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 ПРОТИДІЇ ВТОРГНЕННЯ В ІНФОРМАЦІЙНУ СИСТЕМУ НА БАЗІ РІШЕННЯ ESET SMART SECURITY PREMIUM»

Виконав студент 4 курсу, групи БСД-42
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Терно Я. А.
(прізвище та ініціали)

Керівник Марченко В. В.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконтролер _____
(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

Терно Ярослав Анатолійович
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розробка рекомендацій щодо протидії вторгненням в інформаційну систему на базі рішення ESET Smart Security Premium»
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
науково-технічна література, документація та програмний засіб, аналіз методів та засобів захисту від загроз, дослідження та порівняння функціональності ESET, розробка рекомендацій щодо протидії вторгненням в інформаційну систему на базі рішення ESET Smart Security Premium.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми захисту інформації в мережі інтернет.
2. Зміст методів та засобів захисту від загроз.
3. Дослідження та порівняння функціональності ESET з іншими антивірусами.
4. Розробка рекомендацій щодо протидії вторгненням в інформаційну систему на базі рішення ESET Smart Security Premium.

5. Перелік графічного матеріалу

1. Тема бакалаврської роботи.

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

3. Результати аналізу методів та засобів захисту від загроз.

4. Результати дослідження та порівняння функціональності ESET з іншими антивірусами.

5. Призначення та можливості рішення ESET Smart Security Premium.

6. Рекомендації, щодо протидії вторгненням в інформаційну систему на базі рішення ESET Smart Security Premium.

7. 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 безпечного користування інтернетом, та захисту свого комп'ютера від кіберзагроз.	25.02.2023 р.	
2.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	18.03.2023 р.	
3.	Дослідження та порівняння функціональності ESET Smart Security Premium з іншими антивірусами.	14.04.2023 р.	
4.	Розробка рекомендацій щодо протидії вторгненням в інформаційну систему на базі рішення ESET Smart Security Premium.	15.05.2023 р.	
5.	Оформлення результатів дослідження.	22.05.2023 р.	
6.	Підготовка доповіді до захисту.	29.05.2023 р.	

Студент _____ Терно Я. А.
(підпис) прізвище та ініціали

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

ВІДГУК РЕЦЕНЗЕНТА
на бакалаврську роботу

студента Терна Ярослава Анатолійовича
на тему: «Дослідження шляхів та розробка рекомендацій щодо протидії вторгненням в інформаційну систему на базі рішення ESET Smart Security Premium»

Актуальність: В сучасному світі інформаційна безпека стає все більш важливою темою. Зростання кількості кібератак та вірусів стає серйозною загрозою для компаній, організацій і громадян. Тому розробка різноманітні рекомендацій, які попереджають суспільство щодо протидії вторгнення в інформаційну систему, яке має значення для забезпечення інформаційної безпеки в різних сферах діяльності.

Для підвищення ефективності безпеки від кіберзагроз застосовують антивіруси, як для дому, малого та середнього бізнесу, так і державних установ. Тому тема бакалаврської роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу в роботі було встановлено зміст методів та засобів захисту від загроз.
2. Було досліджено та порівняно функціональності ESET з іншими антивірусами.
3. Розроблення рекомендацій щодо протидії вторгненням в інформаційну систему на базі рішення ESET Smart Security Premium.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

Недоліки:

1. У бакалаврській роботі бажано було б провести аналіз можливих умов функціонування засобу багатовимірного візуального аналізу ESET Smart Security Premium з різними інформаційними системам.
2. Експеримент із застосуванням рішення ESET Smart Security Premium бажано було б провести на вихідних даних, які відображають конкретну кіберзагрозу.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговує оцінку **добре**, а студент **Терно Я.А.** – присвоєння кваліфікації: 3439. Фахівець з організації інформаційної безпеки.

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 Терно Я.А 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 протидії вторгненням в інформаційну систему на базі рішення ESET Smart Security Premium».
Бакалаврська робота і рецензія додаються.

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

Довідка про успішність

Терно Я.А 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 ***Терно Я.А.*** обрав тему роботи, метою якої було дослідження шляхів та розробка рекомендацій щодо протидії вторгнення в інформаційну систему на базі рішення ESET Smart Security Premium. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Терно Я.А. 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 Терна Ярослава Анатолійовича на оцінку **«добре»** та присвоїти йому кваліфікацію: 3439. Фахівець з організації інформаційної безпеки.

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

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Терна Я.А
(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 ініц

“____” _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: 73 сторінок, 29 рисунків, 6 таблиця, 16 джерел.

Об'єкт дослідження – дипломної роботи є інформаційна система, що працює на базі рішення ESET Smart Security Premium. Конкретніше, робота фокусується на дослідженні шляхів та розробці рекомендацій щодо протидії вторгнення в інформаційну систему. Враховуючи те, що в даний час кібербезпека стає все більш актуальною темою, об'єкт дослідження є важливим та потребує уваги.

Предмет дослідження – є розробка рекомендацій та аналіз шляхів захисту інформаційної системи на базі рішення ESET Smart Security Premium від різних видів кіберзагроз та злочинних дій, які можуть статися в онлайн-середовищі. Конкретні аспекти дослідження включають аналіз функціональних можливостей програмного забезпечення ESET Smart Security Premium, дослідження основних методів захисту від вірусів, шпигунських програм та інших видів кіберзагроз, вивчення методів виявлення та аналізу інцидентів кібербезпеки, а також розробка рекомендацій щодо захисту інформаційної системи.

Мета роботи – дослідження є вивчення шляхів та розробка рекомендацій щодо протидії вторгненню в інформаційну систему на базі рішення ESET Smart Security Premium. Для досягнення мети були визначені наступні завдання:

Аналіз функціональних можливостей рішення ESET Smart Security Premium.

Дослідження загроз, які можуть виникнути в інформаційній системі та їх характеристики.

Визначення шляхів проникнення в інформаційну систему та методів захисту від них.

Розробка рекомендацій щодо налаштування рішення ESET Smart Security Premium з метою підвищення рівня захисту від потенційних загроз.

Проведення тестування розроблених рекомендацій на базі рішення ESET Smart Security Premium.

Результатом роботи будуть рекомендації щодо застосування рішення ESET Smart Security Premium для захисту інформаційних систем від вторгнень, які забезпечать підвищений рівень захисту та забезпечать безпеку інформації в онлайн-середовищі.

Методи дослідження – що використовуються в дипломній роботі "Дослідження шляхів та розробка рекомендацій щодо протидії вторгнення в інформаційну систему на базі рішення ESET Smart Security Premium", включають:

Аналіз літературних джерел та статистичних даних з проблеми кібербезпеки та захисту інформації в комп'ютерних системах.

Дослідження функцій та можливостей програми ESET Smart Security Premium з метою визначення рівня захисту інформаційної системи.

Проведення тестування програми ESET Smart Security Premium за допомогою спеціально створених тестових наборів вірусів та шкідливих програм з метою визначення її ефективності.

Розробка рекомендацій щодо підвищення ефективності захисту інформаційної системи на базі програми ESET Smart Security Premium.

Оцінка ефективності запропонованих рекомендацій.

Застосування цих методів дозволило детально проаналізувати проблему кібербезпеки та захисту інформації в комп'ютерних системах, визначити рівень

захисту інформаційної системи з використанням програми ESET Smart Security Premium, оцінити ефективність цієї програми та розробити рекомендації щодо підвищення її ефективності.

Галузь використання – дослідження інформаційна безпека та кібербезпека, зокрема захист комп'ютерних систем від кібератак та злочинних дій в онлайн-середовищі. Дане дослідження може бути корисним для IT-спеціалістів, керівників організацій, які займаються обробкою інформації, а також всіх користувачів комп'ютерів, які бажають збільшити рівень захисту своїх даних в мережі Інтернет.

ESET SMART SECURITY PREMIUM, ПРОТИДІЯ ЗАГРОЗАМ, КІБЕРБЕЗПЕКА, ЗАХИСТ АНТИВИРУСОМ, ЕФЕКТИВНИЙ ЗАХИСТ КОМП'ЮТЕРА, УНІВЕРСАЛЬНИЙ АНТИВІРУС НА ВСІ ОС, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КОМП'ЮТЕРА.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ - програмне забезпечення

ЕОМ - електронно обчислювальна машина

ОС - операційна система

ЕОТ - електронно-обчислювальної техніки

КСЗІ - комплексна система захисту інформації

ЕЦП - електронний цифровий підпис

BIOS - Basic Input/Output System

RSA - Rivest, Shamir і Adleman

ВСТУП

Актуальність дослідження. В сучасному світі, коли інформаційні технології поширюються в усіх сферах життя, забезпечення інформаційної безпеки є однією з найбільш актуальних проблем. Кіберзлочини стають все більш поширеними і складнішими, тому важливо забезпечити безпеку інформаційних систем від зовнішніх та внутрішніх загроз.

Одним із рішень для захисту інформаційних систем є використання антивірусного програмного забезпечення. Один з таких продуктів - ESET Smart Security Premium - надає комплексний захист від різноманітних загроз, включаючи віруси, шпигунське програмне забезпечення, хакерські атаки та інші види кіберзлочинів.

Об'єкт дослідження – дипломної роботи є інформаційна система, що працює на базі рішення ESET Smart Security Premium. Конкретніше, робота фокусується на дослідженні шляхів та розробці рекомендацій щодо протидії вторгнення в інформаційну систему. Враховуючи те, що в даний час кібербезпека стає все більш актуальною темою, об'єкт дослідження є важливим та потребує уваги.

Предмет дослідження – є розробка рекомендацій та аналіз шляхів захисту інформаційної системи на базі рішення ESET Smart Security Premium від різних видів кіберзагроз та злочинних дій, які можуть статися в онлайн-середовищі. Конкретні аспекти дослідження включають аналіз функціональних можливостей програмного забезпечення ESET Smart Security Premium, дослідження основних методів захисту від вірусів, шпигунських програм та інших видів кіберзагроз, вивчення методів виявлення та аналізу інцидентів кібербезпеки, а також розробка рекомендацій щодо захисту інформаційної системи.

Мета роботи – дослідження є вивчення шляхів та розробка рекомендацій щодо протидії вторгненню в інформаційну систему на базі рішення ESET Smart Security Premium. Для досягнення мети були визначені наступні завдання:

Аналіз функціональних можливостей рішення ESET Smart Security Premium.

Дослідження загроз, які можуть виникнути в інформаційній системі та їх характеристики.

Визначення шляхів проникнення в інформаційну систему та методів захисту від них.

Розробка рекомендацій щодо налаштування рішення ESET Smart Security Premium з метою підвищення рівня захисту від потенційних загроз.

Проведення тестування розроблених рекомендацій на базі рішення ESET Smart Security Premium.

Результатом роботи будуть рекомендації щодо застосування рішення ESET Smart Security Premium для захисту інформаційних систем від вторгнень, які забезпечать підвищений рівень захисту та забезпечать безпеку інформації в онлайн-середовищі.

Методи дослідження – що використовуються в дипломній роботі "Дослідження шляхів та розробка рекомендацій щодо протидії вторгнення в інформаційну систему на базі рішення ESET Smart Security Premium", включають:

Аналіз літературних джерел та статистичних даних з проблеми кібербезпеки та захисту інформації в комп'ютерних системах.

Дослідження функцій та можливостей програми ESET Smart Security Premium з метою визначення рівня захисту інформаційної системи.

Проведення тестування програми ESET Smart Security Premium за допомогою спеціально створених тестових наборів вірусів та шкідливих програм з метою визначення її ефективності.

Розробка рекомендацій щодо підвищення ефективності захисту інформаційної системи на базі програми ESET Smart Security Premium.

Оцінка ефективності запропонованих рекомендацій.

Застосування цих методів дозволило детально проаналізувати проблему кібербезпеки та захисту інформації в комп'ютерних системах, визначити рівень захисту інформаційної системи з використанням програми ESET Smart Security Premium, оцінити ефективність цієї програми та розробити рекомендації щодо підвищення її ефективності.

1 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВІД ЗАГРОЗ

1.1. Засоби та методи захисту інформації

Комплексна система захисту інформації (КСЗІ) — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС [1].

У фінансових установах існує два підходи до захисту інформації:

Автономний - направлений на захист конкретної дільниці або частини інформаційної системи, яка як правило є найбільш вразливою або може бути джерелом зловживань.

Комплексний - захищає інформаційну систему в цілому, всі її складові частини, приміщення, персонал тощо.

У фінансовій діяльності, попередження комп'ютерних злочинів є критично важливим завданням. Одним із ключових елементів такого попередження є використання сучасних технічних засобів захисту інформації. Термін "захист" у цьому контексті означає обмеження доступу до комп'ютерних систем, а також їх частини. У Положенні про технічний захист інформації в Україні зазначено, що технічний захист інформації з обмеженим доступом в автоматизованих системах та засобах обчислювальної техніки спрямований на запобігання порушенню цілісності інформації з обмеженим доступом та її просочення шляхом:

- несанкціонованого доступу;
- приймання й аналізу побічних електромагнітних випромі-нювань і наводок;
- використання закладних пристроїв;
- впровадження комп'ютерних вірусів та іншого впливу.

Технічний захист інформації з обмеженим доступом в автома-тизованих системах і засобах обчислювальної техніки, призначених для формування, пересилання, приймання, перетворення, відображення та зберігання інформації,

забезпечується комплексом конструкторських, організаційних, програмних і технічних заходів на всіх етапах їх створення й експлуатації.

Основними методами та засобами технічного захисту інформації з обмеженим доступом в автоматизованих системах і засобах обчислю-вальної техніки є:

- використання захищеного обладнання;
- регламентування роботи користувачів, технічного персоналу,програмних засобів, елементів баз даних і носіїв інформації з обмеженим доступом (розмежування доступу);
- регламентування архітектури автоматизованих систем і засобів обчислювальної техніки;
- інженерно-технічне оснащення споруд і комунікацій, призначених для експлуатації автоматизованих систем і засобів обчислювальної техніки;
- пошук, виявлення і блокування закладних пристроїв.

До основних засобів захисту інформації можна віднести такі:

- фізичні засоби;
- апаратні засоби;
- програмні засоби;
- апаратно-програмні засоби;
- криптографічні;
- організаційні методи.

Фізичні засоби захисту - це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та об'єктів на базі ПК, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів інформаційних систем та інформації, що захищаються.

Щоб запобігти несанкціонованому доступу до інформації, найдоступнішим і надійним рішенням є використання ПК в режимі автономного використання одним користувачем в спеціально виділеному приміщенні, яке не має доступу для сторонніх осіб. У такому випадку, роль захисту виконує саме приміщення, яке

забезпечує фізичний захист, зокрема міцні стіни, стеля, підлога та двері. Якщо обладнання для фізичного захисту відповідає вимогам, таким як наявність охоронної сигналізації на вікнах і дверях, відсутність люків та з'єднань з іншими приміщеннями, то стійкість захисту буде визначатись характеристиками охоронної сигналізації при відсутності користувача в неробочий час.

Під час робочого часу комп'ютер може бути підданий ризику витоку інформації через побічне електромагнітне випромінювання. Щоб запобігти цій загрозі, проводяться спеціальні дослідження щодо апаратного забезпечення та його випромінювання. Основними змістом таких досліджень є атестація та категоризація об'єктів електронно-обчислювальної техніки (ЕОТ) з метою видачі дозволів на експлуатацію. Крім того, двері приміщення повинні мати механічний або електромеханічний замок.

У випадку відсутності охоронної сигналізації, можна зберігати системний блок та машинні носії інформації в сейфі, якщо користувач відсутній на тривалий період. Проте використання апаратного паролю BIOS у системі вводу-виводу не є достатньо надійним заходом для захисту від НСД, оскільки носій паролю може бути замінений на інший з відомим значенням у випадку відсутності механічного замка на корпусі системного блоку та самого власника-користувача. Тому механічний замок, що блокує вмикання та завантаження ПК, є найбільш ефективним заходом захисту в цьому випадку.

Спектр сучасних фізичних засобів захисту дуже широкий. До цієї групи засобів захисту належать також різні засоби екранування робочих приміщень та каналів передачі даних.

Апаратні засоби захисту інформації - це різноманітні за принципом дії, побудовою і можливостями технічні конструкції, що забезпечують припинення розголошення, захист від витоку і протидію несанкціонованому доступу до джерел конфіденційної інформації [2].

Основні функції апаратних засобів захисту:

- заборона несанкціонованого (неавторизованого) зовнішнього доступу віддаленого користувача;

- заборона несанкціонованого (неавторизованого) внутрішнього доступу до баз даних в результаті випадкових чи умисних дій персоналу;
- захист цілісності програмного забезпечення.Ці функції реалізуються шляхом:
- ідентифікації суб'єктів (користувачів, обслуговуючого персо-налу) і об'єктів (ресурсів) системи;
- автентифікації суб'єкта за наданим ним ідентифікатором;
- перевірки повноважень, яка полягає в перевірці дозволу на певні види робіт;
- реєстрації (протоколювання) при звертаннях до заборонених ресурсів;
- реєстрації спроб несанкціонованого доступу.

Реалізація цих функцій здійснюється за допомогою застосування різних технічних пристроїв спеціального призначення. До них, зокрема, належать:

- джерела безперебійного живлення апаратури, а також:
- пристрої стабілізації, що оберігають від стрибкоподібних пере-падів напруги і пікових навантажень у мережі електроживлення;
- пристрої екранування апаратури, ліній зв 'язку та приміщень, в яких знаходиться комп'ютерна техніка;
- пристрої ідентифікації і фіксації терміналів і користувачів при спробі несанкціонованого доступу до комп'ютерної мережі;
- засоби захисту портів комп 'ютерної техніки тощо.
- Засоби захисту портів виконують декілька захисних функцій, а саме:
- "звірка коду ". Комп'ютер захисту порту звіряє код санкціонованих користувачів з кодом у запиті;
- "камуфляж". Деякі засоби захисту портів камуфлюють існування портів на лінії телефонного зв'язку шляхом синтезування людського голосу, який відповідає на виклик абонента;
- "дзвінок назустріч". У пам'яті засобу захисту портів зберігаються не тільки коди доступу, але й ідентифікаційні номери телефонів;

- ведення автоматичного "електронного журналу" доступу в комп'ютерну систему з фіксацією основних дій користувача.

Програмні засоби захисту необхідні для виконання логічних і інтелектуальних функцій захисту, які вмонтовані до складу програмного забезпечення системи.

З допомогою програмних засобів захисту реалізуються наступні задачі безпеки:

- контроль завантаження та входу в систему за допомогою системи паролів;
- розмежування і контроль прав доступу до системних ресурсів, терміналів, зовнішніх ресурсів, постійних та тимчасових наборів даних тощо;
- захист файлів від вірусів;
- автоматичний контроль за роботою користувачів шляхом протоколювання їх дій.

Апаратно-програмні засоби захисту - це засоби, які основані на синтезі програмних та апаратних засобів.

Ці засоби широко використовуються при аутентифікації користувачів автоматизованих банківських систем.

Аутентифікація - це підтвердження того, ким є користувач на вході. Це проходження перевірки автентичності.

Що може перевіряти система:

- чи існує користувач з таким ім’ям;
- чи збігається введений пароль з його обліковим записом;
- може запитувати ще наявність сертифіката, IP-адресу або додатковий код верифікації.

Авторизація - це те, що користувачу дозволяється робити після входу. Це надання і перевірка прав на вчинення будь-яких дій в системі [3]. Для цього використовуються різні методи контролю доступу (ACL, RBAC, ABAC тощо).

Пароль - це код (набір символів), що забезпечує доступ до систем, файлів, апаратних засобів, тощо. Апаратно-програмні засоби захисту використовуються також при накладанні електронно-цифрових підписів відповідальних користувачів.

Найпоширенішим в автоматизованих банківських системах є використання смарт-карт, які містять паролі та ключі користувачів.

Організаційні заходи захисту засобів комп'ютерної інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу.

Досвід інших країн показує, що найбільш ефективним заходом для захисту інформаційних систем є створення в організації посади фахівця з комп'ютерної безпеки або створення спеціальної служби, яка може бути як приватною, так і централізованою, залежно від конкретної ситуації. Наявність такої служби (відділу) у банківській структурі може значно знизити ймовірність вчинення злочинів у сфері використання комп'ютерних технологій, на думку зарубіжних фахівців.

Законодавство України дозволяє створювати в державних установах та організаціях окремі підрозділи та служби, які відповідають за захист інформації та забезпечують рівень безпеки інформації в автоматизованих системах. Ця норма не є обов'язковою, але рекомендується для ефективного захисту інформації. Закон "Про захист інформації в автоматизованих системах" вказує на обов'язковість захисту інформації, але не обов'язковість створення окремої функціональної структури для цього. Така функція може бути частиною іншої організаційної структури та виконуватися в поєднанні з іншими функціями.

У банківських установах обов'язковим є створення спеціальних структур, які забезпечують захист інформації та фінансової безпеки. В рамках існуючих служб економічної безпеки та фізичного захисту мають бути створені спеціальні відділи комп'ютерної безпеки. Діяльністю цих відділів керує спеціально призначений заступник начальника служби безпеки, який має доступ до необхідних людських, фінансових та технічних ресурсів для вирішення завдань, що стоять перед ними.

До функціональних обов'язків таких осіб (структурних підрозділів) має входити здійснення, передусім, таких організаційних заходів:

- забезпечення підтримки з боку керівництва конкретної організації вимог захисту засобів комп 'ютерної техніки;

- розробка комплексного плану захисту інформації;
- визначення пріоритетних напрямів захисту інформації з урахуванням специфіки діяльності організації;
- складання загального кошторису витрат фінансування охоронних заходів відповідно до розробленого плану та затвердження його як додатку до плану керівництвом організації;
- визначення відповідальності співробітників організації за безпеку інформації в межах встановленої компетенції шляхом укладення відповідних договорів між співробітником та адміністрацією;
- розробка, впровадження і контроль за виконанням різного роду інструкцій, правил та наказів, які регламентують форми допуску, рівні секретності інформації, конкретних осіб, допущених до роботи з секретними (конфіденційними) даними тощо;
- розробка ефективних заходів боротьби з порушниками захисту засобів комп 'ютерної техніки.

Надійним засобом підвищення ефективності заходів інформаційної безпеки є навчання та інструктаж працюючого персоналу щодо організаційно-технічних заходів захисту, які застосовуються в конкретній організації. Крім цього, обов'язково мають бути реалізовані наступні організаційні заходи:

Для всіх осіб, що мають право доступу до засобів комп'ютерної техніки, потрібно визначити категорії допуску, тобто коло службових інтересів коленої особи, види інформації, до яких вона має право доступу, а також: вид такого дозволу, правомочність особи, яка уповноважується для здійснення тих або інших маніпуляцій з засобами комп'ютерної техніки:

- слід визначити адміністративну відповідальність за збереження і санкціонування доступу до інформаційних ресурсів. При цьому, за кожний вид ресурсів відповідальність повинна нести одна конкретна особа;
- налагодити періодичний системний контроль за якістю захисту інформації шляхом проведення регламентних робіт як особою, відповідальною за безпеку, так і залученням компетентних фахівців (експертів) з інших організацій;

- провести класифікацію інформації відповідно до Ті важливості, диференціювати на основі цього заходи захисту; визначити порядок охорони та знищення інформації;
- організувати фізичний захист засобів комп'ютерної техніки.

Криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо [4].

Застосування криптографічного захисту, тобто кодування тексту з допомогою складних математичних алгоритмів, завойовує все більшу популярність. Звичайно, жоден з шифрувальних алгоритмів не дає цілковитої гарантії захисту від зловмисників, але деякі методи шифрування настільки складні, що ознайомитися зі змістом зашиф-рованих повідомлень практично неможливо. Основні криптографічні методи захисту:

- шифрування з допомогою датчика псевдовипадкових чисел, яке полягає в тому, що генерується гамма шифру за допомогою датчика псевдовипадкових чисел і накладається на відкриті дані з урахуванням зворотності процесу;
- шифрування з допомогою криптографічних стандартів шифрування даних (з симетричною схемою шифрування), в основі якого використовуються перевірені і випробувані алгоритми шифрування даних з великою криптостійкістю;
- шифрування з допомогою пари ключів (з асиметричною системою шифрування), в яких один ключ є відкритим і використовується для шифрування інформації, другий ключ - закритим і використовується для розшифрування інформації.

Потужним та дієвим є примінення для захисту інформації крипто-захисту, тобто систем, що дозволяють шифрувати та дешифрувати інформаційні потоки. Традиційна криптографія виходила з того, що для шифрування та дешифрування використовувався один і той же секретний ключ, який мав мати відправник повідомлення і отримувач. Одним з поширених, сьогодні, методів шифрування є алгоритм RSA, в основі якого кожен учасник процесу має власний таємний ключ

та відкритий ключ, що не є секретним з допомогою якого проводиться обмін повідом-леннями.

Цифровим підписом (ЦП) - називається результат спеціального криптографічного перетворення, що здійснюється над електронним документом його власником. Мета перетворення - довести неспростовність тексту документа та факту перетворення даних конкретною особою. Основний метод - перевірка факту використання секретного параметра (ключа) підпису (без знання власного ключа) [5].

Криптографічні методи захисту інформації широко використовуються в автоматизованих банківських системах і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту. Використовуючи шифрування повідомлень в поєднанні з правильною установкою комунікаційних засобів, належними процедурами ідентифікації користувача, можна добитися високого рівня захисту інформаційного обміну.

Криптографія є одним з найкращих засобів забезпечення конфіден-ційності і контролю цілісності інформації. Вона займає центральне місце серед програмно-технічних регулювальників безпеки, є основою реалізації багатьох з них і, в той же час, останнім захисним рубежем.

На підставі аналізу засобів та методів захисту інформації можна зробити висновок, що на сьогоднішній день існує велика кількість різноманітних захисних засобів, які дозволяють забезпечити надійний захист інформації від зовнішніх загроз.

Одним з найбільш ефективних заходів є встановлення інтегрованих систем захисту інформації, що включають в себе антивірусні програми, фаєрволи, інструменти для моніторингу трафіку, шифрування даних та інші компоненти.

У будь-якому випадку, важливо розуміти, що жоден захисний засіб не може забезпечити абсолютну безпеку, тому важливо дотримуватись правил безпеки та не відкривати підозрілі файли та посилання. Тільки комплексний підхід до захисту даних та уважність користувачів можуть забезпечити надійний рівень інформаційної безпеки.

1.2 Класифікація загроз інформаційній безпеці

Загроза інформаційній безпеці - це будь-яка потенційна чи фактична подія, дія або ситуація, яка може завдати шкоди або поставити під загрозу конфіденційність, цілісність та доступність інформації чи інформаційних систем.

Конфіденційність інформації базується на понятті створення обмеженого доступу до інформаційних ресурсів третіх, сторонніх осіб. Відомості можуть надаватися виключно користувачам, які мають право взаємодіяти з даними системами, були ідентифіковані та отримали право доступу.

Цілісність інформаційних відомостей – це ніщо інше, як властивість інформації залишатися незмінною, в її первісному вигляді, структурі, під час її зберігання або багаторазової передачі. Змінити, видалити, внести корективи має право тільки людина-користувач, якому належать права доступу. Також це дозволено особам із законним доступом до цієї інформації.

Доступність - це інформаційні дані, що знаходяться у вільному доступі, повинні оперативно надаватися легальним користувачам, без будь-яких зволікань і перешкод.

Достовірність - це відомостей свідчить про те, що інформаційні дані належать довіреній особі або законному власнику, який також є першоджерелом відомостей [6].

Джерела загроз:

1. **Людський чинник.** Ця група загроз пов'язана з діями людини, що має санкціонований або несанкціонований доступ до інформації. Загрози цієї групи можна розділити на:

- *зовнішні* — дії кібер-злочинців, хакерів, інтернет-шахраїв, недобросовісних партнерів, кримінальних структур;
- *внутрішні* — дії персоналу компаній і також користувачів домашніх комп'ютерів. Дії даних людей можуть бути як умисними, так і випадковими.

2. **Технічний чинник.** Ця група загроз пов'язана з технічними проблемами – фізичне і моральне старіння устаткування, неякісні програмні і апаратні засоби опрацювання інформації. Все це приводить до відмови устаткування втрати інформації.

3. **Стихійний чинник.** Ця група загроз включає природні катаклізми, стихійні лиха і інші форс-мажорні обставини, незалежні від діяльності людей.

Всі ці джерела загроз необхідно обов'язково враховувати при розробці системи захисту інформаційної безпеки. Зупинюся лише на одному з них - зовнішніх загрозах, пов'язаних з діяльністю людини.

Шляхи поширення загроз (людський чинник)

1. **Глобальна мережа Інтернет** унікальна тим, що не є чиєюсь власністю і не має територіальних меж. Це багато в чому сприяє розвитку численних веб-ресурсів і обміну інформацією. Зараз будь-яка людина може дістати доступ даним, що зберігаються в Інтернеті, або створити свій власний веб-ресурс. Ці особливості глобальної мережі надають зловмисникам можливість скоєння злочинів в Інтернеті, утрудняючи їх виявлення і покарання. Зловмисники розміщують віруси і інші шкідливі програми на веб-ресурсах, «маскують» їх під корисне і безкоштовне програмне забезпечення.

Скрипт, що автоматично запускаються при відкритті веб-сторінки, можуть виконувати шкідливі дії на вашому комп'ютері, включаючи зміну системного реєстру, крадіжку особистих даних і установку шкідливого програмного забезпечення. Використовуючи мережеві технології, зловмисники реалізують атаки на видалені приватні комп'ютери і сервери компаній. Результатом таких атак може бути виведення ресурсу з ладу, діставання повного доступу до ресурсу, а, отже, до інформації, що зберігається на ньому, використання ресурсу як частини зомбі- мережі. У зв'язку з появою кредитних карт, електронних грошей і можливістю їх використання через Інтернет інтернет-шахрайство стало одним з найбільш поширених злочинів.

2. **Локальна мережа (Інтранет)** – це внутрішня мережа, спеціально розроблена для управління інформацією всередині компанії або приватної

домашньої мережі. Інтранет є єдиним простором для зберігання, обміну і доступу до інформації для всіх комп'ютерів мережі. Тому, якщо якій-небудь з комп'ютерів мережі заражений, решту комп'ютерів піддано величезному ризику зараження. Щоб уникнути виникнення таких ситуацій необхідно захищати не лише периметр мережі, але й кожний окремий комп'ютер.

3. **Електронна пошта**. Наявність поштових застосунків практично на кожному комп'ютері і використання шкідливими програмами вмісту електронних адресних книг для виявлення нових жертв забезпечують сприятливі умови для розповсюдження шкідливих програм. Користувач зараженого комп'ютера, сам того не підозрюючи, розсилає заражені листи адресатам, які у свою чергу відправляють нові заражені листи і т.д. Не рідкісні випадки, коли заражений файл-документ унаслідок недогляду потрапляє в списки розсилки комерційної інформації якої-небудь крупної компанії. В цьому випадку страждають сотні або навіть тисячі абонентів таких розсилок, які потім розішлють заражені файли десяткам тисячам своїх абонентів.

Крім загрози проникнення шкідливих програм існують проблема зовнішньої небажаної пошти рекламного характеру (спаму). Не будучи джерелом прямої загрози, небажана кореспонденція збільшує навантаження на поштові сервери, створює додатковий трафік, засмічує поштову скриньку користувача, веде до втрати робочого часу і тим самим наносить значні фінансові втрати. Зловмисники стали використовувати так звані спамерські технології масового розповсюдження, щоб примусити користувача відкрити лист, перейти по посиланню з листа на якийсь інтернет-ресурс. Отже, можливості фільтрації спаму важливі не лише самі по собі, але і для протидії інтернет-шахрайству і розповсюдженню шкідливих програм.

4. **Знімні носії інформації** - CD-диски, флеш-карти - широко використовують для зберігання і поширення інформації. При активуванні файлу знімного носія, що містить шкідливий код, є загроза пошкодити дані на вашому комп'ютері і розповсюдити вірус на інші носії інформації або комп'ютери мережі [7].

Метою атак:

- отримання конфіденційної інформації;
- розкриття комерційної таємниці;
- викрадення грошей;
- порушення роботи системи.

Це лише деякі з можливих класифікацій загроз інформаційній безпеці, які можуть використовуватися для їх аналізу та подальшого захисту.

На основі класифікації загроз інформаційній безпеці можна зрозуміти, що існує безліч різноманітних загроз, які можуть виникнути в сфері інформаційної безпеки. Ці загрози можуть бути технічними, соціальними, природними або людськими. Тому для забезпечення інформаційної безпеки потрібно застосовувати комплексні заходи, що включають технічні, організаційні та правові заходи.

Важливо розуміти, що заходи по забезпеченню інформаційної безпеки повинні бути постійними і оновлюватися залежно від змін у загрозах. Крім того, необхідно пам'ятати, що інформаційна безпека - це не тільки технічне питання, але і культурне. Кожен користувач має бути свідомим та відповідальним при поводженні зі своїми даними та іншими даними, які йому довіряються.

1.3 Аналіз сучасного шкідливого програмного забезпечення та боротьба з ним

Сучасне шкідливе програмне забезпечення (англ. malware) може мати різні форми та функції, і його розповсюдження може стати серйозною загрозою для інформаційної безпеки.

Для шкідливих комп’ютерних програм характерно:

1. Швидке розмноження шляхом приєднання своїх копій до інших програм, копіювання на інші носії даних, пересилання копій комп’ютерними мережами.

2. Автоматичне виконання деструктивних дій, які вносять дезорганізацію в роботу комп’ютера:

● знищення даних шляхом видалення файлів певних типів або форматування дисків;

● внесення змін у файли, зміна структури розміщення файлів на диску;

● зміна або повне видалення даних із постійної пам’яті;

● зниження швидкодії комп’ютера, наприклад за рахунок заповнення оперативної пам’яті своїми копіями;

● постійне (резидентне) розміщення в оперативній пам’яті від моменту звернення до ураженого об’єкта до моменту вимкнення комп’ютера, і ураження все нових і нових об’єктів;

● примусове перезавантаження операційної системи;

● блокування запуску певних програм;

● збирання і пересилання копії даних комп’ютерними мережами, наприклад пересилання кодів доступу до секретних даних;

● використання ресурсів уражених комп’ютерів для організації колективних атак на інші комп’ютери в мережах;

● виведення звукових або текстових повідомлень, спотворення зображення на екрані монітора тощо.

За рівнем небезпечності дій шкідливі програми розподіляють на:

● **безпечні** - проявляються відео та звуковими ефектами, не змінюють файлову систему, не ушкоджують файли і не виконують шпигунські дії;

● **небезпечні** - призводять до перебоїв у роботі комп’ютерної системи: зменшують розмір доступної оперативної пам’яті, перезавантажують комп’ютер тощо;

● **дуже небезпечні –** знищують дані з постійної та зовнішньої пам’яті, виконують шпигунські дії тощо.

Класифікація шкідливих програм за принципами розповсюдження та функціонування.

Комп’ютерні віруси - програми, здатні саморозмножуватися і виконувати несанкціоновані деструктивні дії на ураженому комп’ютері.

За середовищем існування віруси розподіляють на:

● **дискові (завантажувальні) віруси** – розмножуються копіюванням себе в службові ділянки дисків та інших змінних носіїв, яке відбувається під час спроби користувача зчитати дані з ураженого носія;

● **файлові віруси** – розміщують свої копії у складі файлів різного типу. Як правило, це файли готових до виконання програм із розширенням імені exe або com. Однак існують так звані макровіруси, що уражують, наприклад, файли текстових документів, електронних таблиць, баз даних тощо [9];

● **макровіруси** — це різновид комп'ютерних вірусів, створених засобами макросів, вбудованих у додатку Microsoft Office, CorelDRAW тощо. Зараження виникає, коли заражений документ відкривається у вікні прикладної програми, якщо підтримується можливість виконання макрокоманд. До макровірусів належать також віруси, які розповсюджуються за допомогою вкладених документів, що надсилаються електронною поштою.

Хробаки (черв'яки) комп'ютерних мереж - пересилають свої копії комп'ютерними мережами з метою проникнення на віддалені комп'ютери.

Більшість черв'яків поширюються, прикріпившись до файлів електронної пошти, електронних документів тощо. З ураженого комп'ютера хробаки намагаються проникнути на інші комп'ютери, використовуючи список електронних поштових адрес або іншими способами.

Троянські програми - програми, що проникають на комп'ютери користувачів разом з іншими програмами, які користувач «отримує» комп'ютерними мережами.

Як і інші шкідливі програми, троянські програми можуть виконувати зазначені вище деструктивні дії, але в основному їх використовують для виконання шпигунських дій.

Значна частина шкідливих програм у початкові періоди зараження не виконують деструктивних дій, а лише розмножуються. Це так звана пасивна фаза їхнього існування. Через певний час, у визначений день або по команді з комп'ютера в мережі шкідливі програми починають виконувати деструктивні дії – переходять в активну фазу свого існування.

Серед вірусів виділяють ті, що використовують спеціальні способи приховування своїх дій і знаходження в операційній системі комп’ютера:

- **поліморфні (мутанти) -** віруси, які при копіюванні змінюють свій вміст так, що кожна копія має різний розмір; їх важче визначити, використовуючи пошук за відомою довжиною коду вірусу;
- **стелс (англ. stealth – хитрість, викрут, stealth virus – вірус (невидимка) –** віруси, що намагаються різними засобами приховати факт свого існування в операційній системі. Наприклад, замість дійсного об’єкта, ураженого вірусом, антивірусній програмі надається для перевірки його не уражена копія.

Фішинг — це форма атаки з використанням соціальної інженерії, в ході якої зловмисник, маскуючись під надійний суб'єкт, виманює конфіденційну інформацію жертв.

Прихований майнінг - це шкідливі програми для прихованого майнінгу належать до категорії шкідливого коду, призначеного для використання обчислювальної потужності пристрою користувача з метою видобутку криптовалюти. При цьому, жертви не дають згоду і навіть не підозрюють про таку діяльність.

Брандмауер - у комп’ютерних мережах брандмауер (фаєрвол) виявляє та блокує мережевий трафік на основі попередньо визначених або динамічних правил. Вони захищають мережі та пристрої від вторгнення потенційно небезпечних кіберзлочинців, які можуть інфікувати пристрої та використовувати їх у зловмисних цілях.

DDoS-атака — це вид кібератаки, під час якої зловмисники намагаються порушити роботу веб сайту, мережі чи інших онлайн-сервісів, перевантажуючи їх великою кількістю підроблених або небажаних запитів.

Програми-вимагачі – це шкідливе програмне забезпечення, яке блокує пристрій або шифрує його вміст, вимагаючи гроші у жертв. За певну плату оператори шкідливого коду обіцяють відновити доступ до інфікованої машини або даних.

Шпигунські програми - це вид шкідливого програмного забезпечення, яке використовується для «шпигунства» на вашому пристрої з метою збору особистих даних, таких як електронні листи, паролі, номери кредитних карт, а також для передачі цієї інформації третім особам через Інтернет.

Рекламне ПЗ - це різні спливаючі рекламні оголошення, які відображаються на комп'ютері чи мобільному пристрої користувача. Також рекламне ПЗ може використовуватися у зловмисних цілях, наприклад, для завантаження вірусів та шпигунських програм на пристрій, або для отримання доступу до Вашого браузера.

Бекдор - це шкідлива програма для отримання доступу до робочої станції, сервера, пристрою чи мережі шляхом обходу аутентифікації, а також інших стандартних методів та технологій безпеки.

Експлойт- це шкідливий код, який використовує уразливості в системі безпеки програмного забезпечення для поширення кіберзагроз.

Кет Фишинг (catfishing) -це вид онлайн-шахрайства, коли людина або так званий **кет фішер (catfish),** створює фальшивий профіль у соціальній мережі чи на сайті знайомств з метою шахрайства чи обману. Найчастіше метою зловмисників є фінансова вигода, однак іноді методи кетфішингу використовуються для отримання конфіденційної інформації чи інтимного контенту.

Спам - це **небажані повідомлення у будь-якій формі**, які надсилаються у великій кількості. Найчастіше спам надсилається у формі комерційних електронних листів, надісланих на велику кількість адрес, а також через миттєві та текстові повідомлення (SMS), соціальні медіа або навіть голосову пошту [10].

«Симптоми» зараження комп'ютера вірусом:

- часті зависання і збої в роботі комп'ютера;
- повільна робота комп'ютера при запуску програм;
- неможливість завантаження операційної системи; зникнення файлів і папок або спотворення їхнього вмісту;
- часте звернення до жорсткого диска (часто блимає лампочка на системному блоці);

- браузер зависає або поводиться несподіваним чином (наприклад, вікно програми неможливо закрити).

Методи боротьби з комп’ютерними вірусами

Антивірусні програми - це комп'ютерна програма, спеціально створена для пошуку та знешкодження вірусів. Оскільки вона може виявити вірус, що вона знає і відповідні засоби боротьби з ним. Незважаючи на це, кожен день виходить більше 20 нових вірусів, що антивірусні програми не здатні виявити. Тому регулярне оновлення антивірусних баз є основою для успішного пошуку і знищення цих шкідливих кодів [8].

Антивірусні програми розрізняють за їхнім призначенням.

Детектори - виявляють файли, заражені вірусами.

Лікарі (фаги) - «лікують» заражені програми або документи, видаляючи із заражених файлів віруси.

Ревізори - запам’ятовують стан програм і дисків та порівнюють їх поточний стан із попереднім і повідомляють про виявлені невідповідності.

Фільтри - перехоплюють звернення до системи, які використовуються вірусами для розмноження і заподіяння шкоди.

Блокувальники - перехоплюють вірусонебезпечні дії (відкриття файла для запису, запис у завантажувальний сектор диску тощо) і повідомляють про це користувача.

Сканери - сканують (перевіряють) файли на жорсткому диску і в оперативній пам’яті.

Імунізатори - повідомляють користувача та/або перешкоджають зараженню вірусами.

Звичайно антивірусні програмні пакети мають у своєму складі:

- програму-сканер, яка переглядає всі файли, системні сектори, пам’ять з метою пошуку вірусів, тобто унікального програмного коду;
- антивірусний монітор, який автоматично завантажується в оперативну пам’ять після вмикання комп’ютера та виконує перевірку на віруси всіх файлів, з

якими ведеться робота; також ця програма звичайно відстежує всі звернення до жорсткого диска;

- ревізор змін, який запам’ятовує певні дані кожного файлу та системних секторів. Ці дані зберігаються, і при кожному їх завантаженні та зміненні ревізор порівнює й повідомляє про зміни;
- засоби оновлення антивірусних баз через Інтернет, які дозволяють своєчасно виявити та знищити нові комп’ютерні віруси.

Методи профілактики зараження комп’ютерними вірусами

Усі існуючі заходи боротьби з комп’ютерними вірусами можна поділити на дві категорії:

- профілактичні заходи, спрямовані на резервне збереження даних та недопущення

зараження вірусами через піратське програмне забезпечення;

- заходи щодо знищення комп’ютерних вірусів та лікування заражених програм і даних.

Для профілактики зараження комп’ютера вірусами слід дотримуватись певних правил:

- регулярно оновлювати програми антивірусного захисту;
- систематично перевіряти комп’ютер на наявність вірусів;
- користуватися лише ліцензійним програмним забезпеченням;
- не використовувати для роботи підозрілі й чужі файли, зовнішні носії тощо без попередньої перевірки антивірусними програмами;
- не відкривати приєднані до електронної пошти файли без попередньої їхньої перевірки на наявність вірусів;
- систематично здійснювати резервне копіювання даних на незалежні носії;
- не завантажувати з Інтернету файли з розширенням exe з неперевірених сайтів;
- обмежити коло користувачів вашого комп’ютера, вимагати неухильного дотримання правил антивірусного захисту;

- при використанні ОС Windows працювати під обліковим записом без прав адміністратора.

На підставі проведеного аналізу сучасного шкідливого програмного забезпечення та боротьби з ним можна зробити висновок, що зростаюча кількість його видів та складність нападів на комп'ютерні системи вимагає збільшення уваги до захисту інформації.

Для боротьби з шкідливим програмним забезпеченням необхідно застосовувати комплексний підхід, що включає в себе встановлення та регулярне оновлення антивірусного програмного забезпечення, фаєрволу та інших засобів захисту, а також проведення регулярної підготовки та навчання користувачів.

Захист інформації від шкідливих програм є важливою складовою інформаційної безпеки, і його досягнення потребує постійної уваги та зусиль.

2 ДОСЛІДЖЕННЯ ТА ПОРІВНЯННЯ ФУНКЦІОНАЛЬНОСТІ ESET SMART SECURITY PREMIUM З ІНШИМИ АНТИВІРУСАМИ

2.1 Функціональні можливості Zillya

Антивірус Zillya! від української компанії "Лабораторія Zillya!" був створений у 2009 році та з тих пір активно застосовується для захисту комп'ютерів та інших пристроїв від шкідливого програмного забезпечення. Остання версія програми була випущена 26 травня 2015 року.

Zillya! має кілька варіантів поширення для дому та бізнесу, включаючи окремі версії для бізнесу та держави, смартфонів і планшетів, а також безкоштовну версію. Для дому та бізнесу також доступні різні варіанти розповсюдження, щоб задовольнити потреби різних користувачів.

Zillya! Антивірус найдешевший варіант та найменша кількість можливостей.

Zillya! Internet Security середній варіант між ціною та кількістю можливостей.

Zillya! Total Security максимальна кількість можливостей для комплексного захисту ПК[11].

Як і будь-який інший антивірусний продукт, Zillya! має свої переваги та недоліки. Основними перевагами Zillya! є швидкість та ефективність сканування, а також наявність різних варіантів поширення для різних типів користувачів. Крім того, він має простий та зрозумілий інтерфейс, що робить його доступним для користувачів різного рівня підготовки. Також хотів би виділити що Zillya! дость дешеві ціни.

Проте, серед недоліків Zillya! можна відзначити те, що надані можливості лише для Windows та android. Він може спричиняти затримки в роботі комп'ютера, особливо під час сканування системи. Також, деякі користувачі скаржаться на те, що программа може пропускати деякі загрози безпеки. Крім того, останнє оновлення Zillya! вийшло у 2015 році, що може вказувати на те, що він може бути менш ефективним у боротьбі з останніми загрозами безпеки.

Таблиця 2.1.

Варіанти розповсюдження антивірусу Zillya!

Характеристики	Zillya! Антивірус	Zillya! Internet Security	Zillya! Total Security
Вартовий (файловий монітор) Здійснює постійний моніторинг системи на наявність загроз	Так	Так	Так
Інспектор Слідкує за програмами, на комп'ютері, з метою виявлення шкідливої активності	Так	Так	Так
Поштовий фільтр Сканує пошту на наявність загроз	Так	Так	Так
USB-захист Унеможливлює проникнення вірусних загроз через змінні накопичувачі	Так	Так	Так
Евристичний аналізатор Аналізує код на предмет його збігів із вірусами	Так	Так	Так
Брандмауер (мережевий екран) Налаштовує правила вхідних та вихідних з'єднань для програм, встановлених на ПК		Так	Так
Антифішинг Блокує сайтів, що створені для крадіжки персональних даних користувача		Так	Так
Антиспам Блокує спам-повідомлення на ПК користувача		Так	Так

Продовження таблиця 2.1.

Варіанти розповсюдження антивірусу Zillya!

Характеристики	Zillya! Антивірус	Zillya! Internet Security	Zillya! Total Security
Віртуальна клавіатура Зберігає паролі від крадіжки зловмисниками		Так	Так
Оптимізатор Дозволяє виявляє сміттєві файли системи та звільнити місце на диску		Так	Так
Файл -шредер Забезпечує видалення інформації без можливості відновлення		Так	Так
Батьківський контроль Надає ефективний інструмент контролю батькам за активністю дитини за ПК			Так
Менеджер процесів Дозволяє контролювати та управляти запущеними програмами/процесами.			Так
Менеджер автозапуску Дає можливість переглянути список програм, які завантажуються автоматично із запуском ОС та відключити програми із автозапуску.			Так
Приватність даних Дозволяє очистити дані профілів користувача в браузерах та забезпечити таким чином приватність роботи в мережі.			Так

Таблиця 2.2.

Варіант розповсюдження антивірусу Zillya для мобільного пристрою

Характеристики	Zillya! Internet Security for Android 2.0
Антивірус Забезпечує комплексний захист від кіберзагроз	Так
Оптимізатор Очищає кеш-пам'ять телефону	Так
Прискорення Прискорює роботу системи і подовжує час роботи батареї	Так
Інтернет захист Блокує доступ до небезпечних сайтів	Так
Батьківський контроль Блокує небажані для відвідування сайтів за визначеними категоріям	Так
Антикрадій Забезпечує захист даних на смартфоні в разі крадіжки або втрати пристрою	Так
Веб-фільтр Блокування доступу до фішингових та інших шкідливих сайтів.	Так

У будь-якому випадку, перед вибором антивірусу користувачам слід звернути увагу на те, які функції їм потрібні, який рівень захисту вони потребують, а також наявність технічної підтримки та оновлень. Зіставивши ці критерії з можливостями, які пропонує Zillya!, можна зробити виважений вибір.

2.2 Функціональні можливості ESET

Наступним антивірусом у списку, ESET це словацький антивірус, який, згідно з офіційними даними, має вражаючу базу користувачів у 110 мільйонів людей. Завдяки широкому спектру доступних варіантів розповсюдження, включаючи майже всі популярні платформи, а також кілька версій для окремих

платформ і універсальний варіант, ESET є універсальним антивірусом, який може задовольнити потреби для дому, малого та середнього бізнесу, великого бізнесу та державних установ. Крім того, ESET пропонує спеціалізовані бізнес-пакети, щоб забезпечити безпеку корпоративних систем. Завдяки широкому спектру можливостей і репутації якісного захисту не дивно, що так багато людей довіряють ESET захист своїх пристроїв від загроз.

Для дому ESET Smart Security Premium (Всебічний захист таких пристрої Windows, Mac та Android), ESET Internet Security (Захищає пристрої Windows, Mac та Android), ESET NOD32 Antivirus (Базовий захист тахи пристрої Windows та Mac).

Для малого та середнього бізнесу ESET PROTECT Entry (Централізоване управління,захист робочих станцій, захист файлових серверів, консоль управління, захист мобільних пристроїв), ESET PROTECT Advanced (Централізоване управління, консоль управління, захист робочих станцій, захист файлових серверів, повно дискове шифрування, розширений аналіз у хмарі), ESET PROTECT Complete (Централізоване управління, консоль управління, захист робочих станцій, захист файлових серверів, повно дискове шифрування, розширений аналіз у хмарі, захист поштових серверів, захист хмарних додатків). Всі види антивіруса ESET для бізнесу підтримують такі ОС Windows, macOS, iOS, Android, Linux та інші.

Для великого бізнесу ESET PROTECT Enterprise (Централізоване управління, консоль управління, захист робочих станцій, захист файлових серверів, повно дискове шифрування, розширений аналіз у хмарі, розширений виявлення та реагування), ESET PROTECT MDR (Централізоване управління, консоль управління, захист робочих станцій, захист файлових серверів, повно дискове шифрування, розширений аналіз у хмарі, розширений виявлення та реагування, сервіси з безпеки, преміум-підтримка). Антивіруси ESET для великого бізнесу підтримують широкий діапазон операційних систем, включаючи Windows, macOS, iOS, Android, Linux та інші [12].

Таблиця 2.3.

Варіанти розповсюдження антивірусу Eset для дому з ОС Windows

Характеристики	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
Антивірус та Антишпигун Забезпечує захист від усіх видів цифрових загроз.	Так		
Розширене машинне навчання Функція виявляє складні, раніше невідомі шкідливі програми при мінімальному впливі на продуктивність.	Так		
Сканування у режимі очікування Здійснюючи поглиблене сканування, коли ПК не використовується.	Так		
Управління паролями Зберігає та впорядковує паролі, автоматично заповнювати форми, генерувати складні зашифровані паролі.	Так		
Ігровий режим Автоматичний перехід у фоновий режим відразу після запуску комп'ютерної гри або відкриття програми в повноекранному режимі	Так	Так	Так
Безперебійне оновлення продуктів	Так	Так	Так

Продовження таблиця 2.3.

Варіанти розповсюдження антивірусу Eset для дому з ОС Windows.

Характеристики	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
Захист від експлойтів Захищає від шкідливих програм, прихованих від традиційних методів виявлення.	Так	Так	Так
Сканування на основі хмарних технологій Прискорює швидкість сканування за використанням додавання до «білого» списку безпечних файлів з використанням бази даних ESET Live Grid®.	Так	Так	
Захист від атак на основі скриптів Виявляє атаки шкідливих скриптів із використанням Windows PowerShell, а також шкідливих JavaScripts, які здійснювати через браузери.	Так	Так	Так
Захист від атак методом підбору паролів	Так	Так	
Сканер системного реєстру Виконується пошук посилань на інфіковані файли або шкідливі програми.	Так	Так	Так
Сканування під час завантаження файлів Час зменшується для сканування шляхом перевірки лише певних типів файлів.	Так	Так	Так

Продовження таблиця 2.3.

Варіанти розповсюдження антивірусу Eset для дому з ОС Windows.

Характеристики	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
Технологія Intel® для виявлення загроз (Новинка) Інтеграції апаратної технології Intel функція посилює захист від програм-вимагачів.	Так	Так	Так
Захист від програм-вимагачів Блокує шкідливе ПЗ, яке шифрує конфіденційну інформацію та вимагає викуп.	Так	Так	Так
Система запобігання вторгненням (HIPS) Найновіші можливості відстеження для сканування частин пам'яті.	Так	Так	Так
Сканер WMI Пошук посилань на інфіковані файли або шкідливі програми, вбудовані як дані у WMI.	Так	Так	Так
Розширений сканер пам'яті Покращене виявлення стійкого шкідливого ПЗ.	Так	Так	Так
Сканер UEFI Захищає від загроз, які атакують ПК на найглибшому рівні.	Так	Так	Так

Продовження таблиця 2.3.

Варіанти розповсюдження антивірусу Eset для дому з ОС Windows.

Характеристики	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
ESET LiveGuard Сервіс який знешкоджує нові види загроз, перевіряючи різні типи файлів (документи, сценарії, інсталятори та виконувані файли).	Так		
Антифішинг Запобігає відвідування підроблених сайтів.	Так	Так	Так
Захист онлайн-платежів (Удосконалено) Шифрує зв'язок між клавіатурою та веб браузером для забезпечення безпеки.	Так	Так	
Інспектор мережі (Удосконалено) Перевіряє роутер на наявність вразливостей, серед яких слабкі паролі або застаріле вбудоване ПЗ.	Так	Так	
Захист від ботнетів Запобігає розсилці спаму та здійснення мережевих атак з твого комп'ютера.	Так	Так	
Захист інформації (шифрування) Шифрує файли та знімні носії.	Так	Так	

Продовження таблиця 2.3.

Варіанти розповсюдження антивірусу Eset для дому з ОС Windows.

Характеристики	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
Контроль пристроїв Запобігає несанкціонованому копіюванню особистих даних на зовнішні пристрої.	Так	Так	Так
Батьківський контроль Дозволяє захистити дітей від інтернет-ресурсів з небажаним контентом.	Так	Так	
Захист веб камери Контролює і при необхідності блокує доступ до веб-камери.	Так	Так	
Брандмауер Запобігає несанкціонованому доступу до комп'ютера та використанню персональних даних.	Так	Так	
Захист від мережевих атак Захищає комп'ютер від шкідливого мережевого трафіку,.	Так	Так	
Захист інформації (шифрування) Шифрує файли та знімні носії.	Так	Так	
Антиспам Захищає поштової скриньки від небажаних листів.	Так	Так	

Таблиця 2.4.

Варіанти розповсюдження антивірусу Eset для дому з ОС macOS.

Характеристики	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
Антивірус та Антишпигун Проактивний захист від усіх типів цифрових загроз	Так	Так	Так
Крос-платформний захист Виявляє загрози, спрямовані на операційну систему macOS.	Так	Так	Так
Сканування веб сторінок та пошти Сканує веб-сайти (HTTP) під час перегляду та перевіряє всі електронні листи (POP3 / IMAP).	Так	Так	Так
Контроль пристроїв Запобігає несанкціонованому копіюванню особистих даних на зовнішній пристрій.	Так	Так	Так
Мережеві з’єднання Відображає всі підключення і процеси в мережі, а також швидкість і кількість переданих даних.	Так	Так	Так
Персональний брандмауер	Так		Так
Запобігає несанкціонованому доступу до комп'ютера та використанню персональних даних.	Так		Так

Продовження таблиця 2.4.

Варіанти розповсюдження антивірусу Eset для дому з ОС macOS.

Характеристики	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
Антифішинг Захищає від шкідливих веб-сайтів HTTP, які намагаються отримати конфіденційну інформацію.	Так	Так	
Батьківський контроль Захищає дітей від інтернет-ресурсів з небажаним контентом.	Так	Так	
Управління паролями Допомагає зберігати та впорядковувати паролі, автоматично заповнювати форми та створювати надзвичайно надійні зашифровані паролі.			
Мінімальне споживання системних ресурсів	Так	Так	Так
Додаткові налаштування для користувачів	Так	Так	Так
Швидкі оновлення	Так	Так	Так
Дизайн для macOS	Так	Так	Так

Таблиця 2.5.

Варіанти розповсюдження антивірусу Eset для дому з Android.

Характеристики	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
Перевірка безпеки	Так	Так	
Сканування в режимі реального часу	Так	Так	
Сканування за розкладом	Так	Так	
Сканування на вимогу	Так	Так	
Звіт про безпеку	Так	Так	
Автоматичні оновлення	Так	Так	
Проактивний Антикрадій	Так	Так	
Визначення місцезнаходження	Так	Так	
Захист SIM-карти Дозволяє контролювати телефон, навіть якщо він загублений	Так	Так	
Сповіщення про низький заряд	Так	Так	
Оптимізація проти крадіжок Автоматичні сповіщення при спробі обмеження роботи Антикрадіжки.	Так	Так	
Проактивний Антикрадій Після виявлення кількох неправильних введень пароля на екрані блокування або несанкціонованої зміни SIM-карти пристрій блокується, а зображення автоматично надсилаються на my.eset.com.	Так	Так	

Продовження таблиця 2.5.

Варіанти розповсюдження антивірусу Eset для дому з Android.

Характеристики	ESET Smart Security Premium	ESET Internet Security	ESET NOD32 Antivirus
Відправлення повідомлень на екран пристрою Надає можливість зв'язатися з людиною, яка знайшла смартфон.	Так	Так	
Фото з вбудованої камери	Так	Так	
Антифішинг	Так	Так	
Аудит додатків	Так	Так	
Фільтрація викликів	Так	Так	
Сканер USB-пристроїв	Так	Так	
Захист онлайн-платежів	Так	Так	
Захист доступу до додатків	Так	Так	
Інспектор мережі	Так	Так	

Можемо зробити висновок, що від словацької компанії ESET Smart Security Premium для дому це найнадійніший антивірусний захист, що має широкий спектр функцій та можливостей, які дозволяють захистити комп'ютер. Загалом, ESET є потужним антивірусом, який може задовольнити потреби як домашніх, так і бізнес-користувачів, що шукають надійний та ефективний захист від різних видів кіберзагроз.

2.3 Функціональні можливості TotalAV

Наступним антивірусом у списку, TotalAV ця компанія з кібербезпеки, яка пропонує ряд продуктів і послуг для захисту окремих осіб і компаній від онлайн-загроз. Компанія була заснована в 2016 році і базується у Великобританії [13].

Таблиця 2.6

Варіанти розповсюдження антивірусу TotalAV.

Характеристики	Antivirus Pro (Захист від онлайн-загроз)	Internet Security (Онлайн захист, безпека та конфіденційність VPN)	Total Security (100% повний захист і безпека онлайн)
Антивірусний захист у реальному часі	Так	Так	Так
Усунення вірусів, троянів і шкідливих програм	Так	Так	Так
Хмарне сканування нульового дня	Так	Так	Так
Захист PUA	Так	Так	Так
Захист від фішингу	Так	Так	Так
Захист від програм-вимагачів	Так	Так	Так
Інструменти налаштування системи	Так	Так	Так
Очищувач диска	Так	Так	Так
Менеджер і очищувач браузера	Так	Так	Так
Захист Windows, Mac, Android та iOS.	Так	Так	Так
Безпечний перегляд VPN		Так	Так
Повний блок реклами			Так
Сховище паролів			Так

У антивіруса TotalAV є кілька переваг використання у рішені кібербезпеки:

1. Зручність: програмне забезпечення TotalAV розроблено таким чином, щоб бути зручним і простим у використанні навіть для тих, хто має обмежені технічні знання.

2. Служба VPN: TotalAV пропонує службу VPN, яка забезпечує зашифроване та безпечне підключення до Інтернету.

3. Підтримка клієнтів: TotalAV пропонує відмінну підтримку клієнтів, доступну цілодобову підтримку по телефону, електронною поштою та в чаті.

4. Безкоштовна пробна версія: TotalAV пропонує безкоштовну пробну версію свого антивірусного програмного забезпечення, що дозволяє користувачам спробувати програмне забезпечення, перш ніж прийняти рішення про придбання підписки.

Загалом TotalAV це комплексне та зручне рішення для кібербезпеки, який пропонує ефективний захист. Хоча TotalAV має багато переваг, є також деякі потенційні недоліки, які слід враховувати:

1. Обмежене незалежне тестування: TotalAV не пройшов широких випробувань незалежними антивірусними лабораторіями, що може ускладнити оцінку ефективності його антивірусного механізму.

2. Обмежені функції безкоштовної версії. Безкоштовна версія TotalAV досить обмежена щодо можливостей, і користувачам потрібно буде оновити платну підписку, щоб отримати доступ до багатьох розширених функцій.

3. Потенційно агресивний маркетинг: деякі користувачі повідомили, що відчувають тиск, щоб перейти на платну підписку, з деякими спливаючими сповіщеннями та маркетинговими повідомленнями, які можуть сприйматися як нав’язливі.

4. Обмежена інформація про компанію: TotalAV є відносно новою компанією, і доступна обмежена інформація про її історію, власність і команду управління.

Підсумовуючи, TotalAV це відносно нове антивірусне програмне забезпечення, яке пропонує низку функцій для засобів захисту пристрою від онлайн-загроз. Але досить багато недоліків, а саме основий це потенційно агресивний маркетинг.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОТИДІЇ ВТОРГНЕННЯ В ІНФОРМАЦІЙНУ СИСТЕМУ НА БАЗІ РІШЕННЯ ESET SMART SECURITY PREMIUM

3.1 Завантаження та інсталяція

Все починається з офіціального сайту ESET.COM перейшовши до вкладки для дому, комп'ютери та ноутбуки, шукаємо ESET Smart Security Premium та тиснемо на продукт, потім потрапляємо на сторінку продукта та натискаємо на кнопку завантажити, після почнеться завантаження де потрібно обрати потрібну версію Windows та тип інсталятора. (Рис.3.1)

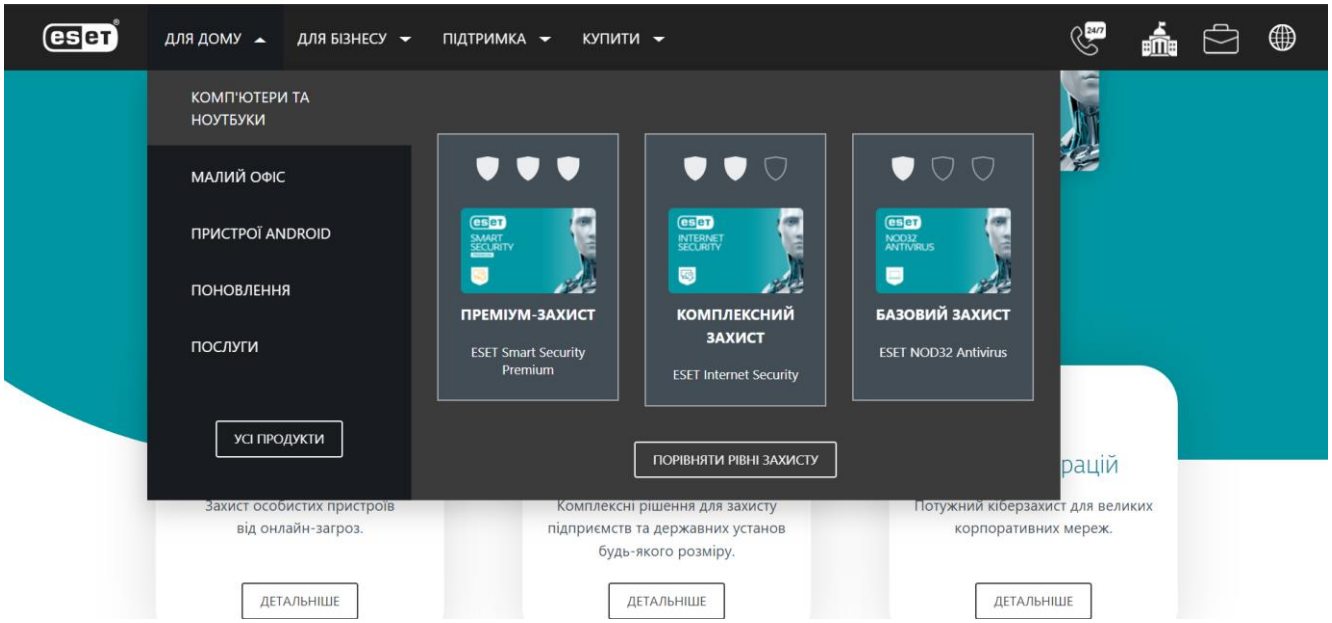

Рис. 3.1. Обираємо ESET Smart Security Premium

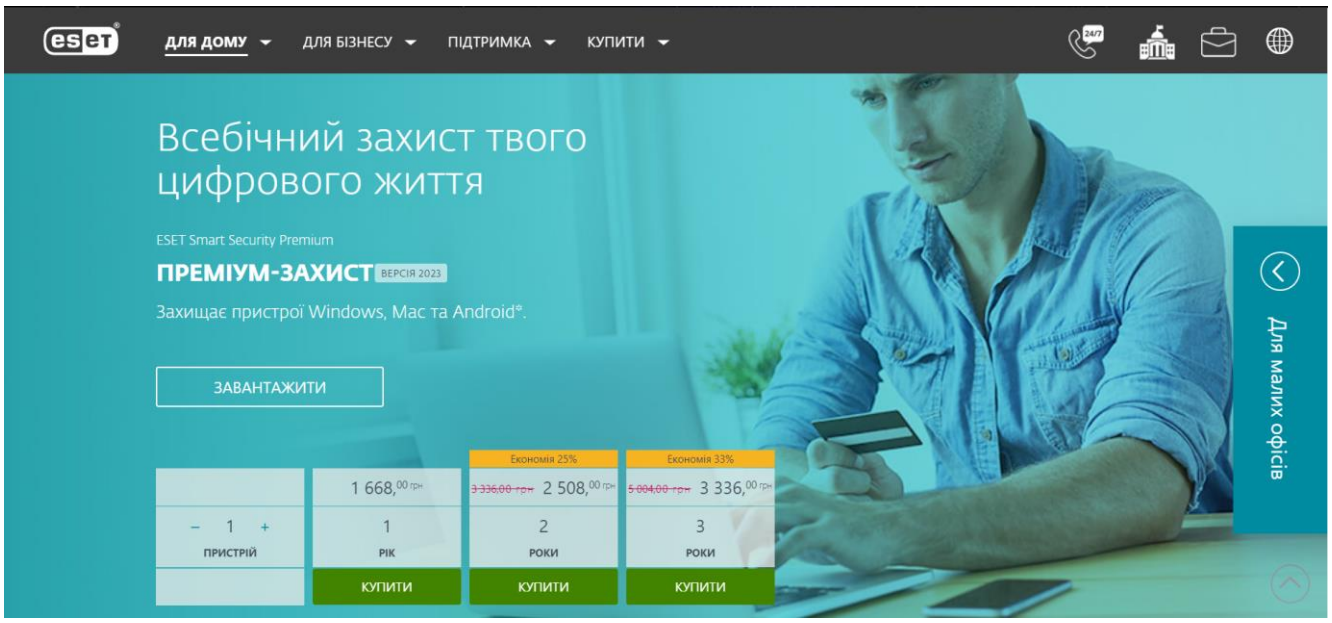

Рис. 3.2. Натискаємо кнопку «Завантажити»

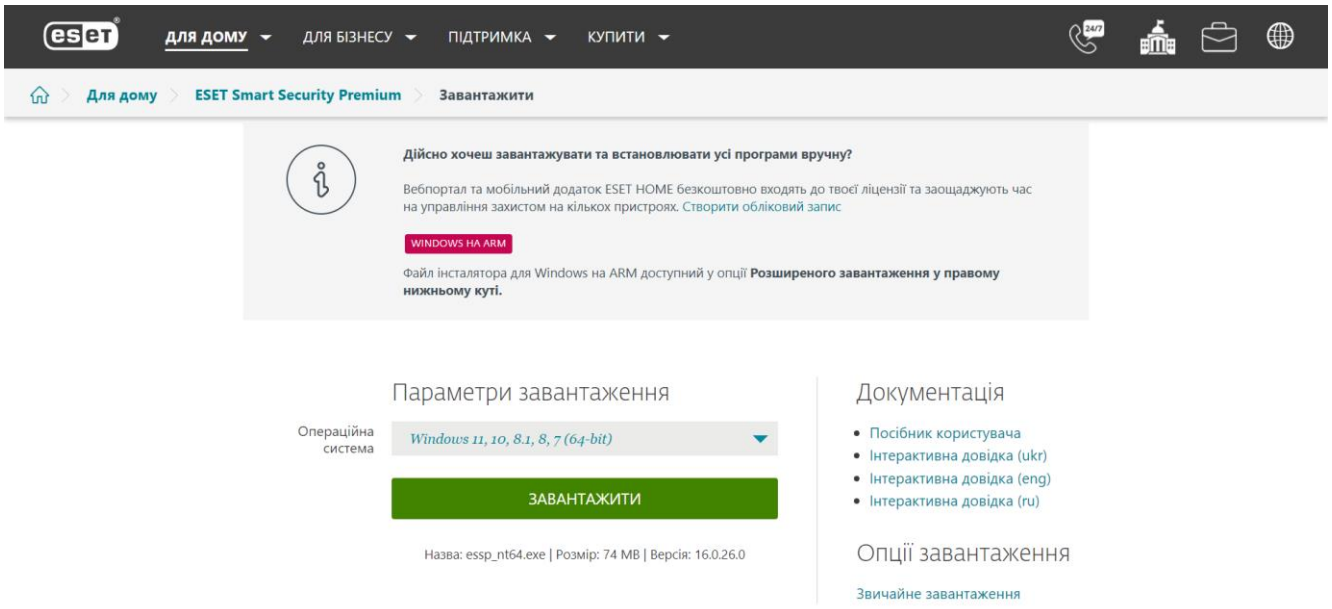

Рис. 3.3. Обираємо версію для Windows (64 bit або 32 bit) потім натискаємо кнопку «Завантажити»

Після завантаження нас зустрічає вікно інсталяції антивірусу. Де обираємо мову програми на якій вона буде працювати після встановлення. (Рис 3.4)

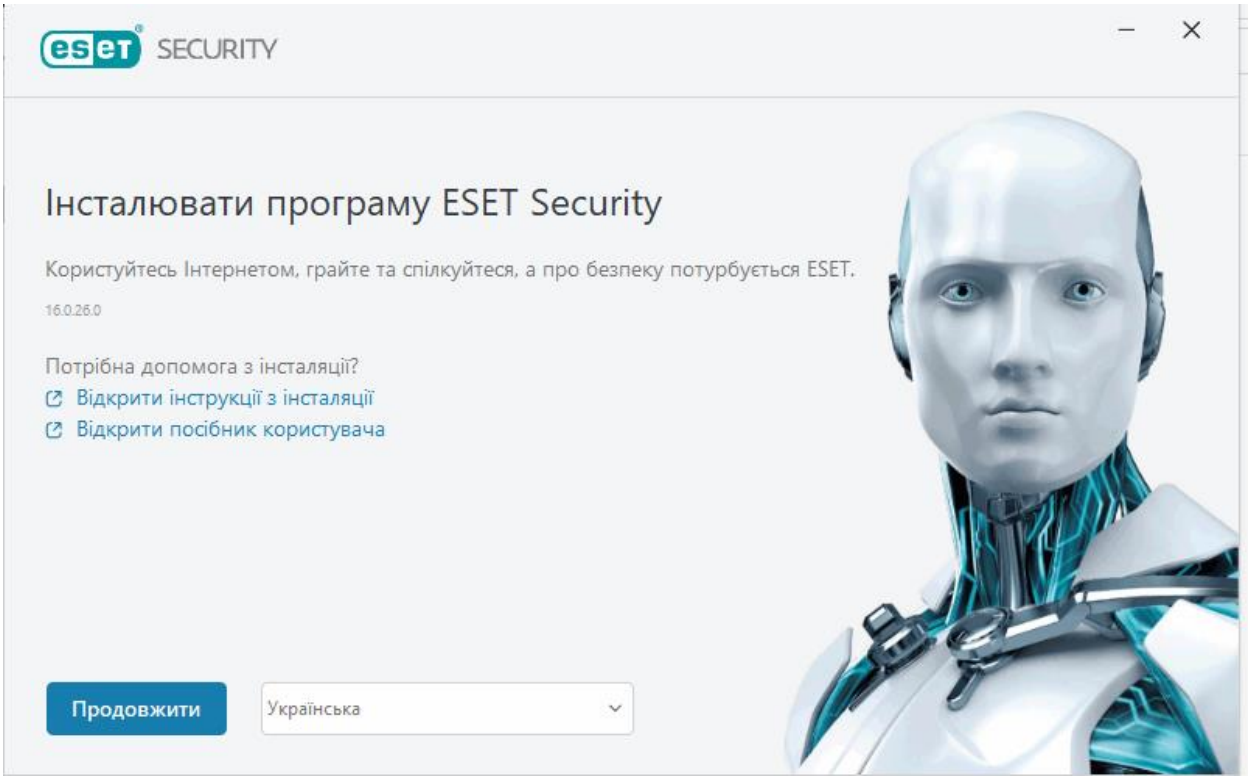

Рис 3.4. Екран інсталяції антивірусу

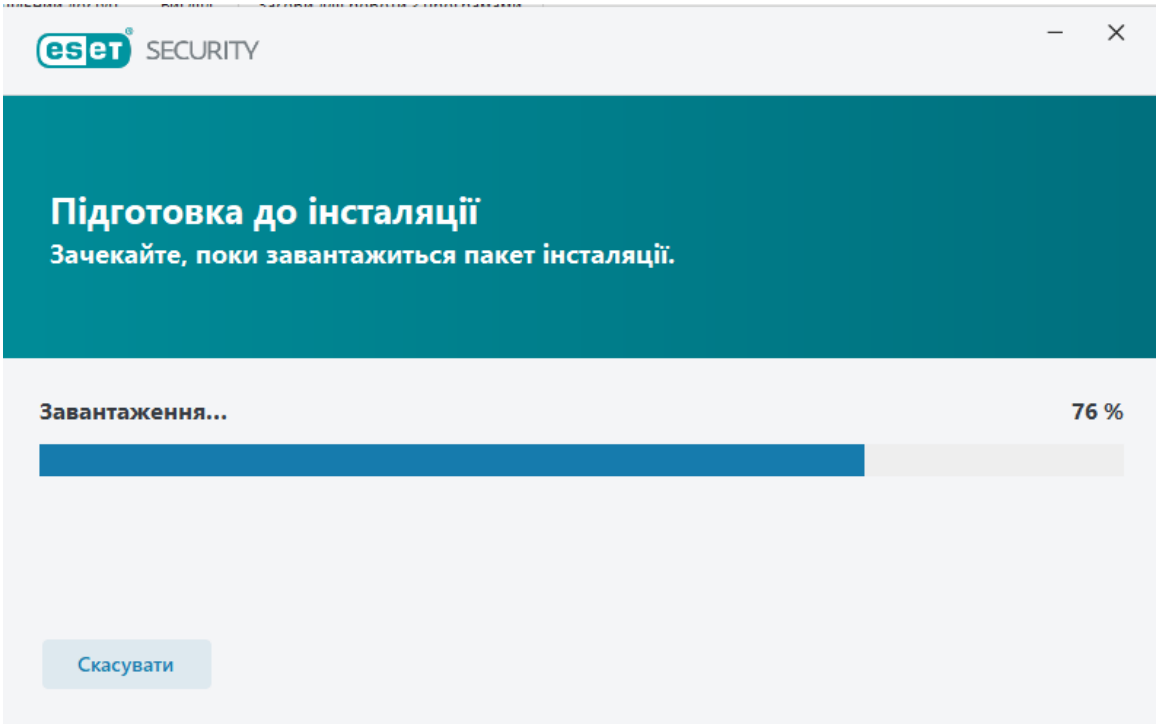

Рис 3.5. Підготовка до інсталяції

Обираємо увімкнути чи ні виявлення потенційно небажаних програм, участь у програмі підвищення якості програмного забезпечення та LiveGrid котра дозволяє антивірусу постійно отримувати інформацію про нові зараження, її можна відключити функціонал програми не зміниться, але ця система дозволяє компанії відправляти дані для докладного аналізу що пришвидшує оновлення бази даних та покращує засоби їх виявлення. (Рис 3.6)

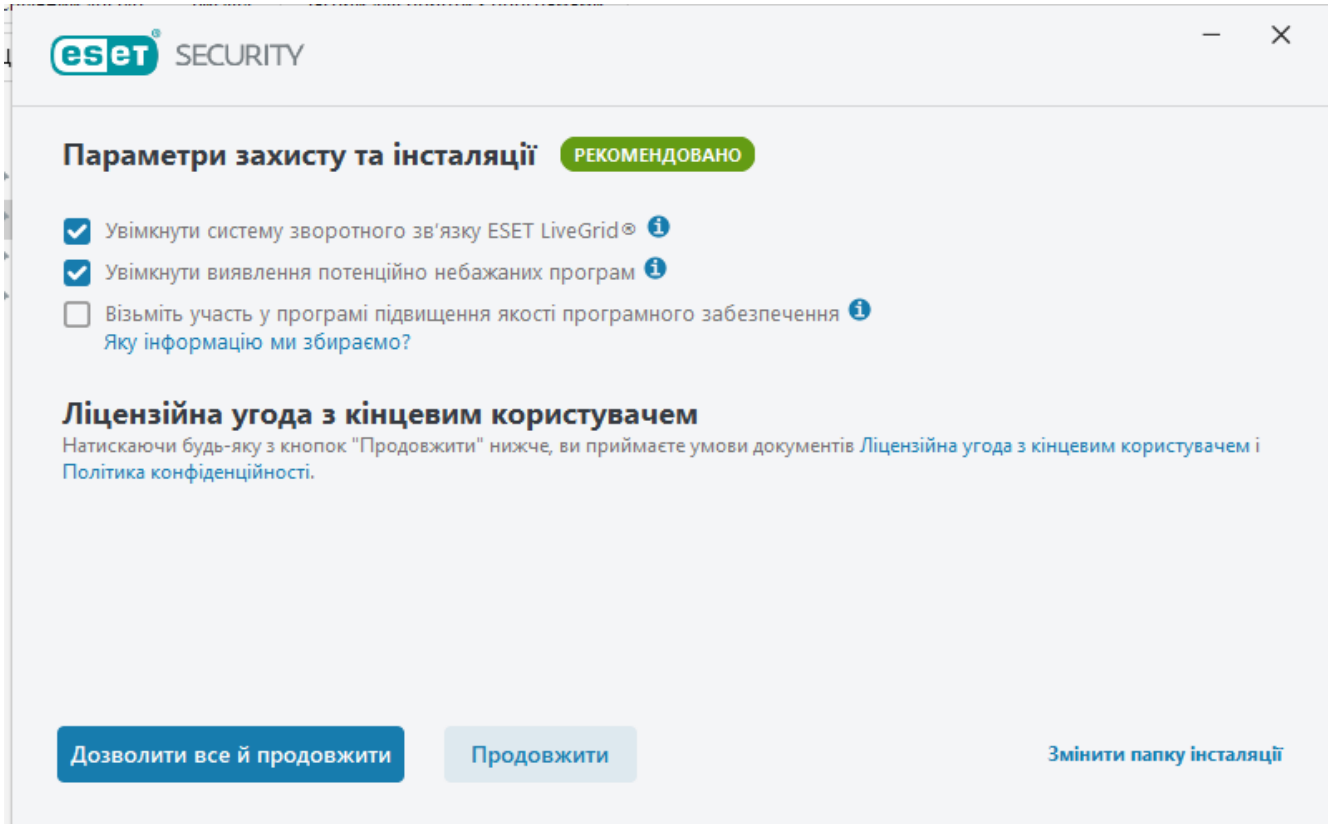

Рис 3.6. Екран вибору увімкнення LiveGrid та систему виявлення потенційно небажаних програм

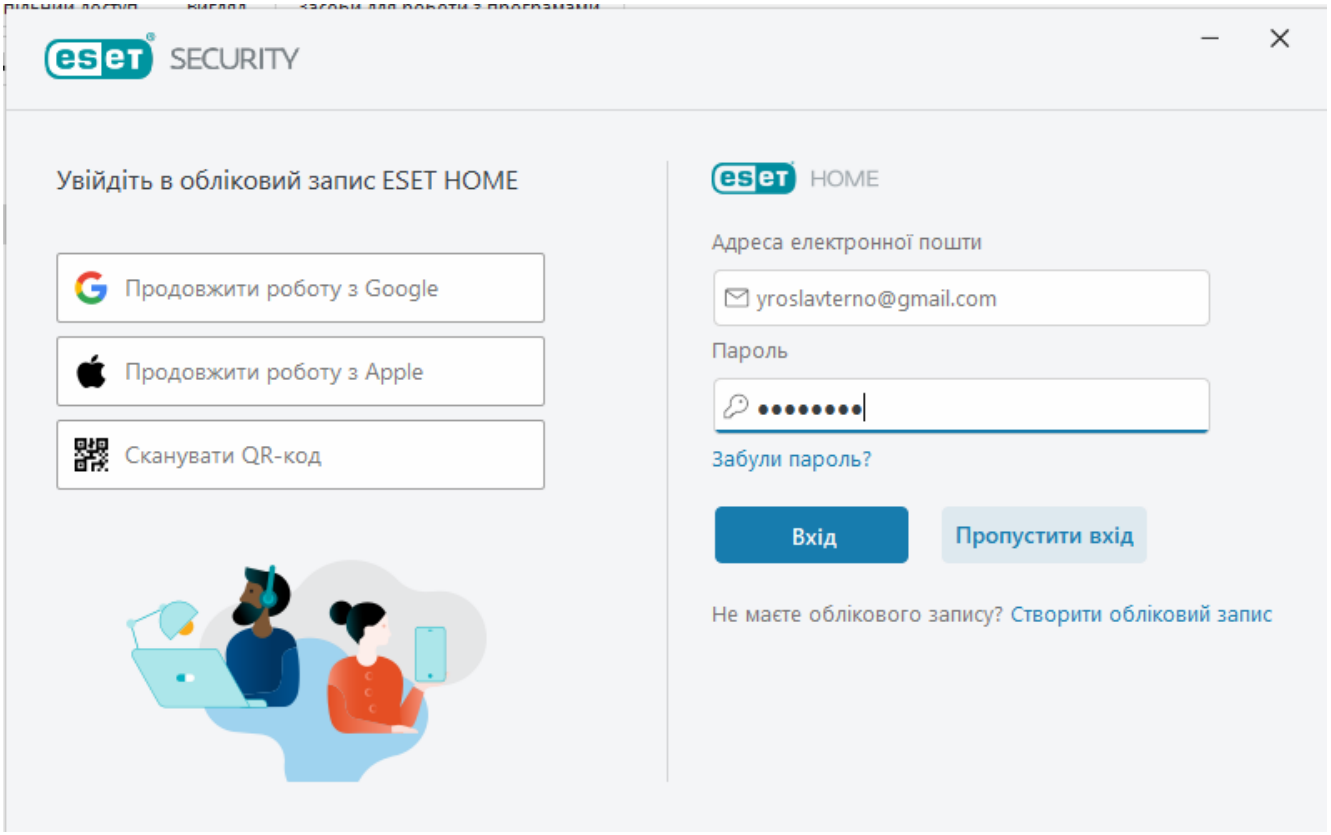

Рис 3.7. Вхід в обліковий запис ESET HOME

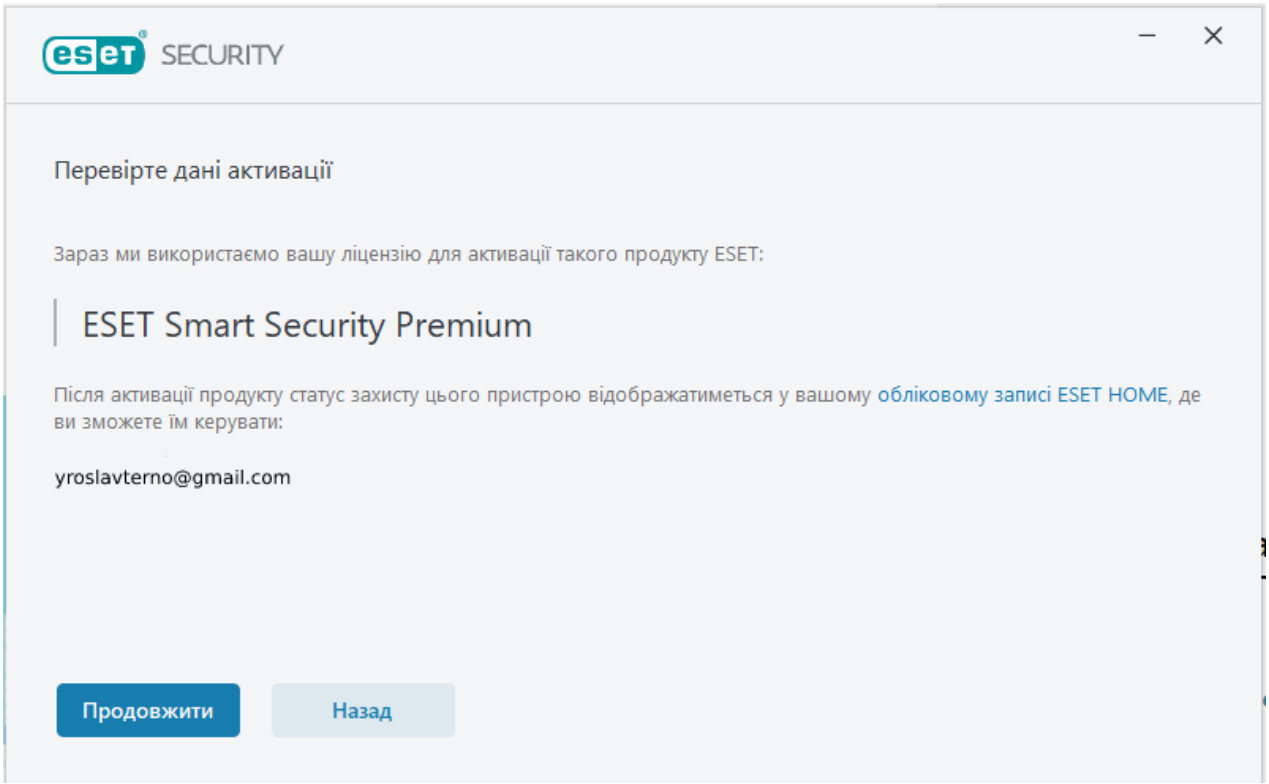

Рис 3.8. Перевірка даних активації

Одразу ж пропонують активувати ліцензію, якщо ми маємо ліцензійний ключ, або якщо компанія в котрій ви працюєте може надати вам ліцензію. Та можливість використати файл ліцензії при відсутності інтернету. В нашому випадку ми просто обираємо «Спробувати БЕЗКОШТОВНО». (Рис 2.9)

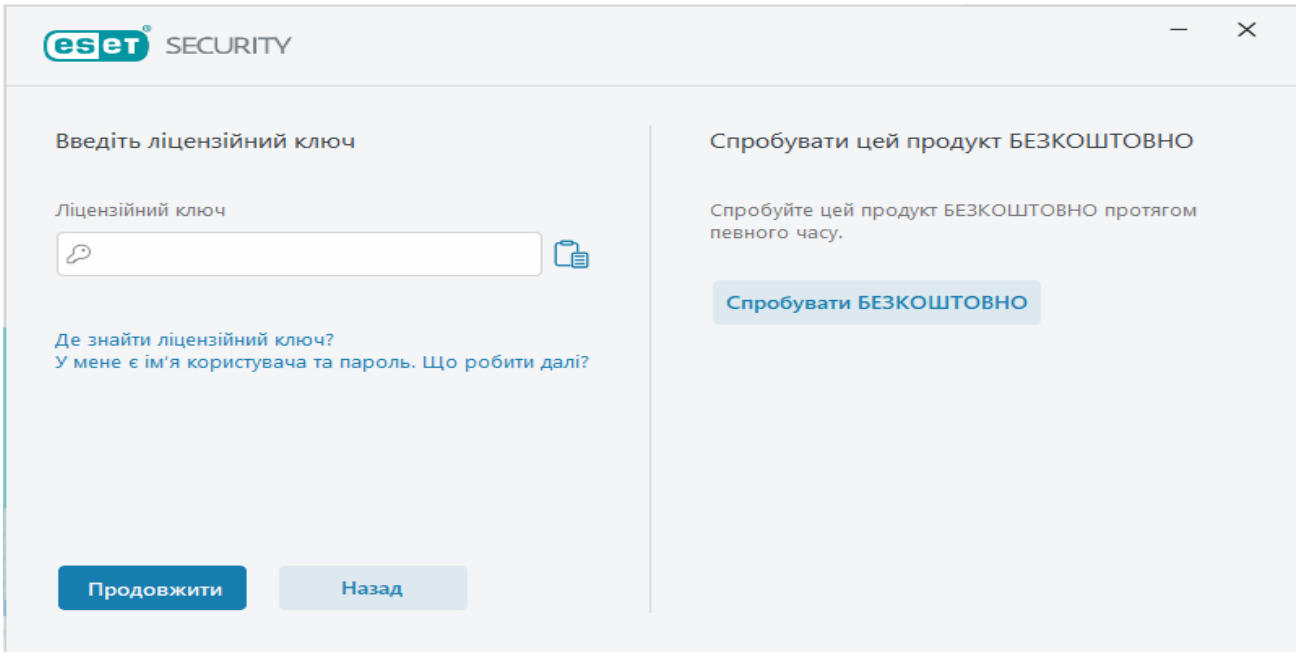

Рис 3.9. Вводимо ліцензійний ключ або обираємо спробувати «Спробувати БЕЗКОШТОВНО»

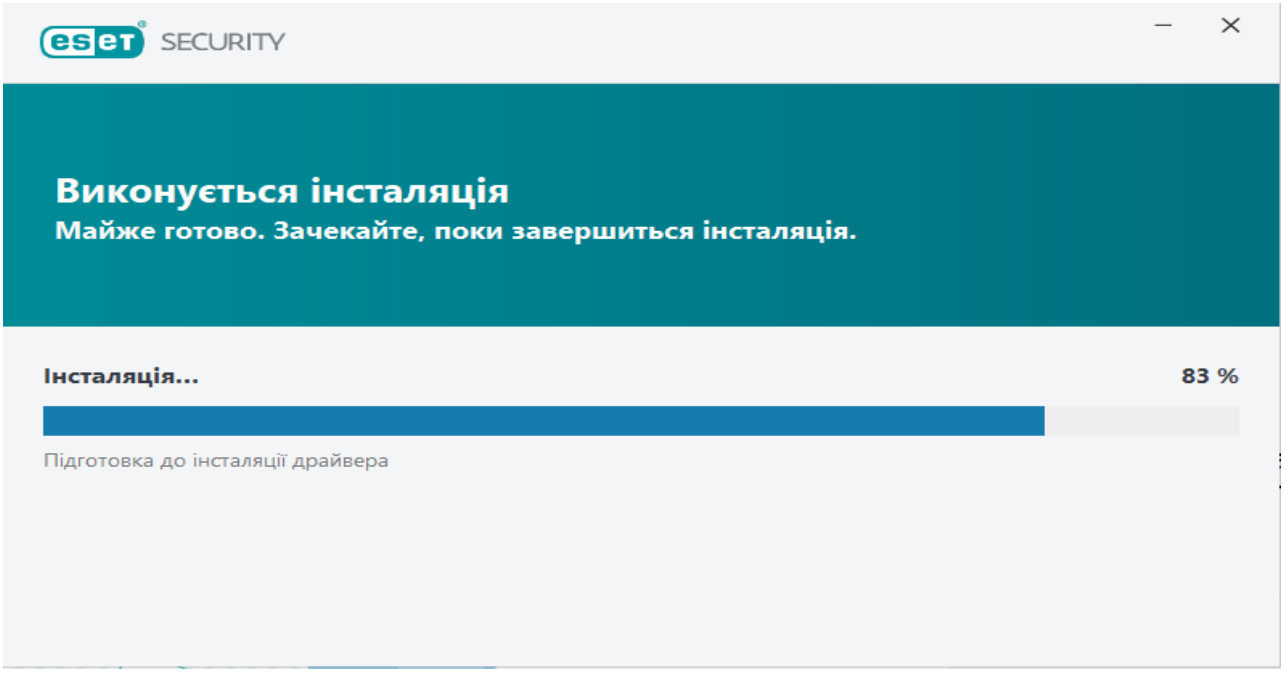

Рис 3.10. Процес інсталяції

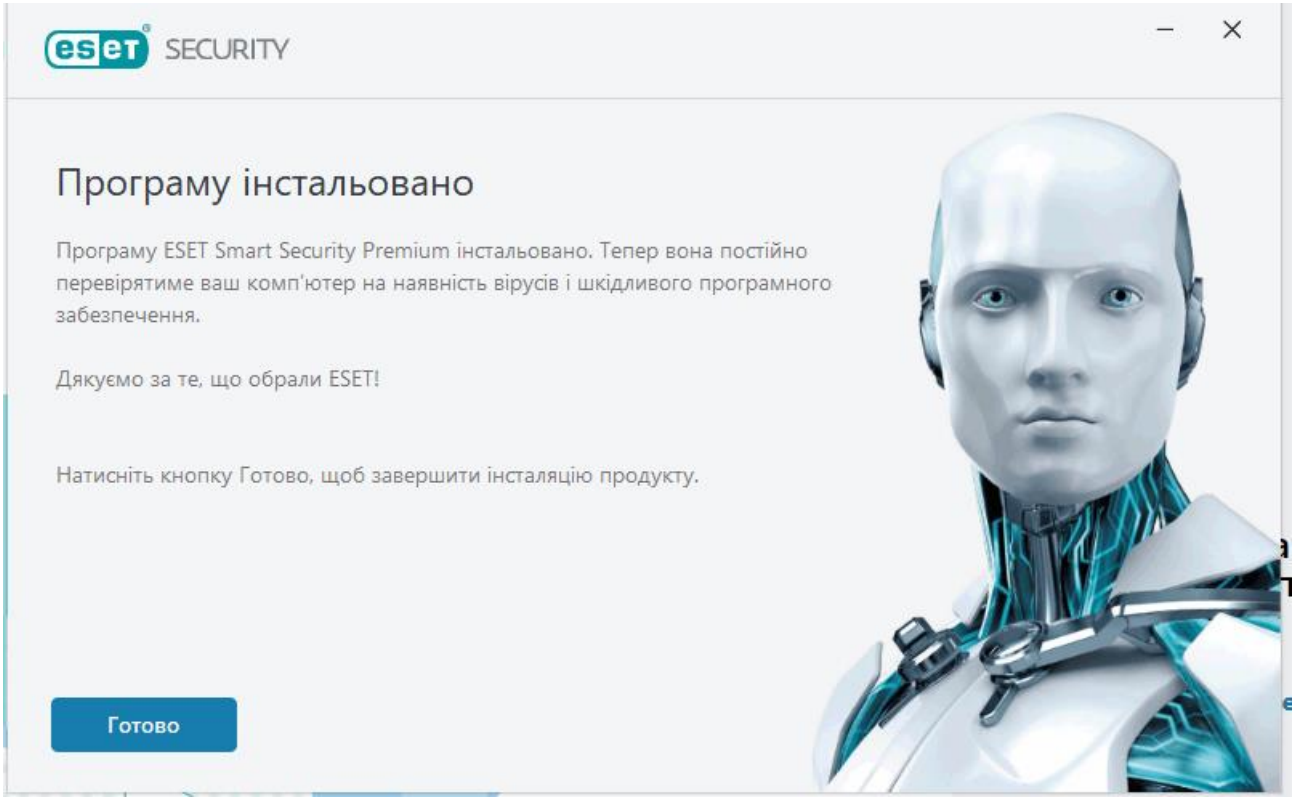

Рис. 3.11. Інформація про успішне інсталювання програми

Розроблено рекомендації щодо пошаговому пошуку ESET Smart Security Premium на сайті завантаження та інсталяції на наш комп'ютер. Антивірус успішно інстальовано.

Під час дослідження функціональних можливостей ESET Smart Security Premium було виявлено, що цей антивірус має багато корисних функцій для захисту комп'ютера від шкідливих програм.

Загалом, ESET Smart Security Premium може бути хорошим вибором для тих, хто шукає надійний та легкий у використанні антивірусний продукт з різноманітними функціональними можливостями. Високий рівень захисту від шкідливих програм, включаючи віруси, шпигунський та рекламний софт, руткіти та інші загрози. Використання продукту не впливає на продуктивність комп'ютера, як вбільшості антивірусів які займають 30% оперативної пам'яті для роботи. Підтримка різних операційних систем, включаючи Windows, Mac та Android.

3.2 Налаштування та використання

Рис 3.12 – Екран завантаження антивірусу

Одразу ж пропонують налаштувати додаткові інструменти безпеки ESET. (Рис 3.13)

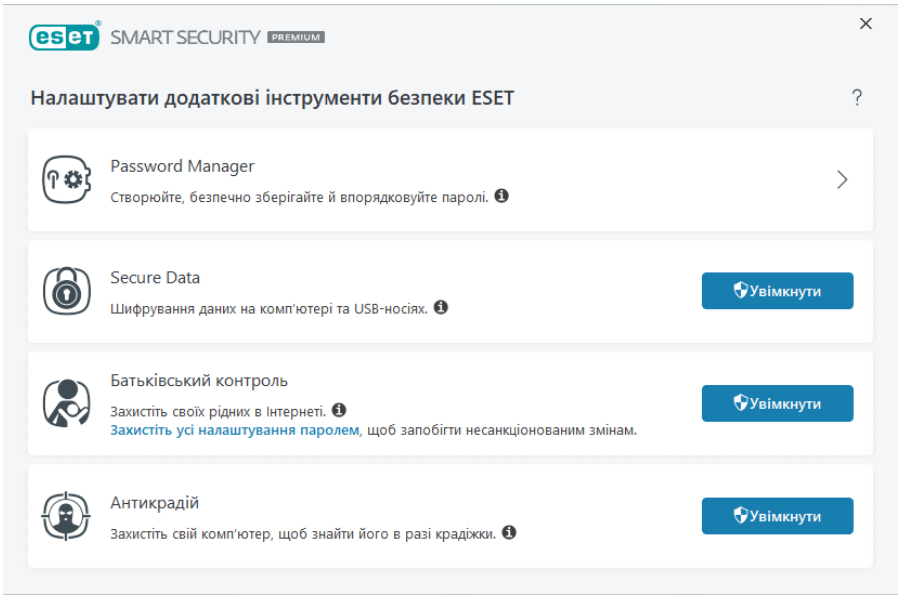

Рис 3.13. Екран з пропозицією з налаштуванням додаткових інструментів безпеки ESET

У вікні Огляд відображається інформація про поточний захист комп’ютера, а також швидкі посилання на функції захисту в ESET Smart Security Premium. (Рис 3.14)

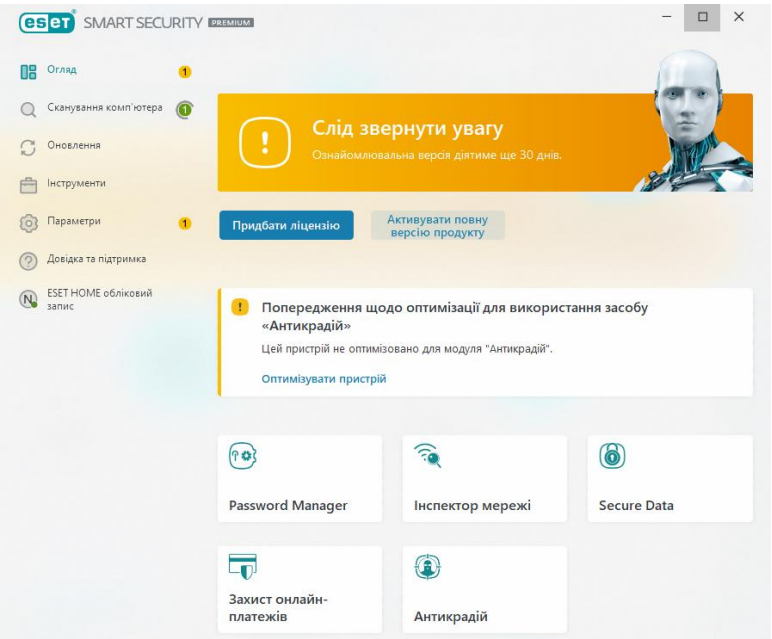

Рис 3.14. Основний екран

Наступне вікно це сканування комп’ютера, де одразу почалося перше сканування, але перед цим проходить оновлення ядра. Сканування змінних носіїв дозволяє сканувати різні змінні носії. А також сканування файлу через просте перетягування в спеціальне вікно. Справа вгорі є кнопка з знаком питання котра відправить нас на сайт з допомогою де можливо знайти відповіді на питання про різні пункти меню. (Рис 3.15)

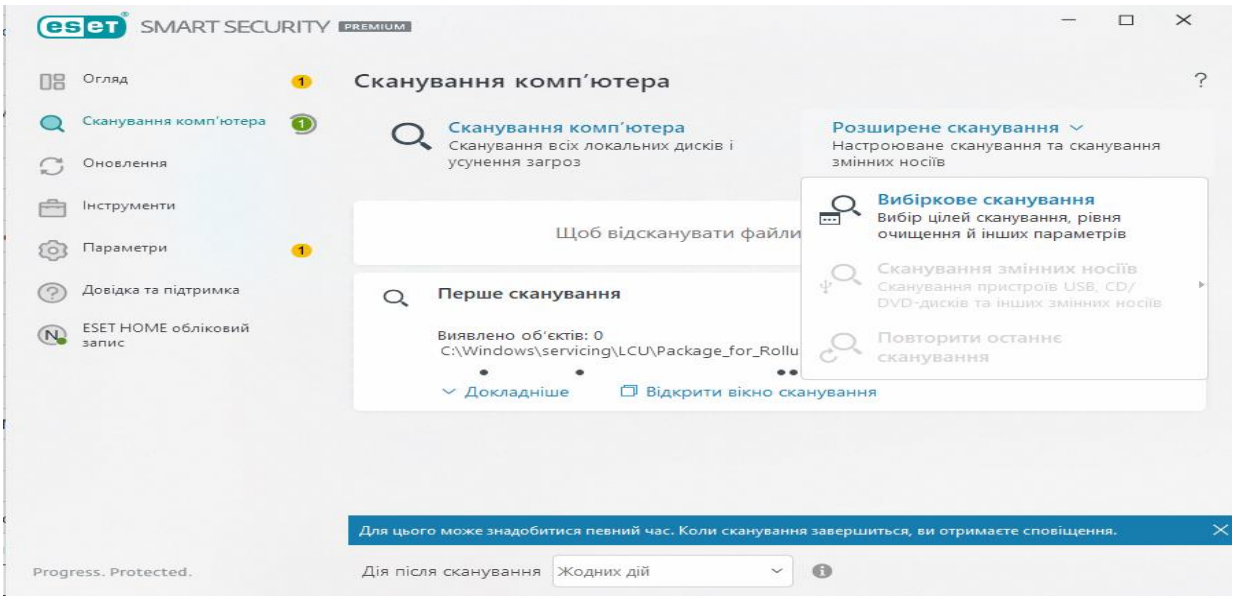

Рис 3.15. Екран сканування комп’ютера

Наступним буде вкладка оновлення де ми можемо перевірити версію програми, останнє оновлення та дата останньої перевірки. Також за допомогою пунктів перевірити наявність оновлень можемо примусово перевірити оновлення, переглянути всі модулі які оновилися та змінити частоту оновлень або додати нове завдання. (Рис 3.16)

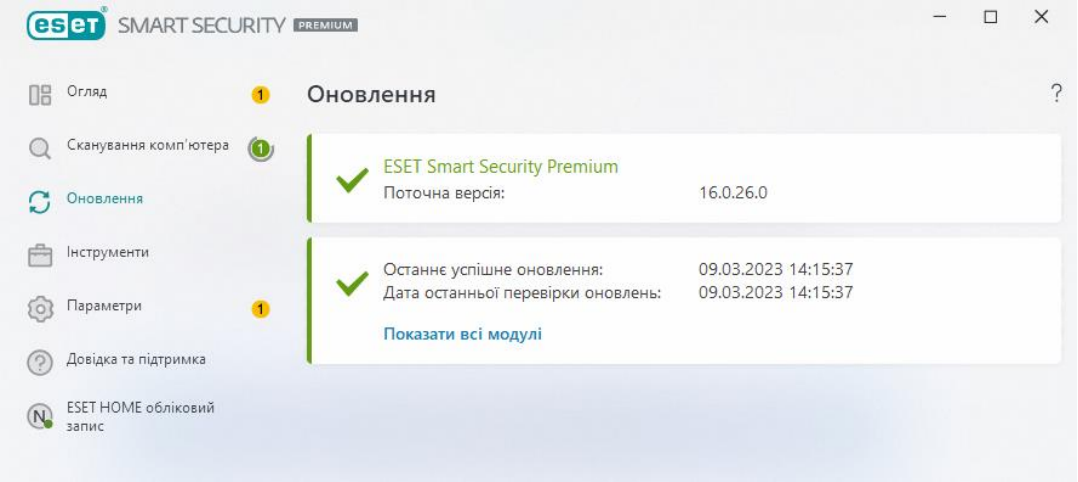

Рис 3.16. Екран оновлення

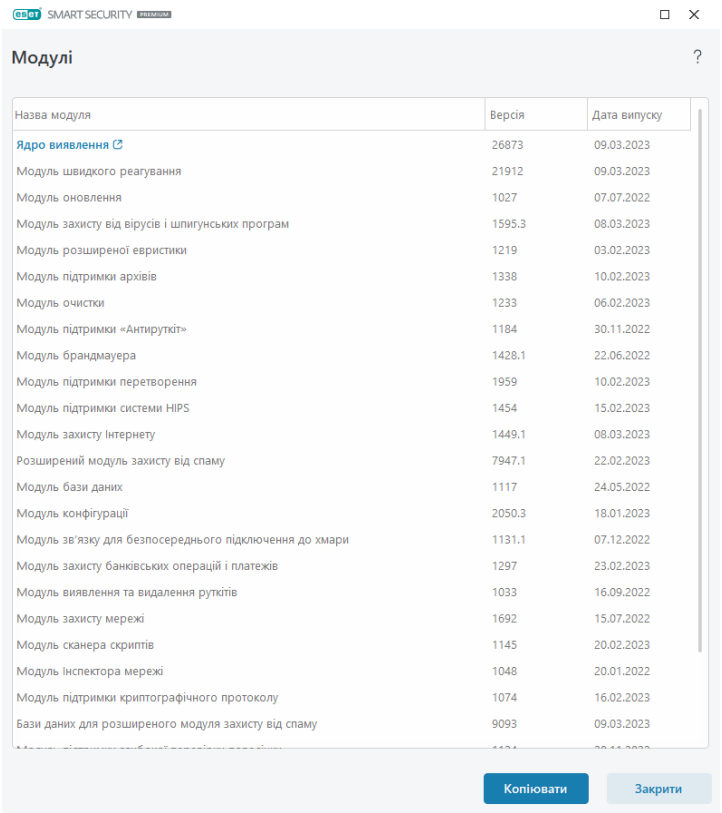

Рис 3.17. Екран з оновленими модулями

Наступним пунктом є інструменти надає доступ до Password Manager, Secure Data, Інспектор мережі, Захист онлайн-платежів, Антикрадій тощо , які спрощують адміністрування програми й відкривають додаткові можливості для досвідчених користувачів. (Рис 3.18)

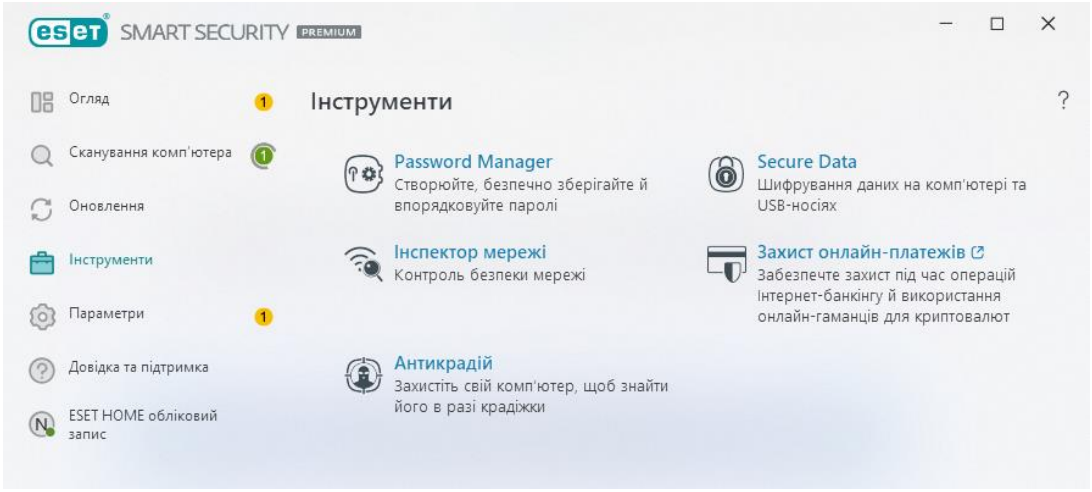

Рис 3.18. Екран інструментів

Наступним буде вікно з параметрами. Де є 4 варіанти параметрів а також можливість імпортувати або експортувати параметри. А також додаткові параметри. (Рис 3.19)

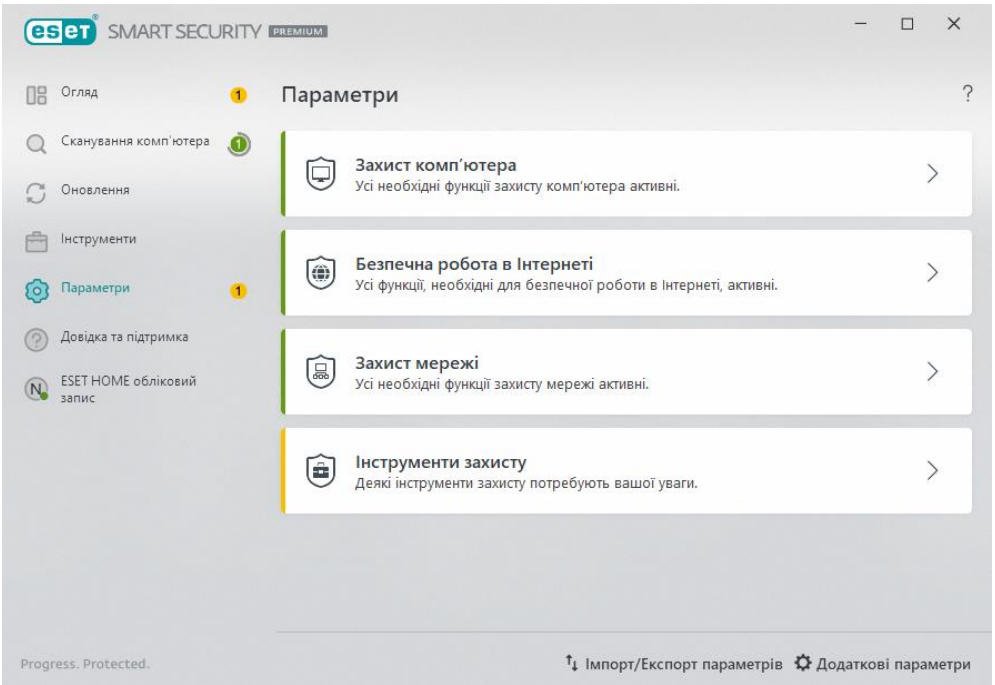

Рис 3.19. Екран з параметрами

В вкладці комп’ютер ми можемо налаштувати основні параметри для захисту ПК. Захист файлової системи допомагає виявляти шкідливе ПЗ на комп’ютері та контроль пристроїв допомагає знешкодити віруси на різних флешках, дисках та інших пристроїв. Звідси ми можемо одразу перейти до додаткових параметрів цих параметрів натиснувши на шестерню. (Рис 3.20)

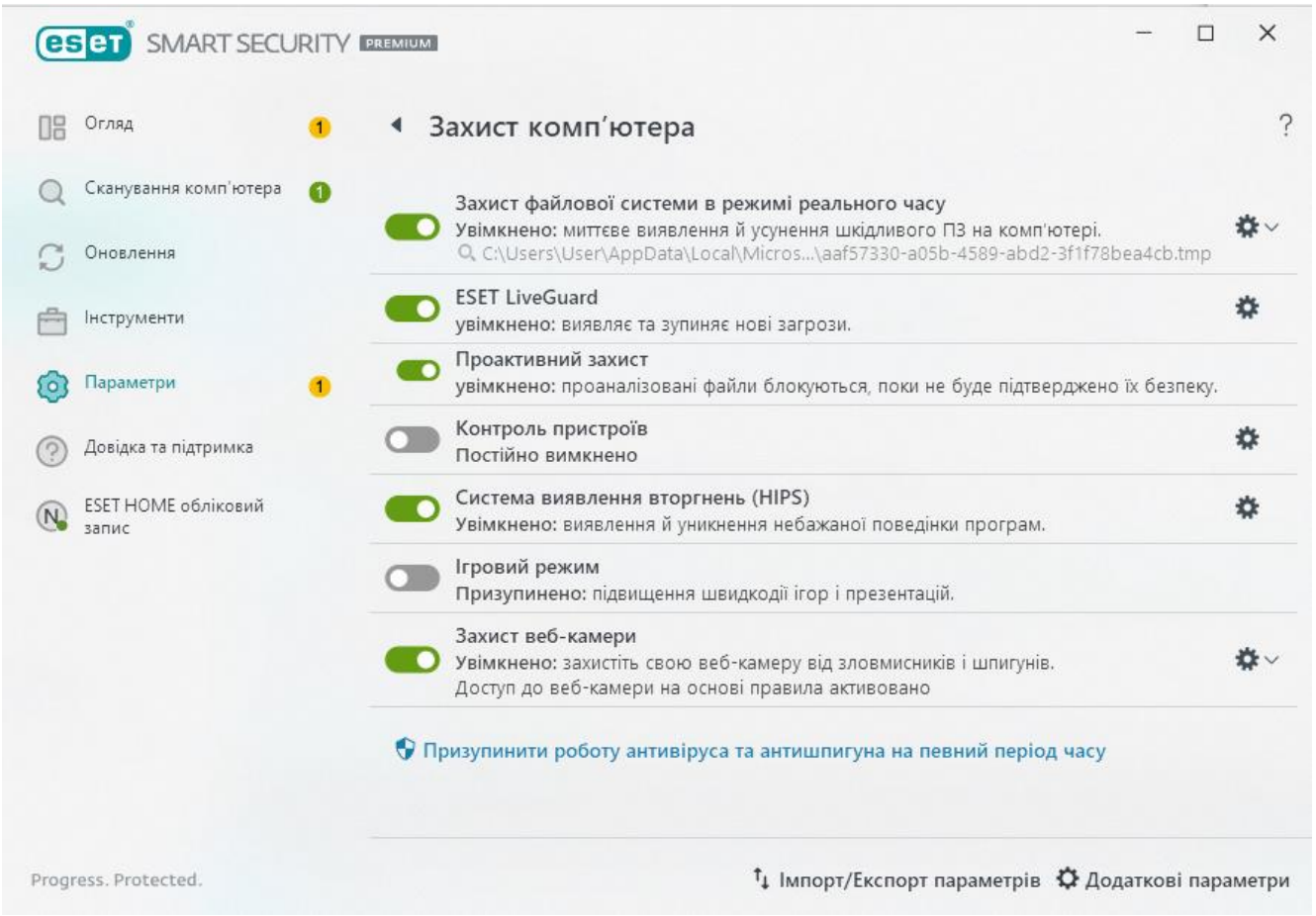

Рис 3.20. Екран вкладки параметрів захист комп’ютера

В вкладці безпечна робота в інтернеті ми можемо налаштувати батьківський контроль, захист доступу до інтернету, захист від фішинг-атак, захист від фішинг-атак та антиспам. (Рис 3.21)

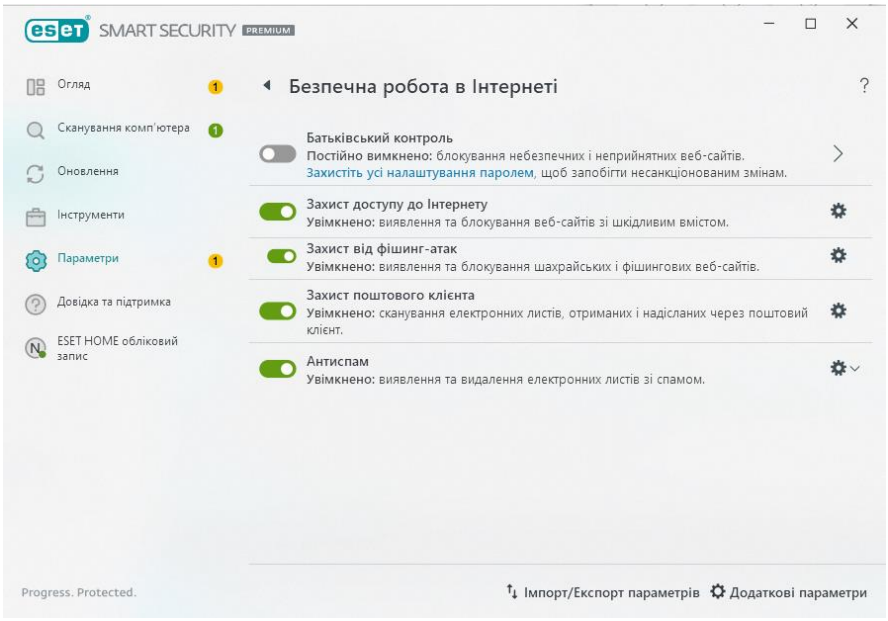

Рис 3.21. Екран вкладки параметрів безпечна робота в інтернеті

Наступним є налаштування захисту мережі. Брандмауер що буде фільтрувати мережевий трафік. захист мережі від атак дозволяє захиститися від мережевих атак, захист від ботнетів. (Рис 3.22)

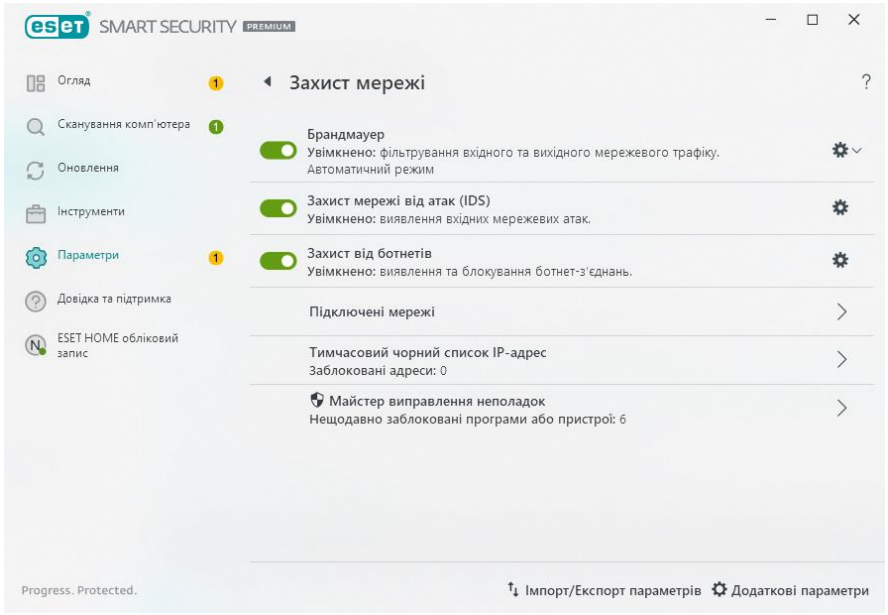

Рис 3.22. Екран вкладки параметрів захист мережі

Наступним є інструменти захисту можна налаштувати модулі Password Manager, Secure Data, Інспектор мережі, Захист онлайн-платежів та Антикрадій. (Рис 3.23)

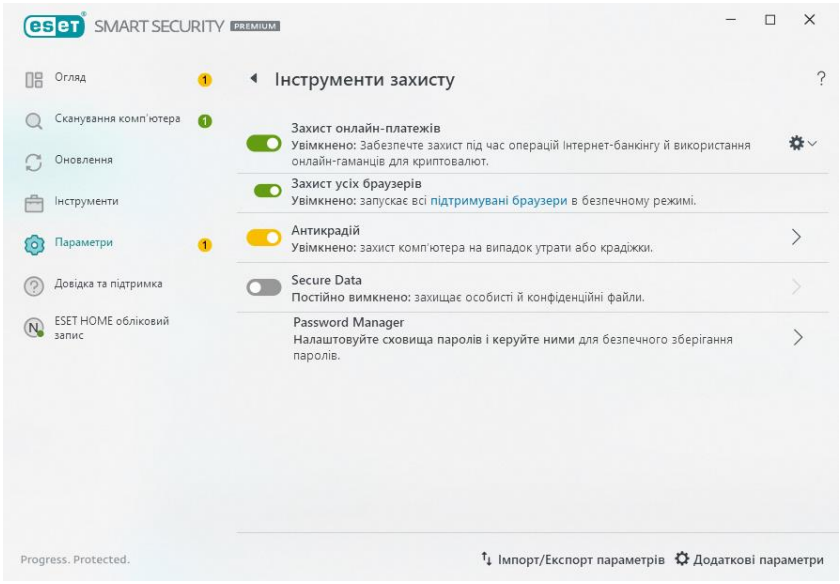

Рис 3.23. Екран вкладки параметрів інструменти захисту

Додаткові параметри дозволяють детальніше настроїти всі параметри антивірусу. Має дуже велику кількість пунктів для гнучкого налаштування параметрів антивірусу. (Рис 3.24)

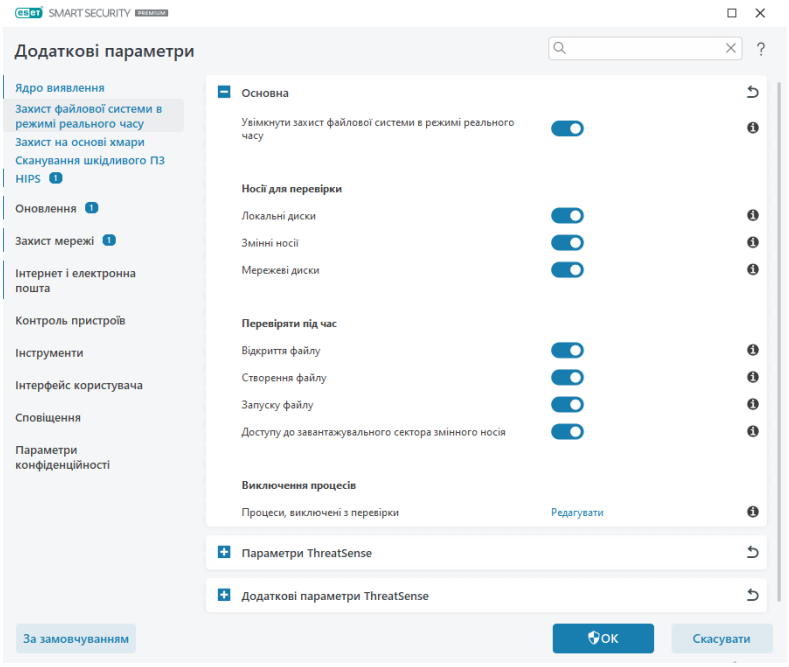

Рис 3.24. Екран додаткових параметрів

В пункті підключені мережі ми можемо подивитися параметри мережі котрій підключені, змінити тип захисту, отримання попереджень через слабке шифрування та інші параметри нашою мережі. (Рис 3.25)

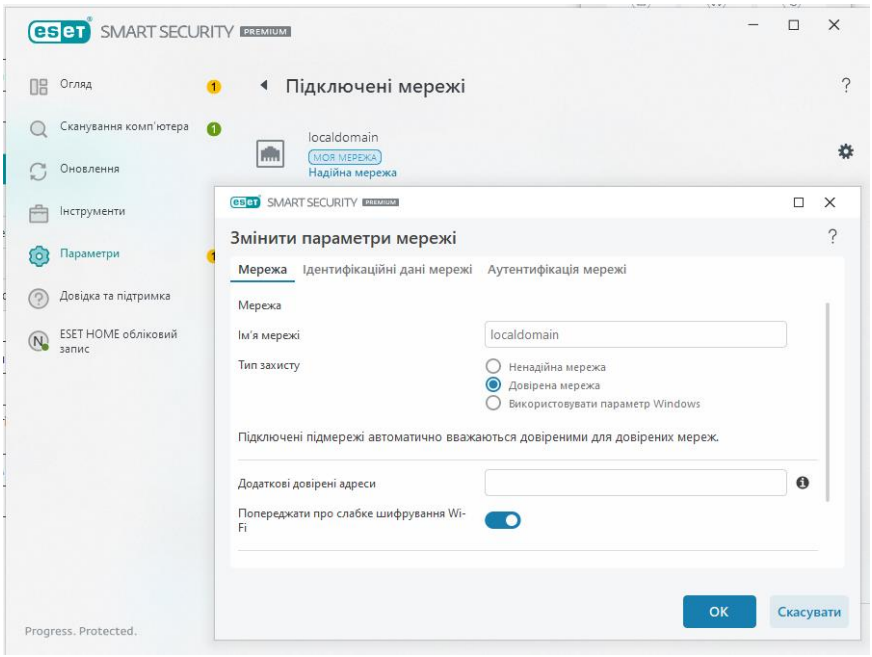

Рис 3.25. Екран підключень до мережі

Тимчасовий чорний список IP-адрес дозволяє додати до чорного списку IP-адрес котрий ми хочемо заблокувати. (Рис 3.26)

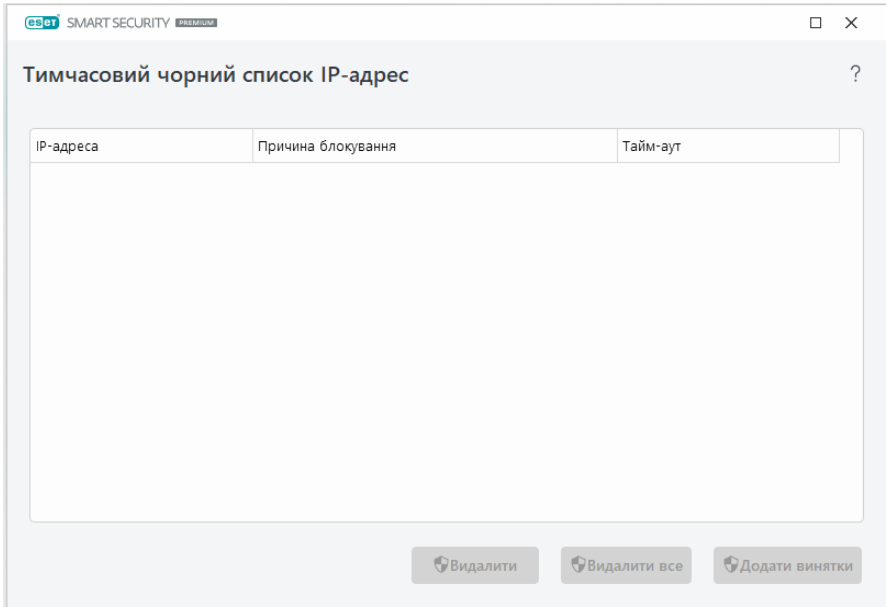

Рис 3.26. Чорний список IP-адрес

Майстер виправлення неполадок допомагає вирішувати різні проблеми з захистом мережі. (Рис 3.27)

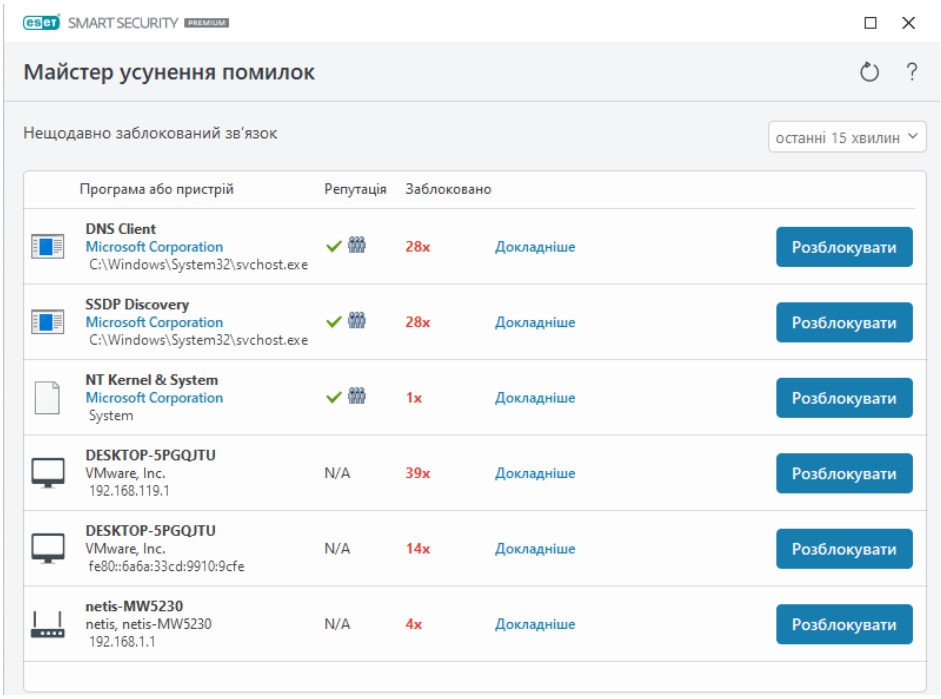

Рис 3.27. Екран виправлення неполадок

Довідка та підтримка відображає інформацію про ліцензію, інстальований продукт ESET, а також посилання на онлайн-довідку, базу знань ESET і технічну підтримку. (Рис 3.28)

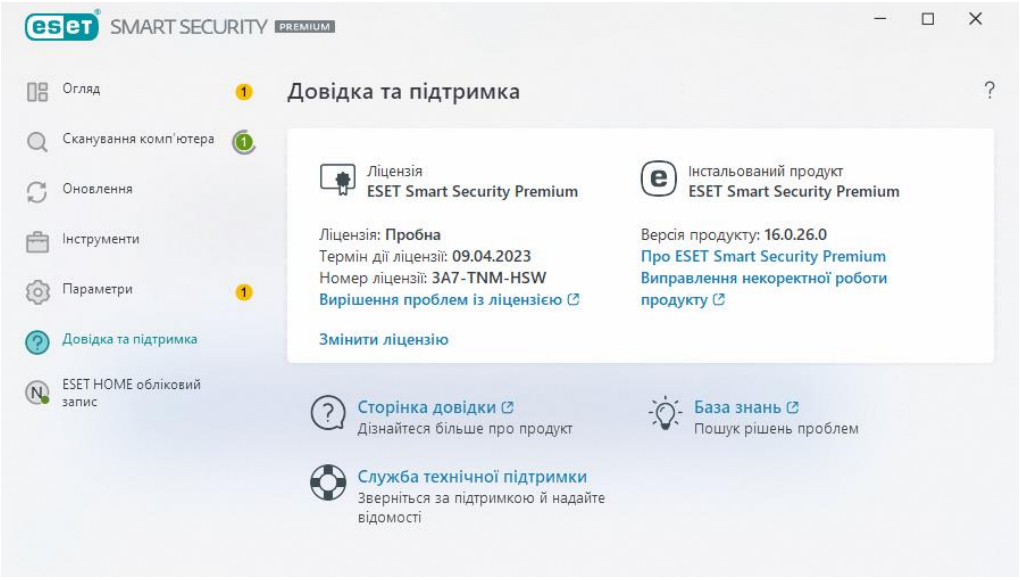

Рис 3.28. Екран з довідкою та підтримкою

Обліковий запис ESET HOME відображає перевірку статусу підключення облікового запису ESET HOME. У ESET HOME можна переглядати параметри Антикрадій і активовані ліцензії та пристрої ESET і керувати ними. (Рис 3.29)

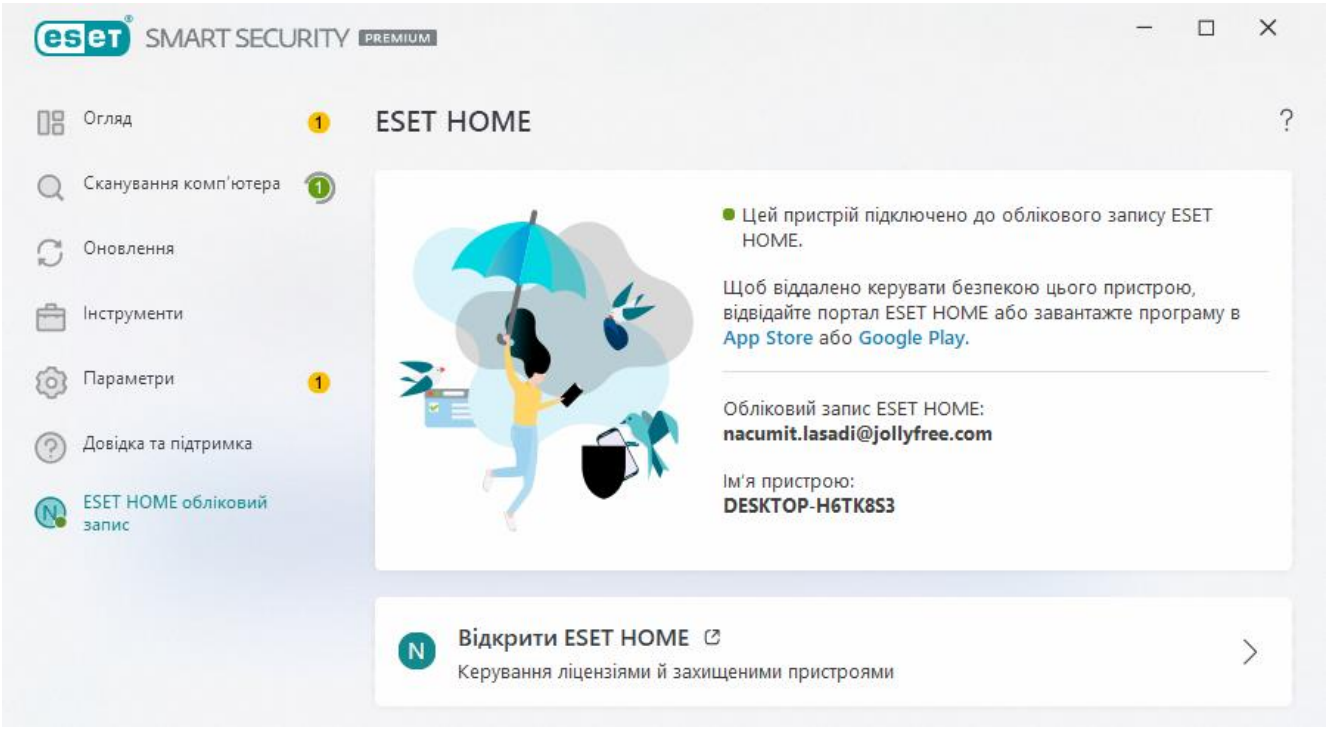

Рис 3.29. Екран з ESET HOME обліковий запис

Як висновок, можна сказати, що ESET Smart Security Premium є потужним антивірусом з багатофункціональним захистом. Інтерфейс є досить зручним та інтуїтивно зрозумілим та легко налаштовується , що дозволяє використовуватися ним навіть користувачам з невеликим досвідом використання антивірусного програмного забезпечення.

3.3 Рекомендацій, щодо протидії вторгнення

Люди все частіше користуються інтернетом це зручно та швидко, але водночас не слід забувати про особисту безпеку в інтернеті. Якщо так сталося що ви не встановили антивірус на свій комп'ютер або смартфон. Не панікуйте, коротко наведено нище найпоширеніші рекомендації, щодо протидії вторгнення.

Для захисту інтернет-акаунтів використовуйте складні паролі. Не встановлюйте однаковий пароль для декількох акаунтів. Налаштуйте двофакторну аутентифікацію всюди, де є така можливість. Тоді для входу до акаунту, крім логіну та паролю, потрібно ввести код-підтвердження, що приходить на телефон [14].

Щоб створити надійний пароль, потрібно використати:

- принаймні 8–12 символів;
- поєднання літер, цифр і символів;
- принаймні одну велику літеру;
- унікальний набір символів для кожного облікового запису;
- незвичайні слова; слова з пісень, цитати або популярні фрази, аби його було легше запам’ятати. Наприклад, на основі перших двох літер кожного слова в реченні "Старе Місто – моя улюблена кав’ярня в Києві" можна створити пароль: StMi-moulkauKy97!.

Нижче наведено приклади надійних паролів.

- Cook-Shark-33-Syrup-Elf.
- Tbontbtitq31!.
- Seat_Cloud_17_Blimey.

Ненадійні паролі часто містять персональну інформацію або комбінації клавіш, що розташовані поруч. Нижче наведено приклади ненадійних паролів.

- 1234567.
- 1111111.
- Qwerty.
- Qwerty123.
- Password.
- Password1.
- 1q2w3e.
- Abc123 [15].

Двофакторна аутентифікація - один із найдієвіших способів захисту облікових записів: електронної пошти, месенджерів, акаунтів у соцмережах та інших.

Додатковим фактором для перевірки може бути підтвердження:

- через код, надісланий у смс;
- через дзвінок на мобільний;
- через лист на e-mail;

● через надсилання сповіщення - така можливість, наприклад, є для акаунтів Google;

● через код, згенерований за допомогою спеціальних мобільних додатків (наприклад, Google Authenticator, Microsoft Authentificator чи інші) тощо.

Як встановити двофакторну аутентифікацію:

1. Увійдіть у потрібний акаунт (наприклад, Facebook, Telegram, Google чи інший).

2. Зайдіть у розділ меню Налаштування, а потім Безпека.

3. Оберіть пункт із налаштуваннями двофакторної автентифікації, якщо така функція є (зверніть увагу, може називатися також - двоетапна перевірка).

4. Виконайте всі необхідні дії за запропонованою інструкцією.

Використовуйте двофакторну аутентифікацію всюди, де це можливо [16].

Не переходьте за сумнівними гіперпосиланнями, адже за ними може ховатися фішинговий ресурс. Фішинг використовують зловмисники для отримання цінних даних, зокрема даних банківських карток. Уважно переглядайте URL-адресу потрібного сайту, будь-яка неточність може свідчити, що ви опинилися на фішинговому ресурсі. Ніколи не вводьте конфіденційні дані на підозрілих сайтах.

Подбайте про захист фінансового номера. Забороніть віддалений перевипуск SIM-карти у мобільного оператора або перейдіть на контрактне обслуговування.

Робіть резервні копії, аби не втратити важливі відомості [14].

Не слід використовувати неліцензійне програмне забезпечення та операційні системи. Так, ліцензія – це дорого, але ви платите за вашу безпеку. Проблема у тому, що зловмисники розповсюджують шкідливе ПЗ через зламані програми. Якщо ви не можете придбати платну версію програми, то користуйтеся безкоштовними аналогами – це значно кращий варіант, ніж зламані версії платних додатків.

Вчасно встановлюйте оновлення ОС та програм.

Поради щодо мережевих з'єднань

Підключайтеся до публічних Wi-Fi-мереж лише у разі крайньої необхідності. Якщо вони вам потрібні, то користуйтеся перевіреним VPN. У деяких браузерах є встановлений VPN (наприклад, Opera).

Встановіть для домашньої Wi-Fi-мережі складний пароль. Якщо у вашому роутері є така функцій, то створіть “гостьову мережу” для тимчасових користувачів, а для власної мережі краще встановити "білий" перелік пристроїв, які можуть приєднуватися.

Розроблено рекомендації щодо протидії вторгнення. Ці рекомендації будуть цікаві як для звичайних, так і для досвідчених користувачів, які допоможуть вам зберегти ваші дані та захистити ваш комп'ютер та смартфон від вторгнення.

ВИСНОВКИ

Варто зазначити, що запропоновані рекомендації не дають сто відсоткової гарантії забезпечення необхідного рівня безпеки інформації. Проте користуючись рекомендаціями, можна максимально ефективно захистити свій комп'ютер від уже відомих загроз.

Проаналізовано теоретичні матеріали щодо засобів та методів захисту інформації.

В результаті проведено аналіз класифікації загроз інформаційній безпеці можна зробити висновок, що існує багато різних видів загроз, які можуть стати причиною порушення безпеки інформації. Класифікація загроз дає можливість усвідомити ці загрози та способи їх прояву, що є важливим кроком у забезпеченні безпеки інформації.

Проведено аналіз сучасного шкідливого програмного забезпечення та боротьба з ним.

Було досліджено антивіруси від компаній Zillya, ESET та TotalAV, порівняння функціональних можливостей. Найефективнішими засобом захисту від кіберзагроз це ESET Smart Security Premium.

Надані рекомендації щодо покрокових дій завантаження та інсталяція ESET Smart Security Premium.

Проведено налаштування та використання. Програма має зручний інтерфейс та легко налаштовується для оптимального захисту комп'ютера.

Було надано рекомендацій, щодо протидії вторгнення.

Рекомендації у своїй роботі можуть використовувати ІТ-спеціалістів, керівників організацій, які займаються обробкою інформації, а також всіх користувачів комп'ютерів, які бажають збільшити рівень захисту своїх даних в мережі Інтернет.

ПЕРЕЛІК ПОСИЛАНЬ

1. Поради (рекомендації) щодо створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет. URL: https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet (дата звернення: 01.03.2023).
2. Апаратні засоби захисту. URL: https://studfile.net/preview/6012701/page:41/ (дата звернення: 03.03.2023).
3. Аутентифікація і авторизація: що це і в чому відмінність. URL: https://qagroup.com.ua/publications/autentyfikatciia-i-avtoryzatciia/ (дата звернення: 06.03.2023).
4. Про захист інформації в інформаційно-комунікаційних системах: Закон України Редакція від 01.07.2022 Відомості Верховної Ради України (ВВР), 1994. 5 липня, № 31, ст.286.
5. Богуш В.М., Мухачов В.А.. Криптографічні застосування елементарної теорії чисел: авч. посіб. Київ: ДУІКТ, 2006. 21 с.
6. Інформаційна безпека: види загроз і методи їх усунення. URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/ (дата звернення: 09.03.2023).
7. Загрози безпеці інформації в автоматизованих системах. Основні джерела і шляхи реалізації загроз. URL: https://sites.google.com/view/rudavska/%D1%83%D1%80%D0%BE%D0%BA%D0%B8/11-%D0%BA%D0%BB%D0%B0%D1%81/%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0/4-%D1%83%D1%80%D0%BE%D0%BA (дата звернення: 11.03.2023).

8. Класифікація антивірусних програм. URL: https://informatika-ptu91.webnode.com.ua/urok-15/ (дата звернення: 13.03.2023).

9. Комп'ютерні віруси та інші шкідливі програми. URL: http://www.zhu.edu.ua/mk_school/mod/page/view.php?id=6547 (дата звернення: 16.03.2023).

10. Енциклопедія Інтернет-загроз. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/ (дата звернення: 18.03.2023).

11. Офіційний сайт Zillya. URL: https://zillya.ua/ (дата звернення: 01.04.2023).

12. Офіційний сайт ESET. URL: https://www.eset.com/us/ (дата звернення: 09.04.2023).

13. Офіційний сайт TotalAV. URL: https://www.totalav.com/ (дата звернення: 14.04.2023).

14. Правила безпеки у кіберпросторі – рекомендації кіберполіції. URL: https://cyberpolice.gov.ua/article/pravyla-bezpeky-u-kiberprostori--rekomendacziyi-kiberpolicziyi-1747/ (дата звернення: 04.05.2023).

15. Що таке захист паролем? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-password-protection (дата звернення: 10.05.2023).

16. Захист облікових записів за допомогою двофакторної автентифікації: роз'яснення Держспецзв'язку. URL: https://biz.ligazakon.net/news/212788_zakhist-oblkovikh-zapisv-za-dopomogoyu-dvofaktorno-avtentifkats-rozyasnennya-derzhspetszvyazku (дата звернення: 15.05.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)