Володимир Миколайович.

Пояснювальна записка: 62 с., 1 додаток, 48 рис., 40 джерел.

Графічна частина: 8 презентаційних слайдів.

СИСТЕМА КОМПЛЕКСНОГО АНТИВІРУСНОГО ЗАХИСТУ, СИСТЕМА ЗАХИСТУ ЛОКАЛЬНОЇ ВІД ВІРУСНИХ ЗАГРОЗ, БЕЗПЕКА ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ.

Мета даної роботи полягає у створенні системи комплексного антивірусного захисту локальної обчислювальної мережі

Для досягнення цієї мети було здійснено дослідження предметної області, проаналізовано теоретичну інформацію про проектування системи комплексного антивірусного захисту, а також створено і розроблену таку систему, яка дозволяє запобігти небезпеки від різного роду загроз. Для досягнення цих цілей використовувалися різноманітні технології, такі як спеціалізоване програмне забезпечення, спеціальне налаштування програмного забезпечення, створення відповідних правил мережевого екрану. Постійний моніторинг стану безпеки локальної мережі та планування заходів з її покращення дозволяє забезпечити надійний захист локальної мережі від небезпечного програмного забезпечення та мережевих атак.

ння прийн

Приміт

Б.В.
ли, прізвище

ли, прізвище

07.06.2023

ANNOTATION

The topic of the qualification work: "System of comprehensive anti-virus protection of the local computer network of the branch of "Oschadbank" in Khmelnytskyi".

Author of the work: Kalchun B.V.

Head of work: Juliy V. M.

Explanatory note: 62 pp., 1 appendix, 48 figures, 40 sources.

Graphic part: 8 presentation slides.

COMPREHENSIVE ANTI-VIRUS PROTECTION SYSTEM, LOCAL VIRUS THREAT PROTECTION SYSTEM, LOCAL COMPUTER NETWORK SECURITY.

The purpose of this work is to create a system of complex antivirus protection of a local computer network

To achieve this goal, a study of the subject area was carried out, theoretical information about the design of a complex antivirus protection system was analyzed, and a system was created and developed that allows you to prevent danger from various types of threats. A variety of technologies were used to achieve these goals, such as specialized software, custom software customization, and creation of appropriate network firewall rules. Constant monitoring of the state of security of the local network and planning of measures to improve it allows to ensure reliable protection of the local network against dangerous software and network attacks.

07.06.2023

ЗМІСТ

ВСТУП 3
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ АНТИВІРУСНОГО ЗАХИСТУ 5
1.1 Аналіз предметної області анивірусного захисту 5
1.2 Аналіз вірусних програм 12
1.3 Постановка задачі 17
2 ТЕСТУВАННЯ АКТУАЛЬНИХ ЗАСОБІВ АНТИВІРУСНОГО ЗАХИСТУ 20
2.1 Вибір та налаштування віртуальної машини 20
2.2 Тестування ативірусів 23
2.2.1 Тестування ативірусу Avast 23
2.2.2 Тестування ативірусу Avg 29
2.2.3 Тестування ативірусу Avira 34
2.2.4 Тестування ативірусу Windows Defender 37
2.3 Аналіз результатів тестувань 40
3 РЕАЛІЗАЦІЯ СИСТЕМИ КОМПЛЕКСНОГО АНТИВІРУСНОГО ЗАХИСТУ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ 42
3.1 Проектування планну приміщення та мережі 42
3.2 Дії при виявленні вірусів 47
3.3 Створення системи комплексного антивірусного захисту локальної обчислювальної мережі 48
ВИСНОВКИ 57
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 58
ДОДАТОК А Копія графічної частини 63

ВСТУП

У сучасному світі, коли майже кожен аспект нашого життя пов'язаний з використанням комп'ютерів та Інтернету, захист від комп'ютерних вірусів та інших шкідливих програм є надзвичайно важливим завданням. Антивірусний захист є ключовим елементом цього процесу та допомагає забезпечити безпеку користувачів та їх даних.

Моя дипломна робота присвячена вивченню основних принципів роботи антивірусного захисту, а також аналізу сучасних методів захисту від шкідливих програм. У моїй роботі будуть досліджені такі аспекти антивірусного захисту, як евристичний аналіз, робота з вірусними базами даних, захист від шкідливих програм через використання поведінкового аналізу та багато іншого.

Під час написання роботи я ретельно вивчив сучасні технології та методи захисту від шкідливих програм та вивчив основні вимоги до безпечної роботи з комп'ютерами та мережами. Я також провів ретельний аналіз інформації про різні види вірусів та шкідливих програм, що допомогло мені зрозуміти, як вони працюють та як можна запобігти їхньому впливу на користувача.

У моїй дипломній роботі я також розгляну різні види антивірусного програмного забезпечення та їхні функції, а також проведу огляд деяких з найкращих антивірусних програм на ринку. Також я проведу дослідження ефективності деяких методів захисту від шкідливих програм та порівняю їх.

Окрім цього, у роботі буде враховано такі важливі аспекти, як антивірусний захист на різних платформах, включаючи комп'ютери, мобільні пристрої та планшети. Я розгляну також важливість регулярного оновлення антивірусного програмного забезпечення та його належної конфігурації для ефективного захисту від нових загроз.

Нарешті, я також досліджуватиму роль користувачів у забезпеченні

безпеки своїх комп'ютерів та мереж. Я розгляну різні аспекти поведінки користувачів, які можуть сприяти зараженню комп'ютерів вірусами та іншими шкідливими програмами, та розгляну рекомендації щодо зменшення ризиків.

Усі ці аспекти допоможуть збільшити розуміння важливості антивірусного захисту та допоможуть користувачам забезпечити безпеку своїх даних та пристроїв.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ АНТИВІРУСНОГО ЗАХИСТУ

1.1 Аналіз предметної області анивірусного захисту

Антивірусний захист [1] - це процес захисту комп'ютерної системи від шкідливого програмного забезпечення, яке може завдати шкоди пристрою, викрасти конфіденційну інформацію, поширюватися на інші системи або використовуватися для злочинних дій.

Предметна область антивірусного захисту [2] досить широка і охоплює наступні аспекти:

- методи виявлення інфікованої програми;
- методи блокування шкідливих програм;
- методи видалення інфікованого програмного забезпечення;
- методи захисту від вразливостей;
- методи захисту від атак на мережу;
- системи автоматизованого управління захистом;

Розглянемо дані методи більш детально.

Методи виявлення інфікованих програм можуть включати сигнатурний аналіз, поведінковий аналіз або гібридний підхід, який комбінує ці дві стратегії. Давайте розглянемо кожен з цих методів докладніше.

Сигнатурний аналіз [3] - цей метод використовує бази даних з відомими сигнатурами шкідливих програм. Сигнатура - це унікальний ідентифікатор або характеристика, яка вказує на наявність певного типу віруса або шкідливої програми. Антивірусна програма порівнює сигнатури з файлами або програмами на комп'ютері, і якщо знаходить відповідність, вона визначає файл як інфікований. Оновлення баз даних сигнатур є важливим аспектом цього методу, оскільки нові віруси постійно з'являються.

Поведінковий аналіз [4] - цей метод спирається на спостереження та аналіз поведінки програми. Замість того, щоб шукати конкретні сигнатури, антивірусна програма аналізує активності програми, її взаємодію з системою та

зміни, які вона вносить. Якщо програма виявляє ненормальну або підозрілу поведінку, вона може визначити її як потенційно шкідливу. Поведінковий аналіз дозволяє виявляти нові, раніше невідомі віруси та шкідливі програми.

Гібридний підхід [5] – даний метод комбінує як сигнатурний аналіз, так і поведінковий аналіз для більш ефективного виявлення інфікованих програм. Він використовує сигнатурний аналіз для швидкого виявлення відомих загроз та поведінковий аналіз для виявлення нових та невідомих загроз. Гібридний підхід поєднує переваги обох методів, дозволяючи швидко розпізнавати відомі віруси за їх сигнатурами та одночасно виявляти різноманітні нові загрози, аналізуючи їх поведінку.

Цей підхід також може включати додаткові технології, такі як евристичний аналіз, машинне навчання та штучний інтелект, для поліпшення точності виявлення загроз. Наприклад, машинне навчання може використовуватись для створення моделей, які виявляють нові паттерни або аномалії, що вказують на наявність шкідливих програм.

Розглянемо методи блокування блокування шкідливих програм[6]. Є такі основні методи блокування шкідливих програм:

- аналіз системних викликів;
- перехоплення мережевих пакетів;
- використання віртуальних машин;

Аналіз системних викликів полягає в моніторингу та аналізі системних викликів, які виконуються програмами. Кожна операційна система має набір системних викликів [7], які програми використовують для взаємодії з операційною системою. Антивірусна програма може перехоплювати ці виклики та аналізувати їх параметри, щоб виявити підозрілу або небезпечну активність. Якщо виявлено шкідливі дії, програма може заблокувати виконання цих системних викликів та запобігти пошкодженню системи.

Перехоплення мережевих пакетів використовується для виявлення та блокування шкідливого мережевого трафіку. Антивірусна програма може

перехоплювати мережеві пакети, які надходять або відправляються комп'ютером, і аналізувати їх. Вона може порівнювати їх з базою відомих шкідливих пакетів або виявляти підозрілі шаблони та аномалії у мережевому трафіку. При виявленні шкідливих пакетів програма може блокувати їх передачу або сповіщати користувача про потенційну загрозу.

Використання віртуальних машин полягає в запуску програм у віртуальному середовищі або віртуальній машині[8], що імітує операційну систему. Віртуальна машина надає ізольоване середовище, в якому можна виконувати потенційно небезпечні програми без ризику пошкодження основної системи. Антивірусна програма використовує віртуальні машини для аналізу поведінки програми і виявлення підозрілих або шкідливих дій. Віртуальне середовище дозволяє антивірусній програмі спостерігати, як програма взаємодіє з операційною системою, файловою системою, мережею та іншими компонентами. Якщо програма виявляє підозрілу або небезпечну активність, вона може блокувати або ізолювати цю програму від основної системи, щоб запобігти пошкодженню.

Ці методи, такі як аналіз системних викликів, перехоплення мережевих пакетів і використання віртуальних машин[9], можуть бути поєднані і використовуватися в антивірусних програмах як частини комплексного підходу до блокування шкідливих програм та забезпечення високої безпеки комп'ютерної системи.

Методи видалення інфікованого програмного забезпечення включають в себе такі методи[10]:

- автоматична процедура;
- ручна процедура;
- комбінований підхід;

Автоматична процедура є в більшості сучасних антивірусних програм. Після виявлення інфікованого файлу або програми антивірусний програмний засіб автоматично виконує процедуру видалення. Вона може включати

карантин, видалення файлів, виправлення або видалення пошкоджених компонентів програми, а також видалення посилань на шкідливе програмне забезпечення з системних файлів або реєстру.

Ручна процедура використовується у деяких випадках, наприклад, якщо інфіковані файли вже завдали значної шкоди, або їх складно видалити. Це може вимагати спеціалізованих інструментів або знань. Ручне видалення може включати видалення файлів та ключів реєстру, прибирання запусків програм з автозапуску, видалення додаткових компонентів або виправлення налаштувань системи, які можуть бути пошкоджені.

Важливо пам'ятати, що видалення інфікованого програмного забезпечення може бути складним процесом[11], особливо якщо шкідлива програма має високий рівень впливу на систему або використовує складні методи приховування. У деяких випадках може бути необхідно звернутися до професіоналів з безпеки комп'ютерів або сканерів шкідливих програм для отримання допомоги.

У сучасному світі антивірусний захист стає все більш важливим, оскільки зростає кількість шкідливого програмного забезпечення, яке може завдати шкоди користувачам та компаніям. Компанії, які працюють в галузі антивірусного захисту, зазвичай розробляють інноваційні технології, щоб бути ефективними проти нових загроз. Такі технології включають в себе машинне навчання, штучний інтелект, аналіз великих даних та інші.

Для користувачів антивірусний захист є важливим аспектом безпеки комп'ютера або мобільного пристрою[12]. Багато компаній пропонують різноманітні продукти антивірусного захисту, які можуть бути безкоштовними або платними. Такі продукти зазвичай включають в себе антивірусні програми, мережеві фаєрволи, захист від шкідливих посилань та інші функції.

Основні вимоги до ефективної системи антивірусного захисту включають[13]:

- ефективність виявлення та ефективність блокування шкідливого програмного забезпечення;

- низький рівень помилкових спрацювань;

- надійність та стійкість до атак;

- легкість використання та налаштування;

- сумісність з іншими програмами та операційними системами; Система повинна бути здатною працювати на різних платформах та бути сумісною з різними програмами та операційними системами.

Ефективність виявлення та блокування шкідливого програмного забезпечення повинна забезпечувати здатність виявляти нові види загроз та реагувати на них швидко та ефективно.

При низькому рівні помилкових спрацювань система повинна бути здатною розрізняти шкідливе програмне забезпечення від нормальних програм та файлів, щоб уникнути блокування корисних додатків.

В надійній та стійкій до атак системі повинна бути здатність протистояти спробам обійти її захист та захищати користувачів від різноманітних атак.

Легка до використання та налаштування система повинна бути зрозумілою та простою в налаштуванні та використанні, щоб користувачі могли швидко та легко захистити свої пристрої.

Сумісна з іншими програмами та операційними системами система повинна бути здатною працювати на різних платформах та бути сумісною з різними програмами та операційними системами.

Також необхідно проаналізувати основний функціонал підібраного антивірусного забезпечення

Нові види шкідливого програмного забезпечення з'являються щодня, тому важливо, щоб системи антивірусного захисту були постійно оновлюваними та здатними швидко реагувати на нові загрози.

Зараз існує багато різних типів програмного забезпечення для антивірусного захисту[14], таких як антивірусні програми, антишпіонські

програми, програми для блокування реклами та інші. Кожен з цих типів програмного забезпечення має свої особливості та функціонал, який дозволяє ефективно захищати пристрої та інформацію від різних видів загроз.

Поряд з розвитком програмного забезпечення для антивірусного захисту, також розвиваються технології для виявлення та аналізування нових видів загроз[15]. Наприклад, машинне навчання та штучний інтелект використовуються для виявлення та аналізування нових видів шкідливого програмного забезпечення. Такі технології дозволяють швидко та ефективно виявляти нові загрози та розробляти нові методи їх боротьби.

У загальному, антивірусний захист є важливою складовою захисту інформаційної інфраструктури та даних[16]. Ефективна система антивірусного захисту має забезпечувати виявлення та блокування шкідливого програмного забезпечення, бути надійною та стійкою до атак, мати низький рівень помилкових спрацювань, бути легкою використання та налаштуванні та сумісною з різними платформами та програмним забезпеченням.

Зростання кількості загроз вимагає постійного вдосконалення та оновлення систем антивірусного захисту[17], щоб забезпечити надійний захист від різних видів шкідливого програмного забезпечення.

Крім того, користувачі повинні бути усвідомлені про потенційні загрози та вміти виявляти та уникати небезпечних ситуацій. Наприклад, вони повинні регулярно оновлювати програмне забезпечення на своїх пристроях, уникати відкривання небезпечних електронних листів, завантаження небезпечного контенту з інтернету та використовувати складні паролі для захисту своїх облікових записів.

Задля аналізування методів боротьби з небезпечним ПЗ варто використовувати віртуальні машини, задля забезпечення найбільшої безпеки.

Тестування вірусів за допомогою віртуальної машини є популярним методом в інформаційній безпеці. Віртуальна машина (VM) - це програмне забезпечення, що імітує поведінку фізичної машини, дозволяючи запускати і

виконувати різні операційні системи і програми.

Ось кілька переваг використання віртуальних машин для тестування вірусів[18]:

- ізоляція;

- зручність;

- відновлення;

- моніторинг;

Віртуальна машина надає ізольоване середовище для виконання вірусів. Це означає, що віруси не матимуть доступу до реальної операційної системи та файлів. Якщо віруси виявляться шкідливими, вони не зможуть пошкодити основну систему.

Використання віртуальних машин значно спрощує процес тестування вірусів. Ви можете створити кілька віртуальних машин з різними операційними системами та конфігураціями для тестування різних видів вірусів.

Віртуальні машини можуть бути легко клоновані або створені з резервними копіями, що дозволяє швидко відновлювати пошкоджені або скомпрометовані системи. Це дає можливість проводити повторні тести і аналізувати віруси після їх виявлення.

Віртуальні машини можуть бути налаштовані для моніторингу активності вірусів. Це дозволяє збирати дані про їх поведінку, взаємодію з системою та шкідливі наслідки. Ці дані можуть бути використані для аналізу та розробки протидійних заходів.

Хоча використання віртуальних машин для тестування вірусів є ефективним і зручним підходом, варто зазначити деякі обмеження:

- виявлення нових вірусів;

- поведінка на реальних системах;

- продуктивність;

- захист від експлойтів;

Віртуальні машини можуть бути використані для тестування відомих вірусів, але вони можуть бути менш ефективними при виявленні нових, невідомих вірусів. Це пов'язано з тим, що віртуальні машини іноді можуть мати обмежені можливості виявлення поведінки інших, ще невідомих шкідливих програм.

Віртуальні машини можуть імітувати операційні системи та середовище, але їхнє поведінка може відрізнятися від реальних систем. Деякі віруси можуть виявити це та адаптуватися до віртуального середовища, що приховує їх справжні наміри.

Віртуальні машини можуть мати обмежену продуктивність порівняно з фізичними машинами, що може негативно вплинути на швидкість виявлення і аналізу вірусів.

Віртуальні машини можуть бути вразливими до експлойтів, спрямованих на вразливості віртуального середовища самої машини або гіпервізора. Це може дозволити вірусам впливати на реальну систему або інші віртуальні машини на тому ж хості.

У загальному, використання віртуальних машин є цінним інструментом для тестування вірусів та аналізу їхньої поведінки. Однак, важливо враховувати їх обмеження та поєднувати їх з іншими методами інформаційної безпеки для досягнення найкращих результатів.

1.2 Аналіз вірусних програм

У світі швидкого розвитку технологій та зростання кількості загроз[19], системи антивірусного захисту є важливим елементом захисту інформації та даних. Вони допомагають забезпечити надійний захист від різних видів шкідливого програмного забезпечення та дозволяють користувачам впевнено використовувати свої пристрої та мережі. Проте, ефективний антивірусний

захист має бути постійно оновлюваним та вдосконалюваним, а користувачі повинні бути уважними та усвідомленими щодо потенційних загроз.

Однією з найпоширеніших загроз, які виявляються у віртуальному середовищі, є віруси. Віруси[20] - це програмне забезпечення, яке може самостійно розповсюджуватися та розмножуватися шляхом включення свого коду в інші програми або файлові системи. Вони можуть негативно впливати на функціонування пристроїв, виконувати шкідливі дії, такі як видалення даних або підміна файлів.

Ось деякі типові шкідливі дії, які віруси можуть виконувати[21]:

- руйнування даних;
- викрадення конфіденційної інформації;
- спам та розсилка шкідливих повідомлень;
- перехоплення контролю;
- виконання зловмисних команд;

При руйнуванні даних віруси можуть видаляти або пошкоджувати файли на комп'ютері, що може призвести до втрати важливої інформації або неправильного функціонування системи.

Для викрадення конфіденційної інформації віруси збирають конфіденційних даних, таких як паролі, особисті дані, банківські реквізити тощо. Ця інформація може бути використана для шахрайства або незаконного доступу до вашого облікового запису.

Спам та розсилка шкідливих повідомлень використовують вашу систему для поширення спаму або відправки шкідливих повідомлень іншим користувачам.

Перехоплення контролю позволяє вірусам отримати незаконний доступ до вашої системи та взяти її під свій контроль. Це може призвести до зниження продуктивності, віддаленого керування вашим комп'ютером або використання його в мережі злочинних дій (наприклад, в DDoS-атаках).

Деякі віруси можуть виконувати шкідливі команди на вашому

комп'ютері, такі як встановлення додаткового шпигунського програмного забезпечення або віддалений доступ для зловмисника.ц

Іншою загрозою є шпигунське програмне забезпечення або шпигунські програми[22]. Ці програми збирають та передають конфіденційну інформацію користувача без його дозволу, таку як історію відвідувань сайтів, паролі, електронну пошту та іншу особисту інформацію. Шпигунські програми можуть бути встановлені на комп'ютері через небезпечні посилання в електронних листах, завантаження з небезпечних веб-сайтів або через вразливості в операційних системах.

Ось деякі характеристики та можливості шпигунського програмного забезпечення[23]:

- клавіатурний шпигун;
- віддалений доступ;
- прихованість;
- збір і передача інформації;
- клавіатурний шпигун;
- віддалений доступ;
- прихованість;

Шпигунські програми можуть збирати різні типи конфіденційної інформації, такі як паролі, логіни, історія перегляду веб-сторінок, електронна пошта, переписки в месенджерах та інша особиста інформація. Ці дані потім передаються зловмисникам без знання та згоди користувача.

Клавіатурні шпигуни можуть відстежувати натискання клавіш і записувати введений текст, що дозволяє зловмисникам отримати доступ до паролів, логінів та іншої конфіденційної інформації.

Шпигунські програми можуть надати зловмисникам віддалений доступ до комп'ютера або пристрою. Це дозволяє їм переглядати екран, керувати системою та виконувати інші шкідливі дії здалеку.

Прихованість виражається в тому, що шпигунське програмне

забезпечення зазвичай намагається працювати в тихому режимі, щоб не привертати увагу користувача. Воно може маскуватися під процеси або файли системи, уникати виявлення антивірусними програмами та іншими заходами безпеки.

Троянські програми є іншою загрозою для безпеки інформації[24]. Вони виглядають як безпечні програми, але при цьому містять шкідливий код, який може виконувати небажані дії, такі як крадіжка конфіденційних даних або віддалене керування пристроєм.

Троянські програми приховуються під безпечними або навіть корисними програмами, що дозволяє їм проникати на комп'ютер або пристрій користувача, часто без його відома. Коли троянська програма активується, вона виконує шкідливі дії, які можуть бути різного характеру.

Ось декілька типових дій, які можуть бути виконані небезпечними троянськими програмами:

- крадіжка конфіденційних даних;
- віддалене керування;
- використання для розповсюдження інших шкідливих програм;
- пошкодження системи;

Трояни можуть викрадати різноманітну конфіденційну інформацію з комп'ютера або пристрою, таку як логіни, паролі, номери кредитних карток, особисті дані тощо. Ця інформація потім може бути використана зловмисниками для крадіжки ідентичності або фінансової шахрайства.

Троянські програми можуть надавати зловмисникам віддалений дистанційний доступ до комп'ютера або будь-якого пристрою. Тобто це означає, що зловмисники можуть виконувати різні дії без відома користувача, такі як перегляд вмісту, встановлення інших шкідливих програм або навіть керування системою в цілому.

У разі використання троянів для розповсюдження інших шкідливих програм, вони можуть використовуватись як "backdoor" для введення інших

шкідливих програм на комп'ютер або пристрій. Зловмисники можуть використовувати троянську програму для створення ботнету - мережі зражених комп'ютерів, які використовуються для розсилки спаму, атак на інші системи або для проведення кібератак.

При пошкодження системи деякі троянські програми можуть вносити зміни в операційну систему або програмне забезпечення, що призводить до збоїв, помилок або втрати даних. Це може спричинити значні проблеми для користувача і призвести до втрати чутливої інформації.

Наступною загрозою є рекламне програмне забезпечення або "adware"[25]. Це програмне забезпечення відображає рекламу на комп'ютері користувача, нав'язуючи йому небажані оголошення, які можуть містити шкідливі посилання.

Основною метою adware є генерація прибутку для розробників шляхом показу різноманітної реклами. Це може бути вбудовано у безкоштовні програми, які ви завантажуєте з Інтернету, або установлюється через недоліки в системі безпеки комп'ютера.

Нав'язана реклама adware[26] може бути надокучливою та відволікати користувача. Вона може з'являтися вікнами, вспливаючими банерами, вставками в браузері або настільними підказками. Деякі adware можуть також збирати інформацію про користувача без його дозволу, таку як відвідувані веб-сторінки, особисті дані або звички використання комп'ютера.

Крім неприємностей, adware також може бути потенційно небезпечним, оскільки деякі рекламні оголошення можуть містити шкідливі посилання або приховані програми-шкідники. Клік на такі посилання або взаємодія з рекламою може призвести до інфікування комп'ютера шкідливим програмним забезпеченням або зламом безпеки.

1.3 Постановка задачі

Побудова комплексної антивірусної системи включає ряд задач, які потрібно вирішити для забезпечення ефективного захисту комп'ютерної системи. Розглянемо ключові задачі, які можуть виникнути при створенні комплексної антивірусної системи.

Збір і оновлення інформації про загрози[27] - антивірусна система повинна мати механізми для збору інформації про нові види вірусів, шкідливе програмне забезпечення та інші загрози. Ця інформація може включати сигнатури (хеш-суми) файлів, поведінкові шаблони, аналіз вразливостей і т. д. Завантаження регулярних оновлень для оновлення бази даних загроз є важливим етапом.

Виявлення загроз[28] - антивірусна система повинна бути оснащена механізмами для виявлення потенційних загроз, таких як сигнатурний аналіз, аналіз поведінки та інші методи виявлення. Сигнатурний аналіз базується на порівнянні знакових відміток відомих вірусів та шкідливого програмного забезпечення з файлами, процесами або активностями системи. Аналіз поведінки визначає ненормальні або підозрілі дії програми на основі їхнього виконання. Додаткові методи виявлення можуть використовувати евристичний аналіз, машинне навчання або інші алгоритми для виявлення нових або невідомих загроз.

Завдяки цим механізмам антивірусна система здатна виявити потенційно шкідливі файли, процеси або активності, що становлять загрозу для безпеки системи. Це дозволяє системі реагувати негайно, блокувати або ізолювати шкідливі елементи та запобігати їхньому поширенню. Ефективне виявлення загроз є важливою складовою антивірусного захисту в реальному часі та допомагає забезпечити безпеку системи та захист від шкідливих впливів.

Реагування на загрози - після виявлення загрози антивірусна система повинна мати механізми для реагування на неї. Це може включати блокування

доступу до шкідливих файлів, видалення, карантин, усунення вразливостей або безпосередню ізоляцію компонентів системи для запобігання в подальшому поширенню загрози.

Моніторинг і журналювання - антивірусна система повинна забезпечувати моніторинг активності, що відбувається в системі, і журналювання подій. Це допомагає користувачам виявити аномальну або підозрілу активність, а також аналізувати інциденти з метою поліпшення системи безпеки.

Оптимізація продуктивності - комплексна антивірусна система повинна бути оптимізована для забезпечення мінімального впливу на продуктивність системи. Це означає, що антивірусний сканер, модулі виявлення та інші різномінітні компоненти повинні бути ефективними і споживати мінімум системних ресурсів.

Управління оновленнями – антивірусна система повинна мати механізми для управління оновленнями програмного забезпечення. Це включає автоматичні оновлення бази даних загроз, а також оновлення самої антивірусної програми задля отримання різноманітних нових функцій і виправлення вразливостей.

Інтеграція з іншими системами - комплексна антивірусна система може бути інтегрована з іншими системами безпеки, такими як мережеві файерволи, системи виявлення вторгнень (IDS), системи управління загрозами (TMS) і т. д. Це забезпечує ще більший рівень захисту і спільну обробку інформації про загрози.

Аналіз інцидентів - антивірусна система може мати механізми для аналізу інцидентів, включаючи запис інформації про загрози, їх походження та наслідки. Це допомагає вдосконалювати систему безпеки шляхом виявлення трендів, вразливостей та ефективності заходів захисту.

Навчання та освіта користувачів - комплексна антивірусна система може включати механізми навчання та освіти користувачів про загрози та безпеку. Це

може включати пояснення правил безпеки, надання порад щодо уникання шкідливих посилань і завантажень, а також надання інформації про типові загрози і методи їх запобіг

Виявлення інтелектуальних загроз - комплексна антивірусна система може використовувати інтелектуальні методи для виявлення складних і нових типів загроз, які можуть уникнути традиційним методам виявлення. Це може включати використання машинного навчання, аналізу великих обсягів даних та алгоритмів інтелектуального виявлення загроз.

Захист в режимі реального часу[29] - антивірусна система повинна забезпечувати захист в режимі реального часу, що означає постійний моніторинг активності системи та виявлення шкідливих програм негайно під час їх виконання або завантаження. Ця система негайно реагує на будь-яку підозрілу або шкідливу дію, що відбувається в реальному часі, надаючи захист навіть під час виконання програм або завантаження файлів. Це дозволяє уникнути поширення вірусів або шкідливих програм, забезпечувати безпеку даних та запобігати можливим пошкодженням або витокам інформації. Забезпечення антивірусного захисту в реальному часі є важливою складовою ефективної стратегії безпеки комп'ютерних систем.

Аналіз небезпечних посилань та вкладень - комплексна антивірусна система може включати модулі для аналізу небезпечних посилань у електронних листах або веб-сторінках, а також виявлення і блокування шкідливих вкладень у файлах.

Задля ефективної боротьби з небезпечним програмним забезпечення необхідно використовувати найбільш ефективне антивірусне ПЗ. На мій погляд, це і є найбільш важливим елементом. В наступому розділі ми проаналізуємо різноманітне антивірусне ПЗ проти конкретних видів загроз. Задля безпеки робочої станції ми будемо використовувати віртуальну машину.

2. ТЕСТУВАННЯ АКТУАЛЬНИХ ЗАСОБІВ АНТИВІРУСНОГО ЗАХИСТУ

2.1 Вибір та налаштування віртуальної машини

Використання віртуальних машин для тестування вірусів є досить поширеною практикою в галузі інформаційної безпеки. Основна ідея полягає у створенні ізольованого середовища, в якому можна виконувати потенційно небезпечні файли та програми, не поставляючи під загрозу основну систему. В даному розділі ми повинні досягнути таких цілей:

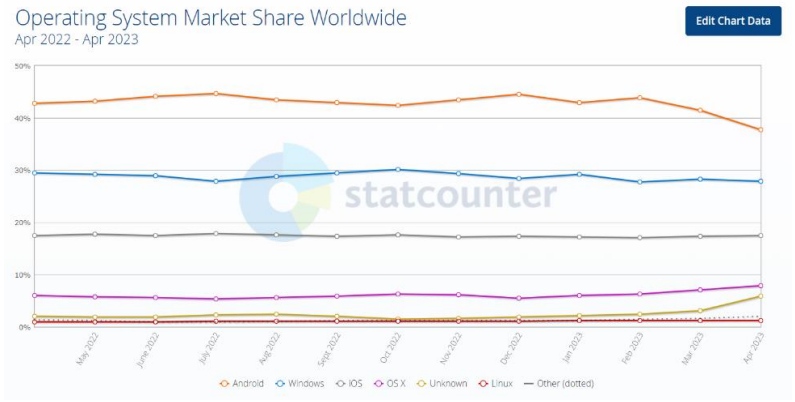
- Вибір віртуальної машини: існує кілька популярних платформ віртуалізації, таких як VMware, VirtualBox, Hyper-V та інші віртуальні машини. Виберіть платформу, яка вам підходить з точки зору функціональності, підтримки та ліцензування.

- Встановлення віртуальної машини. Це включає встановлення необхідного програмного забезпечення та налаштування параметрів віртуальної машини, таких як обсяг пам'яті, простір на диску, мережеві налаштування тощо.

- Вибір операційної системи. Ми оберемо операційну систему, яка найкраще підходить для нашої потреби та має значення для тестування вірусів (наприклад, розповсюджена ОС, яка часто стає об'єктом атак).

- Забезпечення безпеки. Ми забезпечемо необхідні заходи безпеки для віртуальної машини, такі як оновлення операційної системи та встановлення антивірусного програмного забезпечення. Це допоможе запобігти можливим загрозам під час тестування вірусів.

В даному проекті ми будемо використувувати Windows, так як станом на 2023 рік це найбільш популярна операційна система після ОС Android. А серед різних версій Windows, Windows 10 досі є найбільш популярною. На рисунках 2.1 та 2.2 зображено статистику використання операційних систем :



Рисинуок 2.1 – Статистика використання різних операційних систем

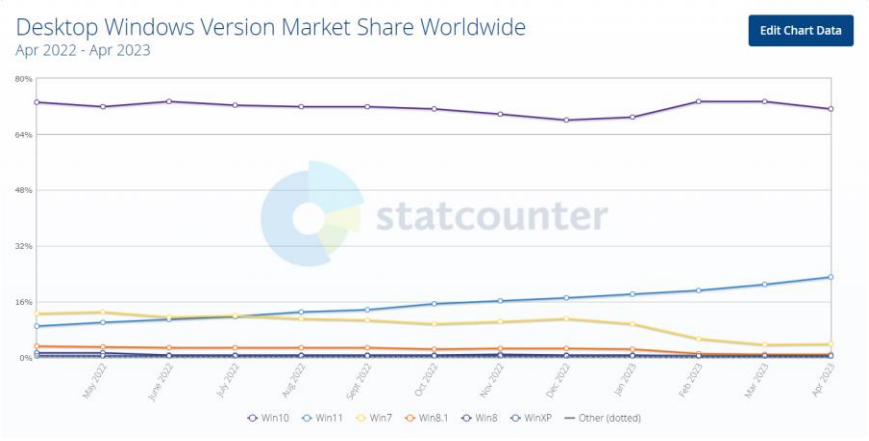


Рисунок 2.2 – Статистика використання різних версій Windows

В своєму проекті, для тестування антивірусів я буду використовувати Virtual box. Він забезпечує ізольоване середовище, де ви можете запускати та виконувати потенційно шкідливий код або програми, не ризикуючи зараженням основної системи. Розглянемо причини, чому VirtualBox може бути ефективним інструментом для тестування вірусів.

Ізоляція - віртуальні машини, створені в VirtualBox, мають власну віртуальну апаратну платформу, операційну систему та ресурси, що забезпечує фізичну та логічну ізоляцію від основної системи. Це дозволяє запускати віруси та інші шкідливі програми у контрольованому середовищі, що зменшує ризик поширення та негативного впливу на основну систему.

Снапшоти - VirtualBox надає можливість створювати снапшоти, які є

точками відновлення віртуальної машини до певного стану. Під час тестування вірусів ви можете створити снапшот перед запуском шкідливого коду, і у разі проблем або зараження, ви зможете швидко повернутися до попереднього стану віртуальної машини.

Мережеві налаштування - VirtualBox дозволяє налаштовувати мережеві параметри віртуальної машини, включаючи обмеження комунікації з іншими системами та мережами. Це дозволяє контролювати доступ вірусів до зовнішнього середовища і уникнути їхнього поширення. Після налаштування віруальної машини наші налаштування мають наступний вигляд (рисунок 2.3):

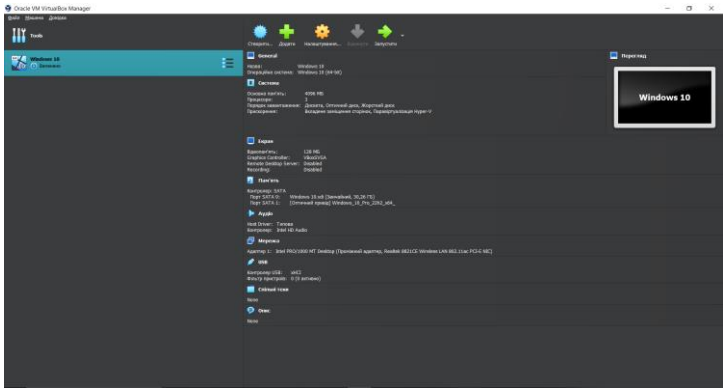


Рисунок 2.3 – вікно VirtualBox з налаштуваннями операційної системи Windows

Як було описано вище, в VirtualBox є функція Snap Shot, яку ми будемо використовувати. На рисунку 2.4 ми можемо побачити наший зріз:

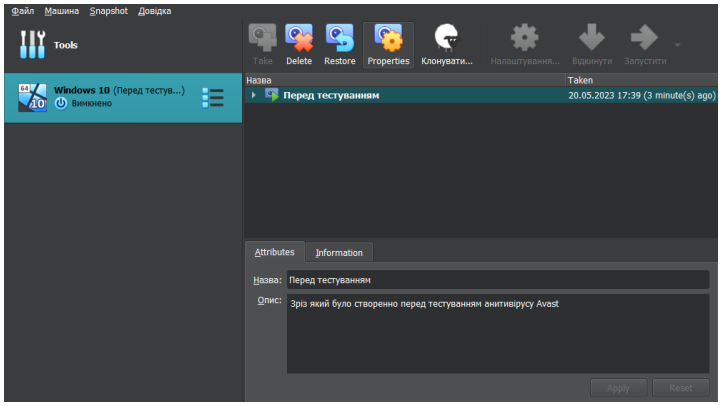


Рисунок 2.4 – Створення зрізу в VirtualBox

2.2 Тестування ативірусів

2.2.1 Тестування антивірусу Avast

Перший антивірус який ми будемо тестувати це Avast[30], оскільки він має ряд таких переваг:

- Avast надає захист в режимі реального часу[31], перевіряючи файли, електронну пошту, веб-сайти та інші джерела на наявність вірусів та шкідливих програм, це дозволяє блокувати загрози ще до того, як вони зможуть завдати шкоди вашому комп'ютеру;

- Avast пропонує різноманітні функції, які допомагають забезпечити повну безпеку вашого комп'ютера, це включає в себе антивірусний сканер, захист від фішингу, файрвол, захист від шпигунського ПЗ та інші інструменти для захисту від загроз;

- Avast має простий та інтуїтивно зрозумілий інтерфейс[32], який дозволяє навіть не досвідченим користувачам легко налаштувати та використовувати програму, він також пропонує автоматичні оновлення, щоб ви завжди мали найновіші захисні функції;

Для початку налаштуємо антивірус. На рисунку 2.5 ми можемо побачити налаштування мережевого захисту.

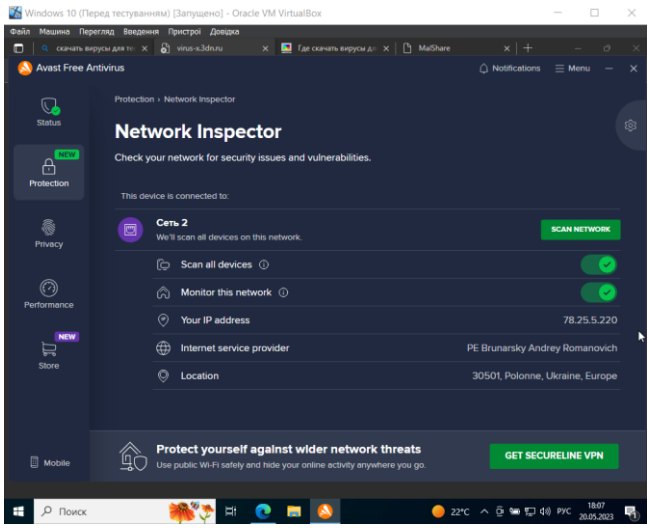


Рисунок 2.5 – Налаштування мережевого захисту

Тепер перейдемо до налаштування брендмаура (рисунок 2.6):

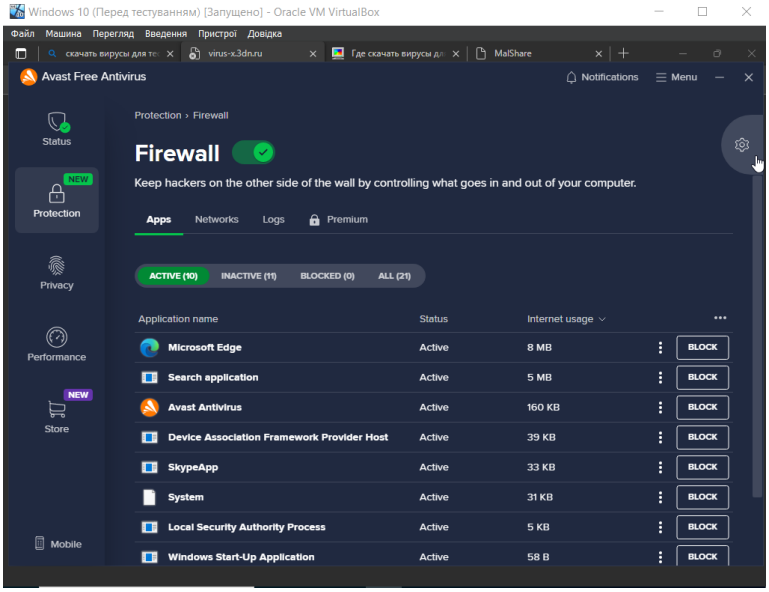


Рисунок 2.6 – Firewall в внтивірусі Avast

Тепер перейдемо до тестування. Для завантаження вірусів я буду використовувати сайт MalwareBazaar, так як так є різноманітні віруси, які є достатньо новими. На рисунку 2.7 показано необхідний нам сайт. Завантажимо різні віруси з даного сайту, та перевіримо реакцію Avast.

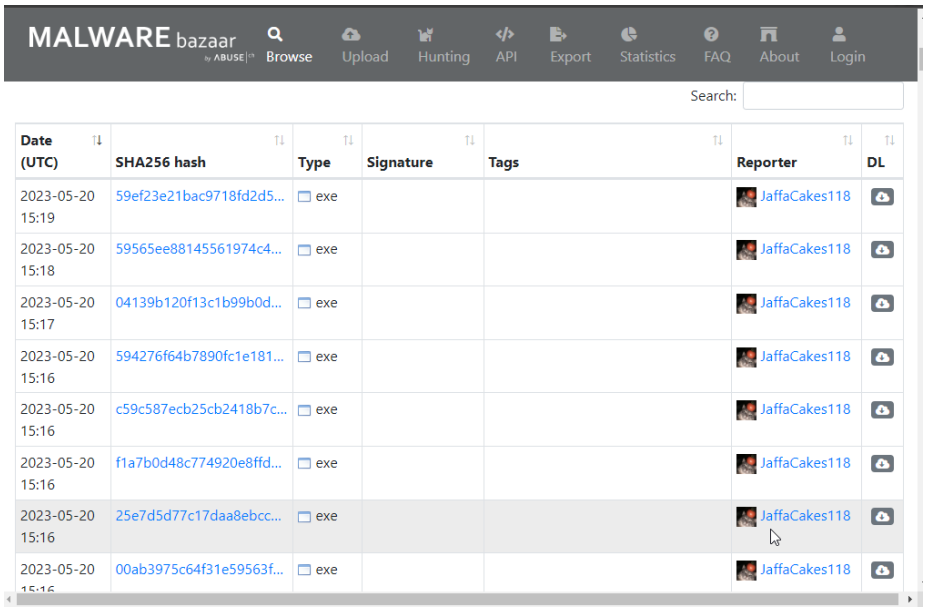


Рисунок 2.7 – Сайт MalwareBazaar

На рисунку 2.8 показано архіви з небезпечним ПЗ. Віруси, переважно формату .exe, знаходяться всередені данних архівів, тож разархівуємо їх та побачимо чи зреагує на це Avast.

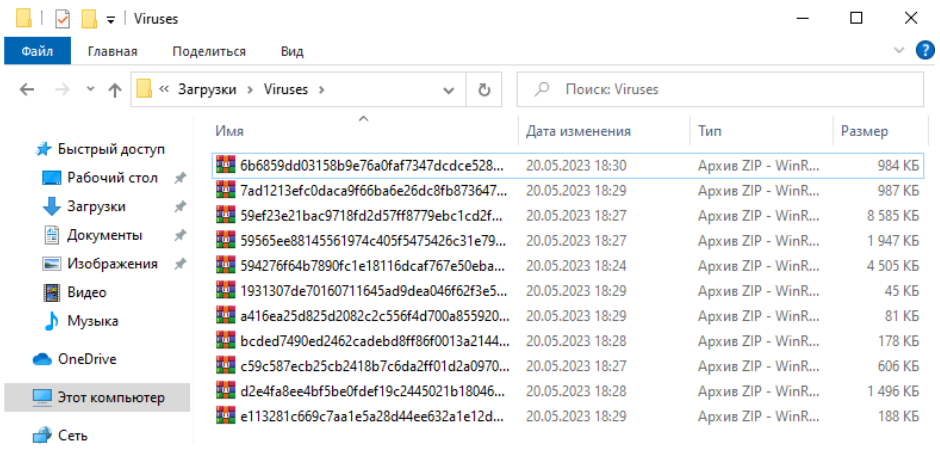


Рисунок 2.8 – Папка з завантаженими вірусами

Як видно з рисунку 2.9 Avast відреагував на загрозу, при тому що він відрегував не після запуску .exe –файлу, а відразу після розархівації, що є доброю ознакою Повторимо процедуру на інших файлах :

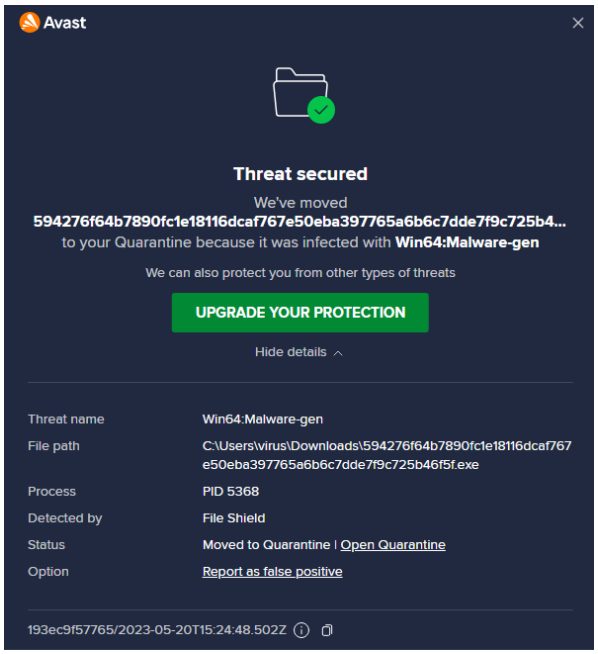


Рисунок 2.9 – Реакція Avast на вірус №1

Як видно з рисунку 2.10 Avast знову відреагував на троян.

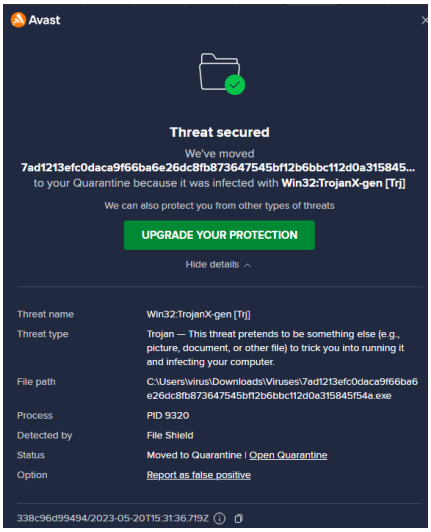


Рисунок 2.10 – Реакція Avast на вірус №2

На рисунку 2.11 ми можмо побачити, що Avast знову відреагував на зогрозу, в данному випадку на черв’як.

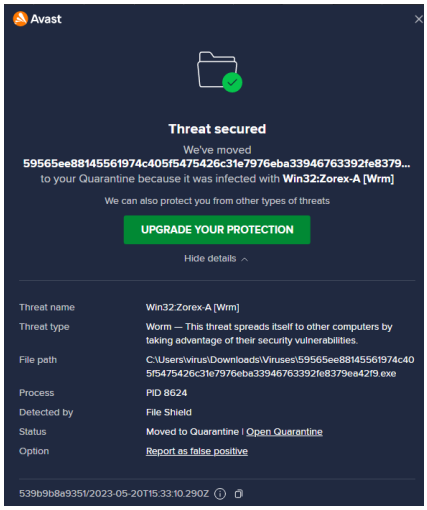


Рисунок 2.11 – Реакція Avast на вірус №3

На перший погляд данний антивірус спрявляється чудово і майже моментально знаходить небезпечне програмне забезпечення, проте, один із вірусів в форматі .exe та вірус в форматі xls, Avast не опізнав як загрозу, на відміну від інших файлів.

На рисунку 2.12 можемо побачити, файли не було видалено на відміну від інших програм після розархівації, що уже є потенційною загрозою для безпеки робочої станції, проте після запуску данного .exe -файлу, Avast все таки розпізнав загрозу.

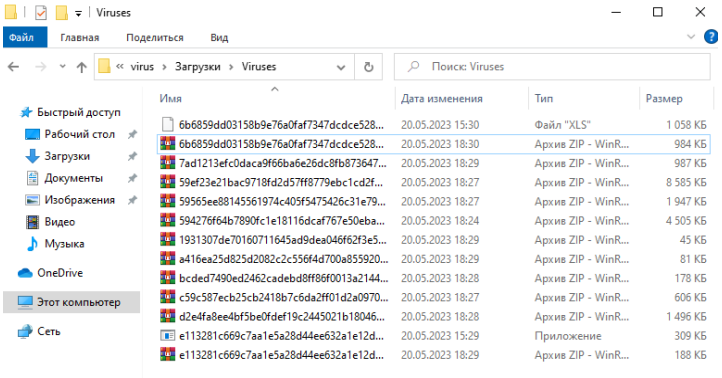


Рисунок 2.12 – Папка з небезпечним програмним забезпеченням

Як видно на рисунку 2.13 Avast відреагував на небезпечний .exe –файл після взаємодії з ним.

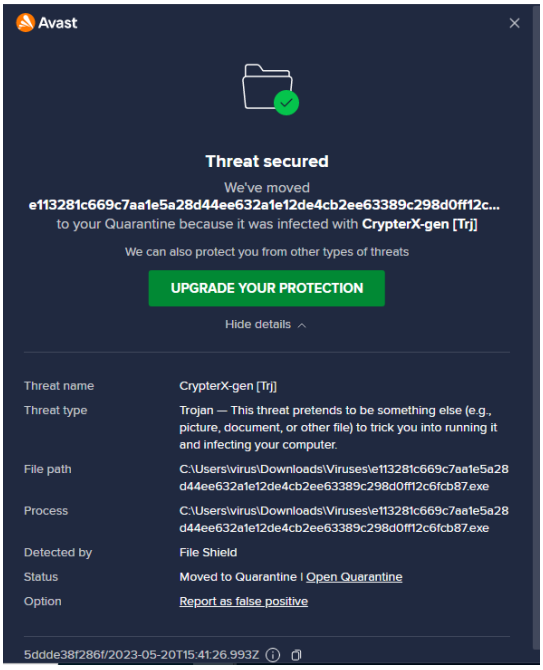


Рисунок 2.13 – Реація Avast на запуск небезпечного ПЗ

Тепер перевіримо як реагує Avast на загрози в інших форматах крім .exe. На рисунку 2.14 ми можемо побачити, що на цей раз відразу після розархівації Avast відреагував лише на 3 віруса, решту не було опізнано як небезпечне ПЗ.

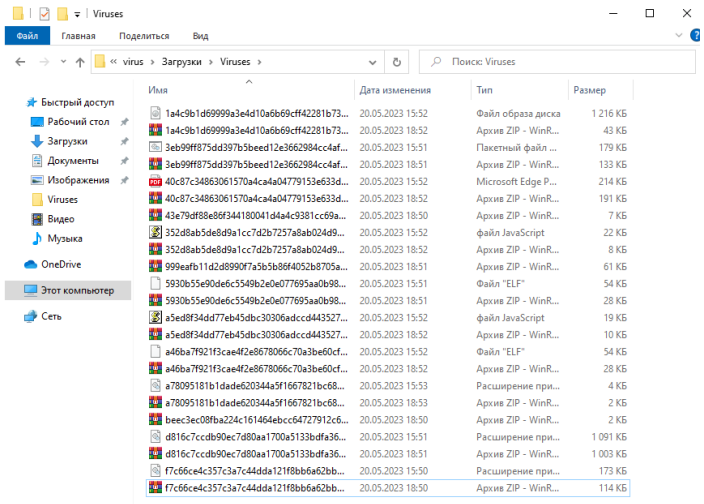


Рисунок 2.14 – Папка з вірусами різних фортматів

Більше того Avast ніяк не відреагував на відкриття .pdf –файлу, що насторожує. Розглянемо даний файл більш детально. Відкриємо його та проаналізуємо потенційну загрозу, яку може нести в собі цей файл.

Проаналізуємо данну загрозу, знайшовши додаткову інформацію про данний файл (рисунок 2.15 та рисунок 2.16)

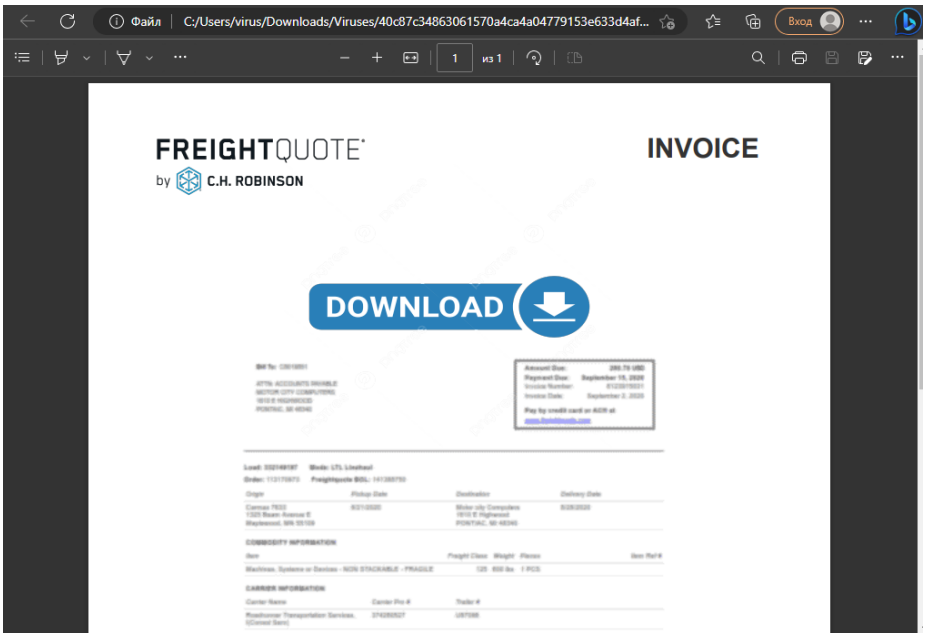


Рисунок 2.15 – Відкриття зараженого файлу формату .pdf

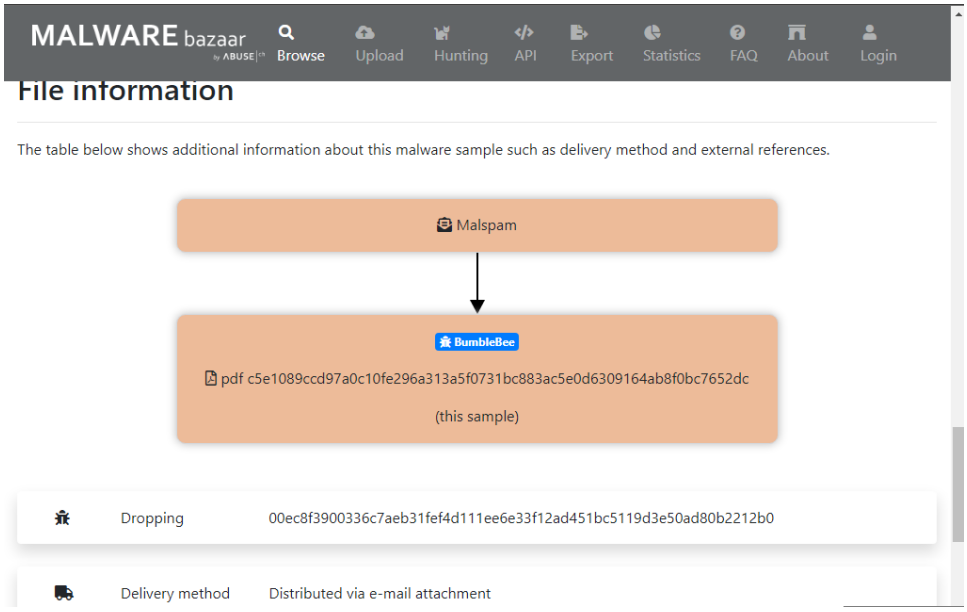


Рисунок 2.16 Інформація про заражений файл формату .pdf

Віруси, троянські програми та інші шкідливі програми можуть бути приховані у PDF-файлах. Дані програми можуть використовувати вразливості в програмному забезпеченні для зловмисних дій, таких як крадіжка особистої інформації, поширення спаму або отримання незаконного доступу до вашої системи.

Після взаємодії з всіма файлами які залишились в папці, Avast ні разу не відреагував, що я досить великою загрозою для системи. Проте щоб краще зрозуміти, наскільки це поганий результат нам варто протестувати роботу інших антивірусних засобів.

2.2.2 Тестування антивірусу Avg

Перед початком тестування антивірусу Avg, застосуємо SnapShot, та відновимо систеиу до попереднього стану. Далі налаштуємо антивірус, а саме активуємо всі можливі функції, які присутні в безкоштовній версії.

Як видно на рисунку 2.17 нам доступний звичайний захист комп’ютера та за захист мережі з поштою.

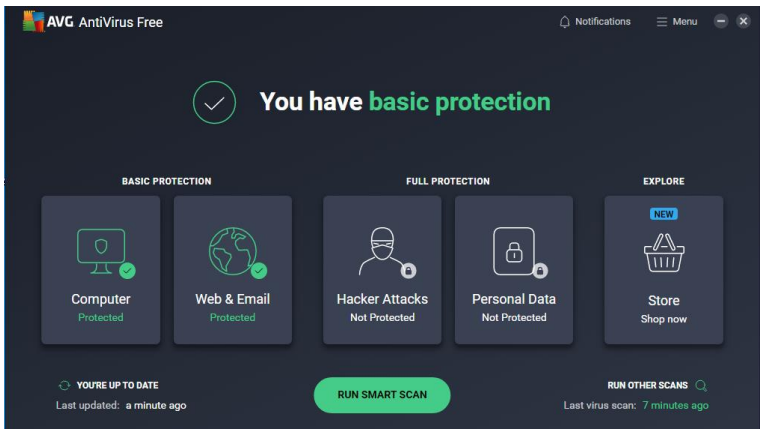


Рисунок 2.17 – Вікно антивірусу Avg

Тепер завантажимо небезпечне ПЗ, та прослідкуємо за реакцією антивірусу. Протестуємо антивірус на загрозу від файлів формату .exe. Як видно по повідомленню від антивірусу Avg на рисунку 2.18, данний антивірус відреагував на загрозу.

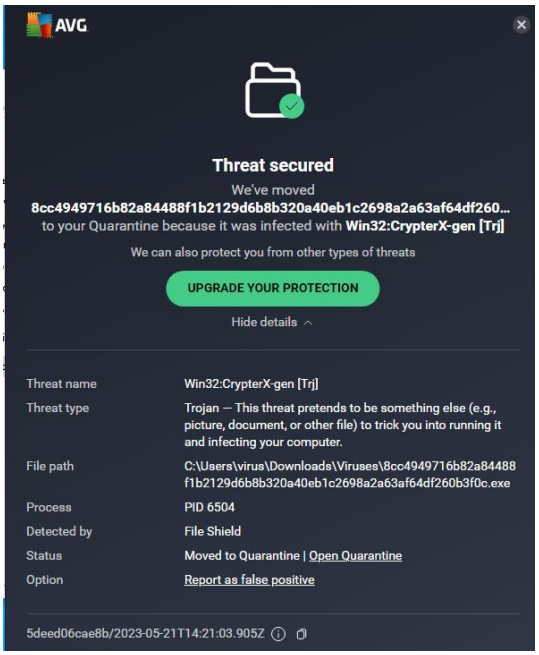


Рисунок 2.18 – Реакція антивірусу Avg на вірус №1

На рисунку 2.19 також видно, що антивірус Avg відреагував на загрозливі файли в форматі .exe, при цьому все шкідливе ПЗ було достатньо швидко видалено.

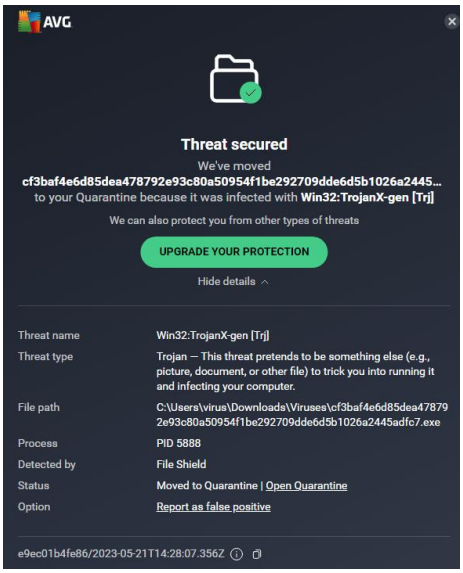


Рисунок 2.19 – Реакція антивірусу Avg на вірус №2

На рисунку 2.20 ми можемо побачити, що антивірус Avg видалив небезпечне ПЗ після розархівації.

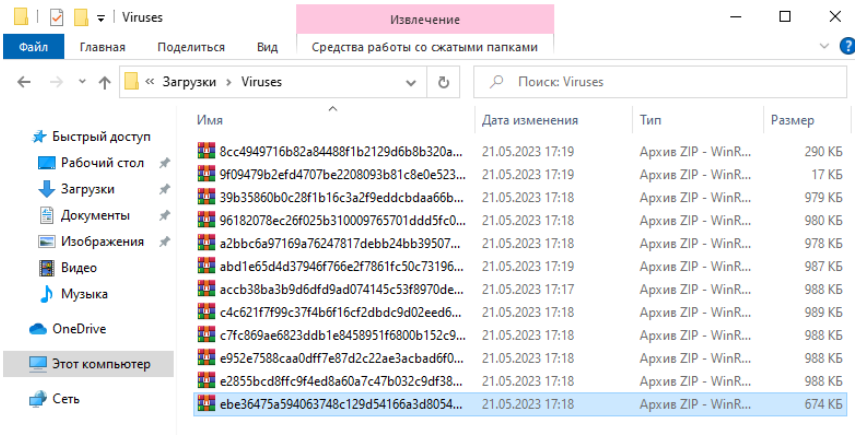


Рисунок 2.20 – Папка з вірусами після реагування антивірусу Avg

Тепер перейдемо до тестування вірусів різних форматів, відмінних від .exe, і прослідкуємо за реакцією ативірусу.

На рисунках 2.21 та 2.22 ми можемо побачити реакції антивірусу Avg на загрози. В двох випадках загрозою виявились троянські програми.

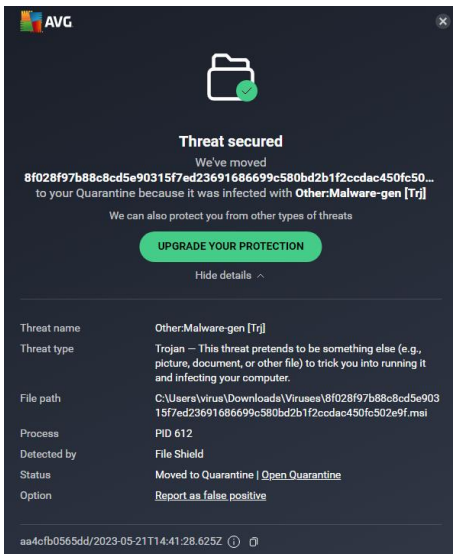


Рисунок 2.21 – Реакція антивірусу Avg на вірус в форматі .msi

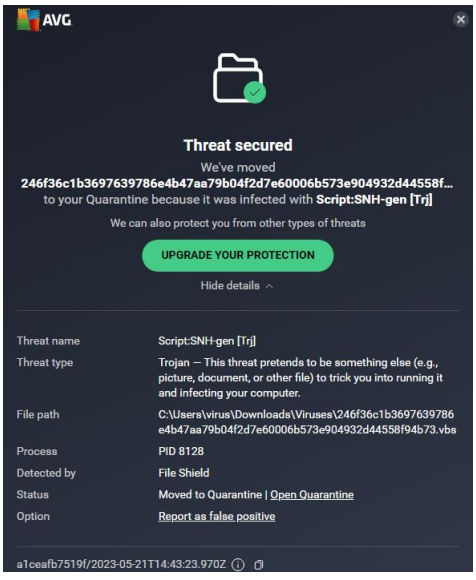


Рисунок 2.22 - Реакція антивірусу Avg на вірус в форматі .vbs

Після тестування антивірусу Avg можемо виділити такі цікаві моменти: на відмінну від антивірусу Avast, Avg відреагував на загрозливе ПЗ в форматі .vbs, тобто потенційно в боротьбі антивірус Avg, може показати себе краще в боротьбі проти шкідливих скриптів[33]. Рисунок 2.23 це підтверджує:

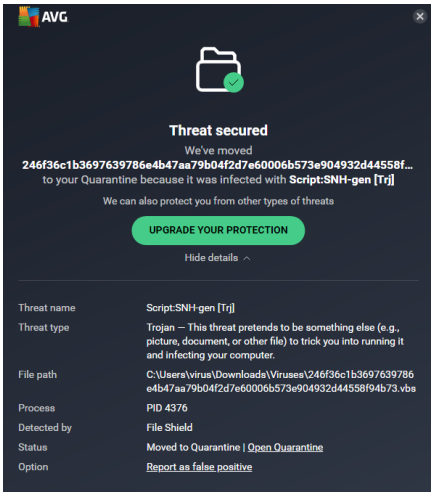


Рисунок 2.23 – Реакція антивірусу Avg на вірус в форматі .vbs

- антивірус Avg на відмінну від антивірусу Avast, зміг розпізнати загрозливе програмне забезпечення в форматі .dll, проте не в всіх випадках;

- антивірус Avg, також не відреагував на можливу загрозу від файлів в форматі .xls та .elf[34]; На наступному рисунку 2.24 ми можемо побачити, що велика кількість небезпечного ПЗ так і не було перенесенно до карантину, або видалено.

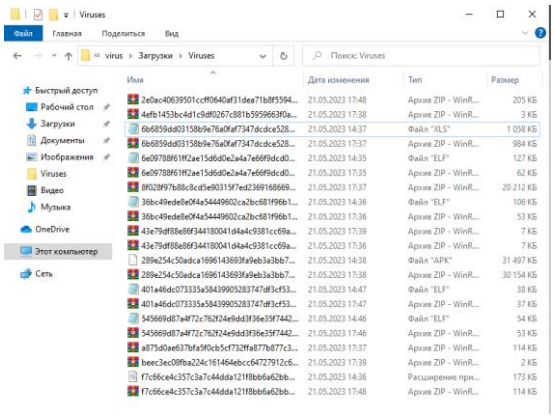


Рисунок 2.24 – Папка з розархівованими вірусами, на які не відреагував антивірус Avg

Антивірус Avg продемонстрував достаньо якісний захист, проте він не відреагував на певні види загроз, що може бути потенційною небезпекою для робочої станції користувача.

2.2.3 Тестування антивірусу Avira

Перед початком тестування необхідно налаштувати дане антивірусне забезпечення. Але на даному етапі ми зіткнемось з проблемою, а саме достатньо малий перелік функцій для безкоштовної версії. На відміну від Avast та Avg, Avira в безкоштовній версії не надає захист мережі та Firewall[35]. На рисунку 2.25 показано перелік функцій для антивірусу Avira в залежності від вибраного плану.

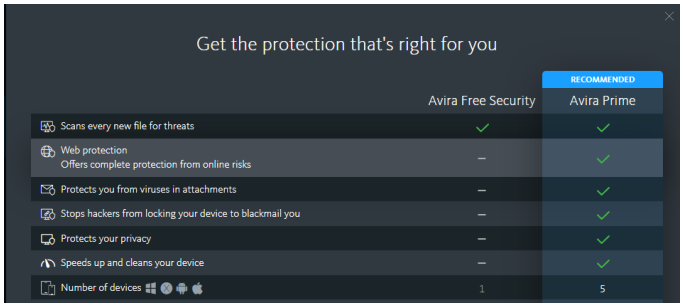


Рисунок 2.25 – Перелік функій Avira в залежності від версії

З налаштовуванням закінчено, перейдемо до тестування реагування Avira на небезпечно ПЗ формату .exe, які переважно являють собою Трояни. На рисунку 2.26 покано першу реакцію на небезпечне ПЗ:

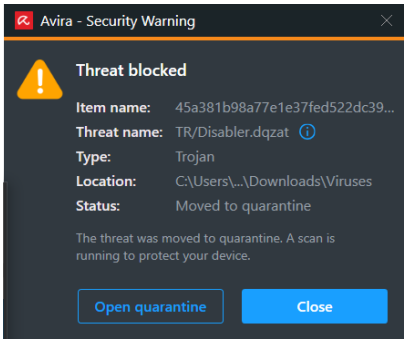


Рисунок 2.26 - Реакція антивірусу Avira на вірус №1

Ми можемо побачити, що данне небезпечне ПЗ являє собою троян, і данну загрозу було перенесено до карантину.

Як видно із наступного рисунку (2.27), Avira не відреагував на деякі загрози відразу після розархівування.

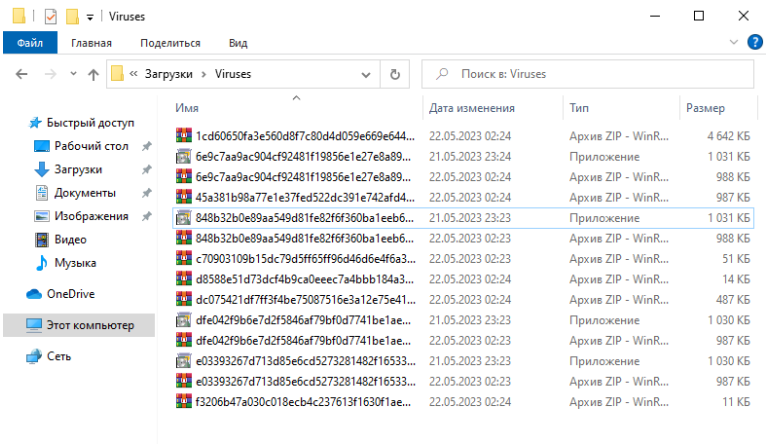


Рисунок 2.27 – Папка з небезпечними ПЗ після тестування Avira

На решту файлів формату .exe Avira відреагувала тільки після взаємодії з данними файлами, що звісно може нести певну потенційну небезпеку. Ми можемо побачити реагування на загрозливе ПЗ після взаємодії на рисунку 2.28:

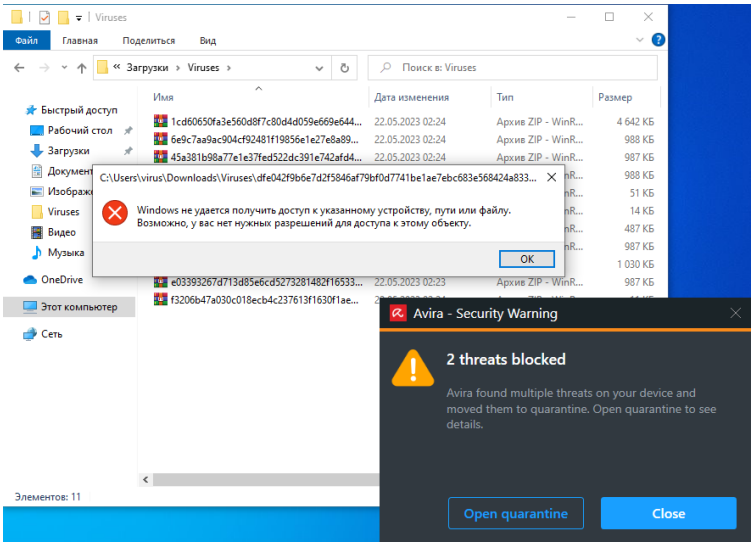


Рисунок 2.28 – Реагування антивірусу Avira, на небезпечне ПЗ після взаємодії з файлом

В цілому антивірус показав непоганний результат, але попередні антивіруси в тестуванні вірусів даного типу, реагували краще.

Тепер перевіримо антивірус на більш різноманітних загрозах. Як можемо побачити на рисунку 2.29 антивірус Avira відреагував на загрозу, яка являє собою “backdoor”, тобто небезпечне програмне забезпечення, яке може надати можливість зловмисникам досягнути необхідних їм цілей.

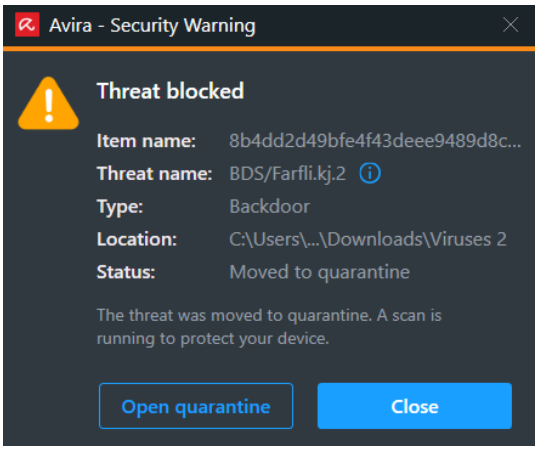


Рисунок 2.29 - Реакція антивірусу Avira на вірус №2

На рисунку 2.30 ми можемо побачити, що антивірус Avira відреагував на загрозу, в даному випадку троян.

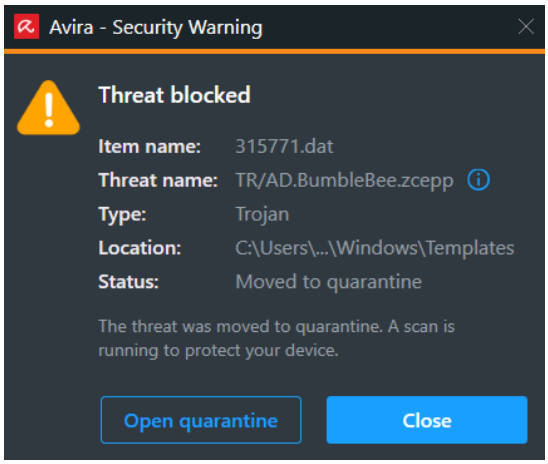


Рисунок 2.30 - Реакція антивірусу Avira на вірус №4

Тепер ми можемо побачити на які загрози не відреагувала Avira без взаємодії на рисунку 2.31

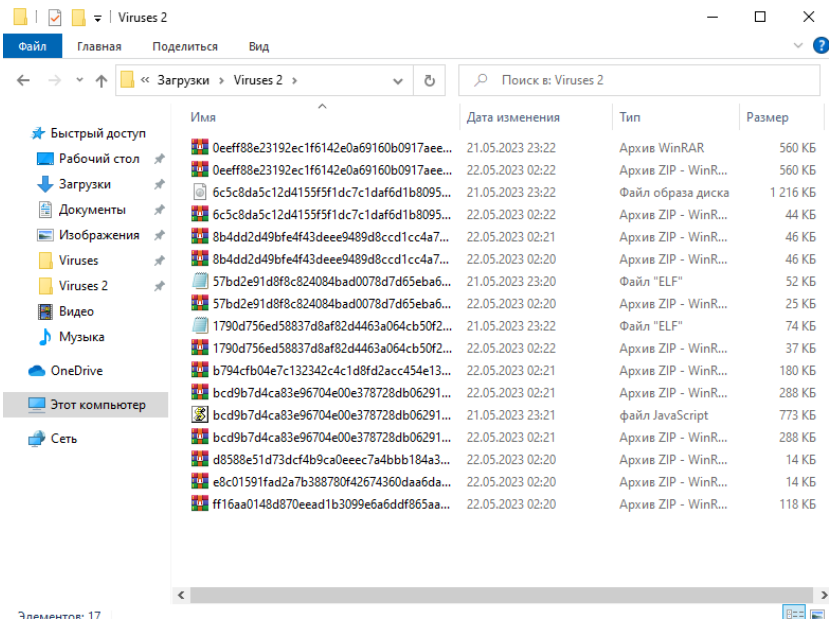


Рисунок 2.31 – Папка з вірусами після регування антивірусу Avira

В цілому антивірус Avira, чудово відреагувала, на разноманітні загрози[36]. На відміну від попередніх антивірусів, Avira відрегувала на більшість небезпечного ПЗ в фоматах .dll, .elf, .js, проте час реагування трішки менший ніж в попередніх. Деяке небезпечне ПЗ не було видалено, а просто переміщено в карантин, але це вже краще ніж в попередніх антивірусних програмах.

Протестувавши різноманітне антивірусне ПЗ від різних компаній, тепер перевіримо, системний антивірус Windows, а саме Windows Defender.

2.2.4 Тестування антивірусу Windows Defender

По аналогії з попередніми антивірусами, активуємо всі можливі функції Windows Defender. Відразу помітно, що в Windows Defender, є достатньо велика

кількість різноманітних функцій[37]. Для початку розглянемо функціонал даного антивірусу (рисунок 2.32):

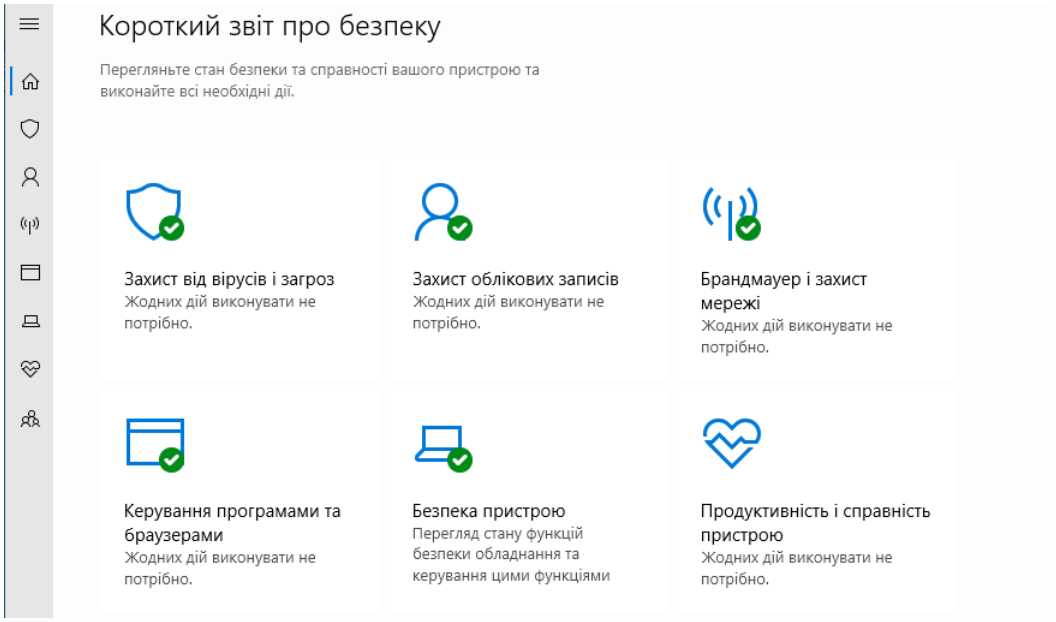


Рисунок 2.32 – Вікно з можливими функціями Windows Defender

Після активування всіх функцій, перейдемо до тестування загроз. Windows Defender показав себе чудово проти різноманітних Троянів, та загрозливого ПЗ формату .exe (рисуноку 2.33). Даний антивірус майже момнтально розпізнав небезпечне ПЗ та видалив його. Проте Windows Defender, не показав більш детальну інформацію про ПЗ, яке він заблокував.

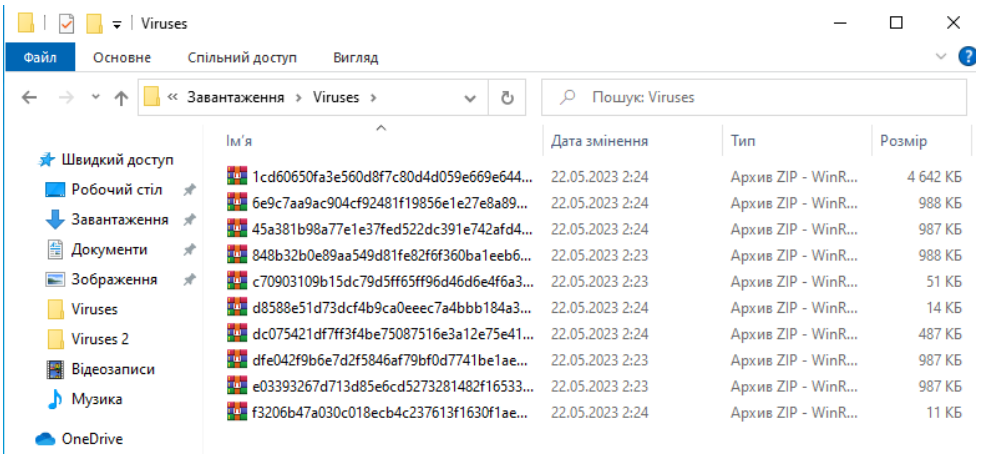


Рисунок 2.33 – Папка з небезпечним ПЗ після роботи Windows Defender

Тепер перейдемо до наступного етапу, а саме перевіримо здатність розпізнавати небезпечне ПЗ інших типів. На рисунку 2.34 ми можемо побачити реакцію антивірусу на небезпечне ПЗ:

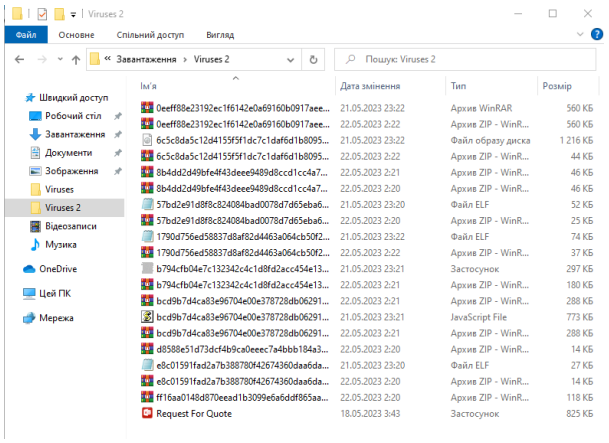


Рисунок 2.34 – Папка з небезпечним ПЗ різних форматів (Windows Defender не відреагував)

Нажаль Windows Defender не відреагував на небезпечне ПЗ після розархівування, на відмінну від попередніх антивірусів, які в половині випадків реагували на подібні загрози. Тепер перевіремо, що відбудеться після взаємодії з данними файлами. Як видно з рисунку 2.35 Windows Defender відреагував на взаємодію з шкідливим ПЗ та видалив загрози, проте не всі.

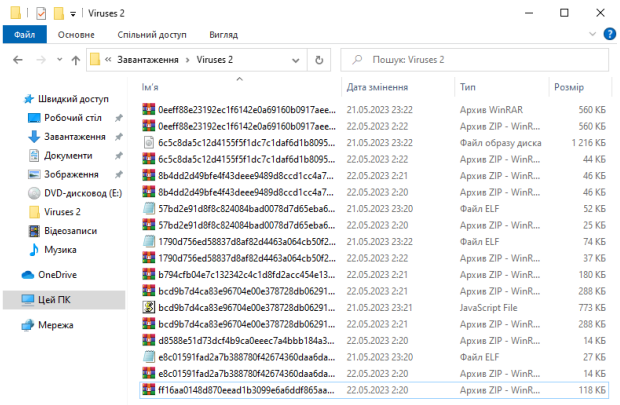


Рисунок 2.35 – Папка з небезпечним ПЗ різних форматів після взаємодії з файлами.

В даному тестуванні Windows Defender, показав непоганий результат, але безкоштовне антивірусне ПЗ від сторонніх розробників показали себе краще, проти різноманітного шклідливого ПЗ. Також з недоліків, можемо виділити непрозорість антивірусного захисту Windows Defender, на відміну від попереднього антивірсуного забезпечення. Антивіруси Avast, Avg та Avira давали достатью велику кількість інформації про заблоковане шкідливе ПЗ.

2.3 Аналіз результатів тестувань

Провівши тестування різномантіного антивірусного ПЗ, ми можемо обрати антивіруси, які найкраще підійдуть для створення комплексної системи антивірусного захисту. Серед данного ПЗ необхідно обрати які антивіруси підійдуть найкраще для захисту мережевого серверу, захисту електронних пошт користувачів та для захисту робочих станцій працівників.

Avira в звичайній версії має досить вузький функціонал, проте в результаті тестування реагування на небезпечне ПЗ, Avira показала себе найкраще, отже данний антивірус чудово підійде для захисту робочих станцій працівників.

Для захисту мережевого серверу, найкаще підійде антивірус Avast, так як в даному антивірусі є влаштовані функції аналізу мережі на наявність небезпек, та є влаштований Firewall. Єдиною альтернативою для забезпечення безпеки мережі може бути Windows Defender, проте швидкість реагування на загрози більша і Windows Defender не надає велику кількість інформації про заблокованні загрози, яку потім ми могли б проаналізувати.

Для захисту поштового сереверу чудово підійде антивірус Avg, так як в безкоштовній версії присутня данна функція та даний антивірус продемонстрував чудову швидкість реагування на загрози та зміг розпізнати загрозу в текствих файлах, через які зазвичай поширюють віруси розсилаючи іх

на пошти користувачів. На відміну від Avast, який не зміг розпізнати загрозу в файлі формату .pdf, який розрахованний на поширення вірусів шляхом розсилання файлів на пошти користувачів.

Таким чином ми обрали та налаштували віртуальну машину, в якій ми протестували найбільш популярні безкоштовні антивірусні програми, та виділили їхні сильні та слабкі сторони. Обрали та розприділили функціїї для яких нам необхідні данні антивірусні програми. Тепер перейдемо до проектування нашої мережі та реалізації комплексної системи антивірсуного захисту обчислювальної мережі філлї “Ощадбанку”.

3. РЕАЛІЗАЦІЯ СИСТЕМИ КОМПЛЕКСНОГО АНТИВІРУСНОГО ЗАХИСТУ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

3.1 Проектування плану приміщення та мережі

Для побудови плану приміщення Ощадбанку слід врахувати кілька факторів, таких як розмір приміщення, вимоги безпеки, організація робочих місць та доступ до необхідного обладнання. Нижче наведено загальну структуру плану приміщення Ощадбанку:

- приймальня та вхідна зона (реєстрація клієнтів, встановлення черги);
- касова зона (розміщення кас і банкоматів);
- клієнтська зона (приміщення для консультацій, оформлення документів тощо);
- адміністративна зона (офісні приміщення для співробітників банку);
- конференц-зала або переговорна кімната (для проведення зустрічей з клієнтами чи переговорів з партнерами);
- технічна зона (приміщення де знаходяться сервери, та все необхідне технічне обладнання);

На території банку розміщенно таке обладнання:

- каси;
- банкомати;
- комп'ютери, сервери та інші технічні засоби (в данному випадку нас хвилюють тільки комп’ютери та сервери).

Схематичне зображення плану приміщення Ощадбанку має наступний вигляд (рисунок 3.1):

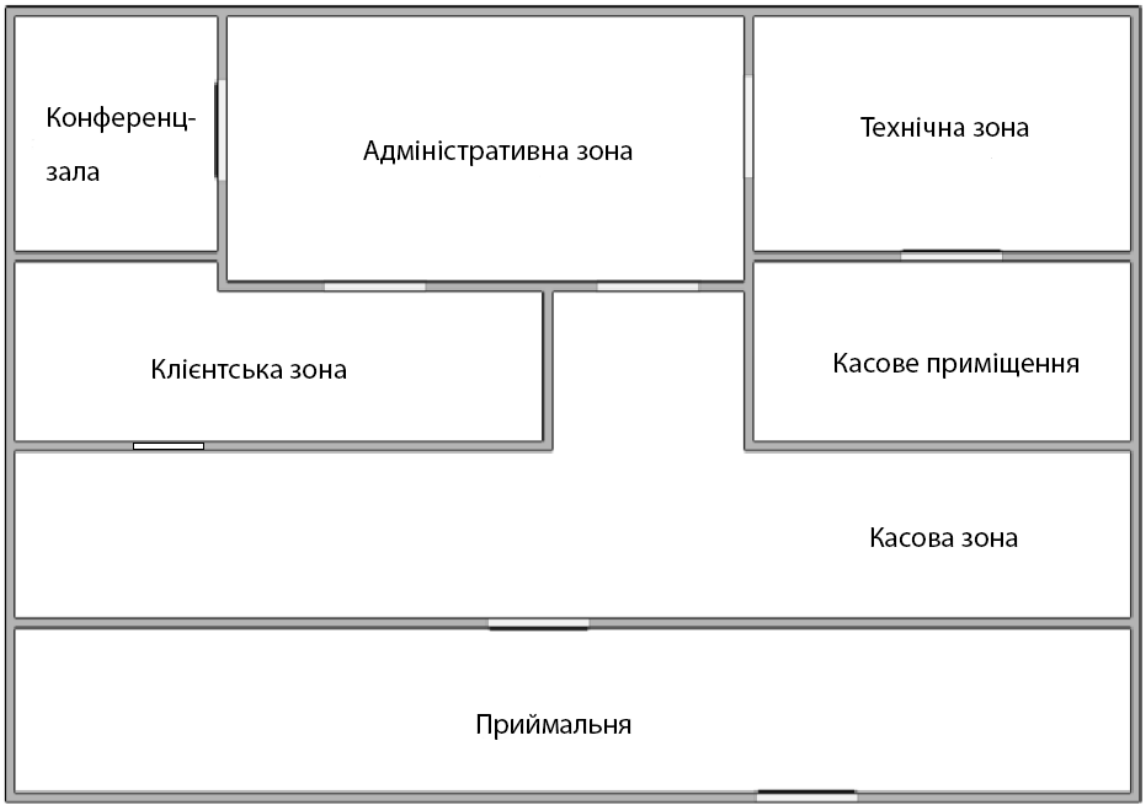


Рисунок 3.1 – План приміщення

Також необхідно врахувати розміщення камер безпеки в приміщеннях банку, оскільки вони також є частиною локальної мережі банку та існує ряд вірусних загроз, а саме:

- втручання в роботу камери, вірус може використовувати вразливості в програмному забезпеченні камери для заблокування її роботи, переривання запису або відправлення недостовірних зображень;

- загрози конфіденційності, атаки на камери можуть привести до компрометації конфіденційної інформації, яка була зафіксована камерами, наприклад, зняття конфіденційних даних або проникнення до захищених приміщень;

- знищення зображень, вірус може змінювати або видаляти зображення, що зафіксовані камерою, що ускладнює їх використання для розслідування подій або ідентифікації осіб.

- контроль над системою відеоспостереження, в деяких випадках вірус може намагатись отримати повний контроль над системою відеоспостереження, зокрема над управлінням камерами та записами.

Побудуємо план розміщення камер відеоспостереження на території банку за допомою програми IP Video System Design Tool 2022 (рисунок 3.2):

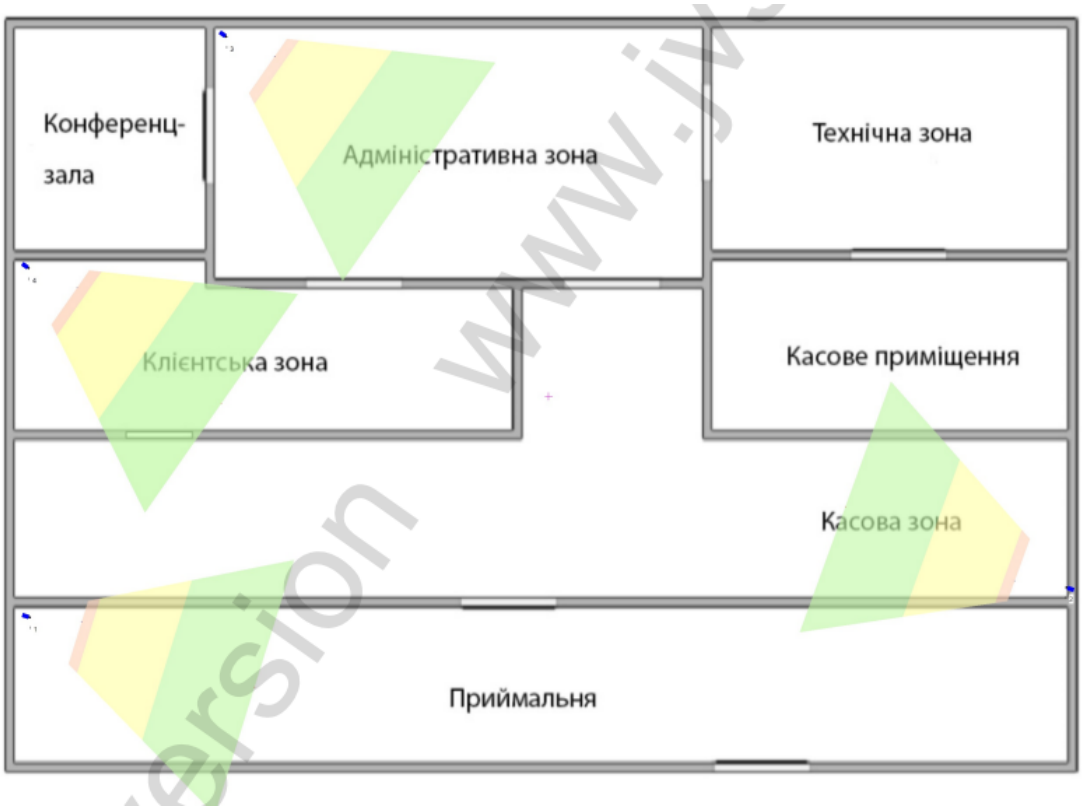


Рисунок 3.2 – Розміщення камер відеоспостереження на території банку

Тут ми маємо камери Hikvision DS-2CE56D0T-IRMMF, доступ до данних камер має комп’ютер, який знаходиться в технічній зоні.

Тепер необхідно побудувати нашу локальну обчислювальну мережу. Типово, локальна мережа банку [38] складається з комп'ютерів, серверів, мережевого обладнання та програмного забезпечення, які забезпечують обмін даними, доступ до спільних ресурсів та інші комунікаційні функції всередині банку. Головною метою локальної обчислювальної мережі банку є забезпечення ефективного обміну даними між різними системами і пристроями

в межах банку. Вона також гарантує безпеку та конфіденційність банківської інформації шляхом застосування різних заходів безпеки, таких як захист мережі від несанкціонованого доступу, шифрування даних та застосування брандмауерів і антивірусного програмного забезпечення.

Важливою складовою локальної обчислювальної мережі банку є підтримка інфраструктури, яка забезпечує постійну доступність мережі та високу швидкість передачі даних. Банк може мати власні дата-центри для забезпечення надійності і резервного копіювання даних.

Враховуючи швидкий розвиток технологій, багато банків також розглядають можливості використання хмарних обчислень для підвищення ефективності та гнучкості своїх мереж і інфраструктури.

Загалом, локальна обчислювальна мережа банку є критично важливою для забезпечення надійності, безпеки та ефективності банківських операцій, а також для забезпечення зручності та задоволення потреб клієнтів.банку.

В нашій мережі присутні:

- 8 робочих станцій;
- 2 серевери;
- 1 роутер;

Для побудови мережі я використав програмне забезпечення від Cisco – Cisco Packet Tracer, так як там є всі необхідні елементи, щоб створити схему локальної мережі.

Локальна мережа пов’язана з такими приміщеннями:

- Клієнтська зона;
- Касове приміщення;
- Технічна зона;
- Адміністративна зона;
- Конференц – зала;

Локальна мережа має такий вигляд (рисунок 3.3):

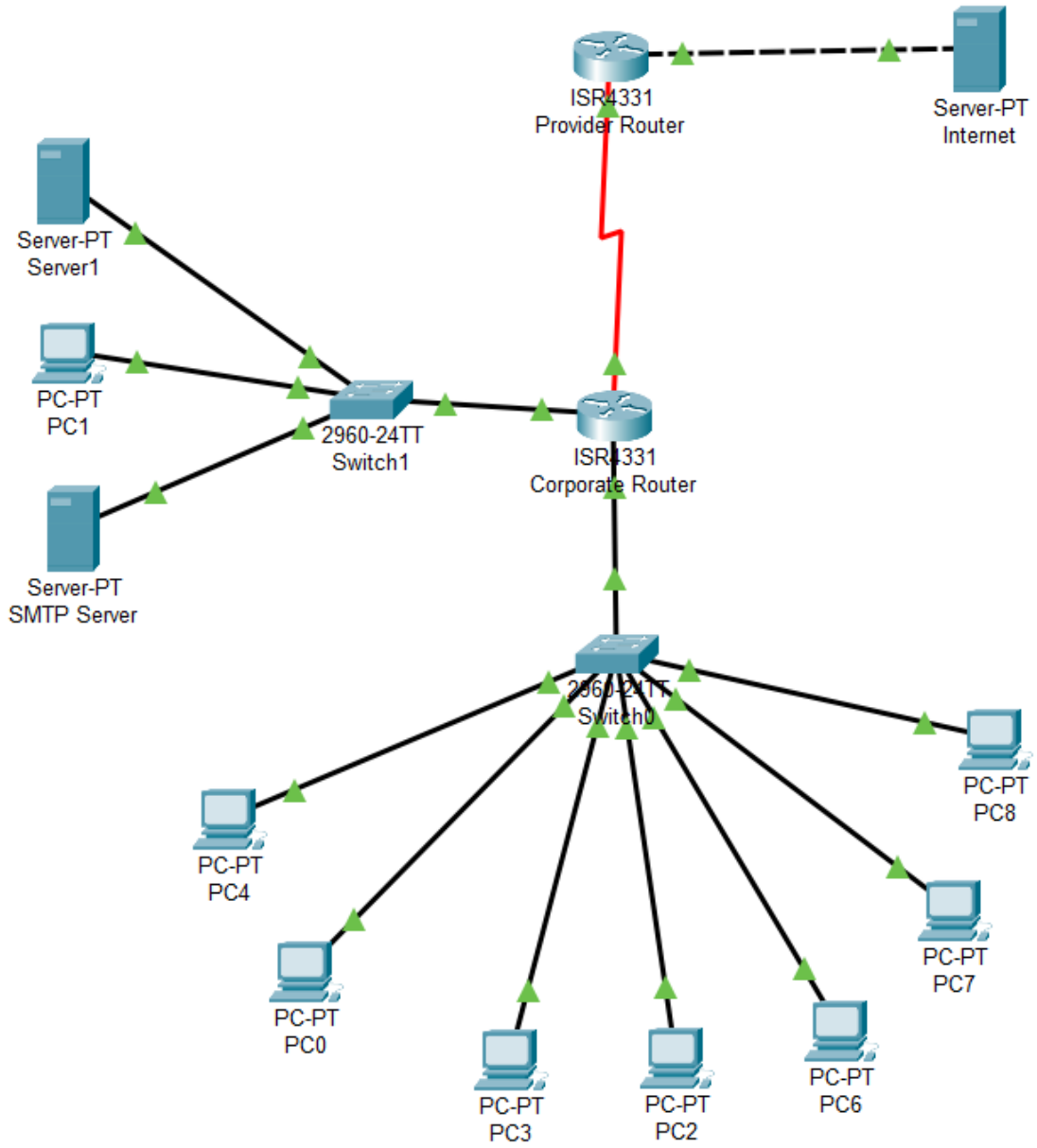


Рисунок 3.3 – Локальна мережа банку

Можемо побачити на рисунку 38, що мережа після роутеру розділяється на комутатори: до одного під'єднанні робочі станції, які знаходяться в Косовому приміщенні, Адміністративній зоні та в Клієнтській зоні; до другого під'єданні серевери та комп'тер, який використовується для спостерігання за камерами відеоспостереження та налашутування серверів.

Тепер зобразимо дану локальну мережу на плані приміщення. На рисунку 3.4 показано локальну мережу банку враховуючи розташування обладнання.

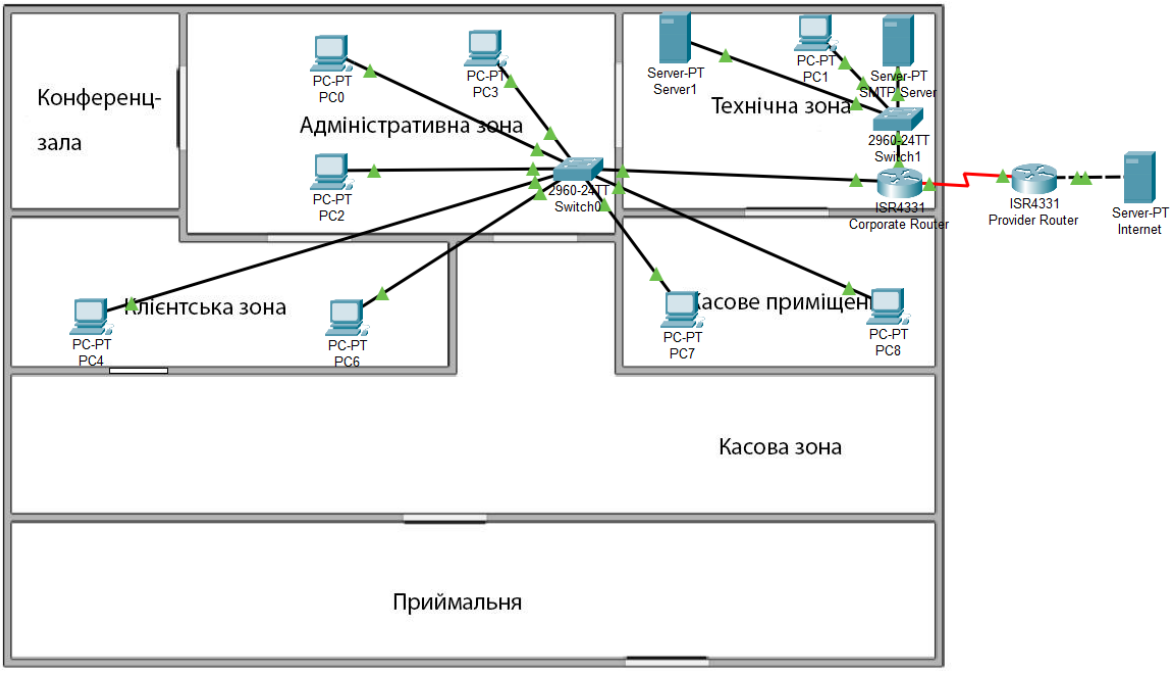


Рисунок 3.4 – Розміщення локальної мережі банку

Схеми плану приміщення та локальної мережі було побудовано, тепер перейдемо до забезпечення комплексного антивірусного захисту.

3.3 Дії при виявленні вірусів

Перед початком налаштування комплексної системи розглянемо вказівоки для працівників та плану дій в разі зіткнення з атакою зловмисників, або в разі винекнення зараження небезпечним ПЗ, оскільки це також є частиною забезпечення комплексного антивірусного захисту.

У разі підозри на наявність комп'ютерного вірусу[39] (нестандартна робота програм, з'явлення графічних та звукових ефектів, спотворення даних, втрата файлів, часті повідомлення про системні помилки та інше), співробітник підрозділу повинен самостійно або разом з відповідальним за забезпечення безпеки інформації підрозділу (технологічного відділу) провести невідкладну перевірку своєї робочої станції на наявність вірусу. У разі потреби можна

залучити спеціалістів організації для визначення факту наявності або відсутності комп'ютерного вірусу.

У разі виявлення заражених комп'ютерними вірусами файлів під час проведення антивірусної перевірки співробітники підрозділів зобов'язані:

- Зупинити роботу;

- Негайно повідомити керівника та відповідального за забезпечення інформаційної безпеки свого підрозділу, власника заражених файлів та суміжні підрозділи, що використовують ці файли;

- Спільно з власником заражених файлів провести аналіз необхідності подальшого їх використання;

- Здійснити лікування або знищення заражених файлів (залучити спеціалістів Організації-адміністратора за потреби);

- У разі виявлення нового вірусу, який не піддається лікуванню антивірусними засобами, передати заражений вірусом файл на гнучкому магнітному диску до Організації-адміністратора для подальшого надсилання його в організацію, з якою укладений договір на антивірусну підтримку;

- Після виявлення заражених вірусом файлів скласти службову записку до відділу забезпечення безпеки інформації, у якій вказати припустиме джерело (відправника, власника тощо) зараженого файлу, тип зараженого файлу, характер інформації, що міститься в файлі, тип вірусу та проведені антивірусні заходи.

3.2 Створення системи комплексного антивірусного захисту локальної обчислювальної мережі

Тепер перейдемо до налаштування системи. В кінці другого розділу ми обрали необхідне нам прогрмне забезпечення задля забезпечення комплексного антивірусного захисту. Розпочнемо налаштовувати систему комплесного

захисту з серверів, яких в нас два: мережевий сервер та SMTP сервер.

Для початку звернемо увагу на SMTP сервер, який необхідний для ефективної роботи електронних скриньок, проте SMTP теж має певний ряд вразливостей:

- Отримання некоректних повідомлень: SMTP сервери можуть бути вразливі до введення некоректних або шкідливих повідомлень, які можуть спричинити переповнення буфера або інші проблеми.

- Використання вразливостей протоколу: протокол SMTP може мати певні вразливості, такі як можливість виконання віддаленого коду або підроблення адреси відправника.

- Слабкі паролі або недостатня аутентифікація: якщо SMTP сервер дозволяє слабкі паролі або має недостатні механізми аутентифікації, зловмисники можуть отримати несанкціонований доступ до поштового сервера.

- Отримання спаму або DDoS-атаки: SMTP сервери можуть стати об'єктом спам-атак або атак типу "затоплення" (DDoS), коли зловмисники намагаються перевантажити сервер запитами.

Встановлення антивірусного забезпечення з функцією забезпечення безпеки електронних пошт користувачів [40], допоможе, як мінімум, запобігти потенційних небезпек, які пов’язанні з зараженним файлами та спамом.

Антивірус з функціоналом захисту електронних пошт виконує ряд таких функцій:

Виявлення та блокування вірусних вкладень - антивіруси можуть сканувати вкладені файли в електронних листах, виявляти потенційно шкідливі файли та блокувати їх перед доставкою на поштовий сервер або в поштову скриньку користувача.

Виявлення та блокування шкідливих посилань - антивіруси можуть аналізувати посилання в електронних листах та перевіряти їх на наявність шкідливих або фішингових сторінок. Вони можуть блокувати доступ до таких

посилань або надавати попередження користувачам про потенційну небезпеку.

Виявлення спаму - багато антивірусних програм мають вбудовані функції виявлення спаму, які допомагають фільтрувати небажані або нежадані повідомлення перед доставкою на поштовий сервер або в поштову скриньку користувача.

Шифрування електронної пошти - деякі антивіруси надають можливість шифрування електронних повідомлень для забезпечення конфіденційності та захисту від перехоплення або несанкціонованого доступу до листів.

Перевірка на вразливості - антивіруси можуть проводити перевірку на вразливості електронної пошти, такі як налаштування сервера SMTP, застосовувані протоколи аутентифікації, контроль доступу тощо. Вони можуть виявляти потенційні слабкі місця та надавати рекомендації з їх виправлення.

Після висновку 2-го розділу, ми прийшли до висновку, що для захисти електронних скринь ми будемо використовувати антивірус Avg.

Встановимо та налаштуємо Avg, для захисту SMTP серверу. Як видно на рисунку 3.5, в Avg наявний необхідний нам функціонал, при цьому данний антивірус дуже простий в налаштуванні та використанні.

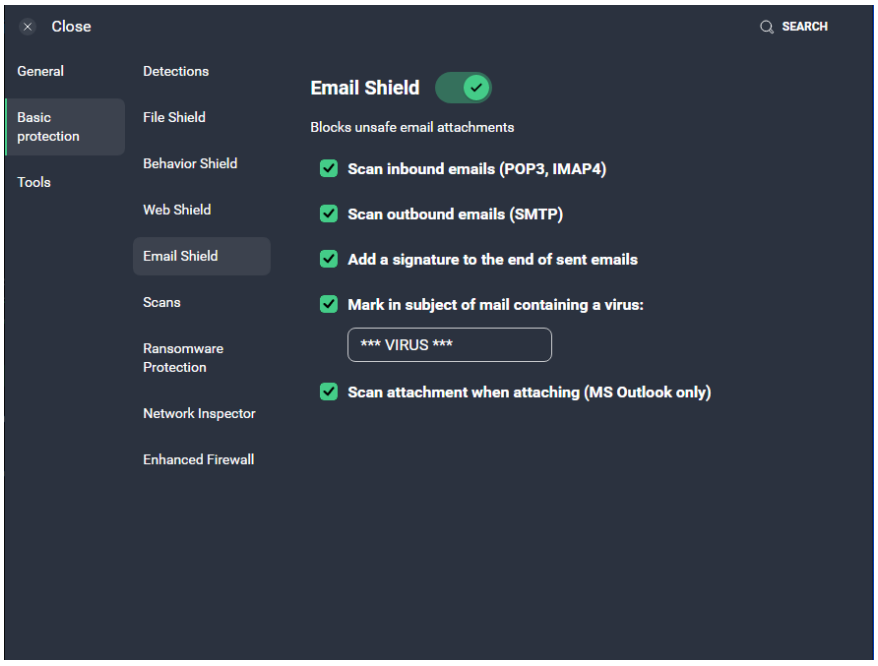


Рисунок 3.5 – Налаштування антивірусу Avg

Тепер забезпечимо антивірусний захист на мережевому сервері. Встановимо та налаштуємо антивірус Avast. Після встановлення перейдемо до налаштування мережевого захисту. Перед цим нам необхідно просканувати нашу мережу. Як видно з рисунків 3.6 та 3.7, сканування мережі пройшло успішно і ми можемо перейти то налаштувань.

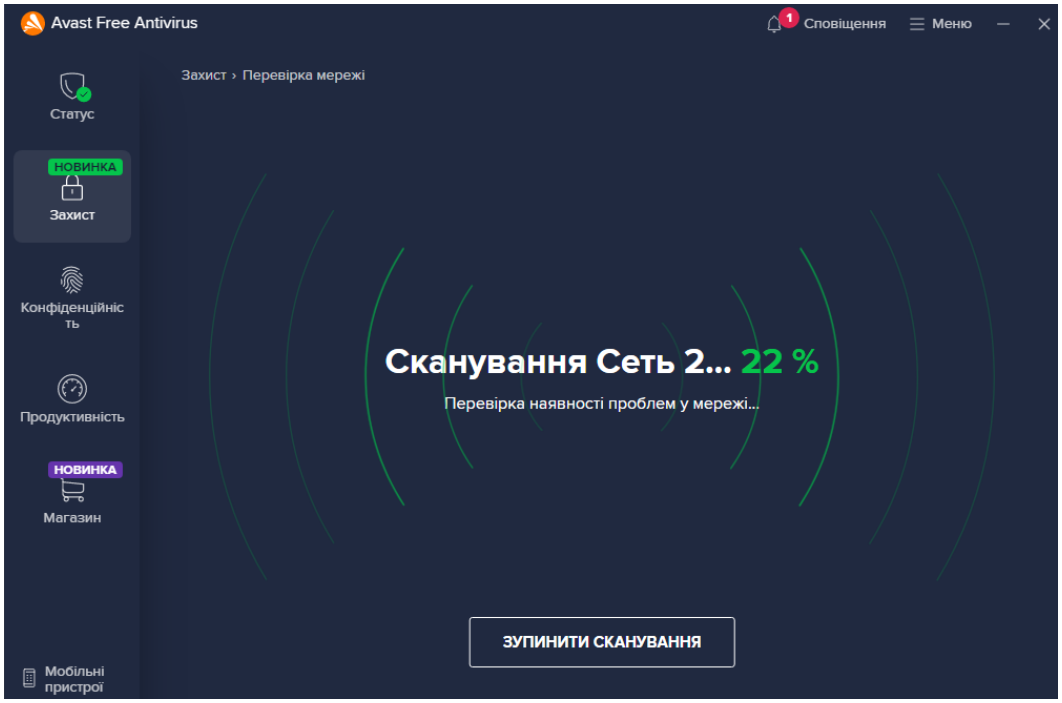


Рисунок 3.6 – Сканування мережі в антивірусі Avast

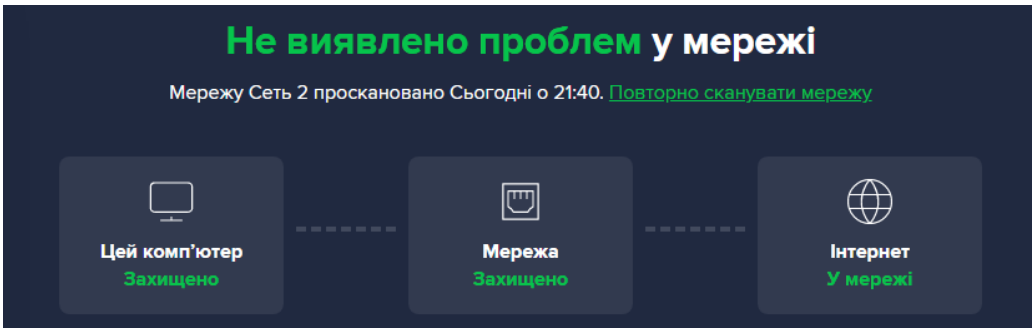


Рисунок 3.7 – Результат сканування мережі

Для цього перейдемо до налаштувань та активуємо всі необхідні функції для мережевого захисту. На рисунку 3.8 продемонстровано налаштування перевірки мережі:

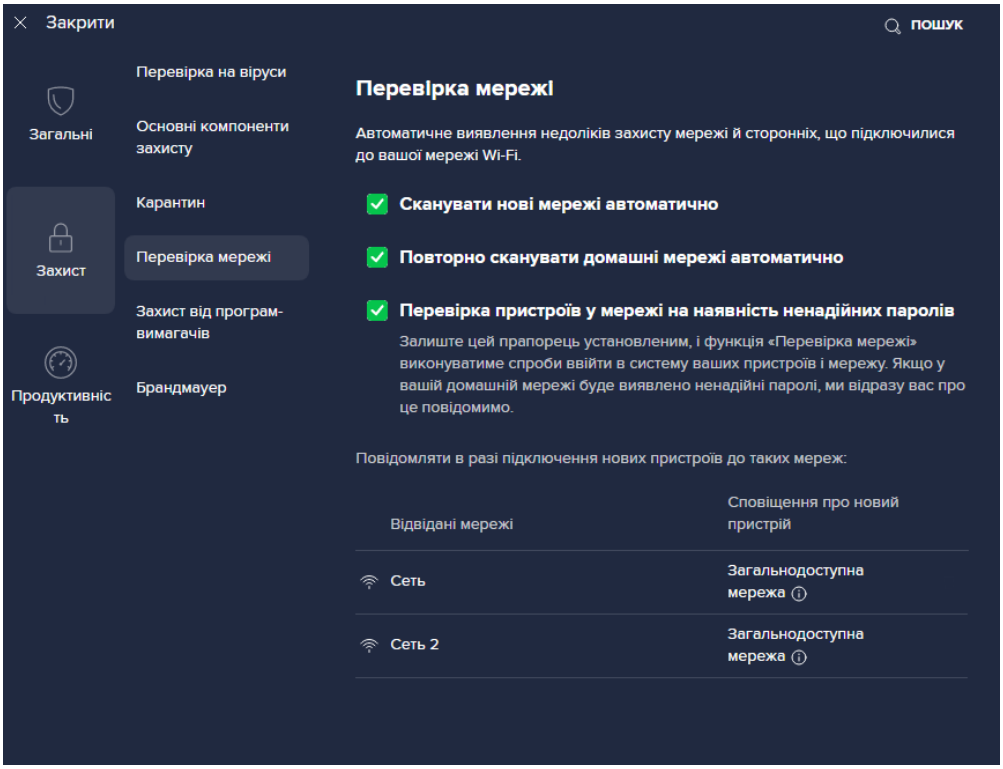


Рисунок 3.8 – Налаштування антивірусу Avast для захисту мережі

Також дотатково ми можемо активувати функцію сканування усіх пристроїв, які налешать до даної мережі та стеження за мережею. Активуємо данні функції (рисунок 3.9):

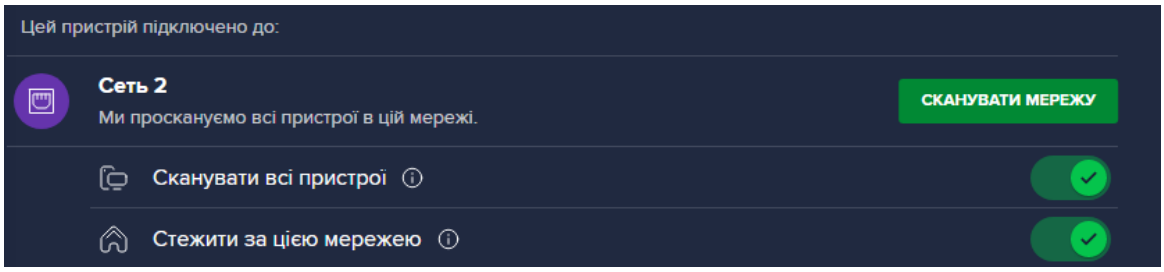


Рисунок 3.9 – Активація функції сканування пристроїм мережі

Далі встановимо та налаштуємо Firewall. В брендмаурі ми маємо налаштування правил програм, велику кількість налаштувань правил мережі та базові правила. Налаштування базових правил брендмаура мають наступний вигляд (рисунок 3.10):

Рисунок 3.10 – Налаштування базових правил брендмаура

Далі налаштуємо правила мережі брендмаура. Налаштування продемонстровано на рисунку 3.11:

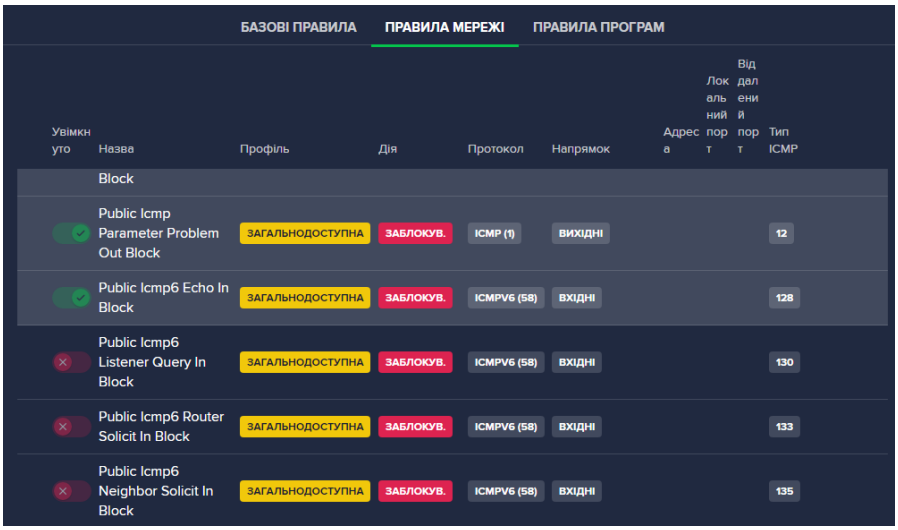


Рисунок 3.11 – Налаштування правил мережі брендмаура

Налаштування брендмаура можуть відрізнятись, все залежить від цілей та задач для яких необхідний сервер. Данного функціоналу цілком достатньо для забезпечення надійного захисту мережі. Залишилось тільки забезпечити антивірусний захист на робочих станціях, як було описано раніше, для цього ми будемо використовувати атівірус Avira.

Встановимо та налаштуємо ативірус Avira для захисту робочих станцій. Нам необхідно активувати всі необхідні нам функції для забезпечення безпеки робочих станцій. Перейдемо до налаштувань антивірусу Avira та перейдемо до розділу «Сканування вірусів». Далі активуємо сканування всіх файлів та сканування архівів всіх форматів. Данні функції можуть використовувати велику кількість ресурсів але враховуючи, що нам не потрібен веб-захист та брендмауер, це не сильно вплине на працездатність робочих станцій і при цьому забезпечить максимально ефективний захист від вірусі. Вмикаємо сканування всіх файлів та сканування архівів. На рисунку 3.12 продемонстрованні наші налаштування антивірусу Avira:

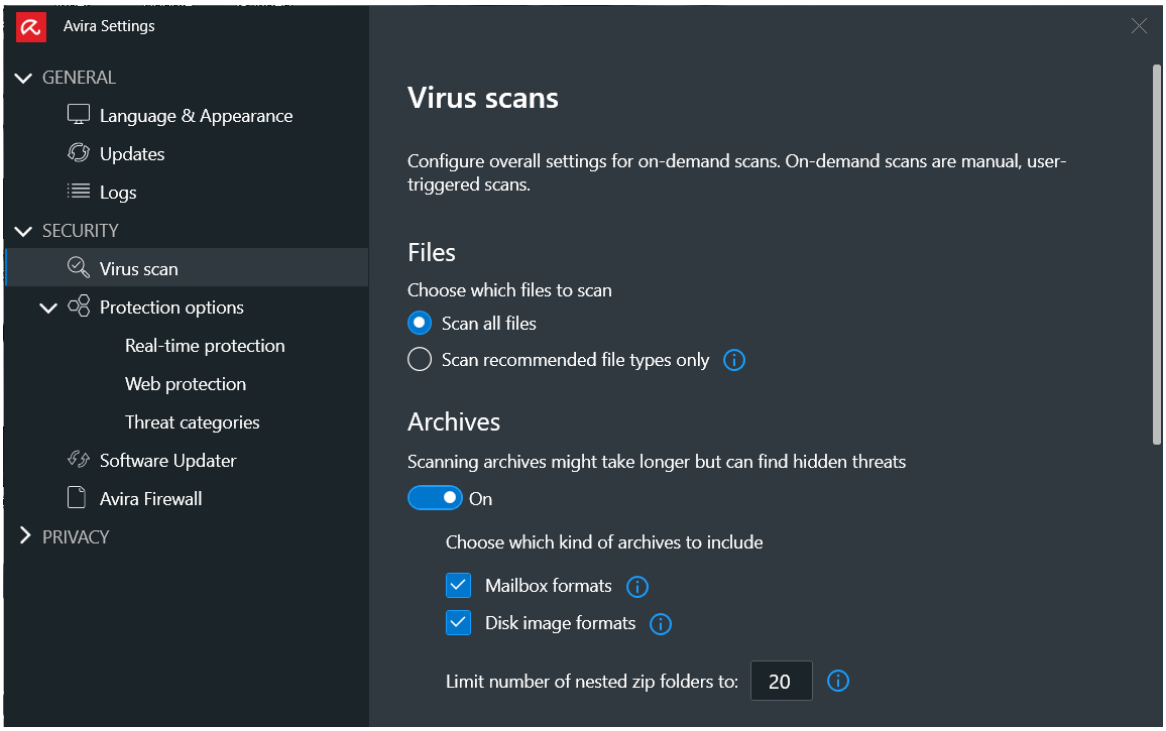


Рисунок 3.12 – Налаштування сканувань в антивірусі Avira

Тепер перейдем до налаштування сканування в режимі реального часу. Данна функція забезпечить надійний захист робочих станцій в будь-який час. Цей функціонал також використовує велику кількість ресурсів і в залежності від потужності комп'ютерів налашутування можуть відрізнятися. Проте ми можемо активувати максимальні налаштування і дану можливість ми маємо

завдяки тому, що ми використовуємо комплексний антивірусний захист. Налаштування сканувань в режимі реального часу мають такий вигляд (рисунок 3.13):

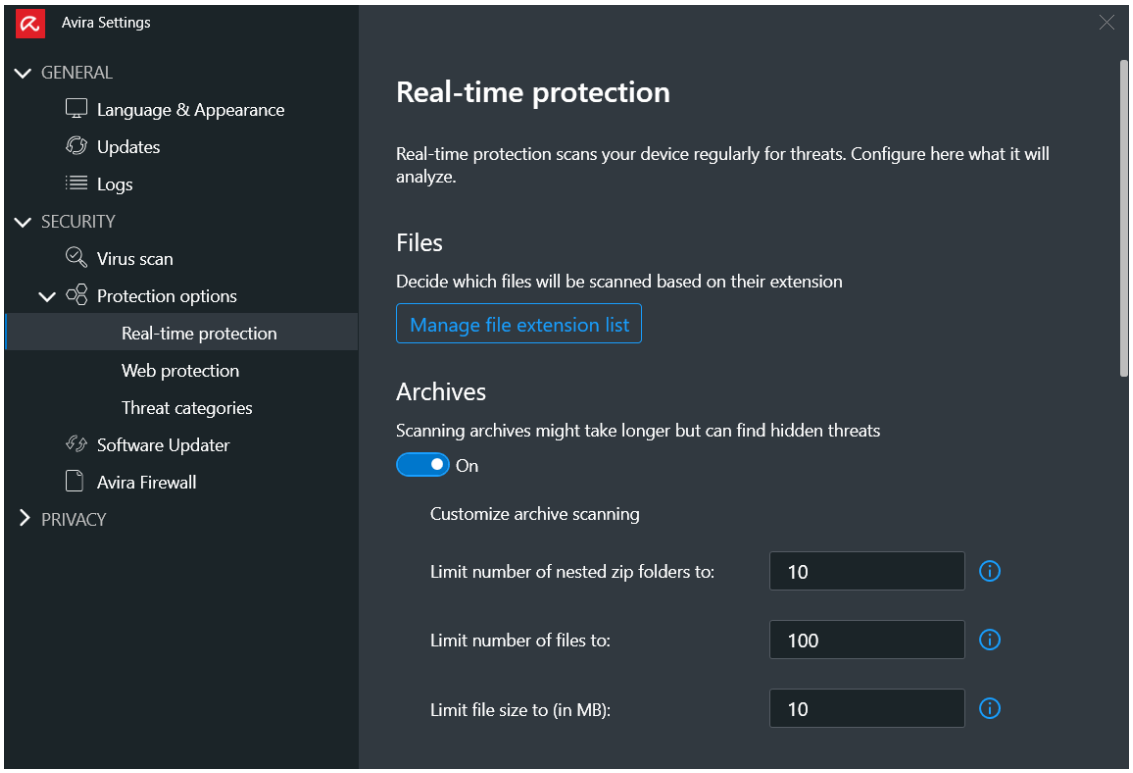


Рисунок 3.13 – Налаштування сканування архівів

Побудувавши систему комплексного антивірусного захисту ми досягли таких цілей:

Забезпечення загальної безпеки системи: система комплексного антивірусного захисту допомагає запобігати атакам та неправомірному доступу до системи. Вона забезпечує захист від вірусів, шкідливих програм, троянських коней та інших загроз, що можуть пошкодити систему або викрасти конфіденційну інформацію;

Захист в реальному часі: система комплексного антивірусного захисту працює в реальному часі, що означає, що вона постійно моніторує активності системи та реагує негайно на потенційні загрози. Це дозволяє виявляти та блокувати шкідливі програми або вразливості ще до їхнього виконання або

завантаження;

Попередження про загрози: система комплексного антивірусного захисту надає інформацію та попередження про потенційні загрози для користувачів. Вона може видавати сповіщення про шкідливі файли, небезпечні посилання або підозрілу активність, допомагаючи користувачам уникнути небажаних ситуацій;

Оновлення та вдосконалення: система комплексного антивірусного захисту постійно оновлюється, щоб виявляти нові загрози та шкідливі програми. Розробники постійно вдосконалюють антивірусні методи та алгоритми, щоб забезпечити максимальний рівень захисту.

Захист корпоративних ресурсів: комплексний антивірусний захист допомагає захищати корпоративні ресурси, такі як мережі, сервери та бази даних, від шкідливих впливів. Він забезпечує безпеку даних, важливих для функціонування організації, та запобігає можливим перервам у роботі.

В даному розділі було виконано всі необхідні задачі: а саме надання вказівок для працівників банку в разі небезпеки та безпосередньо створення та налаштування системи комплексного антивірусного захисту локальної обчислювальної мережі.

ВИСНОВКИ

В ході дипломної роботи на тему «Система комплексного антивірусного захисту локальної обчислювальної мережі філії “Ощадбанку” м. Хмельницький» було досягнуто наступних цілей:

- було проаналізовано ринок різноманітного антивірусного програмного забезпеченння, та відібрано найкращі програми для створення системи комплексного антивірусного захисту локальної обчислювальної мережі;

- досліджено актуальність проблеми захисту комп'ютерних мереж в банківському секторі, особливо з урахуванням поширення вірусів і шкідливого коду, що загрожують конфіденційності і цілісності банківської інформації;

- проаналізовано існуючі методи та підходи до антивірусного захисту локальних обчислювальних мереж, було розглянуто переваги та недоліки різних систем антивірусного захисту;

- розроблено індивідуальну систему комплексного антивірусного захисту для локальної обчислювальної мережі філії “Ощадбанку” м. Хмельницький, так було описано архітектуру системи та її складові частини, включаючи виявлення, блокування та вилучення шкідливих програм, оновлення бази даних вірусних сигнатур та моніторинг активності мережі;

У цілому, досліджена система комплексного антивірусного захисту має великий потенціал для застосування в банківській сфері та може сприяти забезпеченню високого рівня безпеки обчислювальних мереж.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Antonenko N., Horobets Y., Korniichuk A. ANTI-VIRUS PROTECTION OF PROGRAMS AND DATABASES IN THE ACCOUNT. International scientific journal "Internauka". Series: "Economic Sciences". 2022. No. 10(66). URL: https://doi.org/10.25313/2520-2294-2022-10-8366 (дата звернення 02.03.2023).

2. How Does Antivirus Software Work to Protect Your Private Data? URL: https://allaboutcookies.org/how-does-antivirus-software-work (дата звернення 05.03.2023).

3. A Complete Guide to Antivirus Protection & Internet Security in 2023 URL: https://www.security.org/antivirus/ (дата звернення 10.03.2023).

4. Antivirus software guide: what are they for and how to use them URL: https://www.bbva.com/en/innovation/antivirus-software-guide-what-are-they-for-and-how-to-use-them/ (дата звернення 15.03.2023).

5. Antivirus and other security software URL: https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software (дата звернення 23.03.2023).

6. Understanding negotiated anti-malware interruption effects on user decision quality in endpoint security URL: https://www.tandfonline.com/doi/full/10.1080/0144929X.2020.1734087 (дата звернення 25.03.2023).

7. Precise Performance Characterization of Antivirus on the File System Operations URL: https://lib.jucs.org/article/22647/ (дата звернення 29.03.2023).

8. An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404818303080 (дата звернення 01.04.2023).

9. Network Security Basic Training Series: Anti-Virus Protection URL: https://www.netsurion.com/articles/7-things-you-need-to-know-about-anti-virus-

protection (дата звернення 02.04.2023).

10. The Role of Antivirus Software in Cyber Security: A Comprehensive Guide URL: https://www.linkedin.com/pulse/role-antivirus-software-cyber-security-comprehensive-guide (дата звернення 04.04.2023).

11. Outsmarting the Super-Hackers By Securing Smart Autonomous Systems URL: https://partners.wsj.com/tii/catalyzing-change/outsmarting-the-super-hackers/?utm_medium=content_discovery&utm_source=googlesearch&gclid=EAIaIQobChMIr4jO1Pk_wIVvSB7Ch2QUgchEAMYASAAEgIM3_D_BwE (дата звернення 06.04.2023).

12. You Don't Need to Buy Antivirus Software URL: https://www.nytimes.com/wirecutter/blog/best-antivirus/ (дата звернення 08.04.2023).

13. What is an antivirus product? Do I need one? URL: https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product (дата звернення 10.04.2023).

14. Here's Why Antivirus Software Is Important URL :https://greenwireit.com/infosec/heres-why-antivirus-software-is-important/ (дата звернення 11.04.2023).

15. What is Antivirus Protection for Business? URL: https://www.cdw.com/content/cdw/en/articles/security/what-is-antivirus-protection-for-business.html (дата звернення 12.04.2023).

16. Best antivirus software 2023: Which? Best Buys and expert buying advice URL: https://www.which.co.uk/reviews/antivirus-software-packages/article/how-to-choose-the-best-antivirus-software-apUAV8K23gJj (дата звернення 13.04.2023).

17. How Does Antivirus Software Work? URL: https://www.usnews.com/360-reviews/privacy/antivirus/how-does-antivirus-software-work (дата звернення 13.04.2023).

18. Best antivirus software for 2023 URL: https://cybernews.com/best-antivirus-software/ (дата звернення 14.04.2023).

19. What Is Critical Infrastructure Security and Why Is It Necessary? URL: https://eiscouncil.org/criticalinfrastructuresecurity/?utm_source=google_ads&utm_medium=18066543991&ad_group=142265902484&ad=618662762381&device=c&keyword=importance%20of%20cybersecurity&gclid=EAIaIQobChMIsYO2v4Ol_wIVhRDmCh3gzglwEAAYBCAAEgJNdfD_BwE (дата звернення 14.04.2023).

20. Effect of anti-malware software on infectious nodes in cloud environment URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404815001959 (дата звернення 14.04.2023).

21. Antivirus Impact on Build Speed URL: https://intellij-support.jetbrains.com/hc/en-us/articles/360006298560-Antivirus-Impact-on-Build-Speed (дата звернення 15.04.2023).

22. What's The Difference Between Antivirus and Firewall Software? URL: https://www.simplilearn.com/difference-between-antivirus-and-firewall-software-article (дата звернення 17.04.2023).

23. Protect Your Computer Against Viruses and Malware URL: https://ithelp.brown.edu/kb/articles/protect-your-computer-against-viruses-and-malware (дата звернення 17.04.2023).

24. Tech Paper: Endpoint Security, Antivirus, and Antimalware Best Practices URL: https://docs.citrix.com/en-us/tech-zone/build/tech-papers/antivirus-best-practices.html (дата звернення 18.04.2023).

25. 11 Advantages of Using an Antivirus Software – Importance of Online Security URL: https://geekflare.com/advantages-using-antivirus/ (дата звернення 18.04.2023).

26. Is Your Antivirus Software Really Protecting Your Business? URL: https://www.businessnewsdaily.com/6634-antivirus-software-protection.html (дата звернення 19.04.2023).

27. Protect Your Computer From Viruses, Hackers, and Spies URL: https://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer (дата звернення 19.04.2023).

28. Malware Threats Can Easily Bypass Antivirus Software URL: https://www.spiceworks.com/it-security/data-security/articles/malware-threats-can-easily-bypass-antivirus-software/ (дата звернення 20.04.2023).

29. What is antivirus software (antivirus program)? URL: https://www.techtarget.com/searchsecurity/definition/antivirus-software (дата звернення 20.04.2023).

30. Avast blog URL: https://blog.avast.com (дата звернення 21.04.2023).

31. Avast Antivirus Review 2023 URL: https://www.comparitech.com/antivirus/reviews/avast-antivirus-review/ (дата звернення 21.04.2023).

32. Avast Free Antivirus Review URL: https://www.pcmag.com/reviews/avast-free-antivirus (дата звернення 22.04.2023).

33. AVG Signal Blog URL: https://www.avg.com/en/signal (дата звернення 23.04.2023).

34. AVG AntiVirus Free Review URL:https://www.cloudwards.net/avg-review/ (дата звернення 23.04.2023).

35. Avira Blog URL: https://www.avira.com/en/blog/technology-insights/all-articles (дата звернення 24.04.2023).

36. Avira Review: Is It the Best Antivirus in 2023? URL: https://www.safetydetectives.com/best-antivirus/avira/ (дата звернення 24.04.2023).

37. Microsoft Defender Antivirus in Windows URL: https://learn.microsoft.com/enus/microsoft365/security/defenderendpoint/microsoft-defender-antivirus-windows?view=o365-worldwide (дата звернення 25.04.2023).

38. Supervision and Regulation of Network Banks URL: https://firstmonday.org/ojs/index.php/fm/article/view/544/465 (дата звернення 3.05.2023).

39. ANALYSIS AND RESEARCH OF THE CHARACTERISTICS OF STANDARDIZED IN UKRAINE ANTIVIRUS SOFTWARE URL:

https://www.researchgate.net/publication/334198724_ANALYSIS_AND_RESEARCH_OF_THE_CHARACTERISTICS_OF_STANDARDIZED_IN_UKRAINE_ANTIVIRUS_SOFTWARE (дата звернення 10.05.2023).

40. Malware Threats Can Easily Bypass Antivirus Software URL: https://www.spiceworks.com/it-security/data-security/articles/malware-threats-can-easily-bypass-antivirus-software/ (дата звернення 13.05.2023).

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Кальчун Б.В

Тема: «Система комплексного антивірусного захисту локальної обчислювальної мережі філії "Ощадбанку" м. Хмельницький»

Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3 ; кількість сторінок записки 62;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена дослідженню питань та проблем забезпечення безпеки локальних обчислювальних мереж від вірусів та інших шкідливих програм. Для досягнення цієї мети було проведено дослідження різних засобів для забезпечення антивірусного захисту, їх переваг та недоліків, а також методів їх впровадження в підприємство. Робота має на меті допомогти підприємствам забезпечити безпеку своїх даних та інформації, зменшити витрати на їхнє захист та уникнути можливих витоків даних.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи та її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено аналіз існуючих антивірусних методів захисту та загроз для системи підприємства, що дозволило виявити проблеми та завдання, що потребують вирішення; застосування принципів побудови систем комплексного антивірусного захисту стало основою для постановки задачі і проєктування архітектури системи. У другому розділі було проаналізовано та протестоване різноманітне антивірусне програмне забезпечення та відібрано для створення системи комплексного антивірусного захисту. У третьому розділі наведено опис процесу реалізації системи комплексного антивірусного захисту на підприємстві, включаючи планування приміщення, підбір програмного забезпечення, проведено оцінку ефективності впровадженої системи контролю.

4. Позитивні сторони кваліфікаційної роботи полягають у тому що, вона дозволяє розглянути розробку і впровадження ефективної системи антивірусного захисту, що знижує ризик поширення шкідливих програм і вірусів в мережі. Це допомагає захистити конфіденційну інформацію підприємства, запобігає втратам даних та можливим кібератакам.. Підприємство зазнало покращення своєї інформаційної безпеки і здатне ефективно впоратися з потенційними загрозами і порушниками. В цілому, реалізація системи комплексного антивірусного захисту на підприємстві виявилася успішною і відповідає вимогам та потребам підприємства. Застосування відповідних технологій та процедур дозволило забезпечити підвищену інформаційну безпеку і зменшити ризики несанкціонованого доступу. Реалізована система є надійним інструментом для антивірусного захисту цінної інформації та забезпечення безпеки на підприємстві.

5. Негативні сторони проекту: кваліфікаційна робота в певних аспектах має недостатню кількість деталей /аналізу з питання антивірусного захисту локальної обчислювальної мережі. Недостатня глибина аналізу може обмежити розуміння проблеми та можливість запропонувати належні рекомендації.

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі проектування.

8. Інші зауваження Мережеві налаштування та налаштування брандмауера, могли бути показані більш детально.

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «відмінно/ А (4,75)».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) _____

Гурман Іван Васильович, к.т.н, доцент кафедри інженерія програмного забезпечення, Хмельницького національного університету

« 7 » червня 2023 . _____ (підпис)

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Система комплексного антивірусного захисту локальної обчислювальної мережі філії "Ощадбанку" м. Хмельницький

Автор: Кальчун Богдан Володимирович
Спеціальність: 125 – Кібербезпека
Освітня програма: «Кібербезпека»
Науковий керівник: Джулій Володимир Миколайович, к.т.н, доцент
Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 93.04%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про дотримання академічної доброчесності в Хмельницькому національному університеті (http://www.khnu.km.ua/root/files/01/10/03/0005.pdf) така авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту.

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

1. Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 6.96%, з яких 2.03% є збігами з одним джерелом, зумовленими наявністю типових фразеологічних виразів предметної області, а також формулюваннями, які утворюють загальновживані фрази.
2. Інші три збіги є збігами в назвах використаних друкованих видань, розміщених в переліку джерел посилань

Керівник роботи _____ В. М. Джулій

Завідувач кафедри кібербезпеки _____ Ю. П. Кльоц

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 13%**

	Документ		Сумарний збіг по Базі Даних	
ID: 114873 Назва: Система комплексного антивірусного захисту локальної обчислювальної мережі філії “Ощадбанку” м. Хмельницький Додано в БД: 2023-06-05 Автора: Кальчун Б.В. Керівники: Джулій В.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	56833	882	392 (1%)	9 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015445247

Дата перевірки:
05.06.2023 23:21:42 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
05.06.2023 23:22:10 EEST

ID користувача:
100008300

Назва документа: **Кальчун**

Кількість сторінок: **62** Кількість слів: **9500** Кількість символів: **75262** Розмір файлу: **3.08 MB** ID файлу: **1015105526**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

6.96%
Схожість

Найбільша схожість: **2.03%** з джерелом з Бібліотеки (ID файлу: **1015080230**)

6.31% Джерела з Інтернету	468	Сторінка 64
2.31% Джерела з Бібліотеки	86	Сторінка 66

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Підозріле форматування	20 сторінок