ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ СЕРВІСНОГО ЦЕНТРУ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ РІШЕННЯ ESET»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Ващук О.М.
(прізвище та ініціали)

Керівник Марченко В.В.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Ващуку Олексію Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи сервісного центру від шкідливого програмного забезпечення на базі рішення ESET»
керівник бакалаврської роботи Марченко Віталій Вікторович, ст. викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24» лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
інформаційна система сервісного центру;
програмний комплекс захисту інформаційної системи;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту інформаційної системи.
2. Зміст процесу реагування на кіберінциденти в корпоративній інформаційній системі.
3. Методи та засоби захисту інформаційної системи за допомогою ESET.
4. Рекомендації щодо застосування методів та засобів захисту інформаційної системи за допомогою рішення ESET.

5. Перелік графічного матеріалу

1. Тема бакалаврської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу проблеми захисту інформаційної системи.

4. Результати аналізу методів та засобів захисту інформаційної системи.

5. Результати аналізу існуючого стану інформаційної системи сервісного центру

6. Призначення та можливості рішення ESET Smart Security Premium.

7. Рекомендації щодо застосування методів та засобів захисту інформаційної системи.

8. Практична реалізація рекомендацій.

9. Висновки за результатами роботи.

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Визначення актуальності проблеми захисту інформаційної системи сервісного центру.	24.02.2023 р.	виконано
2.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	15.03.2023 р.	виконано
3.	Аналіз методів та засобів захисту інформаційної системи.	12.04.2023 р.	виконано
4.	Розроблення рекомендацій щодо застосування методів та засобів захисту інформаційної системи.	15.05.2023 р.	виконано
5.	Оформлення результатів дослідження.	22.05.2023 р.	виконано
6.	Підготовка доповіді до захисту.	28.05.2021 р.	виконано

Студент _____ Ващук О.М.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на бакалаврську роботу

студента Ващука Олексія Миколайовича
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи сервісного центру від шкідливого програмного забезпечення на базі рішення ESET»

Актуальність: На сьогоднішній день загрози шкідливих програм стають все більш складними та небезпечними, і необхідно постійно вдосконалювати методи захисту. Забезпечення безпеки в сервісних центрах є важливим, оскільки вони мають доступ до конфіденційної інформації і даних клієнтів, тож вразливість їх інформаційних систем може призвести до крадіжки цих даних, шантажу та інших видів кіберзлочинності.

Використання рішення ESET може бути ефективним способом захисту, оскільки ця система має добре визнану репутацію і надійні функції для виявлення та блокування шкідливого програмного забезпечення. Тому тема бакалаврської є актуальною та своєчасною.

Позитивні сторони:

1. У роботі проведено аналіз існуючих загроз та рішень. Розглянуті сучасні варіанти захисту інформаційної системи.
2. Було розглянуто методи та засоби захисту інформації за допомогою ESET Smart Security Premium.
3. Розроблено рекомендації щодо захисту інформаційної системи сервісного центру.

Недоліки:

1. У бакалаврській роботі бажано було б провести порівняння усіх схожих продуктів від ESET.
2. Практичне застосування розроблених рекомендацій бажано було б провести в реальних умовах.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговую оцінку **задовільно**, а студент **Ващук О.М. –** присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Ващук О.М. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи сервісного центру від шкідливого програмного забезпечення на базі рішення ESET»
Бакалаврська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Ващук О.М. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент Ващук О.М. обрав тему роботи, метою якої було дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи сервісного центру від ШПЗ на базі рішення ESET. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Ващук О.М. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану бакалаврську роботу студента Ващука Олексія Миколайовича на оцінку «**задовільно**» та присвоїти йому кваліфікацію: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Ващук О.М.
(прізвище та ініціали)
допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії.
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: 43 сторінок, 22 рисунків, 2 таблиці, 12 джерел.

Об'єкт дослідження – Об'єктом дослідження є інформаційна система сервісного центру.

Предмет дослідження – Предметом дослідження є захист інформаційної системи сервісного центру від ШПЗ на базі рішення ESET.

Мета роботи – Метою даної дипломної роботи є дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи сервісного центру від ШПЗ на базі рішення ESET.

Методи дослідження – Опрацювання літератури та існуючих робіт, аналіз ІС СЦ, функцій та можливостей рішення ESET.

В даній роботі проведено аналіз існуючих загроз, представлені методи та їх класифікації.

Розглянуті приклади програм які надають комплексні рішення захисту інформації.

Проаналізовані основні принципи захисту інформаційної системи.

Досліджено про ключові проблеми та вразливості інформаційної системи.

Проаналізовано принцип роботи захисту системи за допомогою рішення від ESET.

На основі досліджень були побудовані рекомендації щодо захисту та покращення безпеки інформаційної системи.

Галузь використання – кібербезпека інформаційної системи сервісного центру.

ІНФОРМАЦІЙНА СИСТЕМА, ЗАХИСТ СИСТЕМ, ЗАГРОЗИ, КІБЕРБЕЗПЕКА, ESET, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ, СЕРВІСНИЙ ЦЕНТР

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІС – інформаційні системи

ШПЗ – шкідливе програмне забезпечення

СЦ – сервісний центр

ЗІ – захист інформації

ІБ – інформаційна безпека

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

БД – база даних

HIPS - Host-based Intrusion Prevention System

ВСТУП

Актуальність дослідження. Захист інформаційних систем є однією з найважливіших задач для будь-якої організації, особливо тих, які мають справу з обробкою конфіденційної і чутливої інформації.

У сучасному світі загрози кібербезпеці стають все більш складними і високоорганізованими. Шкідливе програмне забезпечення, таке як віруси, троянські програми, шпигунське програмне забезпечення та інші види зловмисного коду, постійно еволюціонує та знаходить нові шляхи проникнення в системи. Це може призвести до ряду негативних наслідків, таких як втрата даних, порушення конфіденційності, пошкодження репутації організації і фінансові втрати. Застосування рішень для захисту інформаційних систем, таких як ESET, стає важливим етапом в забезпеченні кібербезпеки. ESET є одним з провідних постачальників антивірусного програмного забезпечення і відомий своєю ефективністю та надійністю.

Проте, навіть найсучасніші захисні рішення не можуть гарантувати 100% захисту від нових загроз, оскільки зловмисники постійно шукають нові методи обходу захисту.

Тому дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи сервісного центру від шкідливого програмного забезпечення на базі рішення ESET є надзвичайно важливим. Це дозволить організації покращити свої процеси захисту, виявляти нові загрози та реагувати на них, забезпечуючи надійний рівень кібербезпеки. Результати дослідження можуть бути корисні для сервісних центрів, які використовують рішення ESET для захисту своїх інформаційних систем.

Об’єкт дослідження – Об’єктом дослідження є інформаційна система сервісного центру.

Предмет дослідження – Предметом дослідження є захист інформаційної системи сервісного центру від шкідливого програмного забезпечення на базі рішення ESET.

Мета роботи – Метою даної дипломної роботи є дослідження шляхів та розробка рекомендацій щодо захисту інформаційної системи сервісного центру від ШПЗ на базі рішення ESET.

Завдання бакалаврської роботи:

проаналізувати методи захисту інформаційної системи;

дослідити існуючі рішення щодо захисту інформаційної системи;

проаналізувати існуючі загрози інформаційної системи;

дослідити захист інформації за допомогою рішення ESET;

розробити рекомендації для підвищення захисту інформаційної системи сервісного центру;

Мета дослідження – Опрацювання літератури та існуючих робіт, аналіз інформаційної системи сервісного центру, функцій та можливостей рішення ESET *Практичне значення одержаних результатів:* рекомендації щодо покращення безпеки інформаційної системи сервісного центру допоможуть захистити конфіденційну інформацію клієнтів від викрадення або пошкодження.

1 ТЕОРЕТИЧНИЙ АНАЛІЗ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Огляд літератури та існуючих рішень

Інформаційна система містить як організаційні, так і технічні компоненти, які використовуються для зберігання та обробки інформації для задоволення вимог користувачів. Оскільки обсяг даних, які створюються та зберігаються, зростає з великою швидкістю, захист даних стає все більш важливим. Крім того, бізнес-операції все більше залежать від даних і навіть короткий період простою або невелика втрата даних може мати серйозні наслідки для бізнесу. Також необхідно розуміти, що захист інформаційних систем від ШПЗ є складним завданням, оскільки ШПЗ не стоять на місці, а постійно еволюціонують і вдосконалюють свої методи. Поглиблений аналіз наукових та практичних джерел надає можливість дізнатися про існуючі методи та рішення для захисту від ШПЗ. Розглянемо деякі методи захисту наведені у таблиці 1.1.

Таблиця 1.1.

Класифікація методів захисту від ШПЗ

Метод	Класифікація
Антивірусне програмне забезпечення	Антивірусні програми виявляють, блокують та нейтралізують ШПЗ, використовуючи різні методи, такі як сигнатурний аналіз, аналіз поведінки, евристичний аналіз та хмарні технології. Вони сканують систему на наявність вірусів, черв’яків, троянських програм та іншого ШПЗ.

Продовження таблиці 1.1.

Класифікація методів захисту від ШПЗ

Метод	Класифікація
Мережевий екран	Мережевий екран є першим рівнем захисту мережі. Вони контролюють трафік, що проходить через мережеві з'єднання і блокують небажані або підозрілі підключення. Мережеві екрани можуть використовувати різні методи, такі як фільтрація на основі правил, виявлення вторгнень та системи запобігання вторгненням.
Антишпигунське програмне забезпечення	ШПЗ збирає конфіденційну інформацію про користувача без його згоди та передає її зловмисникам. Антишпигунські програми виявляють та видаляють шпигунське ПЗ, а також забезпечують контроль за небажаною активністю.
Антивірусні шлюзи та проксі-сервери	Ці системи встановлюються між внутрішньою мережею організації та зовнішнім Інтернетом. Вони перевіряють вхідний та вихідний мережевий трафік на наявність ШПЗ та блокують його.
Патчі та оновлення	Шкідливе програмне забезпечення може використовувати вразливості в операційних системах або програмах для злому системи. Важливо регулярно оновлювати всі програми та операційну систему, щоб виправити виявлені уразливості.

Розглянемо декілька прикладів програм які надають комплексні системи захисту інформації

Avast [1] – чеська компанія заснована у 1988. Пропонує своїм користувачам захист як для домашніх пристроїв, так і бізнес-рішення. Є безкоштовна версія антивірусного ПЗ яка надає такі послуги:

- Безпеку мережі Wi-Fi
- Безпечне користування електронною поштою
- Захист від програм-вимагачів
- Сповіщення про витік даних

Avast доступний на пристроях з Windows, IOS X та андроїд.

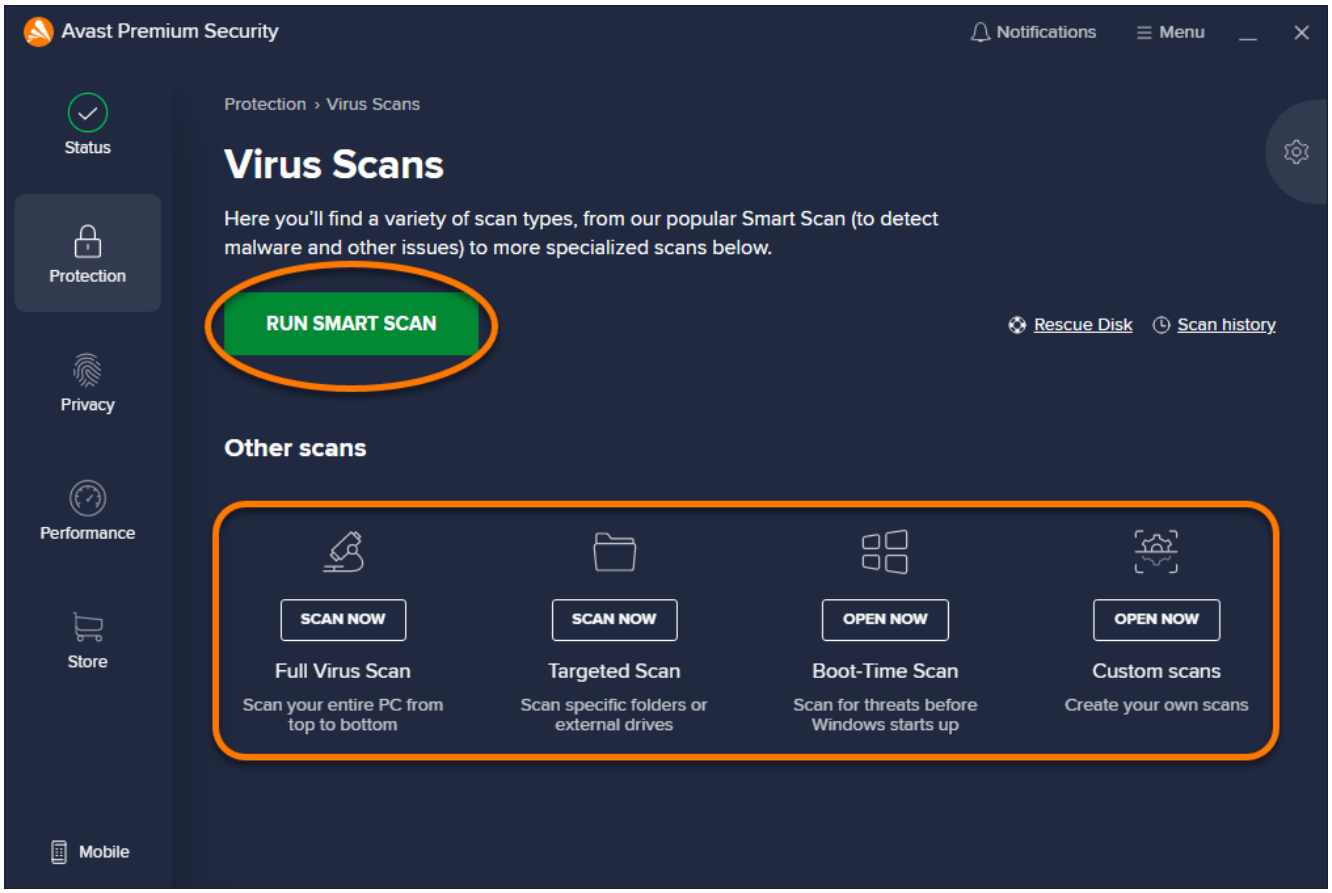

Рис. 1.1. Інтерфейс Avast Premium Security [2]

Bitdefender [3] – румунська компанія пропонує такі послуги:

- Захист від фішингу
- Безпечний онлайн-банкінг

- Bitdefender VPN
- Багаторівневий захист від програм-вимагачів
- Менеджер паролів
- Відстеження використання веб-камери та мікрофона

З недоліків варто відмітити, що були випадки витоку інформації, про що повідомляє сама компанія. [1]

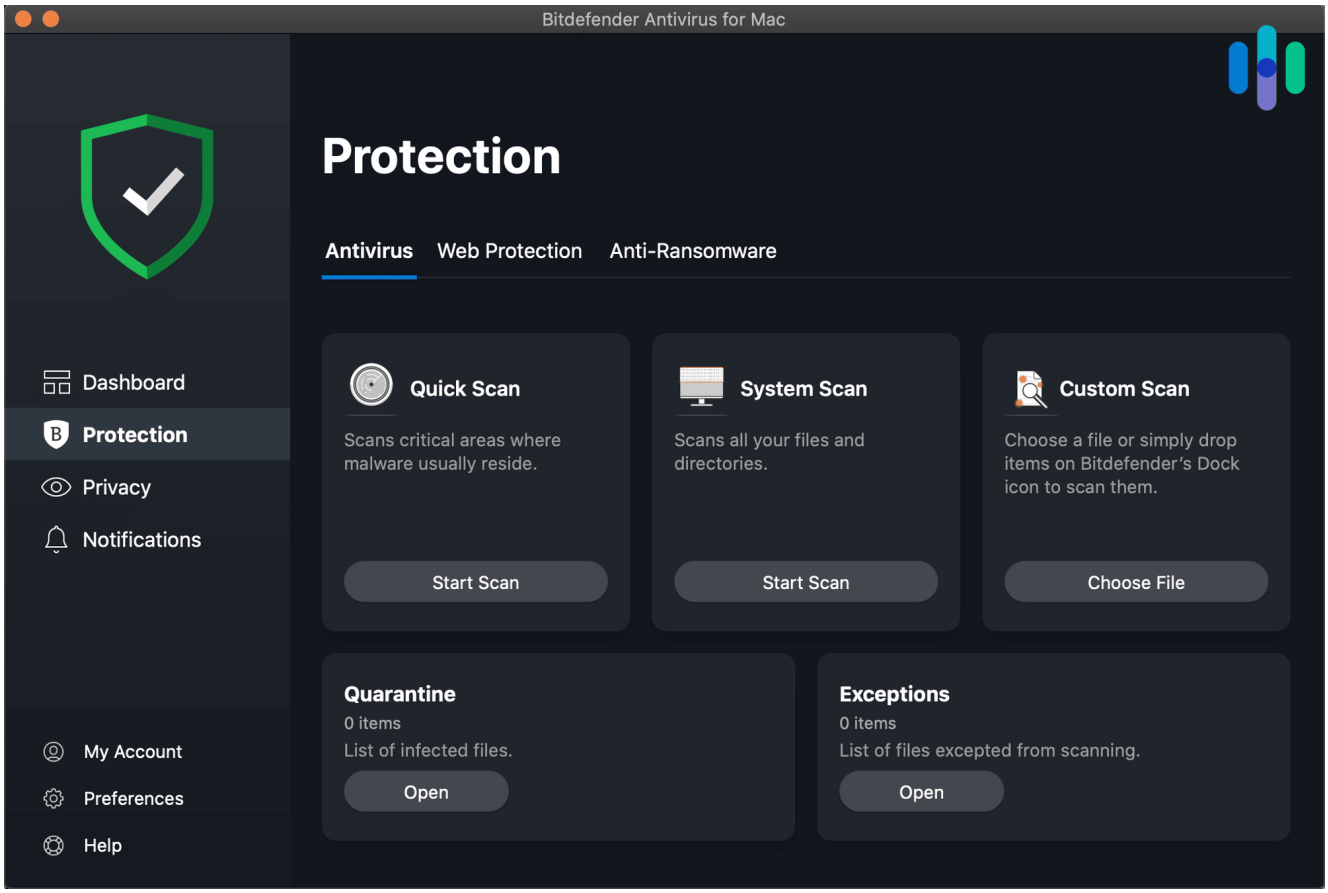

Рис. 1.2. Інтерфейс Bitdefender Antivirus [4]

Kyivstar [5] – українська компанія мобільного зв'язку також пропонує свої послуги у сфері кібербезпеки для бізнесу:

- Захист електронної пошти
- Багаторівневий захист мережі
- Захист Web-додатків від шкідливого трафіку з інтернету
- Захист корпоративної мережі від неавторизованих користувачів
- Система захисту даних для аналізу поведінки користувачів

- Захист кінцевих точок
- Резервне копіювання та аварійне відновлення
- Оптимізація файлового сховища

1.2. Основні принципи захисту інформаційної системи

Захист інформаційних систем є важливою задачею, оскільки ІС містять значну кількість цінної інформації, яка потребує захисту від несанкціонованого доступу, викрадення, пошкодження або знищення. Концепція захисту ІС передбачає впровадження набору заходів, що мають на меті забезпечення конфіденційності, цілісності та доступності інформації, а також забезпечення безпеки самої системи.

Основні підходи до захисту інформаційних систем включають:

1. Інженерний захист: Цей підхід передбачає застосування заходів для захисту фізичного середовища, в якому знаходиться ІС. Це можуть бути заходи, такі як обмеження доступу до приміщення з обладнанням, встановлення контрольного доступу, використання систем відеоспостереження та фізичного замикання пристроїв.

2. Технічний захист: Цей підхід передбачає використання різноманітних технологій та заходів для захисту ІС на рівні програмного забезпечення та мережі. Це можуть бути системи аутентифікації та авторизації, шифрування даних, встановлення мережевих брандмауерів та інші технічні засоби, що допомагають уникнути несанкціонованого доступу.

3. Організаційний захист: Цей підхід передбачає впровадження політик, процедур та норм, що регулюють поведінку користувачів ІС. Це може включати політики паролів, політики використання ресурсів, навчання персоналу щодо правил безпеки та управління ризиками.

4. Криптографічний захист: Цей підхід використовує криптографічні методи для захисту інформації, шляхом шифрування даних, підписування цифрових підписів та інших технік криптографії.

Варто зазначити, що захист інформаційних систем є комплексним завданням, і ефективний захист вимагає комбінації різних підходів та заходів. Компанії та організації повинні використовувати поєднання фізичного, логічного, організаційного та криптографічного захисту для забезпечення найвищого рівня безпеки своїх інформаційних систем.

Основні принципи захисту інформації, які широко використовуються в контексті захисту інформаційних систем, включають [6]:

1. Принцип доступності: Цей принцип встановлює, що інформаційна система та її ресурси мають бути доступні в потрібний час користувачам, які мають право доступу до них. Захист доступності полягає у запобіганні несанкціонованому перериванню чи забороні доступу до системи, що може бути спричинене наприклад, кібератаками або технічними недоліками.

2. Принцип цілісності: Цей принцип встановлює, що інформація має бути цілісною, тобто вона повинна бути захищена від несанкціонованого змінення або втрати. Захист цілісності передбачає застосування заходів, таких як контроль цілісності даних, цифровий підпис, контроль версій, аудит та інші механізми для виявлення та запобігання несанкціонованим змінам інформації.

3. Принцип конфіденційності: Цей принцип встановлює, що інформація повинна бути доступна лише тим особам, які мають право доступу до неї. Захист конфіденційності передбачає використання методів шифрування, аутентифікації, контролю доступу та інших механізмів, що забезпечують конфіденційність інформації та запобігають несанкціонованому доступу до неї.

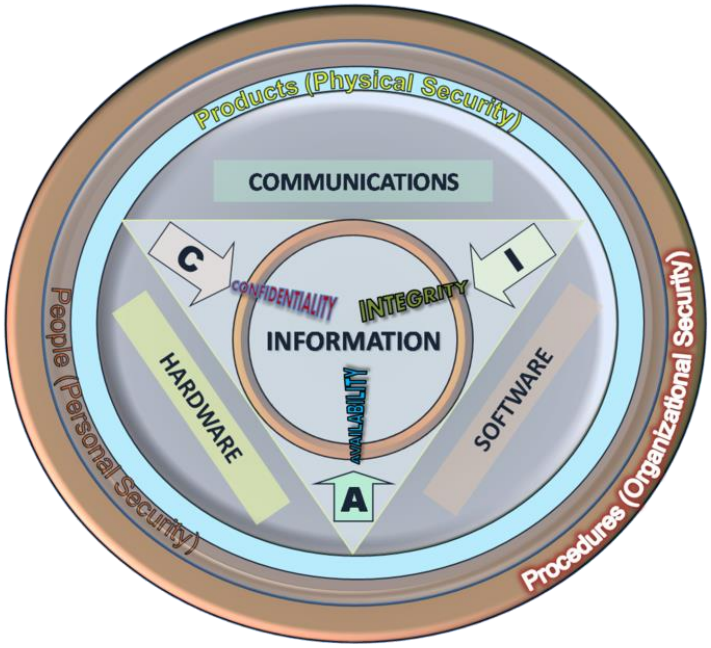

Рис. 1.3. Тріада інформаційної безпеки [6]

Ці три принципи нерозривно пов'язані між собою і становлять основу для розробки та реалізації стратегій та заходів забезпечення безпеки інформаційних систем. Використання цих принципів допомагає забезпечити захист інформації від потенційних загроз і зберегти її конфіденційність, цілісність та доступність.

1.3. Існуючі загрози безпеки інформаційної системи

Інформаційні системи стикаються з різними типами загроз, включаючи шкідливе програмне забезпечення. Основні типи ШПЗ, які можуть вплинути на інформаційну систему, включають:

1. Віруси: Віруси є програмами, які вбудовуються в інші файли або програми та поширюються шляхом їх виконання або взаємодії з ними. Вони можуть пошкодити файли, викрасти інформацію або спричинити інші негативні наслідки.
2. Черв'яки: Черв'яки також поширюються через мережу або засоби зв'язку, але, на відміну від вірусів, вони не потребують вбудовування в інші файли. Черв'яки

можуть самостійно розповсюджуватись і копіювати себе на інші комп'ютери, при цьому споживаючи ресурси системи та можуть переносити шкідливий код.

3. Троянські коні: Троянські коні є шкідливими програмами, які приховуються під невинними або корисними програмами. Коли така програма встановлюється на систему, троянський кінь виконує шкідливі дії, такі як злам паролів, викрадання інформації або надання злочинцям дистанційного доступу до системи.

4. Adware: Рекламне програмне забезпечення є програмами, які відображають непотрібну або небажану рекламу користувачам. Вони можуть сповільнювати роботу системи, перенаправляти на небезпечні веб-сторінки або збирати особисті дані користувачів

5. Spyware: Шпигунське програмне забезпечення приховано відслідковує дії користувача та збирає особисту інформацію, таку як паролі, номери кредитних карток або історія перегляду.

6. Програма-вимагач: Програма вимагач є шкідливим програмним забезпеченням, яке блокує доступ до системи або шифрує файли з метою вимагання викупу в обмін на відновлення доступу або розшифрування даних.

Розуміння цих типів загроз дозволяє розробити та впровадити відповідні заходи захисту, такі як використання антивірусного програмного забезпечення, патчення системи, налаштування мережевих брандмауерів та освіту користувачів про ризики та профілактичні заходи.

Також ШПЗ має різні характеристики та особливості, які допомагають виявити його наявність і розпізнати його тип. Деякі з найпоширеніших характеристик та особливостей шкідливого програмного забезпечення наведені у таблиці 1.2.

Таблиця 1.2

Характеристики шкідливого програмного забезпечення

Особливості	Характеристика
Шифрування	Деякі види шкідливого програмного забезпечення, такі як програми-вимагачі, мають здатність шифрувати файли на комп'ютері або мережі з метою вимагати викупу. Шифровані файли непридатні для використання, доки не буде надано ключ розшифрування.
Самореплікація	Деякі види ШПЗ, такі як черв'яки, мають здатність самостійно розповсюджуватись. Вони можуть копіювати себе на інші системи або поширюватись через мережу, використовуючи вразливості в програмному забезпеченні або слабкі паролі

Продовження таблиці 1.2

Характеристики шкідливого програмного забезпечення

Використання прихованих методів	Шкідливе програмне забезпечення часто використовує різні методи, щоб залишитись непомітним і уникнути виявлення. Наприклад, воно може приховувати свій присутність в системних процесах або файли, зашифровувати свій код, вбудовуватись в інші файли або використовувати техніки поліморфізму для зміни свого вигляду при кожній інфікованій системі.
Спам та фішинг	ШПЗ може бути розповсюджене через спамові електронні листи, які містять шкідливі вкладення або посилання на інфіковані веб-сторінки. Фішингові атаки також можуть використовувати маскування, щоб зманити користувачів на небезпечні сторінки або введення своїх особистих даних.
Зловживання привілеїв	Деякі види ШПЗ, такі як троянські коні, можуть використовувати зловживання привілеїв для отримання доступу до системи або виконання шкідливих дій. Вони можуть підняти привілеї адміністратора або скористатись вразливостями системи для отримання повного контролю.

Продовження таблиці 1.2

Характеристики шкідливого програмного забезпечення

Збір та передача інформації	Деякі шкідливі програми, такі як шпигунське програмне забезпечення, призначені для збору особистих даних користувачів, таких як паролі, номери кредитних карток, історія перегляду та інша конфіденційна інформація. Ці дані потім можуть бути передані зловмиснику через мережу.

1.4. Обґрунтування вибору рішення ESET

Компанія ESET є провідним розробником антивірусного програмного забезпечення і надає надійні та ефективні рішення як для домашніх, так і корпоративних користувачів.

Вона пропонує широкий спектр продуктів, які здатні виявляти і нейтралізувати відомі та нові види загроз. Лінійка продуктів ESET охоплює рішення для захисту робочих станцій, серверів і мобільних пристроїв під управлінням різних операційних систем і платформ.

Ці продукти відрізняються високою ефективністю виявлення загроз і мінімальним використанням системних ресурсів, що призводить до їх широкої популярності в усьому світі. Вони також регулярно отримують визнання від незалежних експертів та авторитетних видань.

Однією з переваг ESET є прогресивний протишпигунський підхід, який виявляє і блокує шкідливе програмне забезпечення, збираючи інформацію про його поведінку. Він також використовує технології sandboxing та машинного навчання для виявлення нових загроз.

ESET пропонує персоналізовані налаштування, що дозволяють користувачам налаштовувати рівень захисту відповідно до їх потреб, а інтерфейс користувача є

простим у використанні і інтуїтивно зрозумілим, спрощуючи управління захистом системи.

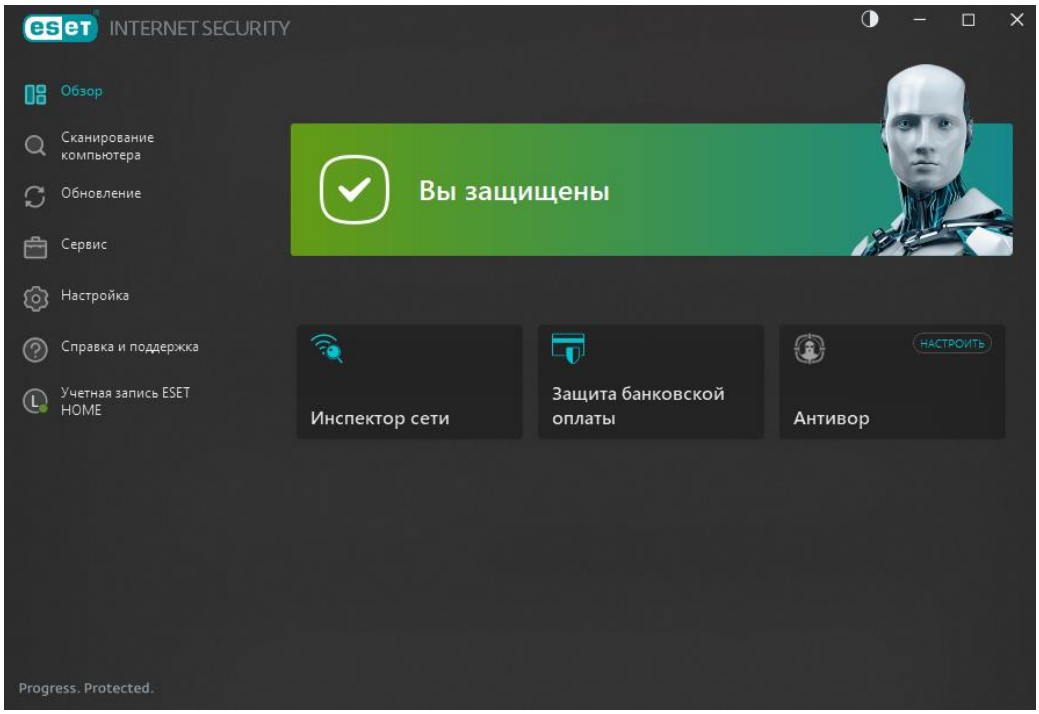

Рис. 1.4. Інтерфейс ESET Internet Security

Одна з головних переваг ESET полягає в його здатності до прогнозування та запобігання новим загрозам завдяки використанню прогресивних технологій, таких як евристика, які дозволяють виявляти вразливості до атак та блокувати їх перед поширенням.

ESET також пропонує захист в реальному часі, що означає, що він постійно перевіряє систему на наявність загроз і негайно реагує на них. Він також включає в себе захист від фішингу та спаму, що допомагає запобігти шахрайським атакам та крадіжці особистих даних.

Завдяки своїй керованості та масштабованості, ESET може бути використаний як для захисту окремих комп'ютерів, так і для корпоративних мереж. Він має можливості централізованого керування, що дозволяє адміністраторам легко встановлювати, налаштовувати та керувати захистом на кількох пристроях чи комп'ютерах.

Крім того, ESET показує високу ефективність та низькі навантаження на систему. Він розроблений з урахуванням оптимізації продуктивності, що дозволяє йому працювати швидко та ефективно, не сповільнюючи роботу комп'ютера чи системи.

Ось чому рішення ESET можуть бути вигідними та зручними для безпечної роботи сервісного центру.

Висновки до розділу

Були розглянуті поняття про інформаційну систему, методи захисту від шкідливого програмного забезпечення та їх класифікація.

Для порівняння були надані відомі антивірусні програми та їх функції.

Також були розглянуті основні підходи та принципи що до захисту інформаційних систем.

Розглянуті переваги та зручність антивірусного рішення від ESET.

2 ДОСЛІДЖЕННЯ ТА АНАЛІЗ ШЛЯХІВ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ СЕРВІСНОГО ЦЕНТРУ ЗА ДОПОМОГОЮ РІШЕННЯ ВІД ESET

2.1 Аналіз існуючого стану інформаційної системи сервісного центру

На даний момент інформаційна система сервісного центру будується на базі профільного рішення програмою «ТЕЛЕМАСТЕР V2.06». Програма надає можливість зручно керувати базою даних клієнтів, простий та інтуїтивно зрозумілий інтерфейс, можливість створення шаблонів для квитанцій про прийняття та видачу апаратів які знаходяться, або поступають у ремонт.

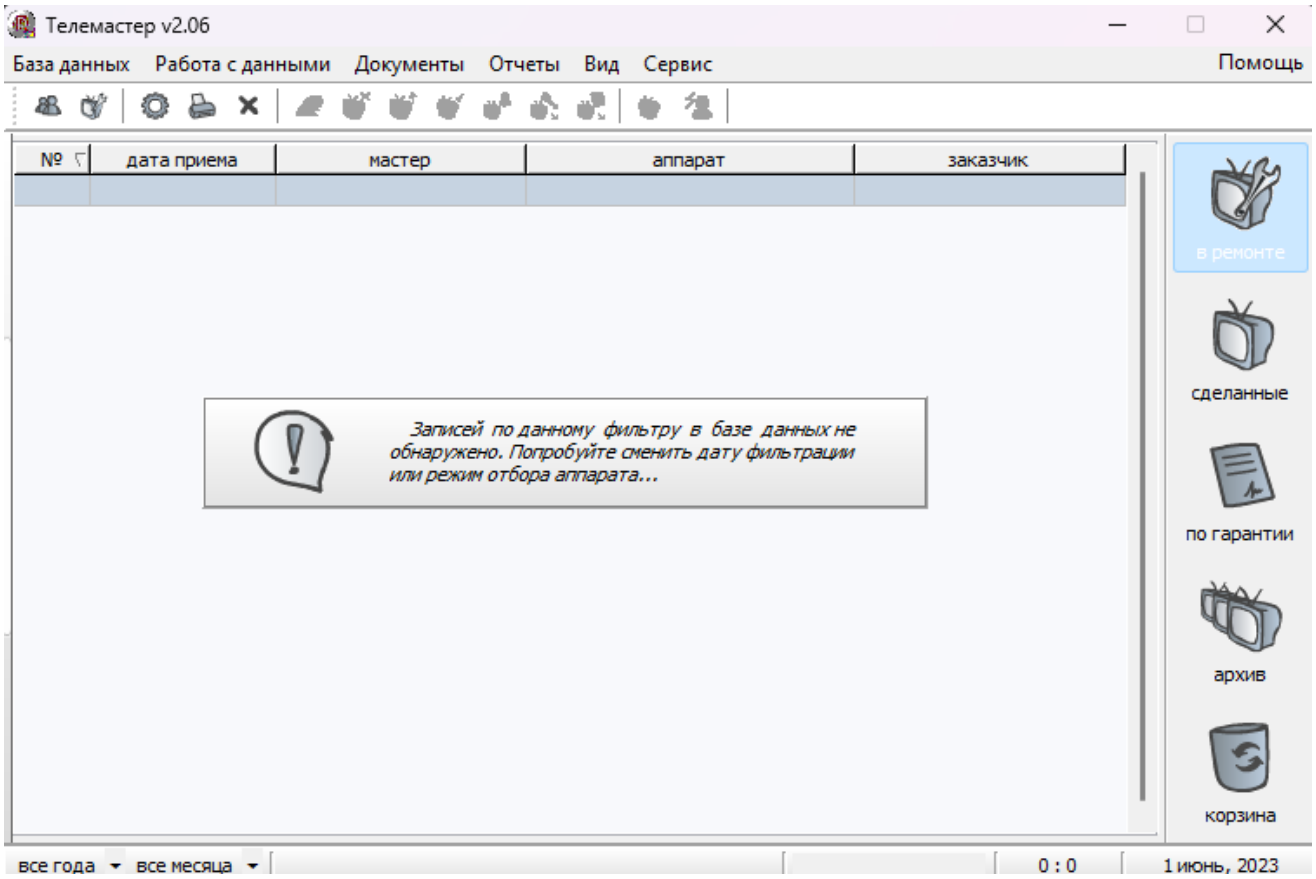

Рис 2.1. Інтерфейс програми Телемастер v2.06

За допомогою цієї програми можна переглядати статистику виконаних замовлень як для цілої організації, так і для окремого співробітника.

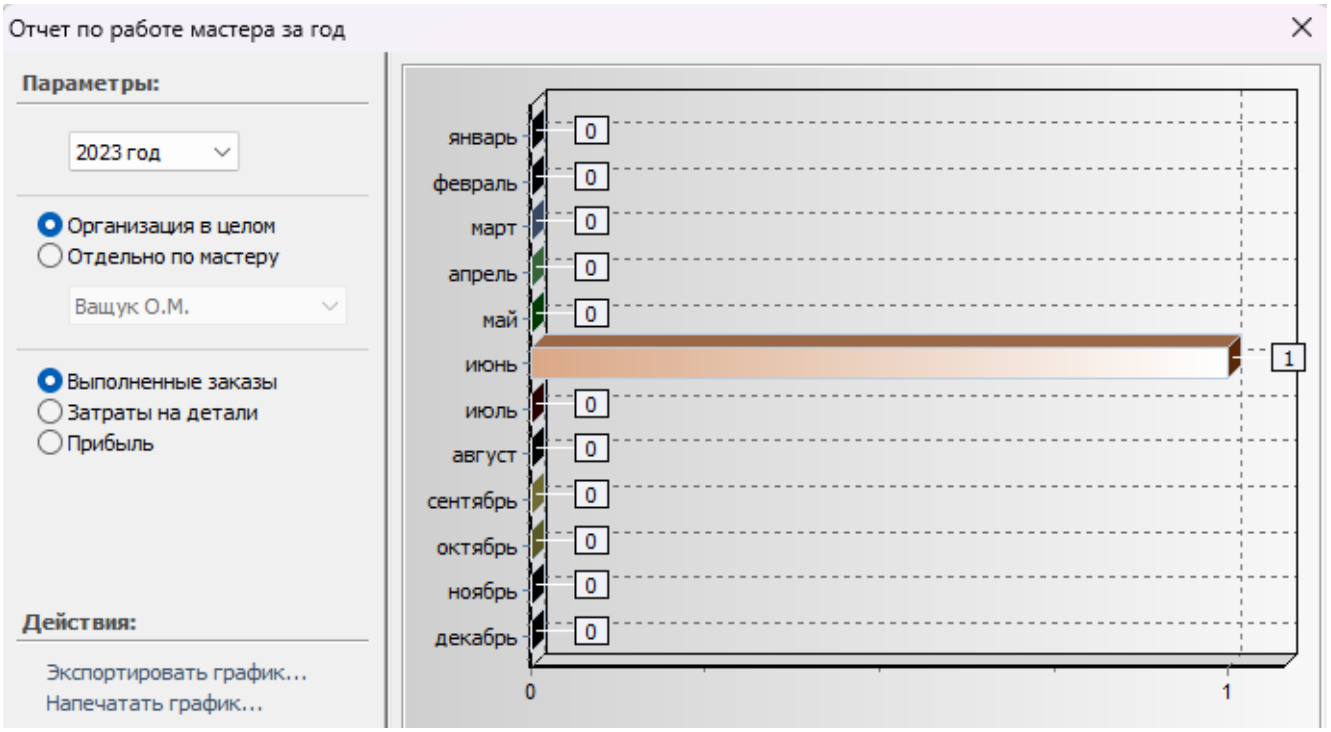

Рис. 2.2. Статистика виконаних замовлень у програмі Телемастер v2.06

Завдяки програмі Телемастер 2.06 можна легко вносити інформацію щодо ремонту апарату, додавати вартість запчастин у ремонт та зв’язуватись з клієнтом.

База даних знаходиться на локальному носії, отже задача з захисту інформаційної системи спрощується.

Розглянемо потенційні вразливості та слабкі місця у цій системі.

Операційна система, на якій знаходиться БД – Windows 7. Тож це перше слабке місце, адже система вже не підтримується компанією Microsoft, що свідчить про те, що бази даних вбудованого захисника Windows не оновлюються.

Не проводиться резервне копіювання БД задля швидкого відновлення у разі пошкодження файлів.

Відсутній захист інтернет з’єднання, а саме робочі браузери через котрі на ПК з базою може потрапити ШПЗ.

2.2 Впровадження та налаштування рішення ESET

Для захисту інформаційної системи сервісного центру будемо використовувати рішення від ESET, а саме – ESET Smart Security Premium.

Перший крок – зайдемо на сайт ESET та завантажимо останню актуальну версію ПЗ

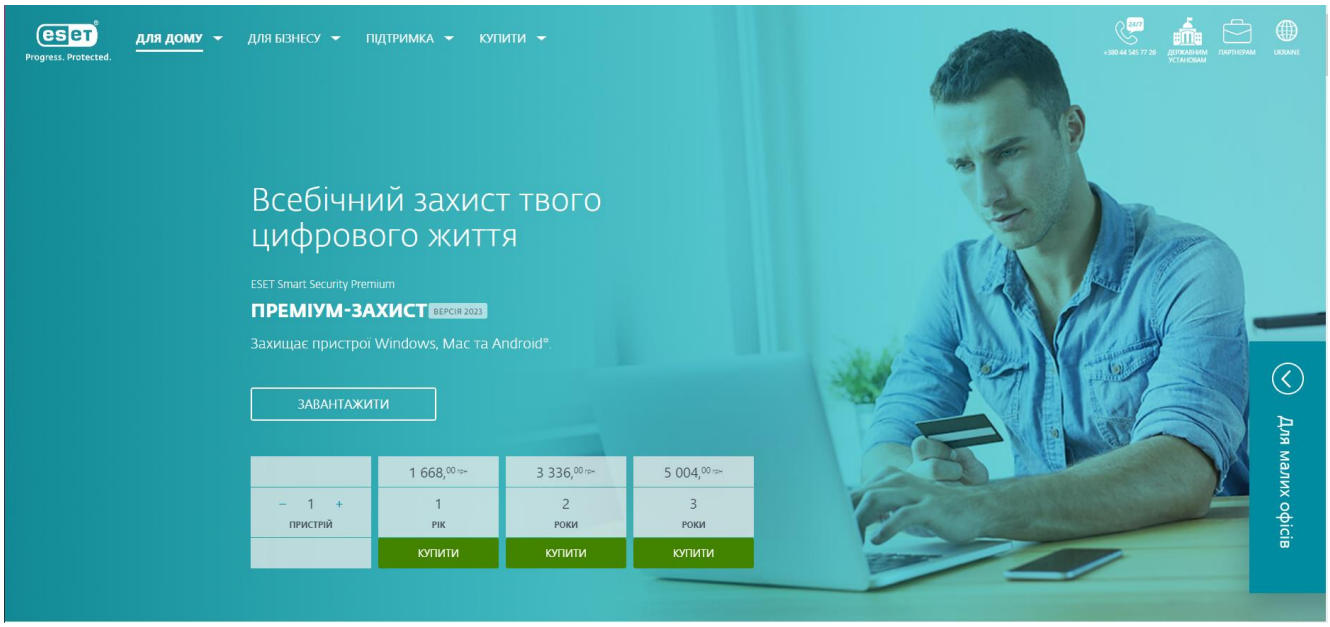

Рис. 2.3. Офіційна сторінка ПЗ ESET [8]

Другий крок – інсталяція.

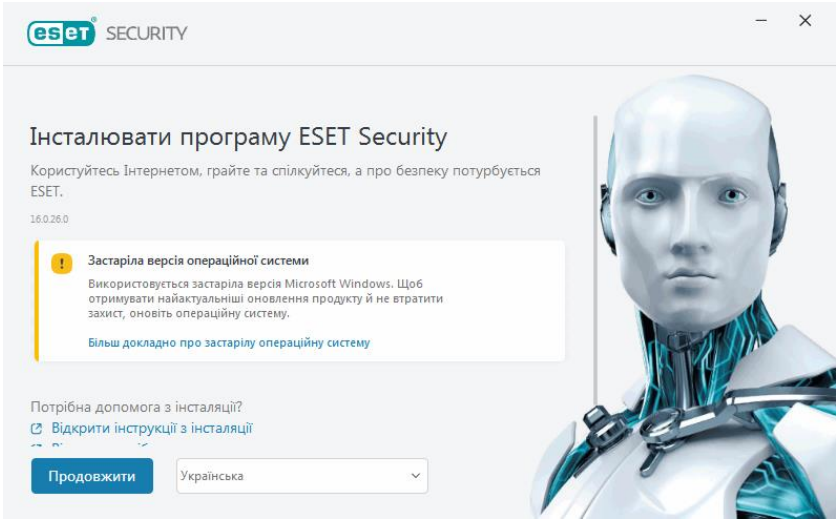

Рис. 2.4. Інтерфейс інсталяції ESET

Як бачимо на рис. 2.4., при установці нас попереджають, що наша ОС застаріла. Тож у майбутньому для підвищення захисту даних необхідно буде оновити версію ОС Windows. Продовжимо інсталяцію.

Після інсталяції нам пропонують налаштувати одразу додаткові інструменти безпеки.

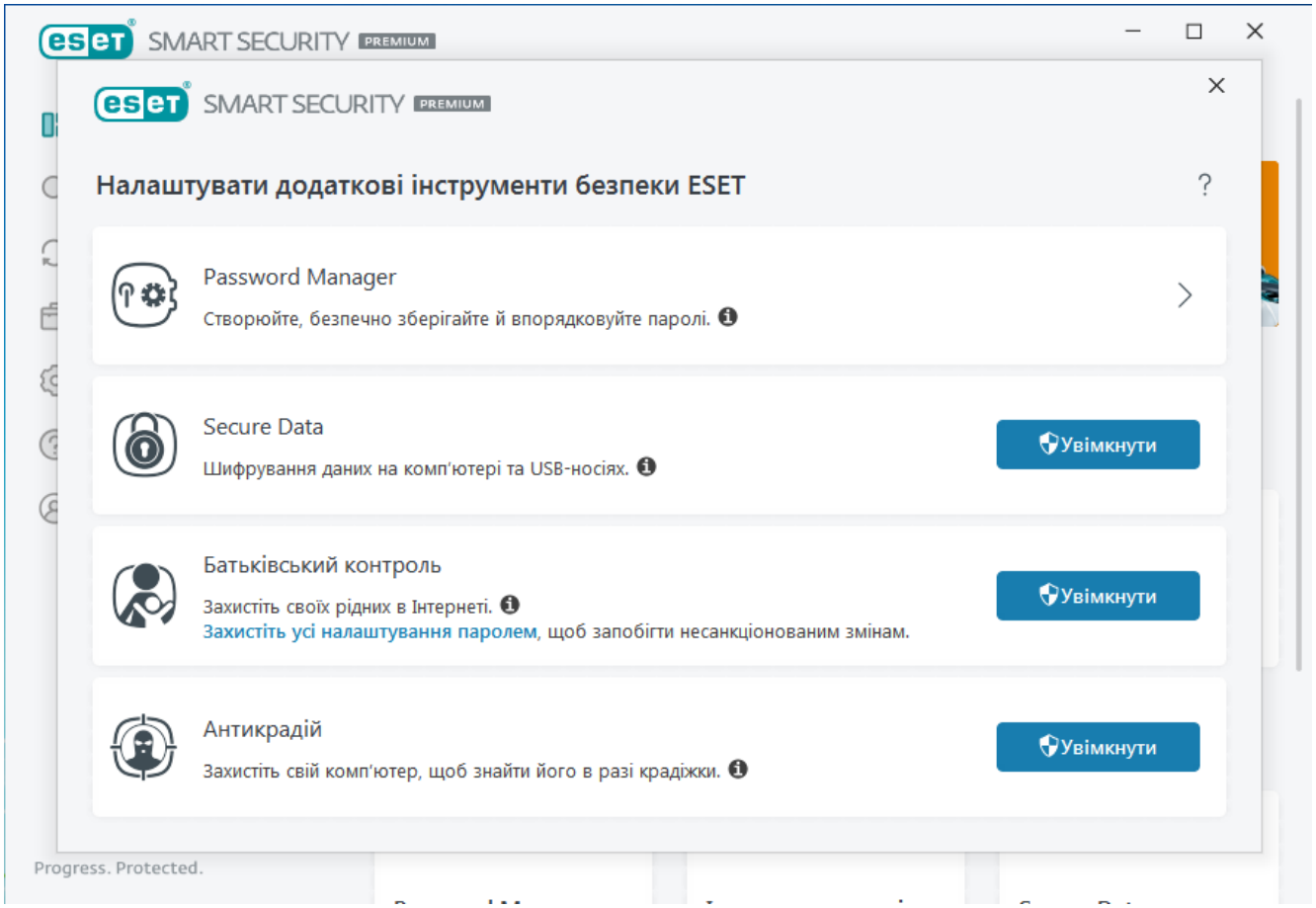

Рис. 2.5. Налаштування додаткових інструментів безпеки ESET

Одразу увімкнемо пункт шифрування даних (Secure Data) для захисту даних нашого ПК та USB-носіїв. Ця функція надає можливість створення на ПК або на зовнішньому носії віртуального сховища

Третій крок – після увімкнення потрібних нам функцій запустимо сканування системи для перевірки на ШПЗ.

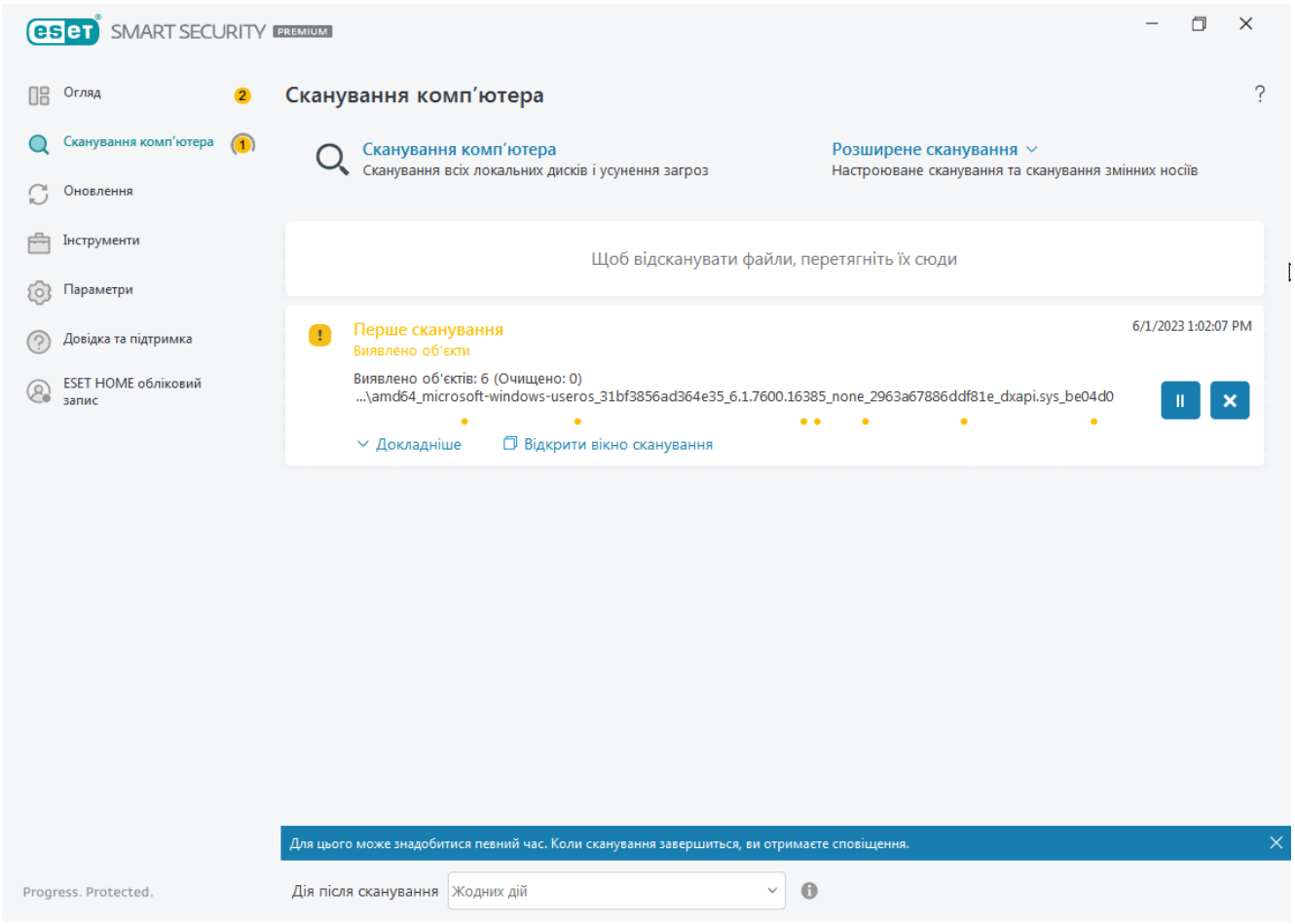

Рис. 2.6. Сканування ПК за допомогою ESET

Під час сканування ПК антивірусна система виявила шкідливе програмне забезпечення і рекомендує його усунути, тож зробимо це.

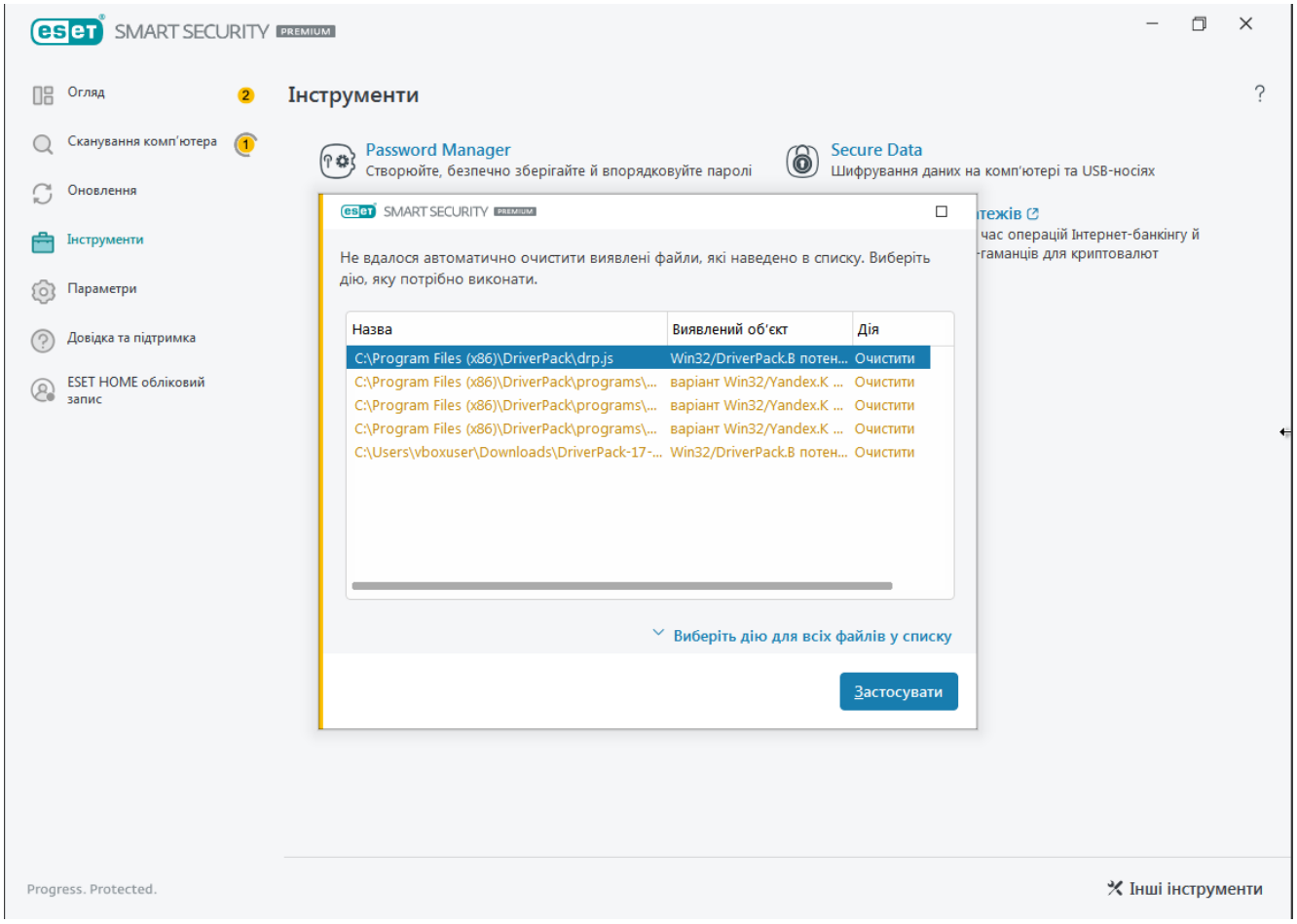

Рис. 2.7. Вікно результатів сканування файлів

Після видалення ненадійних файлів можемо перейти до налаштування безпеки в мережі Інтернет. Для цього нам необхідно зайти в розділ «Параметри – Безпечна робота в Інтернеті – Захист доступу до Інтернету», натиснути на шестерню та увімкнути функцію « Увімкнути розширену перевірку сценаріїв браузеру» рис. 2.8. Тепер наш робочий браузер додатково захищений.

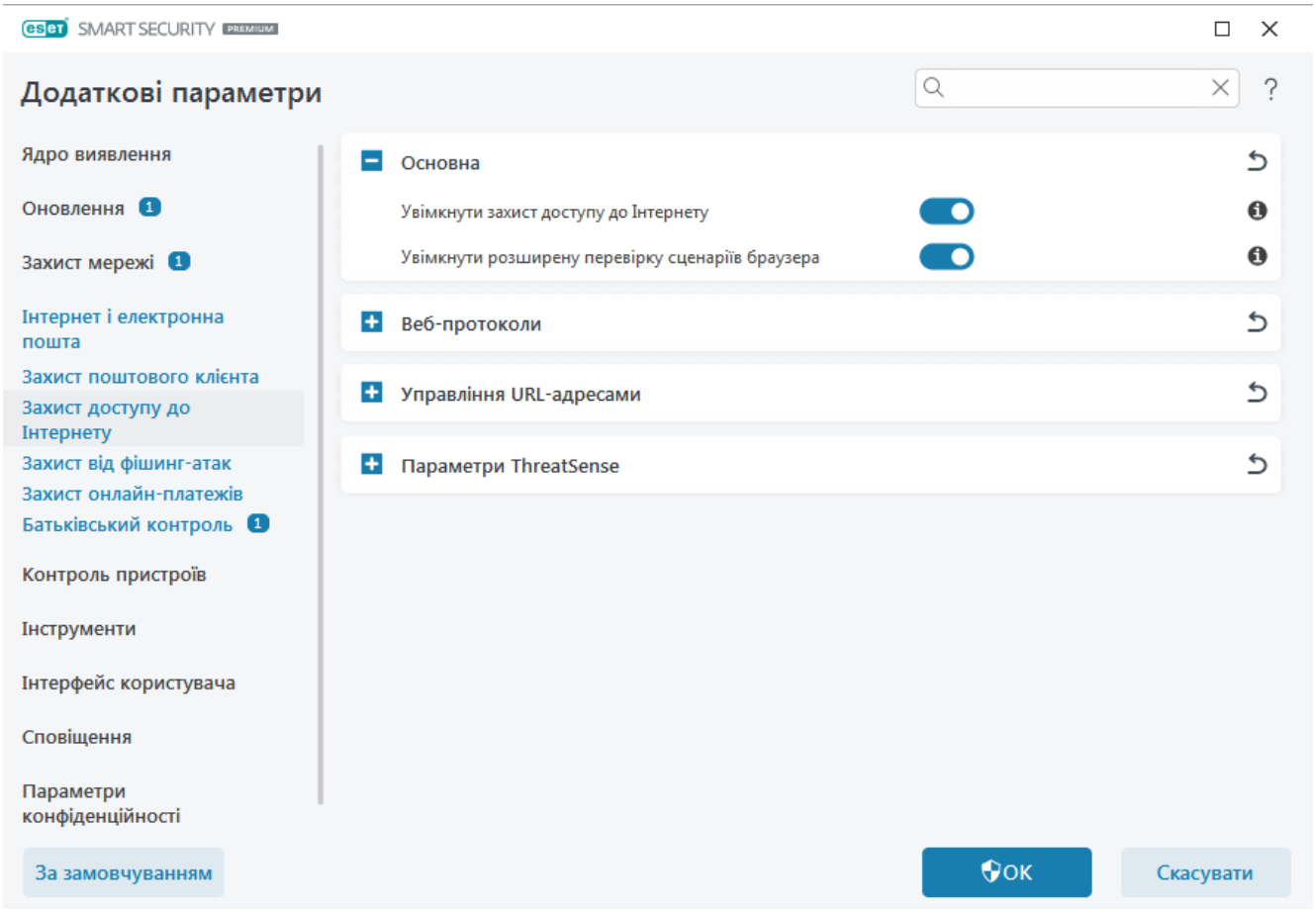

Рис. 2.8. Налаштування безпеки браузера

Після цих простих дій можемо спокійно закрити ESET який у фоновому режимі буде захищати нашу систему.

2.3 Використання рішення ESET для виявлення ШПЗ

У сучасному ландшафті загроз, що постійно змінюється, одного рівня захисту недостатньо. ESET використовує безліч власних багаторівневих технологій, які працюють разом як ESET LiveSense, що виходить далеко за межі можливостей базового антивірусу. ESET також використовує розширене машинне навчання, яке ESET запровадила вперше для боротьби з новими загрозами. Компанія була однією з перших, хто застосував хмарну технологію, завдяки якій глобальна система репутації ESET LiveGrid постійно оновлює інформацію про загрози.

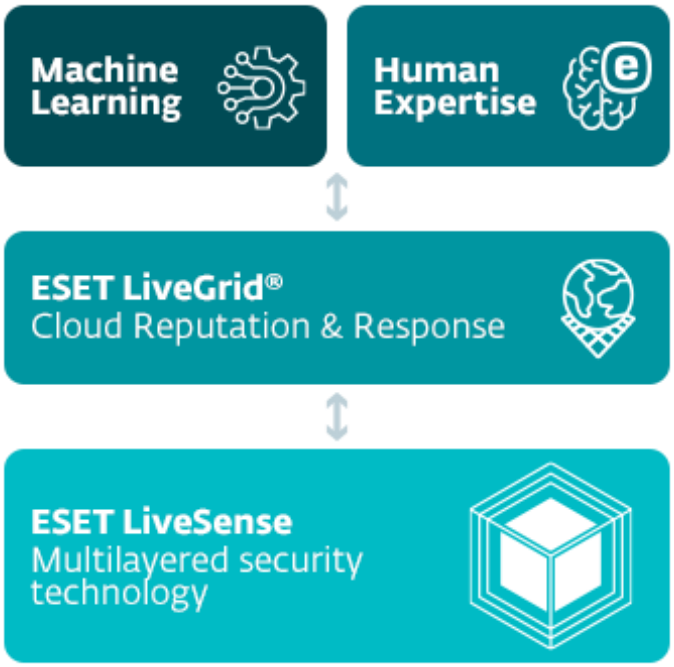

Рис. 2.9. Підхід ESET [10]

ESET був першим постачальником засобів захисту кінцевих точок, який додав спеціальний рівень у своє рішення, що захищає уніфікований розширюваний інтерфейс мікропрограм UEFI. ESET UEFI Scanner перевіряє та забезпечує безпеку середовища перед завантаженням, щоб воно відповідало специфікації UEFI. Він призначений для виявлення шкідливих компонентів у мікропрограмі та повідомляє про них користувача.

Також в ESET є технологія ESET DNA Detection. Ця технологія проводить глибокий аналіз коду та виділяє «гени», які відповідають за його поведінку для оцінки потенційно підозрілого коду, незалежно від того, чи він знаходиться на диску, чи в пам’яті запущеного процесу.

Продукти ESET використовують дві різні форми розширеного машинного навчання. Це потужний механізм виявлення в хмарі та полегшений механізм на кінцевій точці. Щоб запропонувати найкращі показники виявлення та найнижчі показники помилкових спрацювань, розширене машинне навчання використовує результати як статичного, так і динамічного аналізу.

Під час перевірки файлу чи URL-адреси перед початком будь-якого сканування продукти ESET перевіряють локальний кеш на наявність відомих зловмисних або безпечних об’єктів із білого списку. Це покращує продуктивність сканування. Після цього система репутації ESET LiveGrid запитує репутацію об’єкта (тобто чи об’єкт уже бачили десь та класифікували як шкідливий). Це покращує ефективність сканування та дозволяє швидше ділитися інформацією про ШПЗ з клієнтами.

ESET HIPS використовує попередньо визначений набір правил для пошуку підозрілих дій, а також для моніторингу та сканування поведінкових подій, таких як запущені процеси, файли та ключі реєстру. У разі виявлення HIPS повідомляє про шкідливий елемент і, якщо потрібен додатковий аналіз, запитує детальнішу перевірку за допомогою інших технологічних рівнів ESET.

Сучасне ШПЗ часто сильно затуманене та намагається якомога більше уникнути виявлення. Щоб побачити це, та визначити реальну поведінку, приховану під поверхнею, компанія використовує технологію Sandbox в продукті. За допомогою цієї технології рішення ESET відновлюють різні компоненти підозрілого зразка в ізольованому віртуальному середовищі.

Технологія розширеного сканеру пам’яті – це унікальна технологія ESET, яка ефективно вирішує важливу проблему сучасного ШПЗ – інтенсивне використання шифрування. Щоб вирішити ці проблеми, розширений сканер пам’яті відстежує поведінку підозрілого процесу та сканує його, коли він розкривається в пам’яті.

Технологія захисту від експлойтів відстежує типові програми, які можна використовувати (браузери, програми для читання документів, поштові клієнти, Flash, Java та інш.), і замість того, щоб просто націлюватися на конкретні ідентифікатори загальних вразливостей та схильностей до впливів, технологія зосереджується на техніках експлуатації. Після запуску поведінка процесу аналізується, і якщо процес вважається підозрілим – загроза може бути негайно заблокована на машині.

ESET Ransomware Shield – це додатковий рівень захисту користувачів від програм-вимагачів. Ця технологія відстежує та оцінює всі запущені програми на

основі їх поведінки та репутації. Він призначений для виявлення та блокування процесів, які нагадують поведінку програм-вимагачів.

ESET також використовує широкий спектр технологій виявлення для виявлення загроз, які намагаються проникнути в середовище жертви на рівні мережі. Список включає виявлення зловмисного мережевого зв’язку, використання ще не виправлених вразливостей і атаки грубої сили проти різноманітних протоколів, таких як Remote Desktop Protocol, SMB і SQL.

Висновки до розділу

Була проаналізовано існуючий стан інформаційної системи сервісного центру.

Продемонстровано впровадження та налаштування комплексного антивірусного рішення від ESET.

Розглянуто підхід ESET щодо виявлення шкідливого програмного забезпечення.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ СЕРВІСНОГО ЦЕНТРУ

3.1 Виявлення ключових проблем та вразливостей ІС

Для виявлення ключових проблем та вразливостей інформаційної системи в сервісного центру необхідно провести ряд досліджень.

Почнемо з аудиту безпеки. База даних сервісного центру знаходиться на ноутбуці на SSD накопичувачі. ОС система – Windows 7. Встановлений антивірусний засіб – відсутній. Резервне копіювання бази даних – відсутнє.

Проведемо тестування системи на базі рішення від CheckPoint.

CheckMe проводить серію симуляцій, які перевіряють, чи можуть ваші існуючі технології безпеки блокувати стандартні та розширені атаки

Перше, з чого почнемо – зайдемо на сторінку тестування CheckMe. [11]

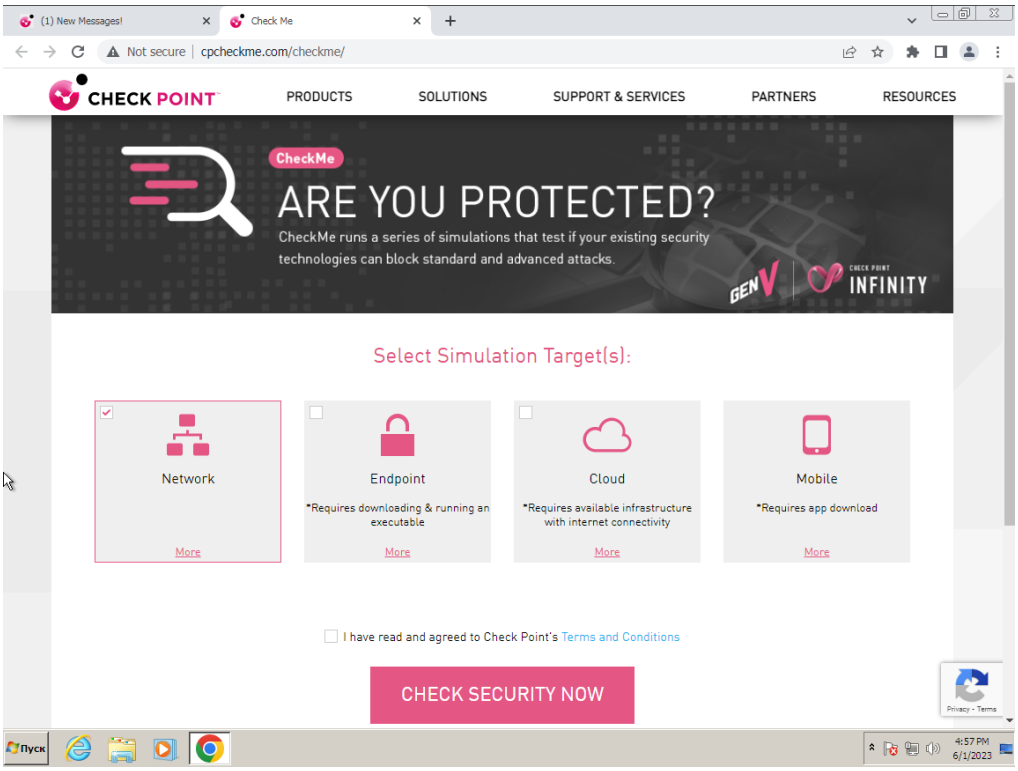

Рис. 3.1 Сторінка сервісу CheckMe

Оберемо потрібні нам пункти, а саме – Network та Endpoint та запустимо тестування. Для початку тестування нам необхідно додатково завантажити додаток який нам запропонують.

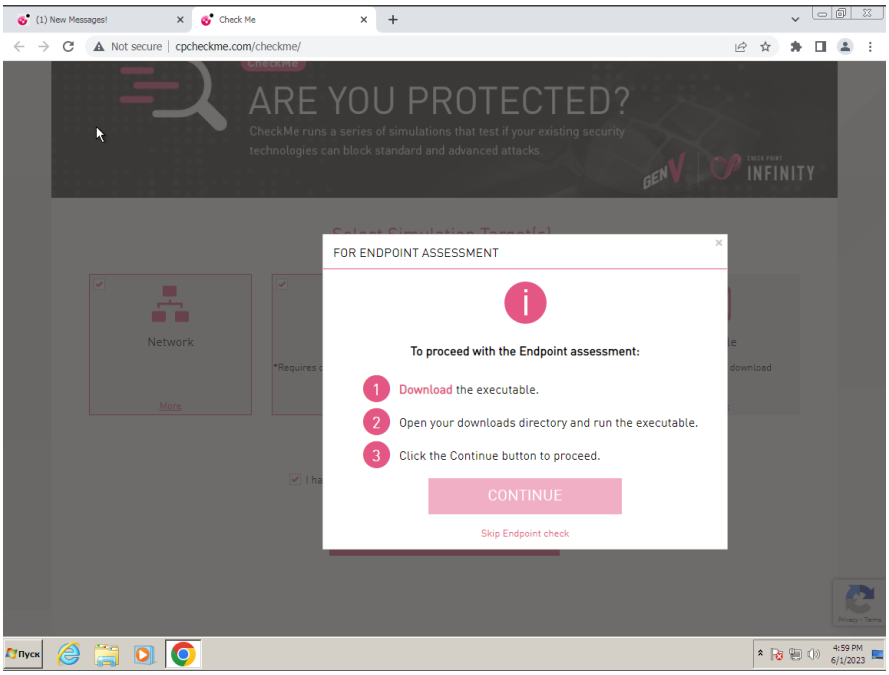

Рис. 3.2 Початок тестування

Після завершення тестування отримуємо результати.

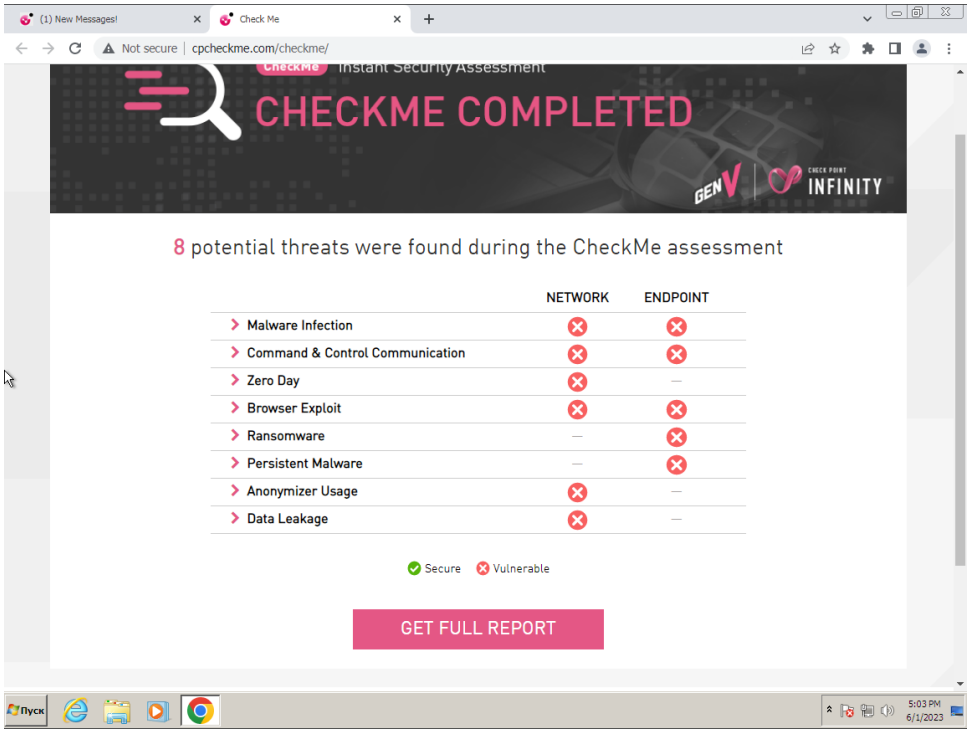

Рис. 3.3 Результати тестування

Як можемо помітити на рис. 3.3, вісім потенціальних загроз безперешкодно могли б зайти у нашу систему.

Далі, що необхідно відмітити, що на ПК стоїть застаріла Windows 7 підтримка якої була завершена у 2020 році, а це означає, що система не отримувала нових патчів безпеки вже три роки.

Також варто відзначити, що небезпека може існувати і збоку співробітників компанії. Хтось може ненавмисно завантажити на свій USB-накопичувач ШПЗ та занести його на ПК з базою даних.

3.2. Розробка рекомендацій щодо вдосконалення захисту

Для вдосконалення захисту інформаційної системи сервісного центру необхідно виконати такі кроки:

1. Оновлення систем та ПЗ: Необхідно оновлювати всі операційні системи, програми та застосунки на комп’ютерах. Встановлення оновлень та патчів є важливим аспектом у запобіганні вразливостям і атакам.
2. Сильні паролі та автентифікація: Застосовуйте політику вимог до паролів, щоб забезпечити використання сильних паролів користувачами. Розгляньте можливості двохфакторної автентифікації.
3. Перевірка прав доступу: Перегляньте права доступу користувачів до різних систем та ресурсів і обмежте їх лише необхідними. Видаляйте колишніх або неактивних співробітників зі списків доступу.
4. Антивірусне ПЗ: Використовуйте надійне антивірусне ПЗ, на базі рішень ESET, і переконайтеся, що воно оновлюється регулярно. Налаштуйте антивірусне програмне забезпечення для автоматичного сканування системи та виявлення потенційно небезпечних файлів та програм.
5. Захист мережі: Використовуйте мережевий екран від ESET для контролю трафіку в мережі.
6. Шифрування даних: Розгляньте можливість використання шифрування для захисту конфіденційної інформації, особливо при передачі через мережу або зберіганні на переносних пристроях.

7. Навчання користувачів: Проведіть навчання з питань кібербезпеки для всього персоналу, щоб підвищити їх усвідомлення про потенційні загрози та навчити їх розпізнавати фішиногові атаки та інші види соціально-інженерних атак.

8. Резервне копіювання даних: Забезпечте регулярне резервне копіювання всіх важливих даних та перевіряйте, щоб відновлення з резервних копій було можливим у разі випадку втрати даних або кібератаки.

Дотримуючись даних рекомендацій, можна буде покращити безпеку інформаційної системи сервісного центру. Варто зазначити, що компанія може редагувати ці рекомендації під свої потреби.

3.3. Практична реалізація рекомендацій

Перейдемо до практичної реалізації рекомендацій. Першим кроком необхідно оновити систему з Windows 7 на Windows 10.

Для цього необхідно зайти на сайт Microsoft та завантажити асистент з оновлень. У нашому ж випадку буде повне перевстановлення системи. Необхідно створити флешку з образом Windows 10.

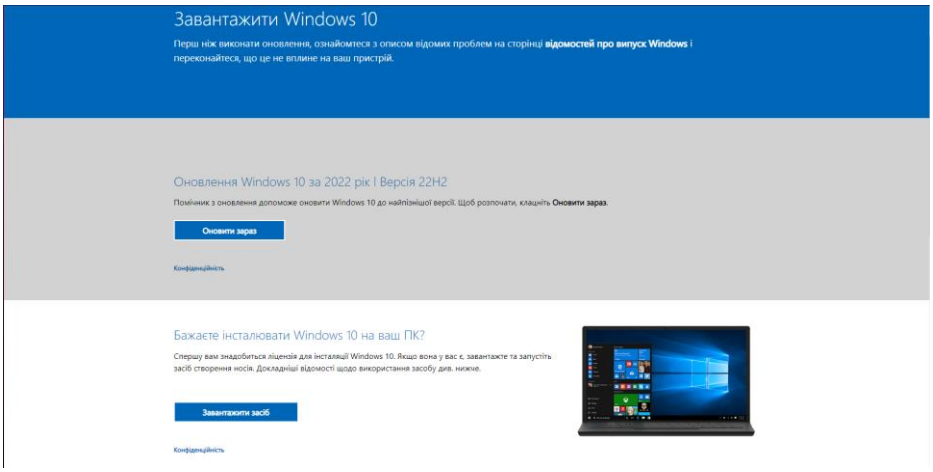

Рис. 3.4. Сторінка завантаження Windows 10 [12]

Другим кроком встановимо паролі на користувача Windows для підвищення захисту. Для цього необхідно зайти в налаштування рис. 3.5.

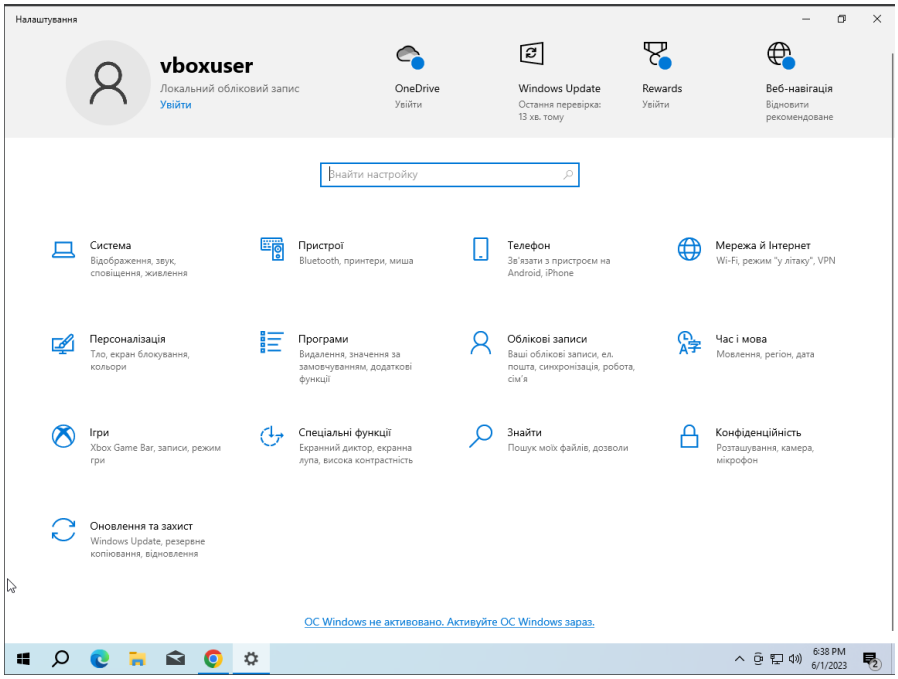

Рис. 3.5. Налаштування Windows 10

Обрати пункт «Облікові записи – Варіанти входу» та створити новий надійний пароль.

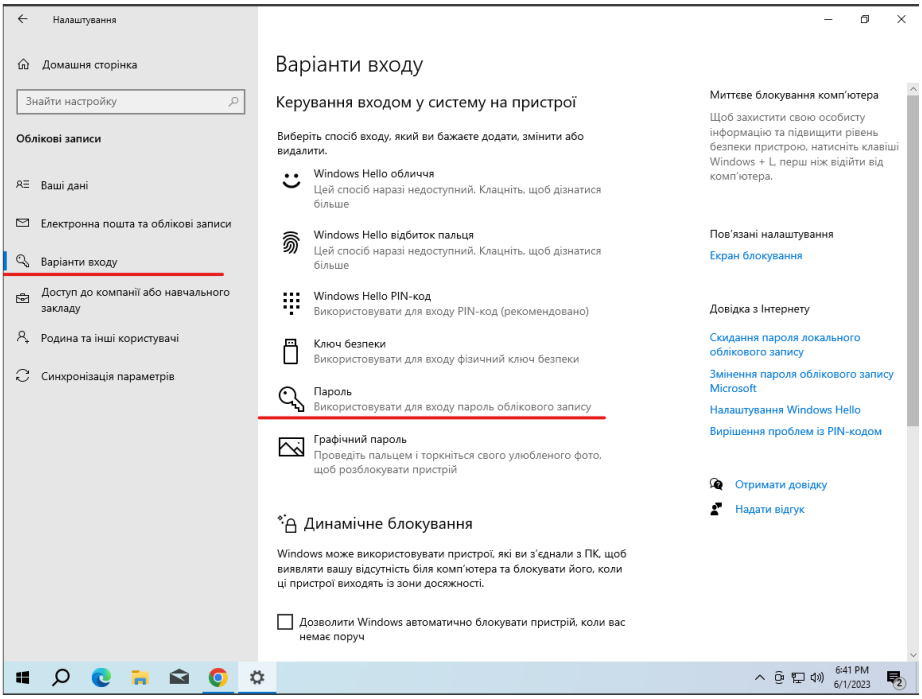

Рис. 3.6. Налаштування паролю у Windows 10

Третім кроком буде інсталяція та налаштування ESET Smart Security Premium.

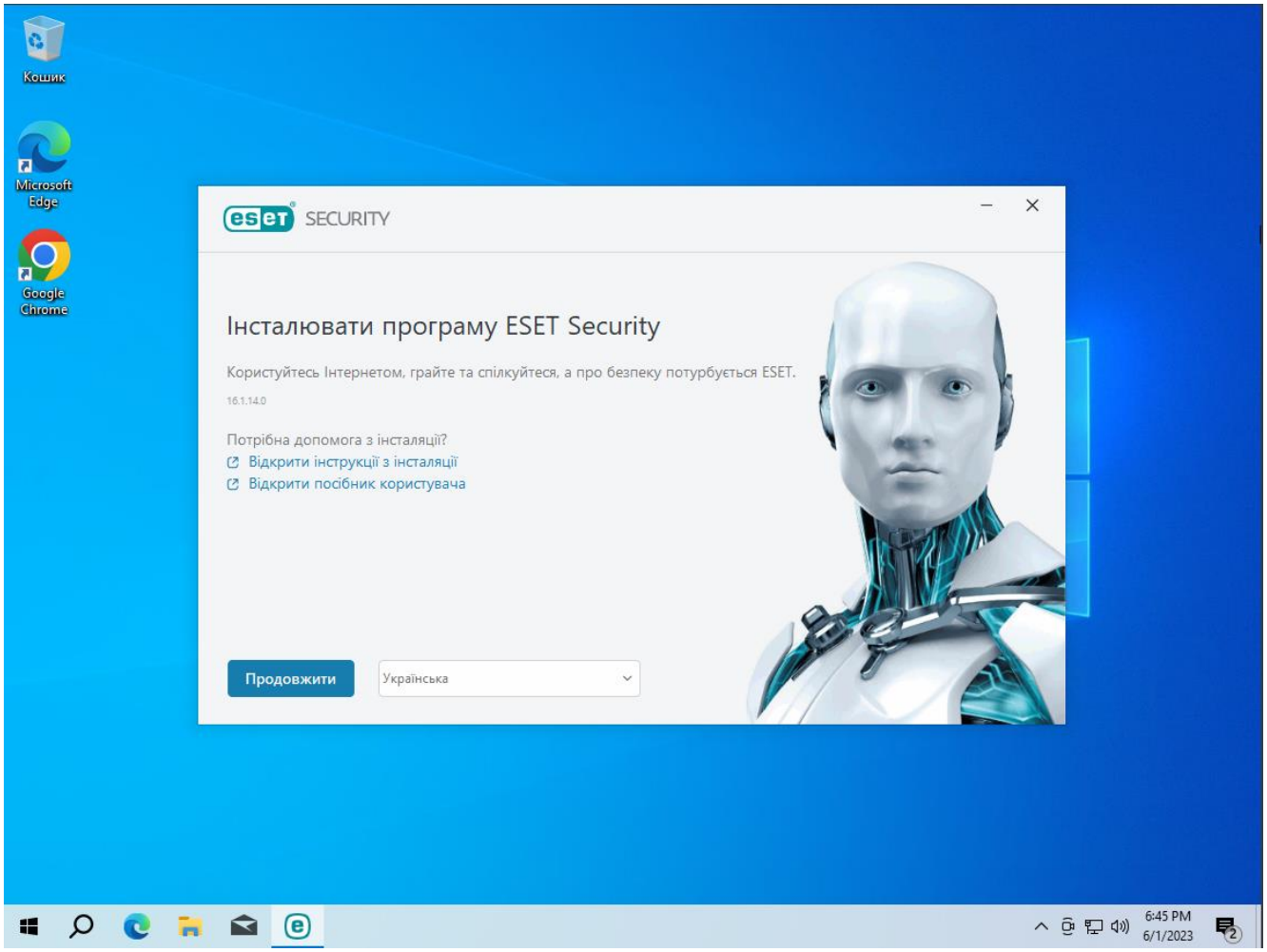

Рис. 3.7. Інтерфейс інсталяції ESET

Для надійного захисту системи нам необхідно включити автоматичне оновлення. Після встановлення ESET воно вже самостійно налаштоване і заданий параметр, що при підключенні до інтернету бази ESET будуть оновлені. Але ми все рівно перевіримо. Для цього нам необхідно перейти у вкладку «Інструменти» та обрати пункт «Розклад».

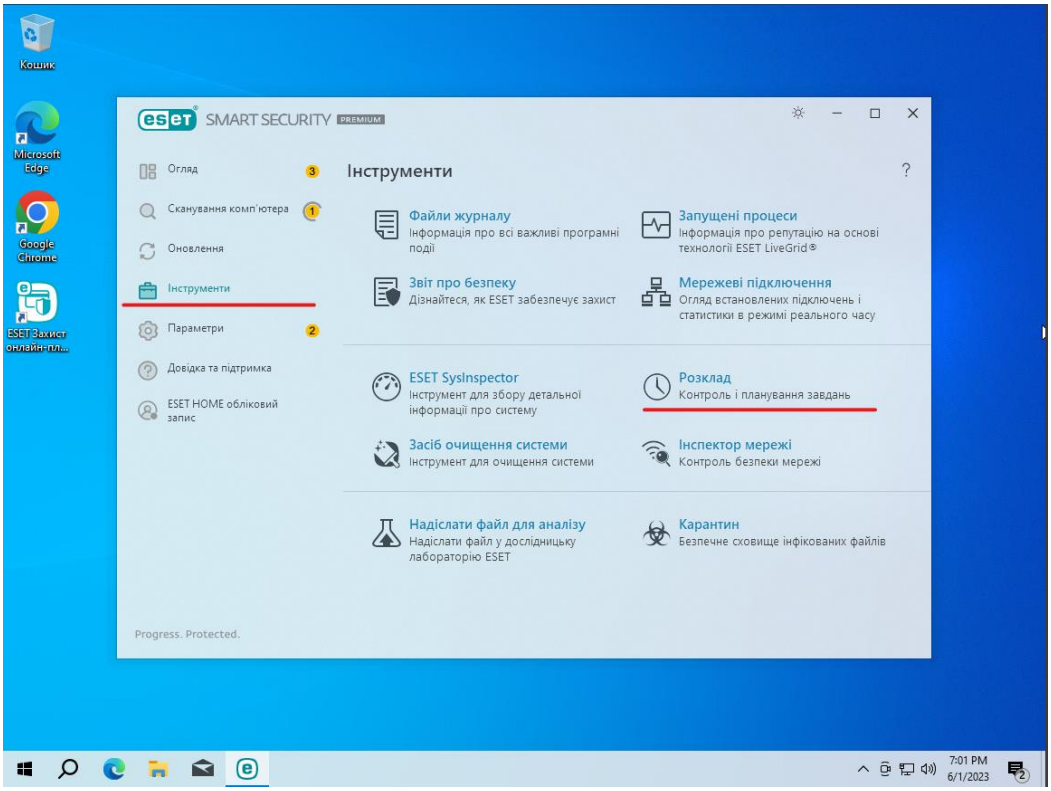

Рис. 3.8. Налаштування розкладу автоматичних оновлень

Після відкриття «Розкладу» нам необхідно знайти пункт – «Оновлення». Як бачимо на рис. 3.9. – автоматичне оновлення вже ввімкнуте, тож ми можемо спокійно виходити з цієї сторінки.

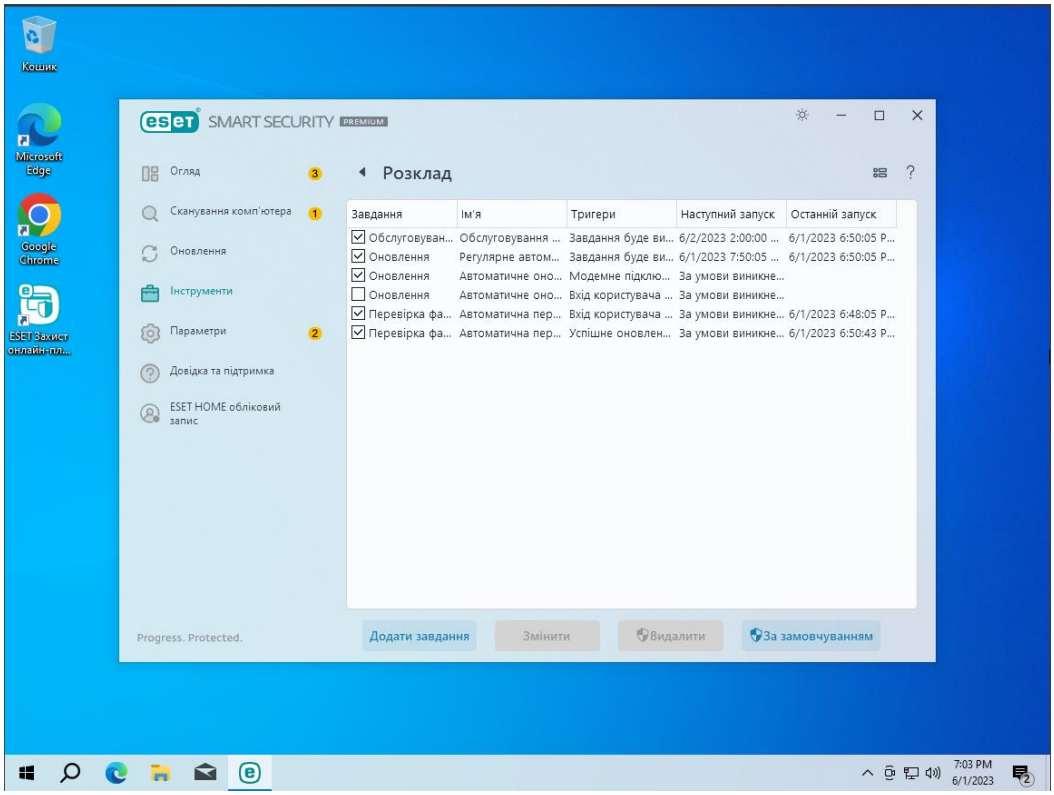

Рис. 3.9. Список запланованих завдань

Захист мережі також вже автоматично увімкнений зі старту у ESET.

Виконавши усі ці дії ми підвищили рівень захисту інформаційної системи сервісного центру.

Висновки до розділу

Були розглянуті ключові проблеми та вразливості інформаційної системи. Проведено тестування системи на стандартні та розширені атаки.

Розроблені рекомендації для вдосконалення та підвищення захисту в інформаційній системі сервісного центру.

Була проведена практична реалізація побудованих рекомендацій.

ВИСНОВКИ

У зв’язку з швидким розвитком інформаційних технологій та збільшенням кількості відкритих інформаційних мереж, інформаційні системи стали дедалі більш вразливими перед загрозами, пов’язаними зі зловмисними діями. Особливо вразливі центри обслуговування, які мають доступ до конфіденційної інформації, що належить клієнтам. Одним з найважливіших аспектів забезпечення безпеки інформаційних систем є захист від шкідливого програмного забезпечення, що може відкривати доступ до конфіденційної інформації та завдавати значної шкоди інфраструктурі інформаційної системи.

Розглянуті методи захисту від шкідливого програмного забезпечення та їх класифікація.

Проаналізовані деякі відомі рішення комплексного захисту від шкідливого програмного забезпечення.

Розглянуті основні підходи до захисту інформаційних систем.

Проаналізовані існуючі загрози безпеки інформаційної системи. Розглянуті їх особливості та характеристики.

Проаналізований існуючий стан інформаційної системи сервісного центру.

Розглянуто та продемонстровано процес налаштування захисту на базі рішення від ESET.

Проаналізовано підхід компанії ESET щодо захисту інформаційної системи.

Були виявлені ключові проблеми та вразливості інформаційної системи сервісного центру. Проведені тестування існуючої системи безпеки.

На основі результатів було розроблено рекомендації щодо захисту інформаційної системи.

На базі наведених рекомендацій було проведено практичну реалізацію.

ПЕРЕЛІК ПОСИЛАНЬ

1. Офіційна сторінка AVAST. URL: https://www.avast.ua/free-antivirus-download#pc (дата звернення: 20.02.2023)

2. Сканирование ПК на наличие вирусов с помощью програмы Avast Antivirus. URL: https://support.avast.com/ru-ru/article/antivirus-pc-virus-scan/#pc (дата звернення: 20.02.2023)

3. Офіційна сторінка Bitdefender. URL: https://support.avast.com/ru-ru/article/antivirus-pc-virus-scan/#pc. (дата звернення: 20.02.2023)

4. Vigderman A., Turner G. Bitdefender Antivirus Review. URL: https://www.security.org/antivirus/bitdefender/review/. (дата звернення: 20.02.2023)

5. Рішення для кібербезпеки вашого бізнесу. URL: https://kyivstar.ua/business/products/cybersecurity. (дата звернення: 20.02.2023)

6. Захист інформації. Матеріал з Вікіпедії – вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/Захист_інформації. (дата звернення: 06.03.2023)

7. Антивірусні рішення на базі продуктів ESET. URL: https://techexpert.ua/it-products/antyvirusni-rishennya-na-bazi-produktiv-eset/. (дата звернення: 19.03.2023)

8. ESET Smart Security Premium. URL: https://www.eset.com/ua/home/smart-security-premium/. (дата звернення: 19.03.2023)

9. Офіційна сторінка ESET. Чому ESET? URL: https://www.eset.com/ua/home/why-eset/. (дата звернення: 19.03.2023)

10. Передові технології ESET. URL: https://www.eset.com/ua/about/technology/. (дата звернення: 20.03.2023)

11. Check Point. Checkme. URL: http://www.cpcheckme.com/checkme/. (дата звернення: 15.05.2023)

12. Завантаження програмного забезпечення Microsoft. Windows 10. URL: https://www.microsoft.com/uk-ua/software-download/windows10. (дата звернення: 15.05.2023)

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

БАКАЛАВРСЬКА РОБОТА

НА ТЕМУ:

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ СЕРВІСНОГО ЦЕНТРУ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ РІШЕННЯ ESET

Виконав:
Ващук Олексій Миколайович

Керівник:
ст. викладач Марченко Віталій Вікторович

Актуальність

Забезпечення безпеки в сервісних центрах є критично важливим, оскільки вони мають доступ до конфіденційної інформації і даних клієнтів. Будь яка вразливість інформаційної системи може призвести до втрати даних.

Об'єкт дослідження

Інформаційна система сервісного центру

Предмет дослідження

Захист інформаційної системи за допомогою рішення від ESET

Мета дослідження

Проаналізувати функції та можливості ESET. Розробити рекомендації щодо захисту інформаційної системи

Завдання дослідження:

- Проаналізувати методи захисту інформаційної системи
- Дослідити існуючі рішення щодо захисту інформаційної системи
- Проаналізувати існуючі загрози інформаційної системи
- Дослідити захист інформації за допомогою рішення ESET
- Розробити рекомендації для підвищення захисту

Методи захисту інформації

Мережевий екран	Контролює трафік, що проходить через мережеві з'єднання. Може використовувати різні методи, такі як фільтрація на основі правил, виявлення вторгнень та системи запобігання вторгненням
Антивірусне програмне забезпечення	Виявляють та видаляють шпигунське програмне забезпечення, також забезпечують контроль за небажаною активністю
Оновлення операційної системи	Шкідливе програмне забезпечення може використовувати вразливості в операційній системі, тому її важливо регулярно оновлювати.

Існуючі рішення захисту інформації

Avast

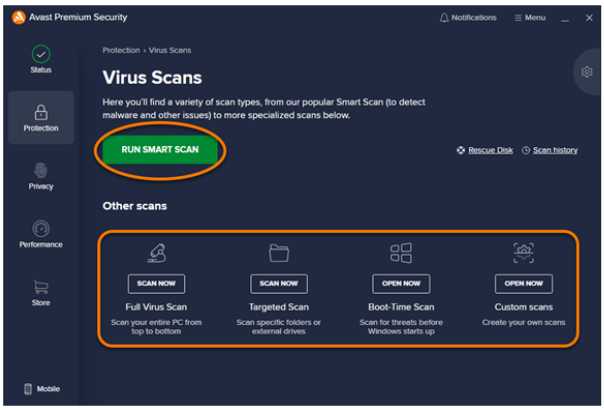

Рис. 1. Avast Premium Security

Надає такі послуги:

- Безпеку мережі Wi-Fi
- Безпечне користування електронною поштою
- Захист від програм-вимагачів
- Надсилає сповіщення про витік даних

Існуючі рішення захисту інформації

Bitdefender

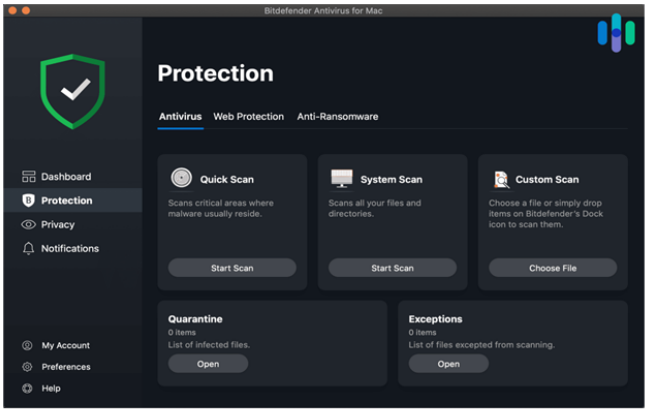

Рис. 2. Bitdefender

Надає такі послуги:
- Захист від фішингу
- Безпечний онлайн-банкінг
- VPN сервіс
- Захист від програм вимагачів
- Відстежує використання веб-камери та мікрофона

Існуючі рішення захисту інформації

Київстар Бізнес

Рис. 3. Київстар Бізнес

Надає такі послуги:
- Захист електронної пошти
- Захист мережі
- Захист Web-додатків
- Система захисту даних для аналізу поведінки користувачів
- Захист кінцевих точок
- Резервне копіювання та аварійне відновлення

Існуючі загрози інформаційної системи

ВІРУСИ
Вбудовуються в інші файли або програми та поширюються шляхом їх виконання або взаємодії з ними.
Можуть пошкодити файл, викрасти інформацію або спричинити інші негативні наслідки

ТРОЯНСЬКІ КОНІ
Приховуються під невинними або корисними програмами. Коли програма встановлюється на систему, троянський кінь виконує шкідливі дії, такі як злам паролів, викрадення інформації або надання злочинцям дистанційного доступу до системи

ПРОГРАМА-ВИМАГАЧ
Є шкідливим програмним забезпеченням, яке блокує доступ до системи або шифрує файли з метою вимагання викупу в обмін на відновлення доступу або розшифрування даних

Захист інформації за допомогою рішення ESET

ESET використовує безліч власних багаторівневих технологій, які працюють разом як ESET LiveSense. Також ESET використовує розширене машинне навчання. Компанія була одна з перших, хто застосував хмарну технологію, завдяки якій глобальна система репутації ESET LiveGrid постійно оновлює інформацію про загрози

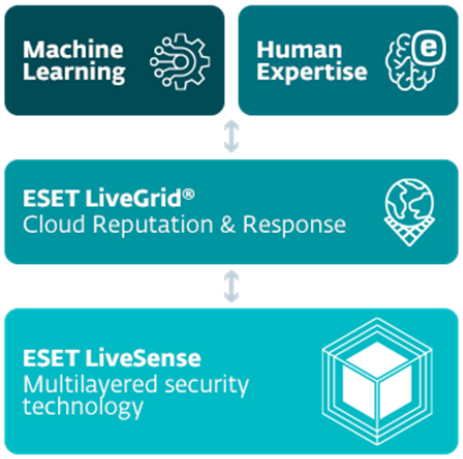

Рис. 4. Підхід ESET

Захист інформації за допомогою рішення ESET

Для забезпечення захисту інформації ESET використовують такі технології:

Сканер UEFI – Сканер перевіряє та забезпечує захист середовища попереднього завантаження

Родові виявлення – комплексно виявляють поведінку та характеристики шкідливих програм

Розширене машинне навчання – використовується дві форми машинного навчання

Рис. 5. ESET

Захист від експлойтів – перевіряє додатки. Під час запуску аналізується поведінка процесу

Захист від програм-вимагачів - перевіряє та оцінює всі виконані програми на основі їхньої поведінки та репутації, а також виявляє та блокує процеси, які нагадують поведінку програм-вимагачів.

Розробка рекомендацій для підвищення захисту

- Необхідно оновлювати операційну систему, програми та застосунки на комп'ютері.
- Слід застосовувати політику вимог до паролів, щоб забезпечити використання сильних паролів користувачам.
- Потрібно переглянути права доступу користувачів до різних систем та ресурсів. Обмежити лише необхідними.
- Використовуйте надійне антивірусне програмне забезпечення, і переконайтесь, що воно оновлюється регулярно.
- Використовуйте мережевий екран від ESET для контролю трафіку в мережі.
- Розгляньте можливість використання шифрування для захисту конфіденційної інформації.
- Потрібно провести навчання з питань кібербезпеки для всього персоналу.
- Забезпечте регулярне резервне копіювання всіх важливих даних..

Висновки

Зростаюча загроза кібератак та необхідність забезпечення безпеки важливих інформаційних систем вимагають постійного вдосконалення методів захисту. Використання надійного рішення, такого як ESET допоможе забезпечити ефективний захист від шкідливого програмного забезпечення та зберегти цілісність інформаційної системи сервісного центру.

Було досліджено:

- методи захисту від шкідливого програмного забезпечення
- сучасні варіанти захисту інформаційної системи
- принцип роботи систем ESET

Для вдосконалення захисту та підвищення рівню безпеки були розроблені рекомендації

ДЯКУЮ ЗА УВАГУ