МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2021 р.

На правах рукопису
УДК 004.056:056.53(079.2)

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система інформаційної безпеки банку

Виконавець: М.П Буяр
Науковий керівник: к.т.н., доцент С.В. Єгоров
Нормоконтролер: к.т.н., доцент С.В. Єгоров

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ С.В. Казмірчук
«___» _____ 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи
здобувача вищої освіти Буяра Мирослава Петровича

1. Тема: *Система інформаційної безпеки банку*
затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.
2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.
3. Вихідні дані: проаналізував систему інформаційної безпеки банку, також, методики аналізу і оцінки ризиків інформаційної безпеки; розробив оцінку ризиків , та спроектував систему інформаційного захисту.
4. Зміст пояснювальної записки: класифікація загроз, загрози інформації , оцінка ризиків інформаційної безпеки, захист інформації.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	19.04.2021	*Виконано*
2.	Аналіз літературних джерел	21.04.2021	*Виконано*
3.	Обґрунтування вибору рішення	23.04.2021	*Виконано*
4.	Збір інформації	29.04.2021	*Виконано*
5.	Дослідження систем інформаційної безпеки	05.05.2021	*Виконано*
6.	Дослідження загроз	09.05.2021	*Виконано*
7.	Оцінка ризиків та захист	11.05.2021	*Виконано*
8.	Проектування системи захисту	15.05.2021	*Виконано*
9.	Перевірка на антиплагіат	20.05.2021	*Виконано*
10.	Оформлення і друк пояснювальної записки	26.05.2021	*Виконано*
11.	Оформлення презентації	04.06.2021	*Виконано*
12.	Отримання рецензій від рецензента	09.06.2021	*Виконано*

Здобувач вищої освіти М. Буяр

(підпис, дата)

Керівник дипломної роботи С. Єгоров

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, двох розділів, загальних висновків, списку використаних джерел, додатків, загальним обсягом робота складає 98 сторінки, має 78 рисунків, 10 таблиці, 4 діаграми. Список використаних джерел містить 30 найменувань і займає 4 сторінки.

Метою дипломної роботи є продемонструвати систему інформаційної безпеки банку. Провести оцінку системи. Під оцінюванням ризиків інформаційної безпеки мається на увазі оцінювання ризиків інформаційної безпеки. Визначити основні загрози та захист системи. Та стан захищеності .

В роботі проведено аналіз ризику інформаційної безпеки, досліджено системи захисту та ризиків ІС. Реалізоване проектування системи інформаційної безпеки банку. Розроблене відповідне моделювання інформаційної безпеки банку

Ключові слова: Система захисту, класифікація систем захисту, підсистеми захисту, оцінка ризику, загрози інформаційній безпеці,

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІБ – інформаційна безпека

ІББ- інформаційна безпека банку

УІБ - управління інформаційною безпекою

СУІБ – система управління інформаційною безпекою

АСУ – автоматизована система управління

ІСУ – інформаційна система управління

КС — комп'ютерна система;

ВСТУП

Актуальність. Інформаційна безпека та її система захисту є процесом забезпечення безпеки інформаційних ресурсів організації, вона побудована на кращих світових практиках. Стандарти банку основані на міжнародних стандартах ISO 27001 та ISO 27002 з додаванням вимог із захисту інформації, зумовлених конкретними потребами сфери банківської діяльності і правовими вимогами.

Об`єкт дослідження – процес захисту інформації.

Предмет дослідження – методи та засоби захисту інформаційних систем

Метою дипломної роботи є розробка системи інформаційної безпеки банку.

Завдання бакалаврської роботи:

- Дослідити загрози інформаційній безпеці банку
- Провести оцінку ризикам
- Реалізація системи безпеки

Метод дослідження – системи, підсистеми та засоби захисту інформації.

Практична цінність Практична цінність полягає у тому, що застосування розробленої системи захисту інформації дасть змогу уникнути витоку інформації, та дозволить застосовувати систему оцінювання ризиків інформаційної безпеки та захисту даних.

З моменту свого створення банки незмінно викликали злочинний інтерес. І цей інтерес був пов’язаний не тільки зі зберіганням коштів у кредитних установах, але і з тим, що важлива і часто секретна інформація про фінансово-господарську діяльність багатьох людей, компаній, організацій і навіть цілих держав була зосереджена в банках. Так, ще в 18 столітті недоброзичливці знаменитого Джакомо Казанова опублікували закриті дані про рух коштів на його рахунку в одному з паризьких банків.

Сьогодні, у зв'язку із загальною інформатизацією та комп'ютеризацією банківської справи, значення інформаційної безпеки банків зросло в рази. Ще 30 років тому ціллю інформаційних атак були дані про клієнтів банку або про діяльність самого банку. Такі напади були рідкісними, коло їхніх клієнтів було дуже вузьким, і шкода могла бути значною лише в особливих випадках. В даний час внаслідок широкого розповсюдження електронних платежів, пластикових карток, комп'ютерних мереж кошти як банків, так і їх клієнтів стали об'єктом інформаційних атак. Будь-хто може зробити спробу крадіжки - вам потрібен лише комп'ютер, підключений до Інтернету. Більше того, для цього не потрібно фізично входити в банк, можна «працювати» і за тисячі кілометрів від нього.

Наприклад, у серпні 1995 року у Великобританії було заарештовано 24-річного російського математика Володимира Левіна. якому за допомогою домашнього комп'ютера в Санкт-Петербурзі вдалося проникнути в банківську систему одного з найбільших американських банків Citibank і викрасти 2,8 мільйона доларів. У 1994 році Володимиру Левіну разом із другом вдалося знайти ключі від банківської системи безпеки Citibank і спробувати зняти з його рахунків великі суми ... За даними московського представництва Citibank, до цього часу нікому це не вдалося. Служба безпеки Citibank з'ясувала, що вони намагалися викрасти у банку 2,8 мільйона доларів, але контрольні системи вчасно виявили це і заблокували рахунки. Їм вдалося вкрасти лише 400 тисяч доларів. Щоб отримати гроші, Левін відправився до Англії, де був заарештований [17, ком. за 01.10.95].

Комп'ютеризація банківської діяльності дозволила значно підвищити продуктивність банківських службовців, запровадити нові фінансові продукти та технології. Однак прогрес у технології злочинності був не менш швидким, ніж розвиток банківських технологій. В даний час понад 90% усіх злочинів пов'язано із застосуванням автоматизованих систем обробки інформації банку

(ASOIB). Отже, при створенні та модернізації ASOIB банки повинні приділяти пильну увагу забезпеченню його безпеки. Саме цій проблемі присвячена більша частина дипломної роботи.

Саме ця проблема зараз є найбільш актуальною та найменш вивченою. Якщо при забезпеченні фізичної та класичної інформаційної безпеки1 вже давно розроблені усталені підходи (хоча розвиток відбувається і тут), то у зв'язку з частими кардинальними змінами в комп'ютерних технологіях методи безпеки ASOIB вимагають постійного оновлення. Як показує практика, не існує складних комп’ютерних систем, що не містять помилок. І оскільки ідеологія побудови великих ASOIB регулярно змінюється, виправлення знайдених помилок та «дірок» в системах безпеки недостатньо надовго, оскільки нова комп’ютерна система приносить нові проблеми та нові помилки, що вимагає перебудови системи безпеки в новий спосіб

Розділ 1. Інформаційна безпека банку

1.1. Інформаційна безпека банку структура та система

Політика інформаційної безпеки банківської установи - це система поглядів на визначення основних сфер, умов та процедур практичного вирішення інформаційного захисту банку від протиправних дій.

Стан захисту інформації про власників, керівництво, клієнтів банку, технології та інформаційні ресурси банку від внутрішніх та зовнішніх загроз.

Забезпечення інформаційної безпеки є невід’ємною частиною банку.

Стан інформаційної безпеки банку - це здатність банку протистояти будь-яким спробам нанести шкоду інтересам банку.

Об’єктами безпеки є:

- інформація про персонал (керівництво, відповідальні виконавці, співробітники);
- інформація щодо технологій, які використовуються банком;
- інформаційні ресурси (інформація з обмеженим доступом, що складає банківську та комерційну таємницю, інша конфіденційна інформація,

надана у виді документів і масивів незалежно від форми і виду їхнього представлення), в тому числі:

- інформація щодо діяльності та фінансового стану клієнта, що стала відома банку у процесі обслуговування;
- інформація щодо всіх операцій банку та фінансова звітність банку.
- конфіденційні електронні мережі банку.

Секретні електронні мережі в банку з низкою електронних пристроїв, допоміжних та спеціальних пристроїв та програмного забезпечення для обробки, передачі та зберігання інформації про всі речі в банку та фінансових звітів до банку, які знаходяться в оперативних відділах під банком, а також у секретній базі даних клієнтів банку.

Інформація, отримана від банку та комерційного банку, включає секретну інформацію, втрата якої може завдати шкоди інтересам клієнтів.

Інформація про рахунки, депозити та операції з клієнтами.

Інформаційні технології в банківській, адміністративній, фінансовій та інших видах діяльності в банку (переказ, витік), можуть зашкодити інтересам банку, комерційну таємницю банку:

- відомості, втрата яких може привести до тяжких наслідків для фінансово-економічної діяльності банку чи його банкрутства, присвоюється гриф таємності “цілком конфіденційно ” (ЦК).
- відомості, втрата яких може нанести значних збитків конкурентно спроможності банку та його операційним актам, присвоюється гриф таємності “Конфіденційно” (К);
- інші відомості з питань технологічної банківської діяльності, управління фінансів та інших доходів Банку становлять комерційну таємницю без присвоєння грифу таємності.

План визначає мету та частину системи інформаційної безпеки, принципи правової бази для її організації та функціонування, типи загроз безпеці та джерела, які слід зберігати, а також основні компоненти стандартів та захисту для розвитку систем безпеки.

Проста система захисту даних.

Головне - забезпечити стійку роботу банківських та інформаційних систем безпеки, запобігти загрозам їх безпеці, захистити від незаконного втручання, розголошення, втрати, втрати, корупції та знищення офіційних даних, а також порушень цих технічних засобів. повідомити.

Задачами системи інформаційної безпеки є:

- віднесення інформації до категорії обмеженого доступу (банківській і комерційній таємницям);
- протидія витоку такої інформації;
- віднесення КЕМБ до найбільш небезпечного об’єкту для витоку інформації і з цієї точки зору приділення їй додаткової уваги;
- прогнозування, своєчасне виявлення й усунення погроз інформаційній безпеці банку; причин і умов, що сприяють нанесенню фінансового, матеріального і морального збитку, порушенню нормального функціонування і розвитку банку;
- створення механізму й умов оперативного реагування на погрози інформаційній безпеці банку;
- ефективне припинення посягань на інформаційні ресурси банку на основі правових, організаційних і інженерно-технічних мір і засобів забезпечення безпеки

Принципи організації та функціонування системи захисту інформації банку.

Організація та функціонування системи інформаційної безпеки банку повинні відповідати таким принципам: повнота, своєчасність, стійкість, активність, законність, надійність, спеціалізація, взаємодія та координація можливих втрат та витрат на безпеку, доцільність та можливість збитку (критерій "ефективність) - витрати").

Успішне та ефективне вирішення інформаційної безпеки банку досягається шляхом формування системи правил, правил, інструкцій, положень та правил. Функціональні обов'язки працівників та служб, включаючи службу економічної безпеки. Необхідними передумовами забезпечення інформаційної безпеки банку є правила в'їзду (виходу) осіб до банку, правила застосування

(вилучення) документів, у тому числі знімних електронних носіїв інформації, а також правила зберігання даних. приватний комп’ютер та комп’ютерна мережа.

Функціональні підрозділи відповідають вимогам банку щодо захисту інформації. Керівники окремих відділень банку несуть персональну відповідальність відповідно до вимог інформаційної безпеки.

Враховуючи надійність, використання технології, які використовуються в даних, інформаційна безпека повинна стати одним з основних фундаментальних частин існування , банківських систем. Одним з основних напрямків інформаційної безпеки будь-якої установи є захист конфіденційності.

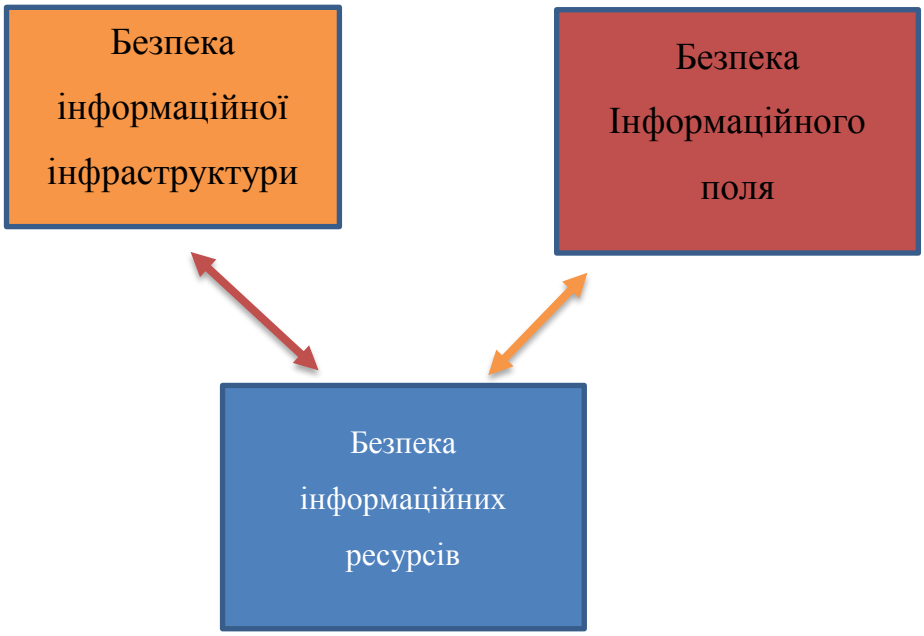
У структурі захисту даних банківської установи, виділяють основні компоненти:

1. Безпека інформаційних ресурсів:
2. Безпека інформаційної інфраструктури,
3. Безпека "інформаційне поле".

Інформаційні ресурси залежно від Інформації про установу - це взаємопов’язана систематизована і закріплена на матеріальних носіях інформація, яка належить банківській установі.

- ***Безпека інформаційних ресурсів-*** захищати таку інформацію від несанкціонованого розповсюдження, використання та порушення конфіденційності (конфіденційності)

Складові інформаційної безпеки



Безпека інформаційної інфраструктури – Статус безпеки комп'ютерів, мереж та банківських установ забезпечує цілісність та доступність інформації.

Захист інформаційного поля - установа, яка спеціалізується на несистематичних потоках інформації (розповсюджується конкурентами, ЗМІ, органами влади тощо).

Безпека банку базується на системі заходів безпеки, основні вимоги ІБ:

1. Оцінка ризиків організації
2. Вимоги визначені законом та правові

Вразливості які несуть загрози ІББ:

- Системи управління
- Дані персоналу та інших користувачів
- Фізичне середовище
- Банк в цілому

Система інформаційної безпеки банку – процес забезпечення безпеки джерел інформації. Стандарти Національного банку України базуються на міжнародних стандартах ISO 27001 та ISO 27002, з доданими вимогами щодо захисту даних до банків та законодавчими вимогами.

Процес управління інформаційною безпекою складний. Управління інформаційною безпекою є постійним процесом і може застосовуватися до стандарту СОУ Н НБУ 65.1 СУІЬ 1.0: 2010 PVPD (План - Виконання - виконання - Дія), наведеного Порівняння даних із використанням СУІБ.

Процес управління ризиком безпеки може бути описаний у наступній таблиці:

Фаза СУІБ	Процес захисту інформаційної безпеки
Плануй	Аналіз ресурсів СУІБ Оцінка загроз План оброблення загроз
Виконуй	Впровадження плану оброблення загроз
Перевіряй	Постійний моніторинг та перегляд загроз
Дій	Підтримка та покращення процесу управління захисту ІБ

Управління інформаційною безпекою - це коректна робота всіх підрозділів банку .Це стосується насамперед керівників підприємств - власників бізнес-процесів, або банківських продуктів.

Аналіз джерел СУІБ та бізнес-процесів або банківських продуктів базується на існуючих заходах безпеки та інформації, яка загальнодоступна та систематизована на етапі опису інформації в інфраструктурі. На цьому етапі ми розглянемо раніше визначені та описані критичні банківські продукти, програмне та апаратне забезпечення щодо інформаційної безпеки та можливих втрат у разі порушень.

Цей аналіз дозволить більш детально оцінити ризики інформаційної безпеки в майбутньому та визначити план управління ризиками. Для кожного з вищезазначених комплексів важливо врахувати, наскільки ефективно працюють основні служби захисту інформації та як вони можуть вплинути на роботу:

- Цілісність
- Конфіденційність
- Доступність
- Спостережність.

Визначимо основні терміни:

Конфіденційність - властивість інформації, яка полягає в запобіганні розповсюдженню інформація, тобто інформація не може бути отримана неавторизованим користувачем або процесом;

Цілісність - Властивість інформації полягає в тому, що інформація не може бути змінена неавторизованим користувачем або процесом.

Цілісність системи - особливість системи, що жоден з її елементів не може бути вилучений, змінений або доданий з порушенням політики безпеки ;

Доступність - властивість системного ресурсу , що користувач та / або процес з відповідними привілеями може використовувати ресурс відповідно до правил, визначених у політиці безпеки, не чекаючи довший за заданий (невеликий) період, тобто коли знаходиться у формі, яку вимагає користувач, у місці, про яку користувач запитує , і коли йому це потрібно;

Спостережливість - системна властивість, що дозволяє реєструвати користувачів та процеси, використання пасивних об’єктів та індивідуально встановлені ідентифікатори користувачів та процесів у кожній події для запобігання порушенням політики безпеки та / або для забезпечення відповідальності за певні дії .

Для різних бізнес-процесів або банківських продуктів можуть бути виявлені однакові ризики втрати основних сервісів безпеки, що буде

свідчити про те, що певним питанням інформаційної безпеки не приділяється необхідної уваги. У такому випадку рекомендується вирішувати питання зменшення ризиків однаково для всіх продуктів банку.

Однак найпоширеніша ситуація полягає в тому, що існують різні рівні ризику в різних бізнес-процесах та банківських продуктах, що вимагає застосування спеціальних заходів безпеки для конкретного бізнес-процесу та конкретного банківського продукту

Через це докладна оцінка ризиків не може бути загальною для банку в цілому та потребує розгляду як загальних для банку питань, так і конкретних питань для кожного бізнес-процесу та банківського продукту. Крім того, особливу увагу слід приділити розгляду обміну інформацією між різними бізнес-процесами чи програмно-технічними комплексами.

Після виконання такого аналізу з точки зору впливу порушень інформаційної безпеки на бізнес-процеси можна переходити до більш докладної оцінки ризиків інформаційної безпеки.

Загрози можуть пошкодити ресурси СУІБ, включаючи інформацію, персонал, клієнтів, обладнання, процеси та програмне та апаратне забезпечення, бізнес-процеси / банківські продукти та банківську діяльність. Загрози можуть бути природними або людськими, а можуть бути випадковими або навмисними. Потрібно визначити як випадкові, так і навмисні джерела загрози. Загрози можна визначити за їх загальною формою або типом.

Наявність вразливих місць безпеки не може впливати лише на джерела та бізнес-процеси чи банківські продукти, оскільки має існувати загроза Скористайтеся цими вразливими місцями. Вразливість , яка не реагує на відповідну загрозу, не вимагає заходів безпеки, але повинна бути виявлена та відстежена на предмет змін які звязані з СУІБ .Це стосується джерела СУІБ та бізнес-процесу чи банківського продукту . Неправильно впроваджені або неефективні заходи безпеки є одним із видів уразливостей безпеки .

Слабкі сторони можуть бути пов’язані з характеристиками ресурсу СУІБ. Залежно від критичності даних та робочого процесу або банківського продукту,

а також інформаційних та телекомунікаційних технологій, для виявлення слабких місць можуть бути використані різні проактивні методи тестування. До таких методів тестування належать:

- інструментарі для сканування вразливостей;
- тестування та оцінка безпеки;
- тести на проникнення в систему;
- перегляд коду програмно-технічних комплексів;
- аналіз відомих порушень безпеки;
- аналіз відомих вразливостей (ОС,БД, телекомунікаційних технологій та протоколів).

Такі методи допоможуть ідентифікувати вразливості. Слід зазначити, що іноді ці методи можуть надавати інформацію про вразливості, які не представляють реальної загрози. Тому необхідно чітко задавати параметри програмно-технічних комплексів та їх конфігурацію для тестування.

Наслідками реалізації загроз можуть бути втрати ефективності, бізнес-процесів, зниження репутації тощо. Необхідно проаналізувати негативні наслідки для банку, які можуть виникати якщо ідентифіковані загрози будуть використовувати відповідні вразливості або набір вразливостей і призведуть до інциденту інформаційної безпеки. Такий інцидент інформаційної безпеки може впливати на один або більше ресурсів СУІБ, бізнес-процес,
банківський продукт. Таким чином, ресурсам СУІБ можуть бути приписані значення їх фінансової вартості, а також бізнес наслідків, якщо ці ресурси будуть пошкоджені або скомпрометовані.

1.2 Загрози інформаційній безпеці банку

Загроза інформаційної безпеки – сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки.

Під загрозою розуміється потенційно можлива подія, дія, процес або явище, які можуть призвести до нанесення шкоди чиїм-небудь інтересам.

Під загрозою інтересів суб`єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище , яке з допомогою впливу на інформацію або інші компоненти інформаційної системи, може прямо або інші компоненті інформаційної системи, може прямо або опосередковано призвести до нанесення шкоди інтересам даних того чи інших суб`єктів.

Класифікації

Загрози інформаційної безпеки можуть бути класифіковані за різними ознаками :

«За аспектом інформаційної безпеки, на який спрямовані загрози: є Загрози конфіденційності (неправомірний доступ до інформації). Загроза порушення конфіденційності полягає в тому, що інформація стає відомою особі, яка не має права на доступ до неї. Це відбувається, коли вони отримують доступ до деякої обмеженої інформації, яка зберігається в комп'ютерній системі або передається від однієї системи до іншої. Через загрозу вторгнення в приватне життя використовується термін "гвинт". Такі загрози можуть виникати внаслідок "людських факторів" (наприклад, випадкова передача прав користувача тому чи іншому користувачеві), збоїв програмного та апаратного забезпечення. Інформація з обмеженим доступом включає державну таємницю (комерційну таємницю, персональні дані, професійну таємницю: медичну, юридичну, банківську, службову, нотаріальну таємниці щодо страхування, розслідування та судових процесів, листування, телефонних розмов, поштових відправлень, телеграм чи інших повідомлень). суть винаходу, корисна модель або промисловий зразок (ноу-хау тощо), необхідні для офіційного опублікування.

Загрози цілісності (незаконне змінення даних). Порушення цілісності - це загроза, пов'язана з ймовірністю зміни інформації, що зберігається в інформаційній системі. Порушення цілісності можуть бути спричинені різними факторами - від навмисних дій персоналу до виходу з ладу обладнання.

Погрози доступності (операції, що перешкоджають або ускладнюють доступ до ресурсів інформаційної системи). Порушення доступності - це створення умов, за яких доступ до послуги або інформації або блокується, або дозволяється протягом певного періоду, який не забезпечує досягнення певних бізнес-цілей.

За розташуванням джерела загроз:

- Внутрішні (джерела загроз розташовуються всередині системи);
- Зовнішні (джерела загроз знаходяться поза системою).

За розмірами нанесеного збитку:

- Загальні (нанесення збитку об'єкту безпеки в цілому, заподіяння значної шкоди);
- Локальні(заподіяння шкоди окремими частинамиоб'єкта безпеки);
- Приватні(заподіяння шкоди окремим властивостям елементів об'єкта безпеки).

«За ступенем впливу на інформаційну систему:

- Пасивні(структура і зміст системи не змінюються);
- Активні(структура і зміст системи піддається змінам).

"За характером походження:

- Природний (об’єктивний) - спричинений впливом об’єктивних фізичних процесів або природних явищ, що не залежать від волі людини, на інформаційне середовище;
- - ненавмисні (випадкові) загрози, збої програмного забезпечення, персонал, збої системи, відмови комп'ютерного та комунікаційного обладнання;
- Навмисні загрози - - несанкціонований доступ до даних, розробка спеціального програмного забезпечення, що використовується для несанкціонований доступ, розробка та розповсюдження вірусних програм тощо. Умисні загрози спричинені діями людини. Основні проблеми інформаційної безпеки в основному пов’язані з

навмисними загрозами, оскільки вони є основною причиною злочинів та злочинів.

Згідно з інформацією, визначеною експертами з питань інформаційної безпеки, у інформаційних ресурсах є понад 65,96 збитків, спричинених ненавмисними помилками. Це основа для зосередження уваги на більш безпечному впровадженні комп'ютерних систем

Класифікація джерел загроз інформаційній безпеці

Носіями загроз інформаційній безпеці є джерела загроз. Джерелами загроз можуть бути суб'єкти (особи) та об'єктивні прояви, такі як конкуренти, злочинці, корупціонери, державні органи.

Джерела загроз включають такі цілі: доступ до приватної інформації, корисливі модифікації та знищення для прямого матеріального збитку.

Через дії суб'єкта - суб'єктів, діяльність яких полягає в інформаційній безпеці, ці дії можуть бути класифіковані як умисні або випадкові злочини. Джерела, які можуть призвести до порушень інформаційної безпеки, можуть бути як зовнішніми, так і внутрішніми. Ці ресурси можуть передбачити та вжити відповідних заходів.

Завдяки технічним засобам - ці небезпеки менш передбачувані, безпосередньо залежать від характеристик технології, і тому потребують особливої уваги.

Ці джерела загроз інформаційній безпеці можуть бути як внутрішніми, так і зовнішніми. Це можна передбачити, але не можна запобігти), такі об'єктивні та абсолютні обставини стосуються всіх. Такі джерела загрози абсолютно непередбачувані, тому проти них потрібно завжди вживати заходів.

Природні ресурси, як правило, перебувають за межами об'єкта, що охороняється, і, як правило, їх розуміють як стихійні лиха.

Несанкціонований доступ до інформації - доступ до інформації, що порушує службові повноваження працівника, доступ громадськості особам, які

не мають дозволу на використання цієї інформації. Несанкціонований доступ іноді називають доступом до інформації тих, хто має право на доступ до цієї інформації понад те, що необхідно для виконання службових обов'язків.

Причини доступу до несанкціонованої інформації

- "помилки конфігурації (права доступу, брандмауери, обмеження обсягу запитів до бази даних)
- " погана безпека авторизації (викрадення пароля, крадіжка смарт-карт; фізичний доступ до погано захищених пристроїв, доступ до розблокованих співробітників за відсутності співробітників)
- збій програмного забезпечення під час "зловживання енергією (викрадення резервних копій, копіювання інформації на зовнішні носії з правом доступу до інформації)" канали зв'язку, використовуючи незахищені з'єднання в локальній мережі
- використовують шпигунське програмне забезпечення клавіатури, віруси та троянські програми на комп'ютерах співробітників

Тим саме проблема ЗІ є одним з найважливіших питань для банківської сфери.

Інформаційна Безпека - Це формування інформаційних ресурсів банку та організація їх гарантованого захисту . Це було досягнуто шляхом створення відповідних заходів щодо збору, зберігання та розподілу даних в банку шляхом визначення категорій та статусу банківських даних, правил та положень доступу. ,дотримання банківськими стандартами та нормативами всіх співробітників, клієнтів та акціонерів банківської інформації, своєчасне виявлення спроб та можливих даних про витоки та їх перетинання .

Перш за все, проблема починається з нерозуміння порушень захисту даних з точки зору таких категорій, як "загроза", "ризик", "джерело загрози", "фактор загрози". "Чутливість ", "Негативні фактори впливають на "," Негативні прояви "," Перешкоди ". Їх спільною рисою є те, що всі вони характеризують категорію

"загроза " на відміну від" безпека ". Незважаючи на подібність, умови не однакові, тому, незважаючи на численні дослідження в цих областях, досі немає чіткого і однозначного тлумачення таких понять, як "ризик" і "загроза".

Загроза є досить цікавою формою ризику, тим саме ми можемо підкреслити те, що :

1) ризик стосовно загрози є первинним, тоді як загроза вторинна і випливає з ризику;
2) ризикуючи, банк може отримати як збитки, так і доходи, тоді як реалізація загрози не приносить доходи чи прибутки
3) ризик – неминучий супутник банківської діяльності, тоді як загроза може виникати тільки за наявності певних умов

Можна зробити висновок, що , під впливом деяких факторів(це можуть бути несприятливі чинники впливу) , джерело загрози через певну чутливість створює певні ризики та загрози для СБ.

Така модель інформаційної безпеки може відображати низку об’єктивних зовнішніх та внутрішніх факторів та їх вплив на стан інформаційної безпеки об’єкта та захист інформаційних ресурсів .

Отже, відомо, що інформаційна безпека поділяється на дві

категорії загроз: зовнішню та внутрішню.

Чим успішнішими будуть люди у боротьбі із зовнішніми загрозами, тим більш рішучими вони будуть. Згідно зі статистичними даними, внутрішні загрози пов’язані з приблизно 70% усіх інцидентів безпеки.

Захист банківських даних є рівною мірою технічним, правовим та організаційним завданням.

Щоб запобігти порушенням інформаційної безпеки джерел інформаційного банку , необхідно виявити та проаналізувати слабкі місця інформаційної системи банку та джерела, які необхідно захищати від атак. Потім потрібно виявити ризики даних для конкретного джерела даних, вибрати контрзаходи відповідно до обраної банківської політики та застосувати їх за допомогою механізмів безпеки та служб.

Політика безпеки банку повинна визначати взаємопов'язані механізми та послуги безпеки. має відповідати захищеним джерелам та середовищу, в якому вони використовуються.

Виходячи з вищесказаного, що конкретне порушення інформаційної безпеки - це також особливий „механізм", який починається з негативних факторів і закінчується відповідними результатами. У той же час, повинен постійно розглядати джерела потенційних загроз як у зовнішньому, так і у внутрішньому середовищі, щоб бути готовим до можливих зовнішніх ризиків. Однак оскільки внутрішні загрози нещодавно перевершили зовнішні загрози, пов'язані між собою, не слід розглядати в чистому вигляді . З цієї причини розробка системи захисту інформації для банків повинна бути комплексною

Потенційні загрози системі

Ми класифікували загрози як внутрішні та зовнішні загрози. Внутрішні загрози надходять від когось, хто працює всередині банку, тоді як зовнішні загрози походять від сторонніх осіб.

Внутрішні загрози:

Неправдиві рахунки: органи банку можуть відкрити неправдиві рахунки від імен вигаданих клієнтів та дозволити привілеї на цей рахунок. Вони можуть надавати таким рахункам позики та кредити. Пізніше вони можуть конвертувати ці гроші в особисте користування.

Шахрайські позики. Одним із способів вилучити гроші з банку є отримання позики. Однак шахрайська позика - це позика, в якій позичальником є суб'єкт господарювання, який контролюється нечесним банківським службовцем або співучасником; «Позичальник» може оголосити про банкрутство або зникнути. Зрештою гроші зникли. Позичальник може бути навіть неіснуючим суб'єктом господарювання, а позика - просто штучна вигадка для приховування крадіжки великої суми грошей у банку.

Банківське шахрайство: банківський переказ такі мережі, як міжнародний переказ міжбанківських фондів SWIFT, часто є цілями, оскільки якщо переказ

здійснюється, його важко або неможливо повернути назад. Оскільки ці мережі використовуються банками для розрахунків між собою, швидкий або нічний банківський переказ великих сум грошей є звичним явищем; в той час як банки встановлюють противаги та противаги, існує ризик того, що інсайдери можуть спробувати скористатися шахрайськими або підробленими документами, які вимагають переказувати гроші вкладника банку в інший банк, часто офшорний рахунок у якійсь далекій зарубіжній країні.

Підроблені або шахрайські документи: підроблені документи часто використовуються для приховування інших крадіжок. Банки , як правило, ретельно розраховують свої гроші, тому кожну копійку потрібно враховувати. Таким чином, документ, який стверджує, що сума грошей була позичена як позика, вилучена індивідуальним вкладником або переведена або інвестована, може бути цінним для банкіра, який хоче приховати незначну деталь, і припустив, що гроші були вкрадені і зараз їх немає.

Крадіжка особистості: Нечесні працівники банку, як відомо, розкривають особисту інформацію вкладника для використання у крадіжці з шахрайством . Потім зловмисники використовують цю інформацію для отримання ідентифікаційних карток та кредитних карток, використовуючи ім’я та особисту інформацію жертви.

Шахрайство з вимогою вимагати: Це шахрайство зазвичай робить один або кілька нечесних працівників банку .

Вони вилучають із запасу мало листків чернеток або книг та пишуть їх як звичайний. З вони є інсайдерами, вони знають кодування та штампування чернетки попиту. Ці Проекти попиту будуть видані , що підлягають оплаті у віддаленому місті без дебетування рахунку, і будуть зняті у платіжному відділенні. Для платіжного відділення це лише черговий проект попиту. Цей вид шахрайства буде виявлений лише тоді, коли головний офіс здійснить примирення у галузевому масштабі, що зазвичай триває 6 місяців. На той час гроші не підлягають відновленню.

Зовнішні загрози: це загрози сторонніх осіб, і їх може зробити крадіжка чи хакер.

Хтось, хто використовує Інтернет-банкінг для здійснення транзакцій, має щоб бути обережними з хакерами. Номер безпеки та пароль

- життєво важлива інформація для Вашої транзакції в Інтернеті. Нижче ми перерахували деякі загрози:

Шахрайство з кредитною карткою: Зазвичай шахрай використовує кредитну картку іншої особи для стягнення плати за покупку . Деякі з шахрайських операцій з кредитними картками - це шахрайства з вкраденими картками, шахрайство з поглинанням рахунку, поштою з кредитною карткою

Замовлення та обробка.

Шахрайство з викраденими кредитними картками: коли клієнт втрачає картку, можливо, злодій здійснювати несанкціоновані платежі на картці, доки її не буде скасовано.

Шахрайство з поглинанням рахунку: шахраї телефонують та видають себе за справжніх власників карток, використовуючи їх викрадену особисту інформацію. Вони змінюють адресу та іншу інформацію власника картки на адресу , яку вони контролюють. Додаткові картки та, можливо, поштові скриньки запитуються та видаються на нову адресу та використовуються шахраями для здійснення покупок або отримання авансових платежів

Шахрайство із замовленням поштою за допомогою кредитної картки: Використовуючи викрадений номер кредитної картки або згенерований комп'ютером номер, злодій замовляє викрадені товари.

Скімінг. ; зазвичай це робиться в барах чи ресторанах. Ці люди або копіюють номери вручну, або використовують зчитувач із магнітною смужкою для отримання коду захисту картки.

Фішинг або шахрайська пошта: Фішинг - це спосіб шахрайства, який використовується для получення цифр та паролю шахраям. Хакер надсилає шахрайський лист, спеціально розроблений для того, щоб розкрити деталі безпеки потрібній особі. Ця пошта розроблена таким чином, що, здається, вона

надійшла з відповідального джерела, наприклад; у вашому банку. Ця пошта може також надати вам гіперпосилання із URL-адресою домашньої адреси вашого банку , яка знову є сайтом шахрайства.

Найбільшою загрозою для безпеки інформаційних ресурсів є витік або втрата таких ресурсів (включаючи інформацію про банківську таємницю). Джерелам інформації можуть загрожувати:

- підкуп осіб, які мають прямий доступ до банківської таємниці та іншої інформації з обмеженим доступом до банківської установи;
- Необережне, недбале поводження з банками таємницею та невиконання вимог щодо зберігання обмеженої інформації у відносинах з контролюючими та наглядовими органами через юридичну та психологічну неготовність відповідального персоналу банківської установи тощо

Боротьба з такими загрозами повинна включати, зокрема:

- визначення надійності працівників компанії, які працюватимуть із банківською таємницею та іншою обмеженою інформацією;
- організація спеціальних записів сертифікація та закріплення диференційованого доступу співробітників до банківської таємниці та іншої інформації з обмеженим доступом, при якій працівник може лише читати та виконувати певні операції з ним для виконання
- підтвердження особистої відповідальності працівника за збереження переданих йому або підготовлених ним документів, інших носіїв даних, які мають обмежений доступ до банківської установи;

- обмежує доступ працівників та третіх осіб до приміщень, де обробляється (зберігається) інформація з обмеженим доступом до банківської установи,
- здійснення заходів контролю за роботою співробітників, які мають обмежені засоби масової інформації в банківській установі, ефективна система виявлення та реєстрації незаконних актів, що містять таку інформацію,
- запровадження надійної та ефективної системи зберігання носіїв інформації, що виключає несанкціонований доступ, знищення або підробку.

До суттєвих загроз безпеці інформаційної інфраструктури належать:

- неофіційний доступ до технічної інформації та видалення її власності;
- перехоплення інформації, що циркулює мовою пристроїв та систем та комп'ютерних технологій, з технічними засобами прихованого видалення інформації, несанкціонованого доступу до інформації та її навмисних технічних ефектів під час обробки та зберігання,
- перехоплення в офісах, що використовують технічні засоби конфіденційних переговорів, транспортні засоби тощо. Дія проти таких загроз насамперед має передбачати широке та, що найголовніше, економічно доцільне використання технічних засобів захисту інформаційної інфраструктури.

Для усунення загроз безпеці інформаційної інфраструктури банківських установ необхідно вжити конкретних заходів:

- для створення цілісності безпека, технічне та програмне середовище, що узгоджує програмне середовище, виконання

засобів захисту передбачених функцій, відокремлення засобів захисту від користувачів;

- використання захисту шифрування найціннішої інформації в комп'ютерах, системах та корпоративних комп'ютерних та телекомунікаційних мережах;

- Надання диференційованого доступу працівникам для виконання певних операцій (створення, читання, запис, модифікація, видалення) за допомогою програмного та апаратного забезпечення, а також обмеження доступу до електронних комп'ютерів (комп'ютерів), систем, комп'ютерних систем різних рівнів цілі даних у своїх мережах та телекомунікаційних мережах;
- ідентифікація користувачів та процесів, які вони виконують в електронних комп'ютерних системах та комп'ютерних мережах; телекомунікаційні мережі установи, засновані на використанні паролів, ключів, магнітних карток, цифрових підписів та біометричних ідентифікаторів особи, таких як доступ до інформації та телекомунікаційних систем;
- реєстрація (із записом дати та часу) Дії користувачів з інформаційними та програмними ресурсами на комп'ютерах, системах та комп'ютерних мережах, зокрема спроби незаконного доступу;

1.3. Висновки до першого розділу

В першому розділі ми розібрали інформацію про інформаційну безпеку банку, систему та загрози ІС.

Існує загальна потреба у подальшому вивченні та розробці чіткої концепції "загрози", і слід зосередитись на створенні ефективної та реалістичної системи моніторингу та управління та інші інформаційних загроз

Стратегічною місією банку є запобігання існуючим та потенційним загрозам інформаційній безпеці та забезпечення інформації безпеки забезпечити механізм для. В інформаційній галузі забезпечує послідовну систематичну діяльність, низку заходів та державні та правоохоронні органи, які забезпечують належну реалізацію національних інтересів держави. пов’язані людські інтереси та суспільство, запобігання недолікам інформації та їх швидке вирішення. З огляду на активну глобалізацію інформаційно-комунікаційних мереж, співпраця важлива не лише для банку, держави, але й для міжнародних організацій у боротьбі з агресією різних держав.

РОЗДІЛ 2. Захист та ризики інформаційної безпеки банку

Проектування системи захисту інформації

2.1 Захист інформації банку

Основним способом захисту інформації вважається впровадження так званих засобів ААА або 3А (authentication , authorization, administration- автентифікація , авторизація, адміністрування) Серед засобів ААА значне місце займають апаратно- програмні системи ідентифікації та автентифікації(СІА) до пк.

При використанні СІА співробітник отримує доступ до пк або в кооперативну мережу тільки після успішного проходження процедури ідентифікації і автентифікації. Ідентифікація полягає в розпізнаванні користувача по властивій йому ознаці або по наданій йому ідентифікаційній ознаці. Перевірка належності користувачеві представлено їм ідентифікаційної ознаки здійснюється в процесі автентифікації

Сучасні СІА по виду використовуваних ідентифікаційних ознак поділяються на електронні, біометричні, комбіновані та разові паролі (рис 1)

Рис 1 Класифікації систем ідентифікації та автентифікації

Підсистема захисту від шкідливого програмного забезпечення

Згідно з чисельними дослідженнями на сьогоднішній день найпоширенішою і той , що завдає найбільших збитків, інформаційною загрозою є віруси , «троянські коні», утиліти- шпигуни і інше шкідливе програмне забезпечення Для захисту від нього використовуються антивіруси.

Причому цим засобом забепечення безпеки повинен бути обладнаний кожен комп незалежно від того, підключений він до Інтернету чи ні.

Визнані в усьому світі антивірусні технології захищають комп`ютер від таких сучасних інформаційних загроз як:

- Віруси, троянські програми, черв`яки, шпигунські, рекламні програми та інше.
- Нові невідомі загрози , які швидко поширюються.
- Руткіти, буткіти та інші витончені загрози.
- Ботнети на інші незаконні способи

Підсистема резервного копіювання та архівування

Ця підсистема повинна виявляти всі атаки(на всіх рівнях) , спрямовані на конкретний вузол мережі. Також підсистема повинна мати можливість

проведення аналізу захищеності і виявлення вразливостей на контрольованому вузлі. Повинна контролювати журнали реєстрації ОС, а також журнали реєстрації будь-яких додатків, що функціонують під управлінням цих ОС. Крім того, необхідно виявлення атак в мережах TCP,IP I SMB/NetBios, побудованих на базі будь-яких мережевих архітектур, підтримуваних контрольованим комп`ютером.

Підсистема захисту інформації в локальних обчислювальних мережах

Підсистема захисту інформації в локальних обчислювальних мережах повинна складатися з наступних механізмів захисту

- Посилена ідентифікація і автентифікація
- Повноважне і виборче розмежування доступу
- Замкнуте програмне середовище
- Криптографічний захист даних
- Інші механізми захисту

Адміністратору безпеки має надаватися єдиний засіб управління всіма захисними механізмами, що дозволяє централізовано керувати і контролювати виконання вимог політики безпеки

Вся інформація про події в ІС, що мають відношення до безпеки , повинна реєструватися в єдиному журналі реєстрації. Про спроби скоєння користувачами неправомірних дій адміністратор безпеки повинен дізнаватися негайно.

Також повинні бути засоби генерації звітів, попередньої обробки журналів реєстрації, оперативного управління віддаленими робочими станціями

Краще використовувати клієнт-серверну архітектуру даної підсистеми, при якій серверна частина забезпечує централізоване зберігання і обробку даних системи захисту, а клієнтська частина забезпечує захист ресурсів робочої станції або сервера і зберігання управляючій інформації у власній базі даних.

Сервер безпеки с цьому випадку встановлюється на виділений комп`ютер або контролер домену і забезпечує вирішення наступних завдань:

- Ведення центральної бази даних (ЦБД) системи захисту, що містить інформацію, необхідну для роботи системи захисту.
- Збір інформації про події, що відбуваються з усіх клієнтів в єдиний журнал реєстрації та передача обробленої інформації підсистемі управління .
- Взаємодія підсистемою управління та передача керуючих команд адміністратора на клієнтську частину системи захисту.

Підсистема управління в цьому випадку встановлюється на робочому місці адміністратора безпеки і надає йому такі можливості :

- Централізоване управління захисними механізмами клієнтів.
- Контроль всіх подій, що мають відношення до безпеки ІС.
- Контроль дій співробітників в інформаційній системі організації та оперативне реагування на факти і спроби несанкціонованого доступу.
- Планування запуску процедур копіювання ЦБД та архівування журналів реєстрації.

Подібна схема керування дозволяє управляти інформаційною безпекою в термінах реальної предметної області в повній мірі забезпечити жорсткий розподіл повноважень адміністратора мережі і адміністратора безпеки.

Підсистема забезпечення цілісності даних

Цілісність інформаційної бази будь-якої організації, як правило, забезпечується за допомогою механізмів, які вбудовані, в використану , в даній організації, систему управління базами даних.

Підсистема реєстрації та обліку

Ця підсистема повинна дозволяти переглядати список активних користувачів , тобто тих користувачів, які в даний момент працюють з інформаційною базою. Крім того, необхідно виконання аналізу журналу реєстрації дій, виконуваних користувачами за будь-які періоди часу (історію роботи користувачів). Також необхідна функція архівування журналу реєстрації, з можливістю подальшого його використання.

На цьому найвищому рівні процедури безпеки та контролю починаються з політики безпеки, яка є всеосяжним планом, який допомагає захистити підприємство як від внутрішнього, так і від зовнішнього і повинні відповідати ISO 17799, міжнародним стандартам інформаційної безпеки, що встановлюють найкращі практики безпеки . Цей стандарт включає десять основних розділів: політика безпеки, контроль доступу до системи, управління комп'ютером та , розробка та технічне обслуговування, фізична та екологічна безпека, відповідність , особиста безпека, організація безпеки, управління класифікацією та контролем та управління безперервністю бізнесу. Сучасна тенденція в практиці безпеки полягає у об'єднанні фізичної та логічної безпеки в організації.

Фізична безпека - це будь-які заходи, які організація використовує для захисту своїх об'єктів, ресурсів, або власні дані , які зберігаються на фізичному носії, а логічна безпека використовує технологію для обмеження доступу до систем організації та інформації лише для уповноважених осіб. На додаток до цих процедур безпеки, керівництво повинно мати контроль над людськими ресурсами та ресурсами даних фірми Ці елементи керування на рівні організації настільки важливі, оскільки вони часто мають повсюдний вплив на багато інших елементів керування, таких як загальні засоби управління IT та засоби контролю на рівні додатків.

У світлі того факту, що природні та техногенні катастрофи стають все частішими, фірми та організації будь-якого розміру тепер повинні навмисно розробити та протестувати план відновлення після катастроф на підтримку загального контролю. Крім того, згідно з Rainer & Cegielski , надійний план резервного копіювання має вирішальне значення для інформаційної безпеки, і цей процес для малого бізнесу є більш важливим, оскільки будь-яка втрата даних може означати втрачено клієнтів

У багатьох випадках ця інтеграція вирішує дві великі проблеми. По-перше, інтегровані географічно розподілені підсистеми.

По-друге, користувачі Інтернету мають доступ до відкриття даних LSI. Часто обидва завдання використовують веб-сайт. Практика показує, що робота веб-сайту суттєво впливає на ефективність всієї AIC. Основою веб-сайту є веб-сервер, який забезпечує клієнтів доступ через мережу до веб-сторінки.

Ви можете знайти цей підроблений сайт точно таким же, як оригінальний, де ви легко зможете передати свої дані безпеки хакеру чи шахраю. Як можна уникнути фішингу , перелічено нижче:

По-перше, жоден банк ніколи не надсилатиме лист із запитом про ваш номер безпеки та пароль. Якщо ви отримуєте електронну пошту від свого банку, якою б терміновою ніколи не була на ній інформація про безпеку. Завжди телефонуйте до номера телефону банку, щоб перевірити, чи потрібна їм ця інформація.

По-друге, якщо ви підозрюєте, що це шахрайство, поштою перешліть його до банку, який повідомляє про це шахрайство.

Перевірте сайти банку безпеки: ніколи не слід натискати гіперпосилання або переходити за посиланням, щоб перейти на домашню адресу банку в Інтернеті. Завжди вводити в браузері всю адресу URL-адреси вашого банку. Перевірте , чи сайт банку починається з „https“ та чи є значок замку в нижній частині вашого браузера . Коли ви двічі клацаєте на піктограмі навісного замка, з’являється інформація про замок, яка допоможе підтвердити, чи справжній цей сайт. Якщо замок недійсний або був виданий веб-сайту, який ви не розпізнаєте, не вводьте інформацію про свою безпеку.

Вхід і вихід: Нікому не повідомляйте свій ідентифікатор безпеки та пароль щоб уникнути шахрайства. Не залишайте комп’ютер або ноутбук без нагляду, поки ви все ще ввійшли у свій Інтернет-банк. Завжди виходити з облікового запису , коли сеанс закінчується. Уникайте зберігання ідентифікатора та пароля безпеки на своєму комп’ютері та завжди зберігайте їх у безпечному місці. Також не змінюйте дані безпеки, коли ви користуєтесь комп’ютером у громадському місці.

Істотна частина проблем забезпечення захисту інформації в ІС може бути вирішена організаційними заходами. Тому в попередній лабораторній роботі було вказано чітке розмежування обов'язків та прав посадових осіб на підприємстві, а також Інструкції та Положення щодо правил поведінки з апаратурою для забезпечення конфіденційності та цілісності даних і визначення приватної таємниці.

В якості зміни організаційних заходів та їх суттєвого поліпшення було виконані наступні заходи.

Робота з соціальним фактором.

a. Компартменталізація (обмеження доступу) інформаційної безпеки
   - «Ні» вільному доступу до внутрішніх систем організації для всіх співробітників, включаючи довірених осіб.
   - Надання паролів і логінів тим працівникам, які в цього по-справжньому потребують.
   - Визначення, в яких ситуаціях дійсно потрібно обмінюватися цінною корпоративною інформацією з підлеглими і між підлеглими, щоб не робити цього без необхідності.
b. Лікбез по інформаційної безпеки
   - Проведення семінарів з підвищення знань співробітників в області кібербезпеки.
   - Проведення курсу з безпечного використання мобільних пристроїв і захисту від фішингу.
   - Проведення обговорень останніх потенційних IT-загроз для підприємства.
   - Донесення до відома співробітників, яка відповідальність послідує за випадкові витоки і навмисні корпоративні «зливи» третім особам.

Розповсюдження корпоративної інформації співробітниками.

На думку експертів, для усунення загрози витоку інформації організація повинна вжити ряд дій:

1. Визначити і задокументувати всі привілейовані акаунти в системі, кому вони належать і які взаємозалежності мають між собою.

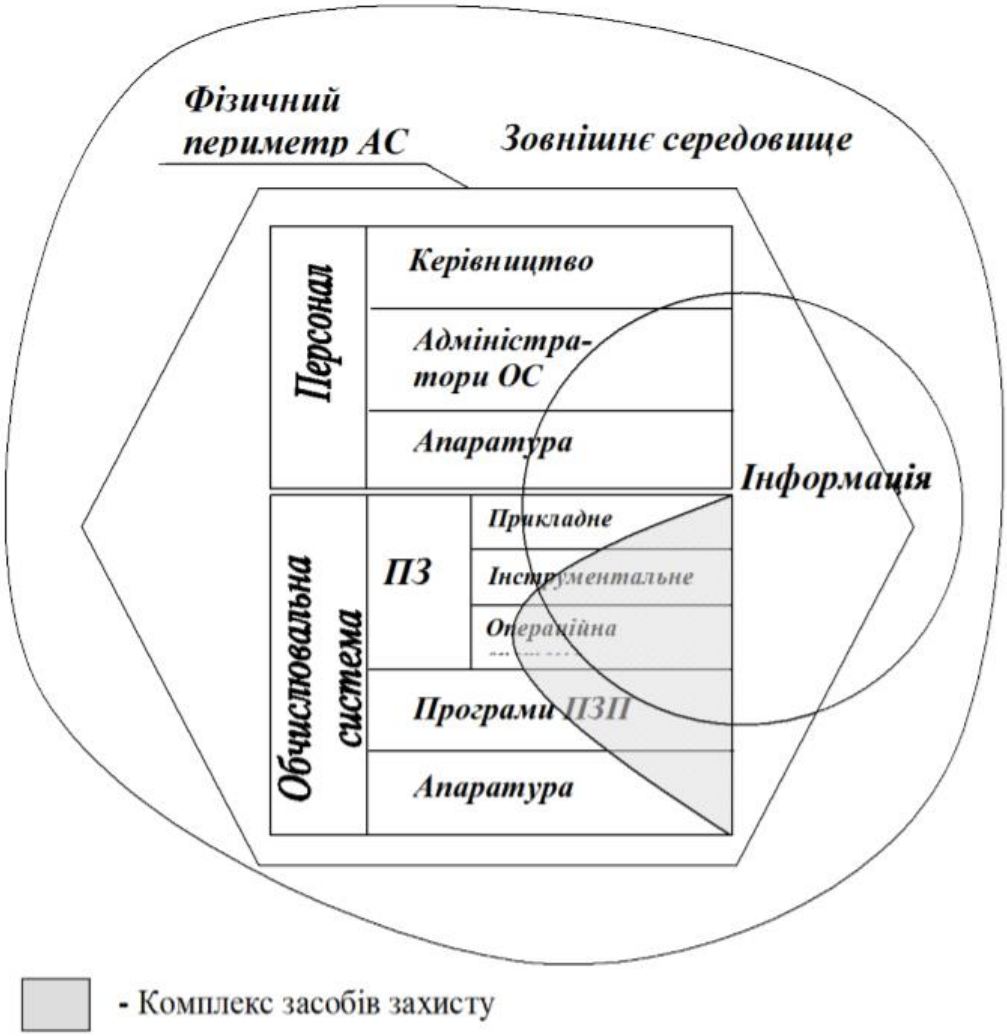
2. Делегувати доступ до привілейованих акаунтів тільки відповідним співробітникам, використовуючи мінімально можливу кількість привілеїв.

3. Встановити правила по мінімальної складності паролів і частій зміні складу паролів, після чого синхронізувати зміни по всім взаємозалежності.

4. Провести аудит і переконатися, що кожна сесія з привілейованого акаунту правильно задокументована, із зазначенням тривалості сесії і її причини, при цьому запис недоступна для фальсифікацій.

Основні напрями захисту

Автоматизована система - це організаційно-технічна система, яка поєднує в собі комп’ютерну систему, фізичне середовище, персонал та оброблену інформацію . Прийнято розрізняти два основні напрямки ТСІ у динаміку - захищати динамік та оброблювану інформацію від несанкціонованого доступу та захищати інформацію від витоків технічних каналів (оптичних). , акустичний, захист від каналів витоку
Набір ND, що базується на ньому, присвячені організації захисту від NSD та побудові пристроїв захисту від NSD. працює як частина акустичної комп’ютерної системи. Організаційні та фізичні заходи захисту, включаючи захист від фізичних компонентів операційної системи NSD-OS та витоку через технічні канали1 , не розглядаються. Проте презентація також зосереджена на деяких нетехнічних аспектах, але лише там, де це впливає на оцінку технічної безпеки.



З точки зору методології проблеми захисту інформації від NSD, слід розділити два напрямки: підтримка інформації, що працює в операційній системі АС, та оцінка захисту даних;

Впровадження та оцінка пристроїв вхідного захисту, отриманих із складу компонентів, що будують комп'ютерну систему АС зовні (програмні продукти, комп'ютерне обладнання тощо) для даного робоче середовище.

Кінцевою метою всіх заходів щодо захисту інформації є забезпечити безпеку інформації під час обробки в АС. Захист інформації повинен забезпечуватися на всіх етапах життєвого циклу АС, на всіх технологічних стадіях обробки інформації та у всіх режимах роботи.

Життєвий цикл АС включає розробку та впровадження експлуатації

Якщо обробка інформації планується в АС, порядок обробки та захисту яких регулюється законодавством України або іншими нормативними актами (наприклад, інформація, що становить державну таємницю), щоб обробляти таку інформацію в цьому АС, ви повинні мати дозвіл відповідного уповноваженого державного органу. Підставою для видачі такого дозволу є завершення тестування на АС, тобто перевірка відповідності запровадженого ІВІ встановленим стандартам.

Якщо процедура обробки та захисту інформаційних даних не регулюється законом, розслідування за бажанням може бути проведено шляхом подання замовнику (АС або власника інформації) .

Аналіз супроводжується оцінкою пристроїв захисту, реалізованих в операційній системі ОС. Захист NSD, реалізований в комп'ютерній системі, вважається підсистемою захисту NSD на ІСНУ в межах. Фізичне середовище, персонал , оброблена інформація та характеристики організаційної підсистеми суттєво суттєво впливають на вимоги до функцій безпеки, що виконуються операційною системою. Апаратне, програмне забезпечення (включаючи програми для ПЗУ) призначене для обробки інформації. Усі компоненти операційної системи можна розробити та продати як незалежні продукти. Кожен із цих компонентів здатний виконувати певні функції захисту інформації, які можна оцінити незалежно від процесу тестування АС та мають оцінки . За результатами сертифікації видається сертифікат відповідності впровадженого засобу захисту відповідним вимогам (критеріям). Наявність сертифіката для комп'ютерної системи АС чи її компонентів може полегшити процес перевірки АС.

Під час оцінки як перевіреної, так і впровадженої сертифікації. функція інформаційної безпеки відповідно до встановлених критеріїв. Ці критерії викладені в ND TZI 2.5-004-99 "Критерії оцінки безпеки даних у комп'ютерних системах від несанкціонованого доступу" З метою стандартизації критеріїв та забезпечення можливості застосування як у процесі перевірки АС (тобто при

оцінці функцій захисту інформації , реалізованої автоматизованою операційною системою системи, яка знаходиться в функція і коли сертифікує програмне та апаратне забезпечення за межами певного операційного середовища, обидві категорії поєднуються з поняттям комп'ютерної системи. КС слід розуміти як набір програмного та апаратного забезпечення, представленого для оцінки

Концепція забезпечення захисту інформації

Інформація в КС існує у формі даних, тобто вона подається у формалізованій формі, придатній для обробки . Далі, під час обробки , сама обробка, а також вхід, вихід, зберігання, передача тощо. Це треба розуміти. (ДСТУ 2226-93). Надалі терміни "інформація" та "дані" використовуються як взаємозамінні.

Для існування інформації завжди потрібен носій інформації. Поле чи матеріал можуть виступати носієм інформації . У деяких випадках людину можна вважати носієм інформації. Втрата інформації (порушення безпеки інформації) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія інформації в КС, як правило, лише інформаційних об'єктів, які діють як приймаються / приймаються дані та потоки інформації (фрагментів інформації, що передаються між об'єктами), незалежно від фізичних загроз інформації, що обробляється в АС, залежно від характеристик операційна система, фізичне середовище, персонал та оброблена інформація. Загрози можуть бути об'єктивними, наприклад, зміни у фізичному середовищі (пожежа, повінь тощо), збої в операційній системі або суб'єктивні, наприклад помилки персоналу або дії зловмисника.

Суб'єктивні загрози можуть бути випадковими або навмисними. Спроба погрози називається атакою, і інформація доступна.

Інформація обробляється конфіденційно, якщо ми дотримуємося встановлених

правил доступу. Інформація збереже свою цілісність, якщо відповідає встановленим правилам її модифікації (видалення). Інформація надалі буде доступною, якщо її можна переглянути або змінити відповідно до встановлених правил протягом будь-якого зазначеного (невеликого) періоду. Погрози, реалізація яких призводить до втрати інформації щодо будь-якого з цих властивостей, є загрозою конфіденційності, цілісності або доступності цієї інформації.

Загрози можуть впливати на інформацію. Побічно. Наприклад, втрата контролю над КС може призвести до того, що КС не зможе забезпечити захист інформації, і як наслідок, деякі властивості оброблюваної інформації можуть бути втрачені.

2.2 Оцінка ризиків Інформаційної безпеки банку

Оцінка ризиків порушення інформаційної безпеки комп`ютерних систем є однією з найважливіших складових процесу управління інформаційною безпекою.

Ризик - це потенційна небезпека заподіяння шкоди підприємству в результаті реалізації певної загрози з використанням наявних вразливостей.

Ризик визначається як поєднання ймовірності події та її наслідків.

Аналіз ризиків – це процедури виявлення факторів ризиків і оцінки їх значущості, по суті, аналіз ймовірності того, що відбудуться певні небажані події і негативно вплинуть на досягнення цілей підприємства. Аналіз ризиків включає оцінку ризиків і методи зниження ризиків або зменшення пов`язаних із цим несприятливих наслідків, тобто ідентифікацію та обчислення рівнів (міри) ризиків на основі оцінок, що присвоєні ресурсам, загрозам та вразливостям ресурсів.

Аналіз ризиків можна поділити на два види, що взаємно доповнюють один одного: якісний та кількісний. Якісний аналіз має на меті визначити (ідентифікувати) чинники, області та види ризиків. Кількісний аналіз ризиків повинен дати можливість чисельно визначити розміри окремих ризиків і ризику підприємства в цілому.

Контроль ризиків полягає в ідентифікації та виборі контрзаходів, що дозволяють знизити ризики до прийнятного рівня.

Метою аналізу ризиків є оцінка загроз та вразливостей, визначення контрзаходів , які забезпечують належний рівень безпеки інформаційної системи. Процес оцінки ризику також спрямований на визначення характеристик ризику інформаційної системи та її ресурсів.

На основі таких даних можна вибрати необхідні запобіжні заходи.

Існують різні підходи до оцінки ризиків, вибір яких залежить від рівня вимог до режиму інформаційної безпеки (ІС) для організації

Зазвичай процес оцінки ризику складається з декількох етапів:

• опис об’єкта

• ідентифікація ресурсу та оцінка його кількісних показників (виявлення потенційного негативного впливу щодо бізнесу у разі пошкодження), втрати, крадіжки тощо);

• аналіз загрози

• оцінка вразливості;

• оцінка ефективності використання існуючих та запланованих інструментів інформаційної безпеки;

• оцінка ризику за результатами всіх попередніх пунктів.

Ризик описує загрози, яким піддається система та організація, що використовуються . і залежить від:

• показників вартості ресурсу;

• оцінка значущості загроз;

• оцінка значущості вразливостей;

• ймовірність пошкодження ресурсів (спричинених загрозами ресурсів);

• ступінь використання вразливостей перед загрозами (вразливості);

• ефективність використання існуючих або запланованих інструментів для надання ІС.

Розрахунок цих показників базується на математичних методах, які мають такі характеристики, як виправдання методу та параметри точності.

Залежно від класу, інформаційна система повинна мати певні формальні характеристики підсистеми безпеки

Залежно від того, як власники оцінюють цінність своїх джерел інформації та можливі наслідки порушення інформаційної безпеки, для аналізу ризиків використовуються два підходи:

• базовий аналіз ризиків;

• повний аналіз ризиків.

Базовий аналіз ризику передбачає, що цінність захищених ресурсів не надто висока для точки зору організації (не оцінюється), і що аналіз ризиків проводиться за спрощеною схемою : найпоширенішу безпеку звичайного набору загроз (віруси, несправності пристроїв, несанкціонований доступ тощо) слід розглядати без оцінки їх вірогідності. У цьому випадку вказано мінімальний або базовий рівень ІС (тобто характеристики загрози не потрібні).

Повний аналіз ризиків вимагає:

• визначає вартість ресурсів,

• додає до стандартного набору перелік загроз, що мають відношення до розглянутої інформаційної системи ;

• оцінити ймовірність загроз;

• визначає вразливості ресурсів;

• Запропонуйте рішення, яке забезпечує необхідний рівень ІС.

Спочатку потрібно розділити всі захищені ресурси на класи.

• фізика;

• програмне забезпечення;

• дані (інформація).

Кожен клас повинен мати свій власний метод оцінки вартості предметів, який допомагає вибрати відповідний набір критеріїв предметів. Ці критерії описують будь-яку шкоду, яка може спричинити порушення конфіденційності та цілісність інформаційної системи та рівень їх доступності відновлення. Потім ці виміри витрат перетворюються на шкалу ранжування (якості), яка також використовується для

джерел інформації.

Програмні ресурси оцінюються відповідно до визначення {{так само, як і фізичне визначення. вартість для : якщо існують спеціальні вимоги щодо конфіденційності або цілісності джерела інформації, ресурс оцінюється за тією ж схемою, тобто з точки зору .

Залежно від профілю організації, в якій використовується інформаційна система, можуть застосовуватися інші критерії.

Джерела слід аналізувати на предмет можливих атак

(заплановані дії) внутрішніх або зовнішніх зловмисників) та різних побічних явищ, що трапляються в природі. Такі потенційно можливі події називаються загрозами безпеці.

Уразливості - це вразливості системи безпеки, що дозволяють виникати загрози.

Фактори:

• привабливість ресурсів (цей показник враховується при розгляді загрози).

- Використання ресурсу

Проведемо оцінку ризику системи безпеки , результати зведемо в таблицю :

Основним етапом при захисті інформації в інформаційних системах є аналіз ризиків.

Імовірність того, що загроза реалізується, визначається наступними основними факторами:

- привабливістю ресурсу (цей показник враховується при розгляді загрози навмисного впливу з боку людини);
- можливістю використання ресурсу для отримання доходу (показник враховується при розгляді загрози навмисного впливу з боку людини);
- простотою використання уразливості при проведенні атаки.

Для оцінки ймовірності настання загрози професіоналами застосовується якісна шкала, що складається з трьох рівнів. Розглянемо їх докладніше.

Рівень 1 - Н («низька ймовірність»)

Відрізняється мінімальної ймовірністю появи. У такої загрози немає ніяких передумов (минулих інцидентів, мотивів) для того, щоб вона була реалізована. Загрози рівня Н, як правило, виникають не частіше, ніж 1 раз в 5 - 10 років.

Рівень 2 - С («середня ймовірність»)

У такої загрози ймовірність виникнення трохи вище, ніж у попередньої, тому, що в минулому, наприклад, вже були подібні інциденти або відомо, що атакуюча сторона має плани по реалізації такої загрози. Загрози з рівнем С призводять до реальних інцидентів приблизно раз на рік.

Рівень 3 - В («висока ймовірність»)

Загроза має високі шанси на реалізацію. На підтвердження тому - статистична інформація, наявність подібних інцидентів в минулому, серйозна мотивація з боку зловмисників. Ймовірна частота виникнення загроз рівня В – раз на тиждень або частіше.

Таблиця 1. Оцінка ризиків існуючої системи безпеки підприємства

підприємства

Назва загрози	**Імовірність настання**	**Збиток від реалізації**	**Ризик**
Стихійні лиха, аварії, пожежі	1	3	3
Перебої електроживлення	1	3	3
Шкідливе програмне забезпечення	3	2	6
Халатність користувачів («погані» паролі, пропуск оновлення системи і т.д.)	1	3	3
Розповсюдження корпоративної інформації співробітниками	2	3	6
Злом та проникнення на територію підприємства сторонніх фізичних осіб	1	3	3
Атаки на домашні робочі місця з боку зловмисників	2	3	6
Несанкціонований доступ користувачів до тих даних, до яких у них не має прав	1	2	2
Неспроможність апаратних і програмних засобів протистояти зовнішнім загрозам	2	3	6
Сума ризиків:	38		

Атаки на домашні робочі місця. На «удаленке» інформаційна безпека співробітника залежить тільки від нього самого. За даними Positive Technologies, до кінця 2020 роки втричі зросла кількість атак, які експлуатують уразливості інтернет-сервісів для роботи. Популярний сценарій - викрадення облікових даних для підключення до корпоративних систем і отримання

несанкціонованого доступу до робочих конференцій. За прогнозами, кількість таких атак буде збільшуватися.

Шкідливе програмне забезпечення. Класичний вірус модифікує файли і створює в них свої (не обов'язково схожі один на одного) копії, а черв'яки поширюються по комп'ютерних мережах і іншим засобам комунікацій, але файлів при цьому не заражають і не модифікують. А ось з приводу шпигують програм (spy software) думки розходяться: одні виробники зараховують до них все шкідливі коди, службовці для крадіжки конфіденційної інформації, стеження за інтернет-звичками користувачів і т. Д .; а інші розуміють під ними лише відносно нешкідливі "фіксатори" інтернет-звичок користувачів і рекламне ПО. При цьому викрадачі паролів і різної банківської інформації виділяються в окремий клас шкідливих кодів. Під Троєю ж зазвичай розуміються програми, що проникають на комп'ютер під виглядом цілком корисних утиліт. А ще бувають боти (віруси-роботи, керовані в дистанційному режимі і використовуються для проведення DoS-атак, крадіжки конфіденційної інформації та інших непорядних цілей), "руткіти", "бекдори" і багато інших класи шкідливих кодів. Всі їх перерахувати практично неможливо.

Перебої електроживлення (проблеми електроживлення). Електроенергія забезпечує можливості для нашої роботи. Відсутність електроенергії навіть на невеликий час може завдати нам значної шкоди. Чисте електроживлення - це таке електроживлення, в якому відсутні перешкоди і перепади напруги. Можливими видами перешкод в електромережі є електромагнітні перешкоди (EMI - electromagnetic interference) і радіочастотні перешкоди (RFI - radio frequency interference). EMI можуть створюватися за рахунок різниці потенціалів між трьома проводами: напругою, нейтрал'ю і землею, або за рахунок впливу магнітних полів. Блискавка або електричні мотори можуть також викликати EMI, які, в свою чергу, можуть порушити нормальний перебіг електричного струму в електромережі всередині будівлі, а

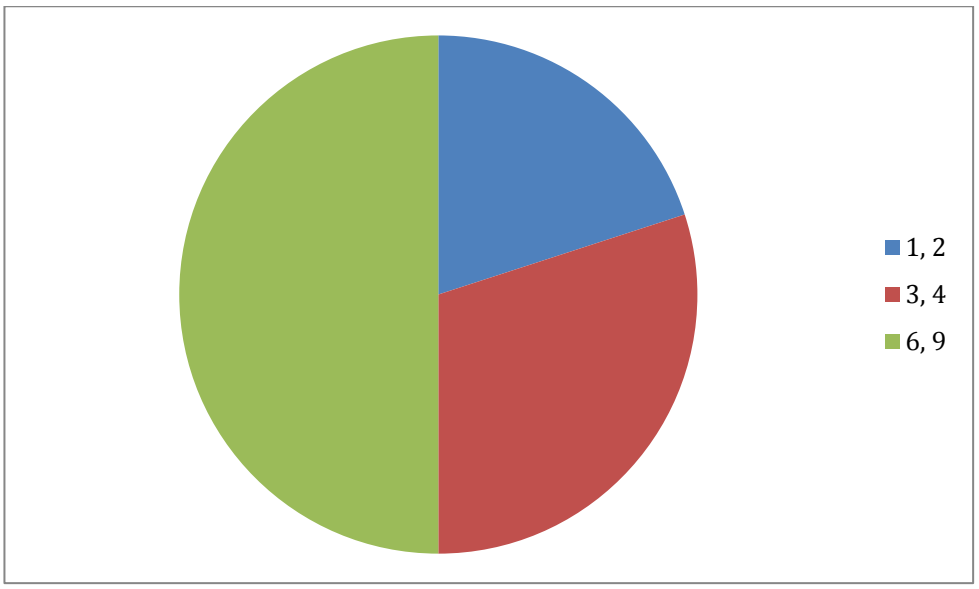
також в лінії електропередачі до або після будівлі. RFI можуть бути викликані будь-яким пристроєм, що створює радіохвилі. В даний час однією з основних причин, що викликають RFI в будівлі, є люмінесцентні лампи. Для вирішення цієї проблеми ви можете відмовитися від використання люмінісцентні освітлення, або використовувати екранованим проводом. Електричні дроти і дроти комп'ютерної мережі не слід прокладати в безпосередній близькості від люмінесцентних ламп. Перешкоди порушують нормальний рух електричного струму і можуть викликати перепади напруги (тобто величина напруги буде відрізнятися від очікуваної). будь перепад напруги може привести до пошкодження обладнання та травм людей.

Халатність користувачів. Нерідко співробітникам доручають завдання зареєструватися в якомусь сервісі в інтернеті, тому що керівнику нема коли або лінь розбиратися? Звичка поспішати і передоручати навіть відповідальні завдання призводить до того, що в попихах паролі вибираються найпростіші – складні можуть загубитися і забутися. Набір «123456» або пара логін: пароль «імясайту: імясайту» до сих пір «в топі». Навіть найпотужніша система інформаційної безпеки для хакера з такими паролями виявиться незакритими дверима сейфу. Йому нічого не залишається, крім як перевірити – чи не замкнений він. Якщо системний адміністратор або відповідальна за ПО в організації особа вчасно не встановить оновлення, то виявлені розробниками помилки рано чи пізно опиняться інструментом в руках зловмисника. Корпоративний шпигунство має успіх там, де сисдамін не виконує сумлінно свої обов'язки.

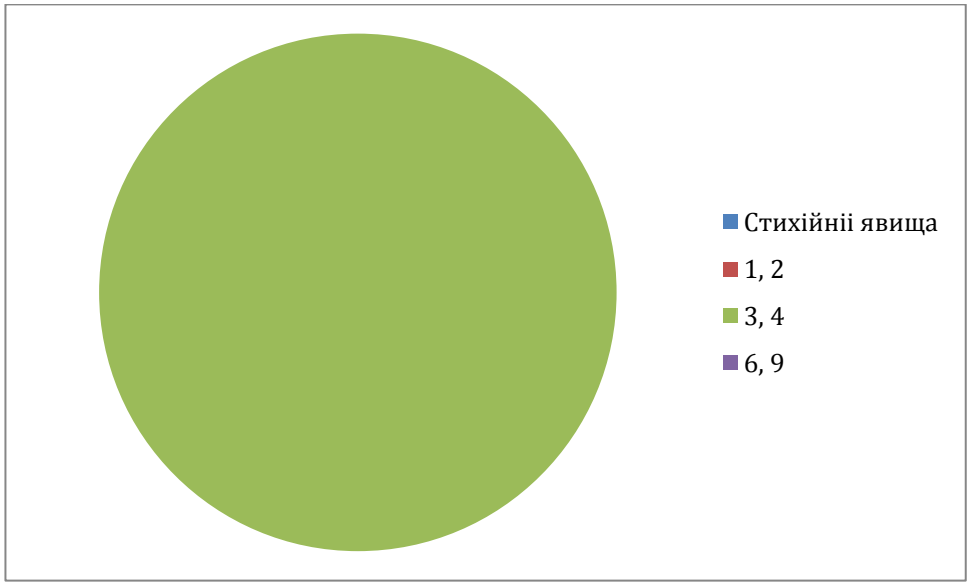
Несанкціонований доступ користувачів до тих даних, до яких у них не має прав, та розповсюдження корпоративної інформації співробітниками. Мораль і лояльність до роботодавця у IT-співробітників не надто висока. Програмісти, системні адміністратори тощо часто можуть безперешкодно

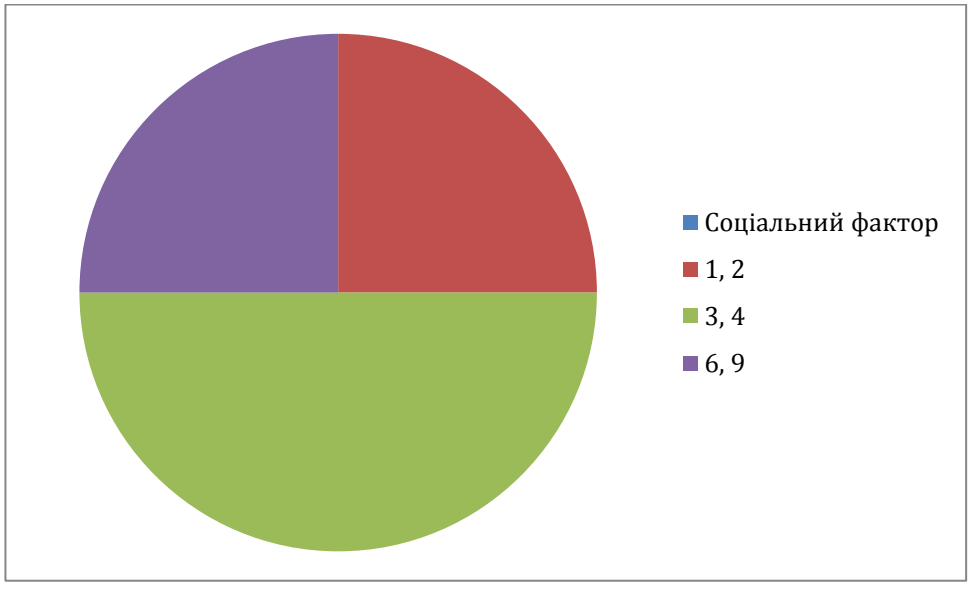
досліджувати корпоративну мережу своєї компанії, отримати доступ до важливих документів - і ніхто цього не виявить. У 68% випадків співробітники IT-відділу мають більше привілеїв в корпоративній мережі, ніж співробітники фінансового відділу, HR-відділу або менеджери компанії. Такі результати отримала компанія Lieberman Software в результаті опитування більше 450 комп'ютерщиків. Опитування показало також, що 39% співробітників IT-відділів мають фактичну можливість доступу до конфіденційних файлів, до яких їм не належить мати доступ, а кожен п'ятий вже користувався цією можливістю. Кожен дев'ятий (11%) зізнався, що в разі загрози звільнення він готовий порушити права доступу і пошукати в корпоративній мережі список співробітників, які будуть звільнені - і перевірити, чи є там його ім'я. Комп'ютерщики готові залишити за собою й іншу корпоративну інформацію, якщо бачать таку необхідність. Наприклад, якщо їм заздалегідь відомо про звільнення, то 11% опитаних висловили готовність прихопити з собою частину корпоративних секретів. Близько третини респондентів сказали, що керівництво компанії не знає, як запобігти такій ситуації.

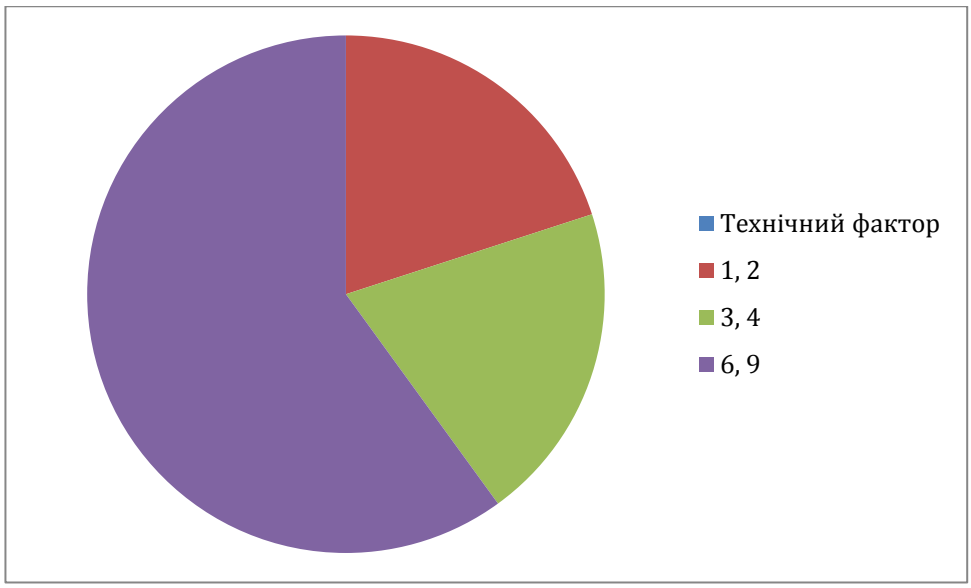
Злом та проникнення на територію підприємства сторонніх фізичних осіб. Природне управління доступом (natural access control) - це управління людьми, що входять і виходять з дверей, через огорож, з освітлених та інших місць. Управління доступом необхідно для обмеження і контролю можливостей переміщення людей з однієї зони безпеки в іншу. Управління доступом має стати практикою і для всіх входів та виходів з нього. Група розробки програми безпеки повинна врахувати всі можливі шляхи, якими порушник може потрапити в будівлю (наприклад, піднявшись на зростаюче поруч дерево, а з нього на дах, верхній балкон і вікно).



Діаграми відповідно до категорій:







Відповідно до отриманих діаграм можна зробити висновок, що рівень безпеки на високому рівні , а рівень технічних та соціальних ризиків – середній та низький рівень

2.3 Проектування та реалізація системи захисту інформаційної безпеки

Проектування невеликих мереж, як правило, не викликає труднощів. Кількість пристроїв в таких мережах і їх типів істотно менше в порівнянні з великими мережами. Топології таких мереж включають зазвичай один маршрутизатор, а також один або кілька комутаторів. Для з'єднання з Інтернетом в невеликої мережі зазвичай передбачається одне WAN-підключення, реалізоване за допомогою DSL-з'єднання, кабелю або Ethernet-з'єднання.

Для управління невеликими мережами потрібні переважно ті ж навички, що і для управління великими мережами. Основну частину роботи складають обслуговування, діагностика та усунення несправностей існуючого обладнання, а також забезпечення безпеки пристроїв і даних в мережі. Управління невеликою мережею здійснюється співробітником компанії або особою, залученими компанією на контрактній основі, в залежності від масштабу підприємства і його типу.

З метою відповідності вимогам користувачів навіть для невеликих мереж потрібне планування і проектування. На етапі планування розглядаються і враховуються всі вимоги, вартість та можливості впровадження. В рамках реалізації невеликої мережі при проектуванні необхідно в першу чергу враховувати тип проміжних пристроїв, які будуть використовуватися для підтримки мережі.

Налаштування мережі та її топологія:

1.1. всі комп’ютери мережі: початкова мережа складається 15-ти комп’ютерів, які розташовані в формі зірки, для можливого масштабування мережі в разі наймання нових співпрацівників.

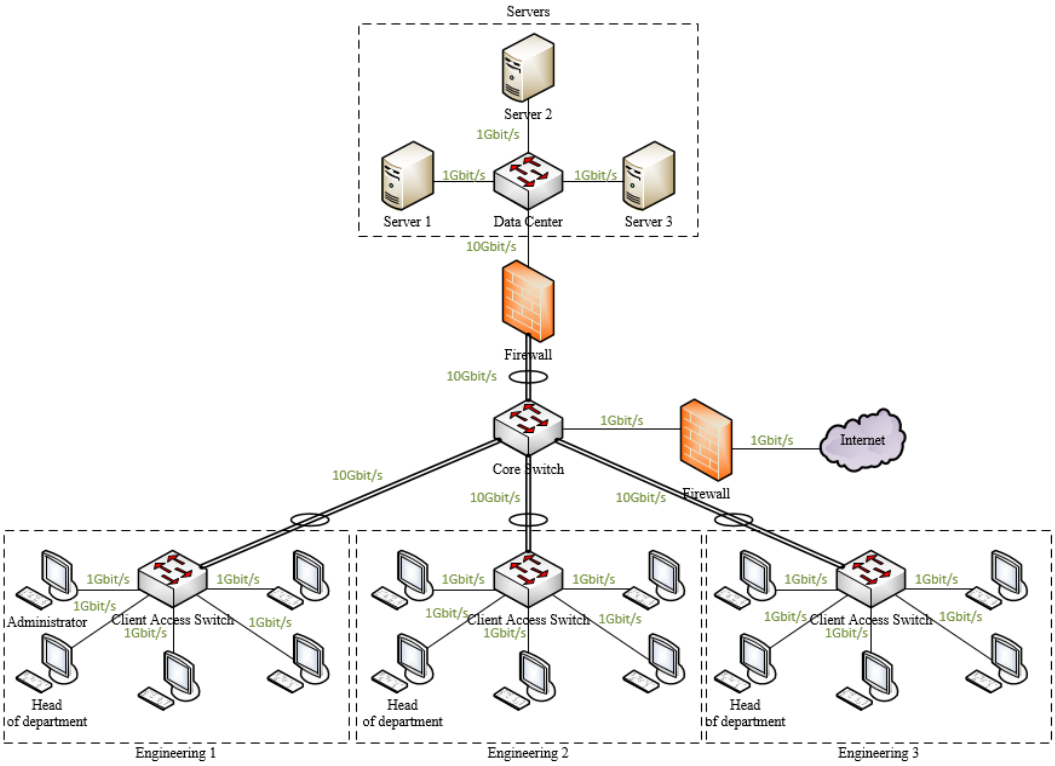
1.2. всі пристрої (в тому числі і мережеві), необхідні для функціонування локальної та глобальної мереж: в якості мережевий пристроїв використовується 5 комутаторів; вони різних типів: 3 комутатори доступу (дозволяють зменшити навантаження на комутатор

доступу; використовуються для встановлення «контакту» з іншими вузлами в мережі).

1.3. вказати за якою технологією організована локальна мережа фірми: локальна мережа реалізована за допомогою технології Ethernet 1Гб.

1.4. все обладнання, яке забезпечує на даний момент захист інформації в мережі даної фірми (не дуже високий, з перспективою *подальшого тестування та покращення):* для захисту інформації використовуються 2 брандмауери: між комутатором ядра (для забезпечення внутрішньої безпеки) і центром обробки даних (для забезпечення безпеки ввід зовнішніх загроз).

Логічна схема представляє собою наступне відповідно до вищесказаного:



Також ватро зазначити, що в даній схемі використовується комутатор ядра третього рівня, на якому встановлений DHCP-сервіс, який здійснює динамічне розподілення всіх IP-адрес. Для серверів та Адміністративної групи IP-адреси виділяються статично. Для кожної групи створений окремий VLAN,

для якого виділена маска /24. Перша адреса в кожній підмережі використовується в якості шлюзу за замовчуванням. Підмережі підприємства: 10.1.1.0/24, 10.1.2.0/24, 10.1.3.0/24.

З розвитком інформаційних технологій спостерігається тенденція зростання потреби застосування технічних заходів і засобів захисту. Тому для технічного захисту інформації в мережі були використані міжмережеві екрани як в самій локальній мережі для попередження несанкціонованого захисту від користувачів, так і для захисту від зовнішніх факторів.

Для підвищення фізичної безпеки необхідно забезпечити контроль доступу.

В якості мережевих пристроїв використовуються пристрої компанії Cisco, оскільки на ринку вони одні з найкращих.

Проведем порівняння комутаторів Cisco Catalyst C9200-24T і TL-SG1024DE

Для якості комутаторів шару доступу використовуються Cisco Catalyst C9200-24T. Характеристики:

	Cisco Catalyst C9200-24	**TL-SG1024DE**
Downlinks total 10/100/1000 or PoE+ copper ports	24 ports data	12 ports data
Uplink configuration	Modular uplink options	-
Default primary AC power supply	PWR-C6-125WAC	
Virtual Networks	4	2
Stacking bandwidth	160 Gbps	48Gbps
Total number of MAC addresses	32,000	8000
IPv4 routing entries	4,000	2,000
IPv6 routing entries	2,000	2,000
Packet buffer per SKU	6 MB buffers for 24- or 48-port	

	Gigabit Ethernet models , 12MB buffers for 24 or 48 port multigigabit models	
Flexible NetFlow (FNF) entries	16,000 flows on 24- and 48-port Gigabit Ethernet models	
DRAM	4 GB	4gb
Flash	4 GB	4GB
VLAN IDs	4096	4096
Wireless bandwidth per switch	Up to 48 Gbps on 24-port and 48-port Gigabit Ethernet model	24-port and 48-port Gigabit Ethernet model
Switching capacity	128 Gbps	128 gbps
Switch capacity with Stacking	288 Gbps	128 gbps
Chassis Dimensions	Inches: 1.73 x 17.5 x 13.8 Centimeters: 4.4 x 44.5 x 35.0	294x180x44

Для якості комутатора шару ядра використовуються Cisco Catalyst C9404R. Характеристики:

Total number of slots	4
Maximum Bandwidth scalability per line-card slot	Up to 480 Gbps on all slots
Power supplies supported	3200W AC, 2100W AC, 3200W DC
Cisco Catalyst C9404R chassis	80 Gbps/slot
10/100/1000BASE-T Gigabit (RJ-45) ports	96
Switched 10 Gigabit Ethernet ports	48
Switched 1 Gigabit	96

Ethernet ports	
Dimensions (H x W x D)	10.47 x 17.30 x 16.30 in. (26.53 x 43.94 x 41.40 cm)

В якості центра обробки інформації вибрано Cisco Nexus 3550-F.

Загальна інформація:

- Вага 11 кг (24 фунтів)
- Стандарт: 100-240 змінного струму змінного струму, 50-60 Гц
- Максимальне споживання: 150 Вт
- Робоча температура: від -5 ° C до 45 ° C
- Відносна вологість при експлуатації: від 5% до 90% (без конденсації)
- Відносна вологість при зберіганні: від 5% до 95% (без конденсації)

Підключення:

- 3 x 16 лінійних карт SFP +, до 48 портів
- 3x лінійні картки 4QSFP, до 12 портів (48x10G)
- SFP + волокно (10GBASE-SR, 10GBASE-LR, 10GBASE-LRM, 1000BASE-SX, 1000BASE-LX)
- SMA для PPS вхід / вихід
- SMA для GPS в
- Порт управління RJ45
- Стандартний послідовний порт RJ45
- USB

Управління:

- CLI через послідовний, SSH та telnet
- API JSON RPC для всіх команд CLI
- Автоматична конфігурація через DHCP
- TACACS + та підтримка для багатьох користувачів
- ACL на інтерфейсі управління
- Оновлення FW через SFTP, TFTP, HTTP та USB
- Вбудовані сценарії BASH та Python

- Вбудовані завдання Cron
- Синхронізація часу за допомогою PPS, GPS, PTP та NTP

Для захисту інформації використовуються 2 файєрволи: між комутатором ядра (для забезпечення внутрішньої безпеки) і центром обробки даних (для забезпечення безпеки ввід зовнішніх загроз). Для цього використані файєрволи Fortinet FG-80C

FG-80C містить в собі функціонал L2/L3 маршрутизатора, брандмауера, VPN-концентратора, антивіруса, антиспам-фільтра, web / content фільтра, системи виявлення вторгнень (IPS), а також додатково функції авторизації користувачів, віртуалізації і забезпечення відмовостійкості рішень. Управління та моніторинг може здійснюватися через WEB-інтерфейс, CLI (ssh, telnet), консоль, а централізоване управління - за допомогою пристрою FortiManager. Передбачено рольове управління декількома Адміністраторами, розмежування прав доступу, використання VDOM для управління віртуальними пристроями. Пристрій підтримує протоколи syslog, SNMP, може інформувати про події на e-mail. Збір, ведення журналів і формування звітів про події мережі тісно інтегровано з FortiAnalyzer.

Також, для підвищення рівня безпеки з боку програмного забезпечення було вирішено використовувати антивірус.

У безлічі мереж є маршрутизатори, міжмережеві екрани, системи виявлення вторгнень, антивірусне програмне забезпечення тощо. Кожен з цих компонентів реалізує певну частину безпеки, але всі вони повинні працювати спільно для забезпечення багаторівневого підходу до безпеки. Якщо компанія використовує антивірусне програмне забезпечення, але не оновлює бази вірусних сигнатур, це вразливість. Ризик в даному випадку – це ймовірність проникнення вірусу в мережу компанії і нанесення їй шкоди. якщо вірус проникне в мережу компанії, уразливість буде використана і компанія виявиться під впливом завданих ним збитків. Контрзаходами в цій ситуації

буде установка антивірусного програмного забезпечення на всі комп'ютери компанії і підтримка актуальності їх баз вірусних сигнатур.

Для вибору придатного антивірусу використовувались наступні критерії:

- Потужний захист від шкідливих програм. Всі рекомендовані мною програми мають перевірену захист від більшості розвинених шкідливих програм – не тільки від вірусів, але також від шпигунських програм, руткітів, програм-вимагачів і будь-яких інших програм, здатних нашкодити мені або моєму пристрою.
- Високоякісні функції. Більшість антивірусів надають додаткові функції забезпечення інтернет-безпеки, однак найчастіше це лише показні опції, які займають зайве місце на вашому комп'ютері і уповільнюють його роботу.
- Швидкість і ефективність. Кращі антивіруси не займають багато місця і не уповільнюють роботу операційної системи навіть на старих і бюджетних комп'ютерах.
- Зручність використання. Захист від вірусів потрібна як новачкам, так і професіоналам.

Ціна якість. Антивірус може коштувати не дешево. При оцінці я враховував всі важливі чинники, в тому числі наявність і якість функцій веб-захисту, кількість захищених пристроїв і наявність безкоштовної пробної версії і гарантії повернення коштів.

Для забезпечення конфіденційності інформації, що зберігається на персональних комп’ютерах, бентежить питання: який антивірус вибрати, які переваги чи недоліки того чи іншого антивірусного продукту. Ми зупинимось на найпопулярніших антивірусах, деякі з яких можуть забезпечити захист. Ми проводимо порівняльний аналіз наданих функцій, отримуємо краще розуміння антивірусів та оцінюємо, наскільки зручно їх налаштовувати та фактично використовувати.

Для порівняння я вибрав 3 антивіруси – Avira, Bitdefender Antivirus Free Edition, 360 Total Security Essentials.

Порівняння я виконав в таблицях

	Avira Free Antivirus	Bitdefender Antivirus Free Edition	360 Total Security Essentials
Антивирусный монитор	+	+	+
Поведенческий анализ	+	+	+
Антируткит	-	+	-
Эвристический анализ	+	+	+
Различные варианты сканирования	+	-	+
Сканирование при загрузке ПК	-	+	-
Система репутации файлов	-	-	-

Захист при роботі в інтернеті

Більшість користувачів, що встановлюють антивіруси, в першу чергу дбають про свою безпеку при підключенні до інтернету. Для одних можливість відключати набридливу рекламу є вкрай важливою

	Avira Free Antivirus	360 Total Security Essentials	Bitdefender Antivirus Free Edition
Веб-антивирус	+	+	+
Черный список URL	-	+	-
Репутация ссылок и веб-сайтов	+	-	-
Антибаннер	+	-	-
Антифишинг	+	+	+
Почтовый экран	-	-	-

Додаткових можливостей антивірусів

	Avira Free Antivirus	Bitdefender Antivirus Free Edition	360 Total Security Essentials
Оптимизация работы Windows	+	-	-
«Игровой» режим	-	-	-
Защита настроек антивируса паролем	+	-	-
Облачное сканирование подозрительных файлов	+	-	+
Пассивный режим	-	-	-
Защита веб-камеры	-	-	+

В порівняльній таблиці ми можемо побачити , що антивірус Avira є більш якісним в захисті і має значну перевагу серед інших антивірусів .
Тому, для захисту своєї системи безпеки буду використовувати цей антивірус і продемонструю його можливості більш детально.

Avira Free Antivirus

Антивірус, безкоштовний для особистого використання. Продукт включає резидентний монітор (який перевіряє процеси при їх спробі отримати доступ до файлів), сканер і програму автоматичного або ручного оновлення

Avira AntiVir Premium

Платна Premium версія персонального антивіруса має ряд переваг в порівнянні з безкоштовною версією, найбільш значні:

• поновлення через Інтернет виконуються набагато швидше (використовуються спеціальні сервери оновлень) і ефективніше (відсутній рекламне вікно і деякі інші обмеження);

• захист від сайтів з шкідливим кодом;

• є можливість перевірки вхідної та вихідної пошти за протоколами POP3 і SMTP.

За результатами тестів AV-Comparatives в лютому 2009 року Avira Premium 8.2 виявила 99,7% вірусів (друге місце), але отримала 2 зірки безпеки через те що посіла восьме місце в тесті на помилкові спрацьовування, а також посіла четверте місце в тесті на швидкість сканування.

Avira Internet Security

Пакет безпеки відрізняється від Premium тим, що були додані персональний Firewall, анти-спам, батьківський контроль (блокування сайтів, небажаних для перегляду дітьми), ігровий режим.

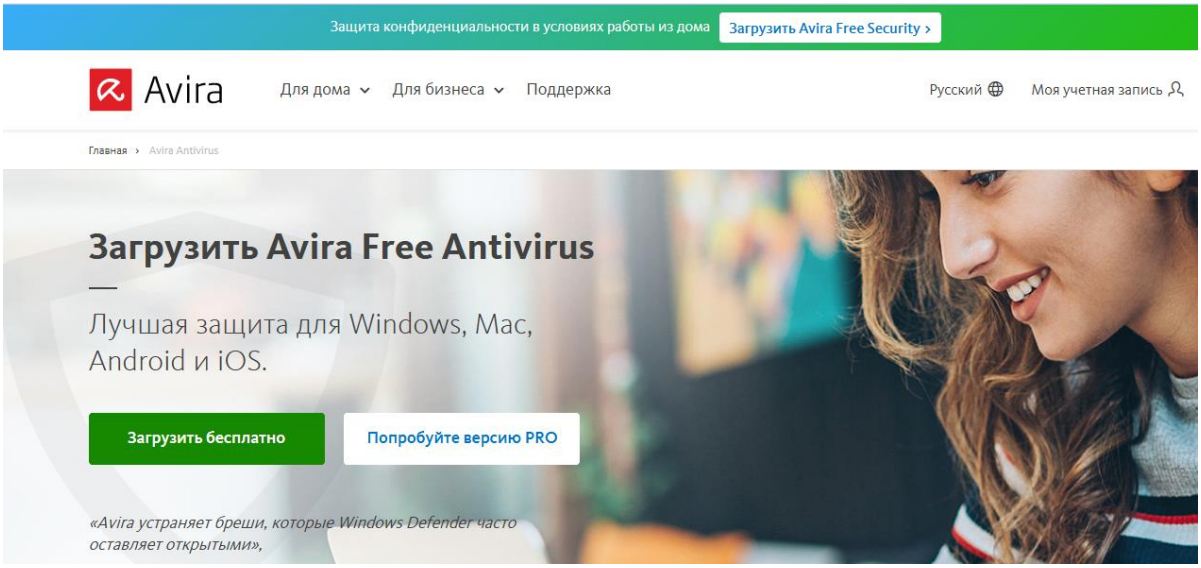
Avira Professional Security

Призначений для захисту робочих станцій при використанні їх в бізнесі. Він має всі можливості Avira AntiVir Premium і крім цього захищає комп'ютери в мережі.

Програма тестувань міжмережевого экрану

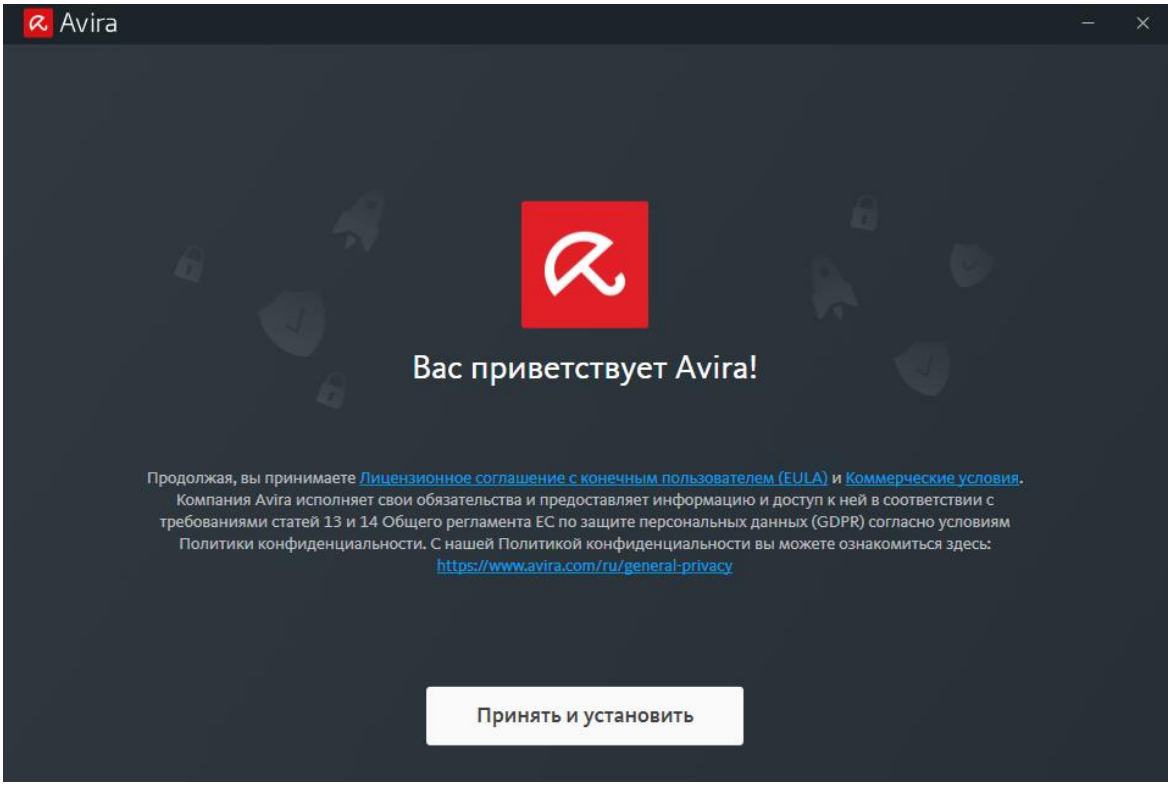
Тестуємо: **Avira Internet Security**

1. Для початку інсталюємо антивірус з офіційного сайту

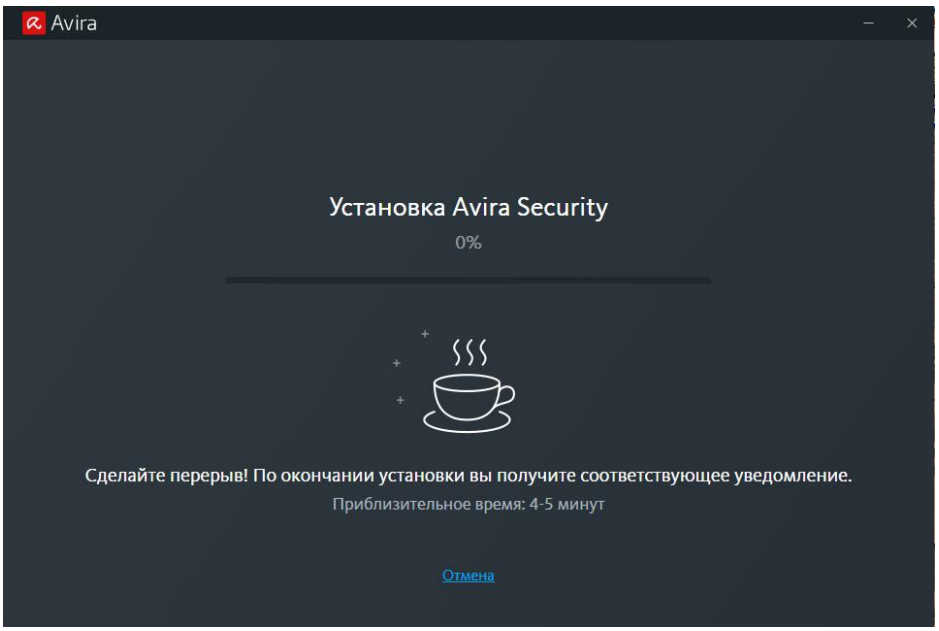


2. Процедура інсталяції дуже проста й зрозуміла

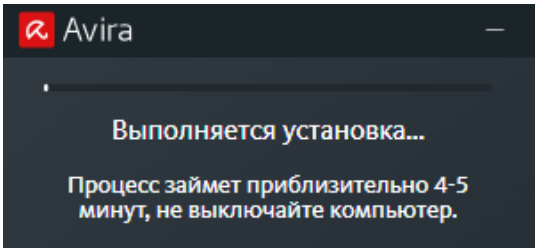
a. Для початку нас просять ознайомитись з ліцензійною згодою, та правилами



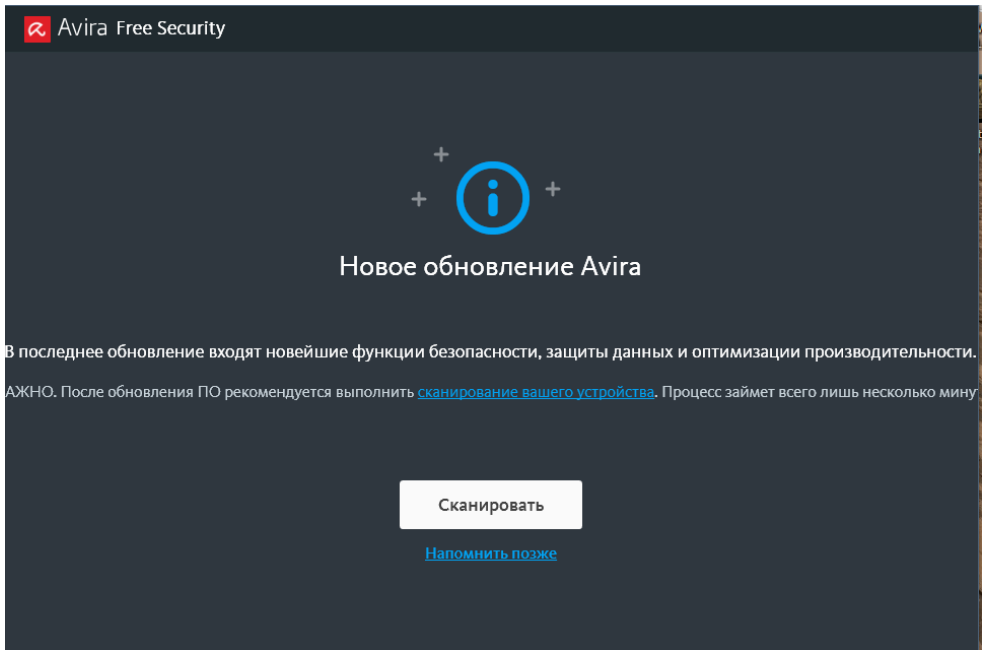
b. Після прийняття умов програма починає інсталяцію повідомляючи що найближчі 5 хв в нас будуть вільні



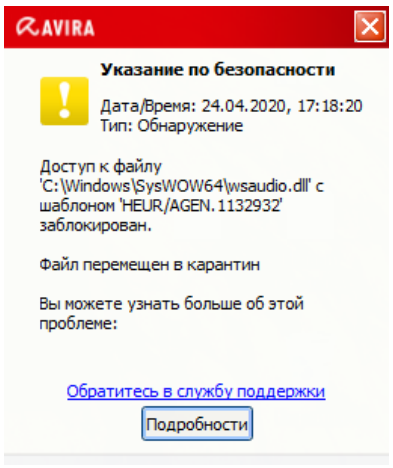
А також у маленькому вікні показує процес виконання в даний час



3. Після завершення відкриваємо програму і вона одразу пропонує провести обстеження

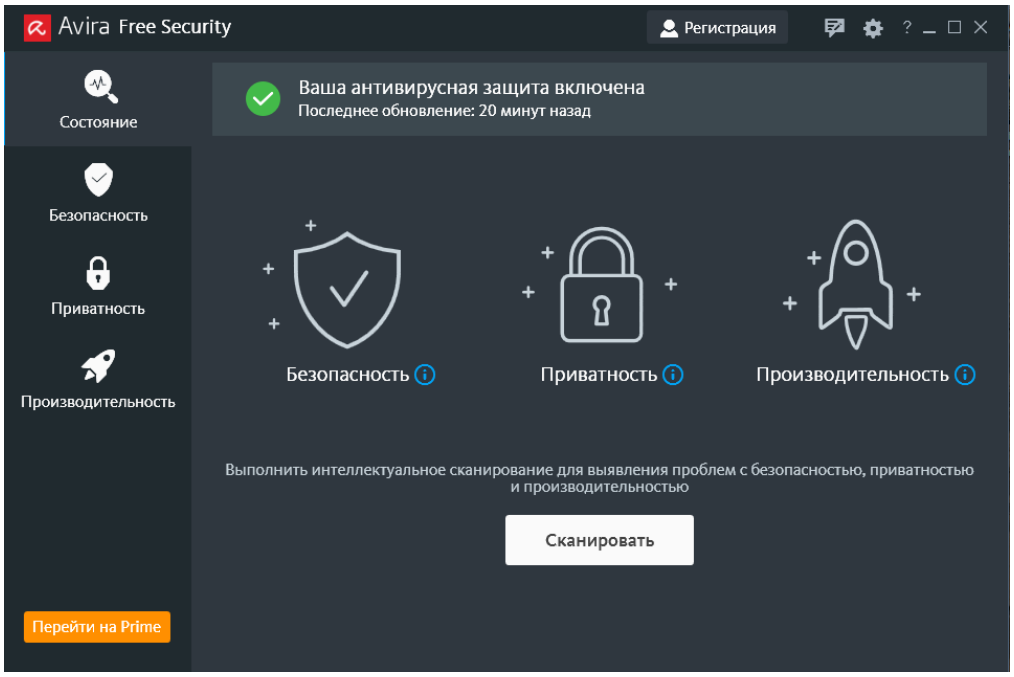


a. Також у спливаючому вікні виводить підозрілі файли

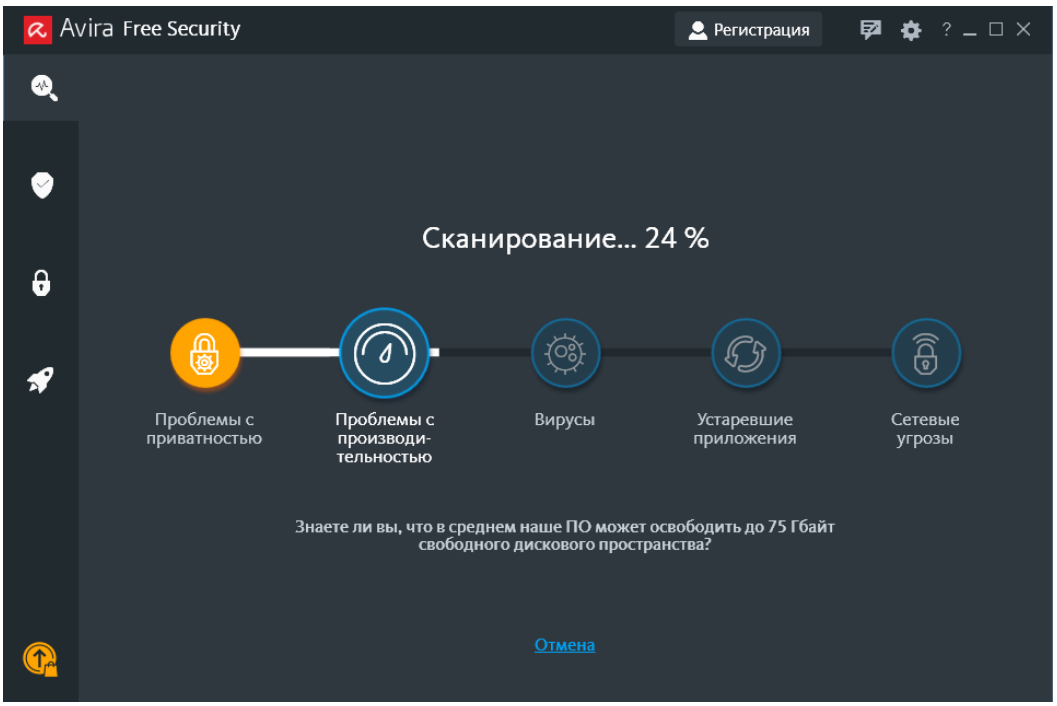


Сканування

Перша вкладинка **СТАН**

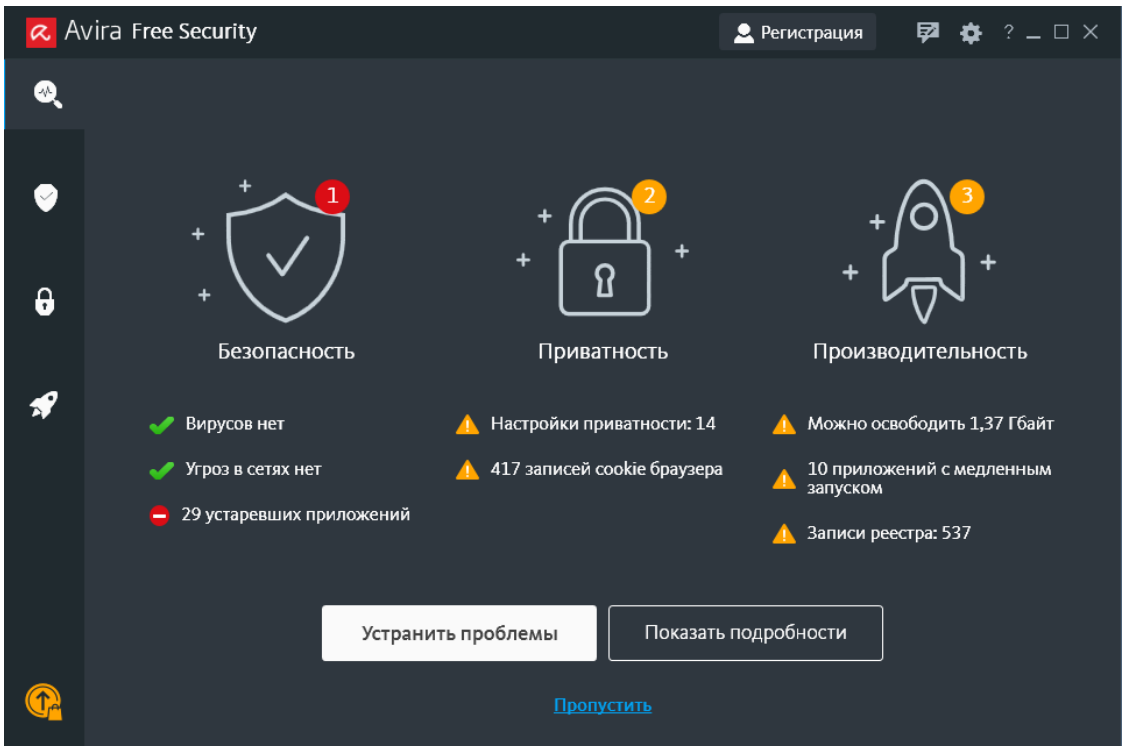


4. Погоджуємось на пункт 3 та запускаємо сканування. Антивірус одразу починає комплексне сканування

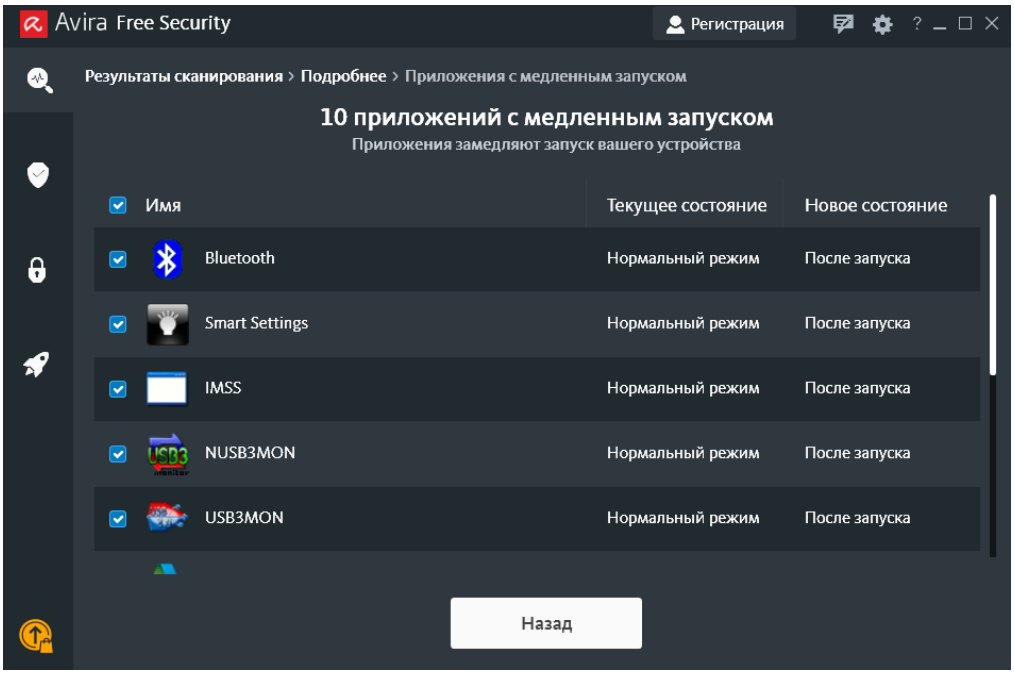


a. Першим пунктом комплексу є приватність – програма одразу вишукує шпигунські(хакерські) програми, які направлені на покушення конфіденційності даних
b. Далі програма оцінює продуктивність ПК та виявляє проблеми
c. Третім пунктом програма виявляє віруси які можуть нанести шкоду інформації (пошкодити, видалити, заблокувати та інше)
d. Після цього програма шукає застарілі та неефективні додатки які знижують швидкість праці
e. На останок антивірус аналізує загрози які йдуть з зовні(вихід у мережу Інтернет)

5. Після закінчення програма виводить результат своєї праці над моїм ПК

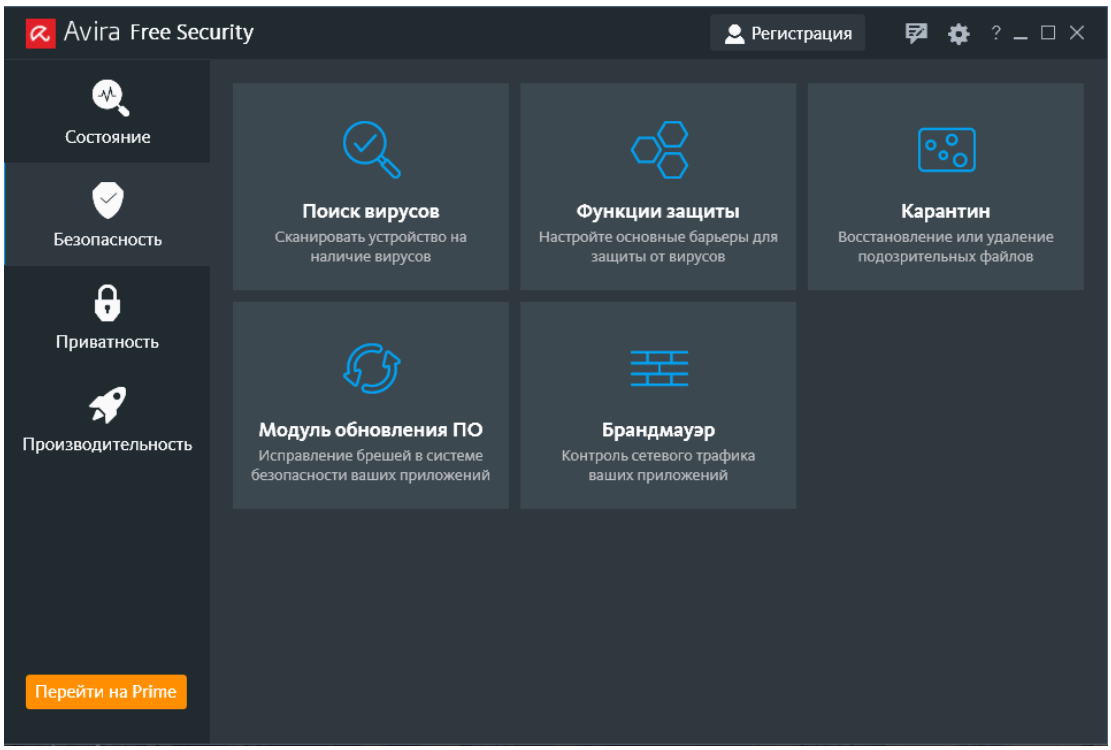


Як бачимо, вірусів або ж загроз з мережі в мене не виявлено, проте є 29 застарілих додатків а також 10 додатків з повільним завантаженням, та майже 1,4 ГБ інформації яку можна видалити. Натиснемо клавішу показати подробиці та подивимось наприклад які додатки повільно завантажуються



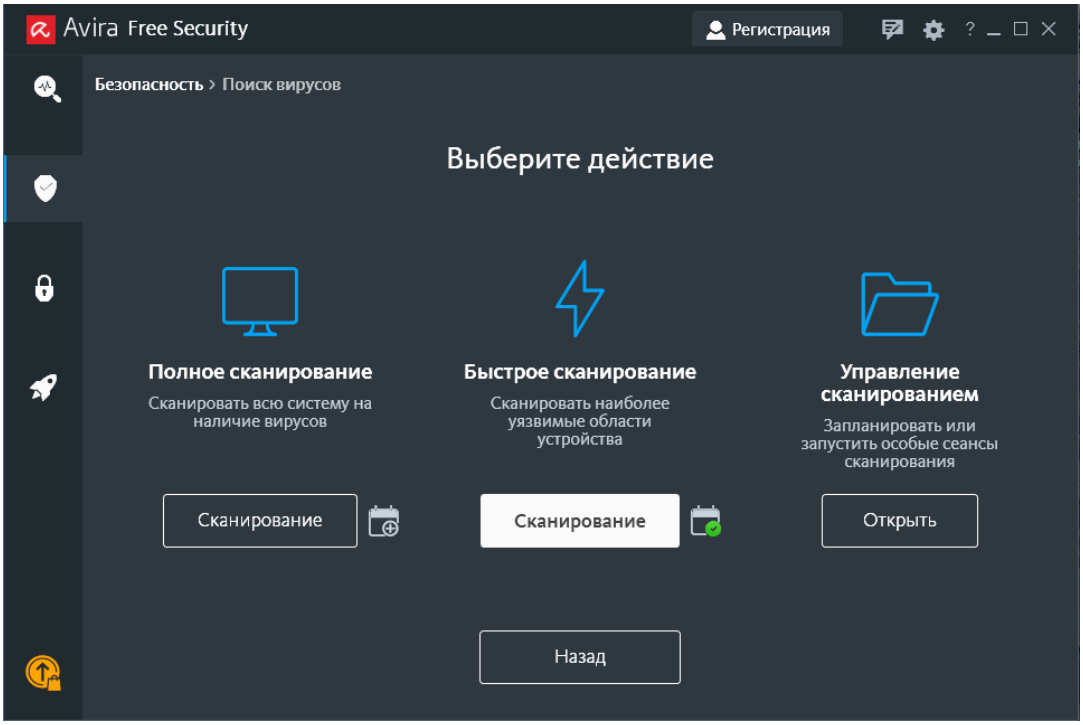
Безпека

Перейдемо до вкладинки безпека



Нам представляється вікно з пятьми функціями

1. Пошук вірусів



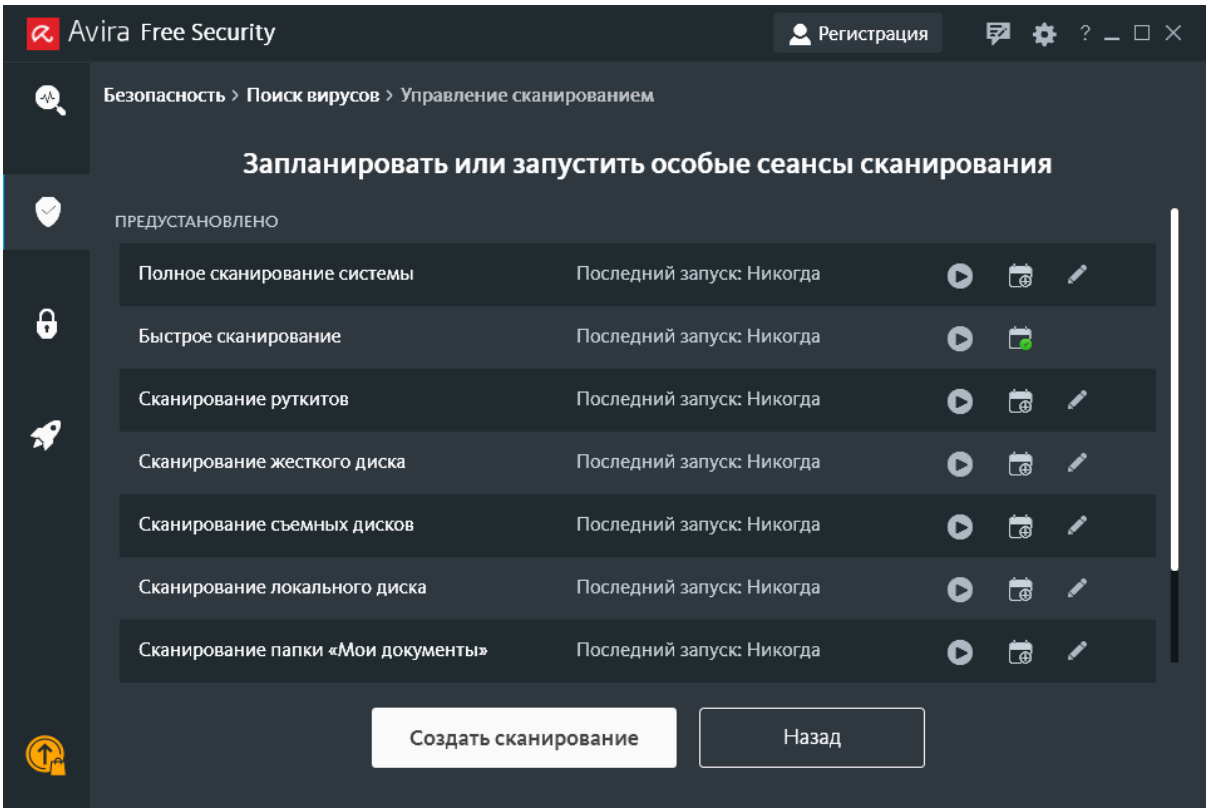
Це вікно дозволяє провести сканування програми трьома способами:

-Перший це повне сканування всієї системи(може зайняти час)

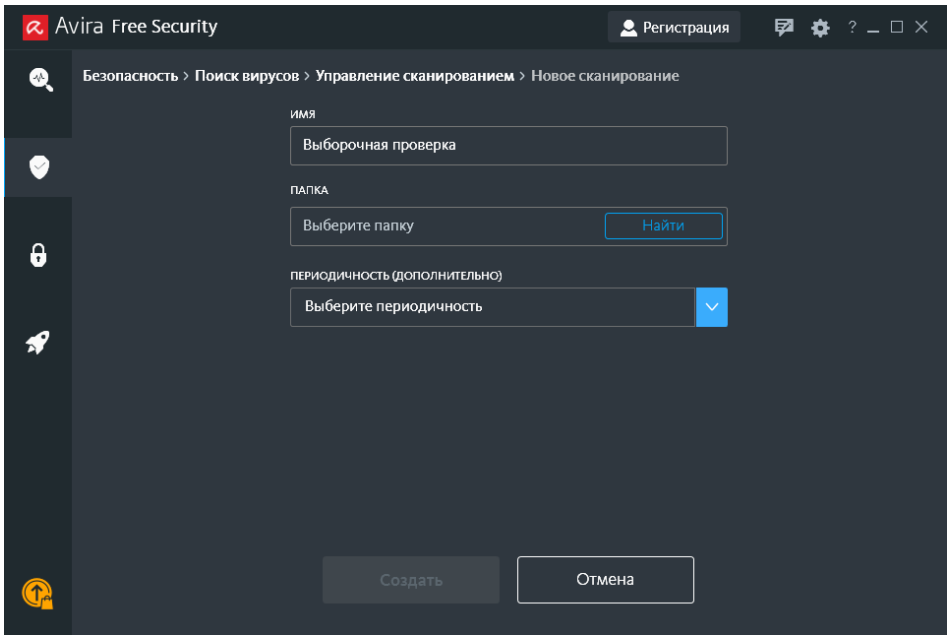
-Другий це швидке сканування проведене в пункті 4

-Третій це вибіркове сканування, ми обираємо об’єкт який хочемо просканувати (зупинимось на ньому більш детальніше)

Переходимо в управління скануванням

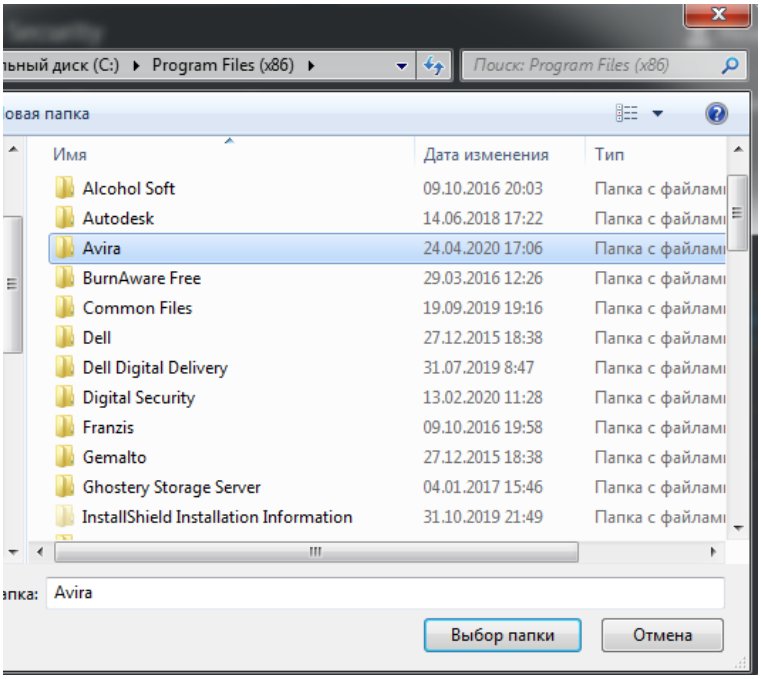


Бачимо що тут є багато різних видів вибіркового сканування, а також кнопка створити власне сканування(натиснемо її)

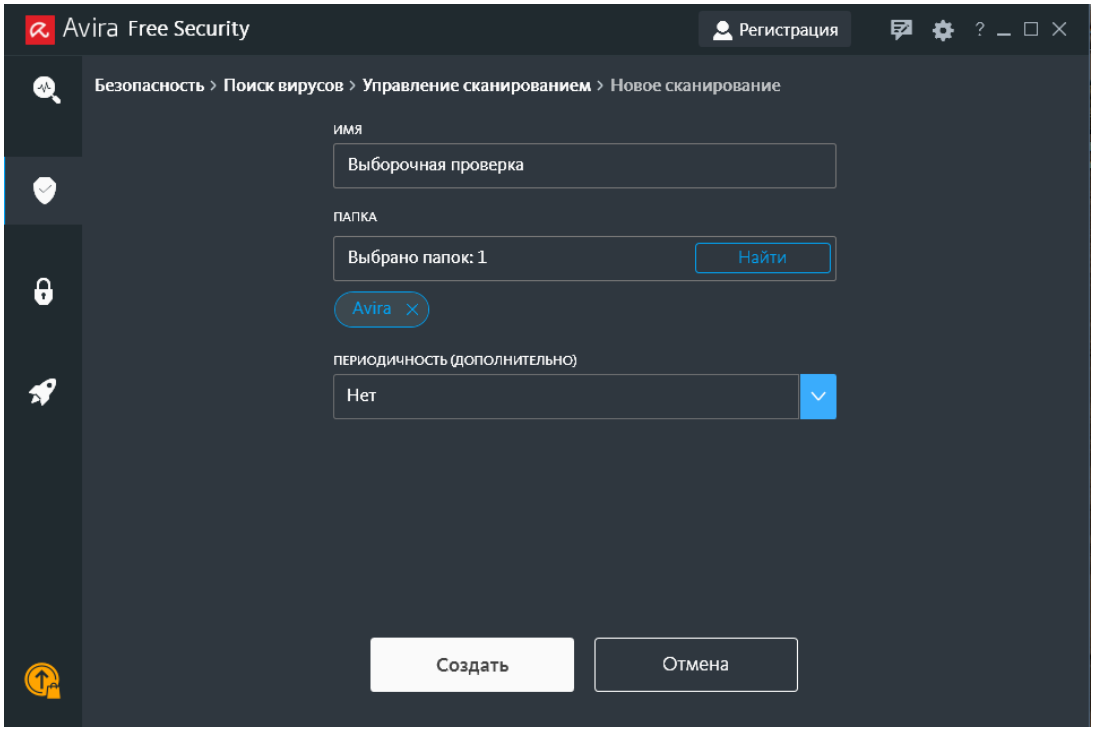


Нам преставляється вікно в якому користувач сам може обрати папку або файл який викликає в нього підозру

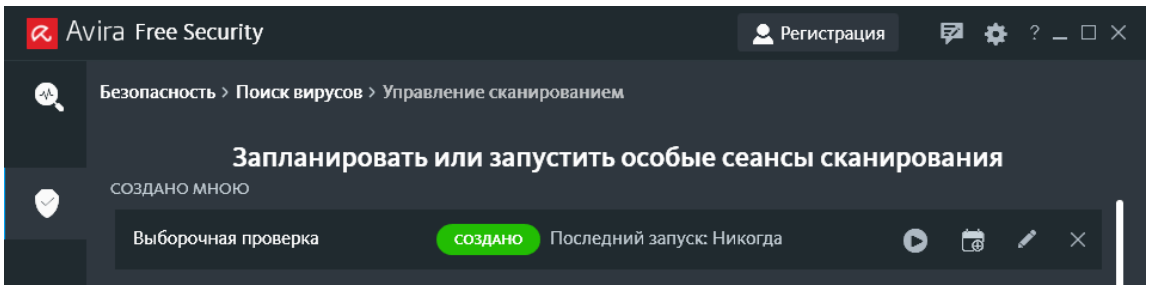
Я для тестування оберу папку з антивірусом **Avira Free Antivirus**



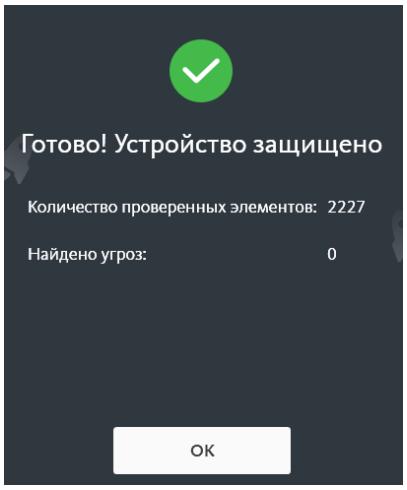
Обираємо та створюємо тестування (выборочная проверка-по умолч.)



Натискаємо кнопку створити після чого наше тестування з’являється серед інших

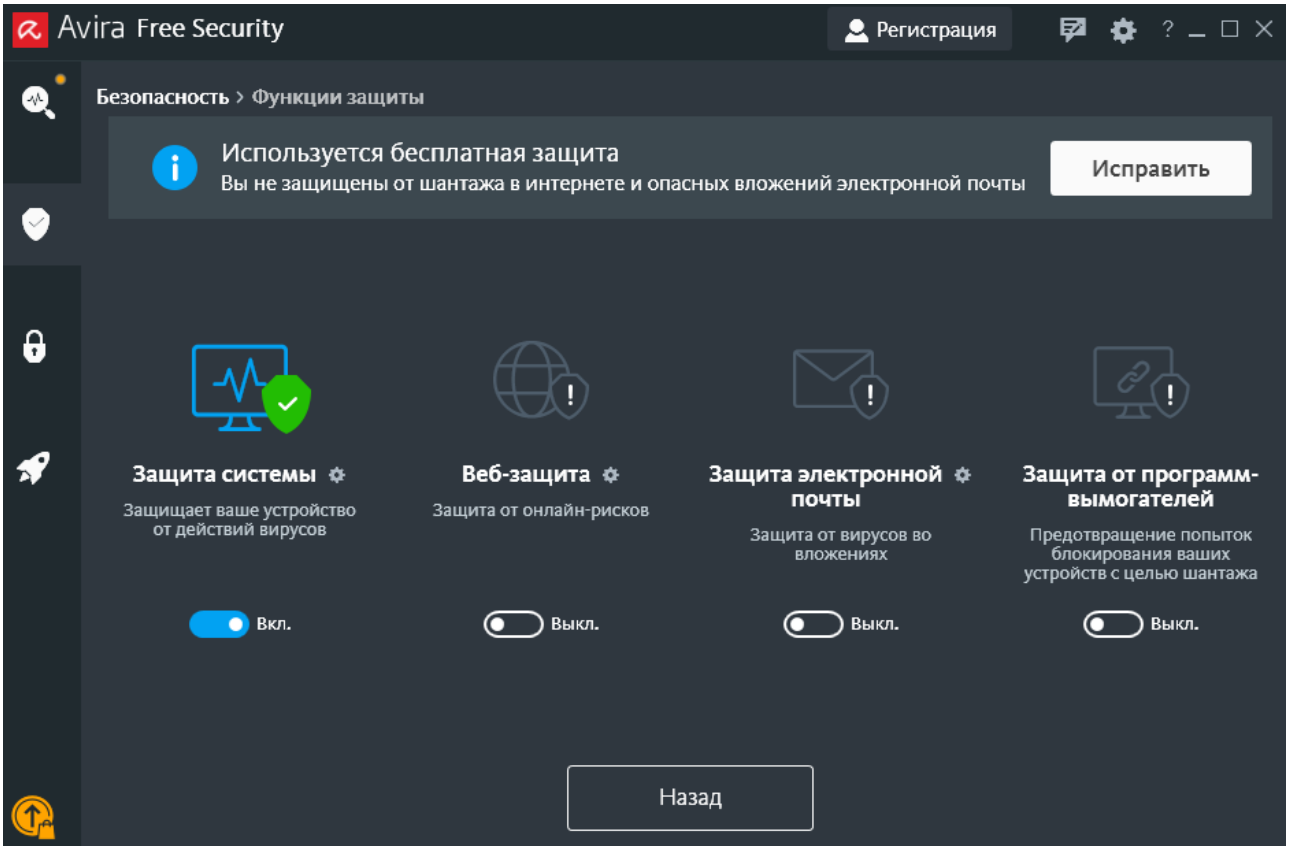


Скануємо цю папку натиснувши клавішу плей та отримуємо результат

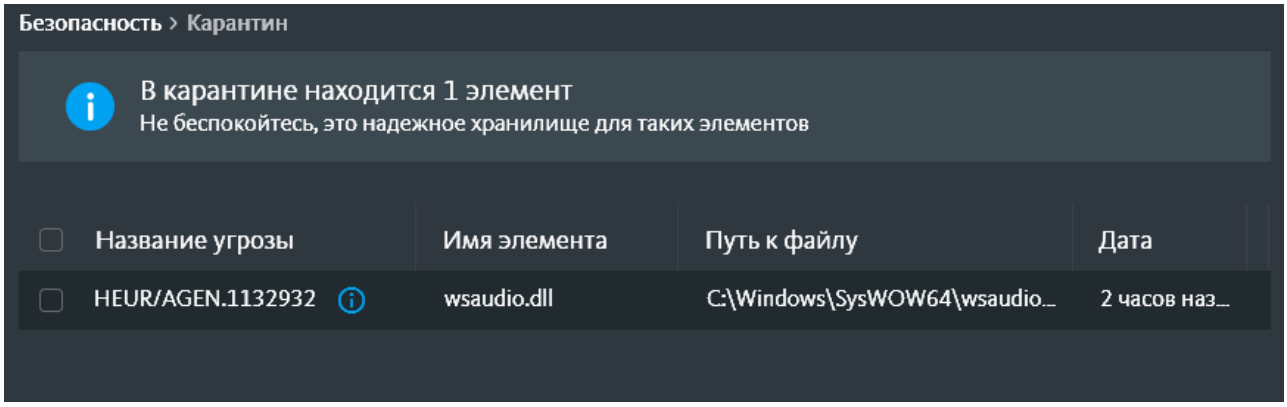


Загроз не виявлено)

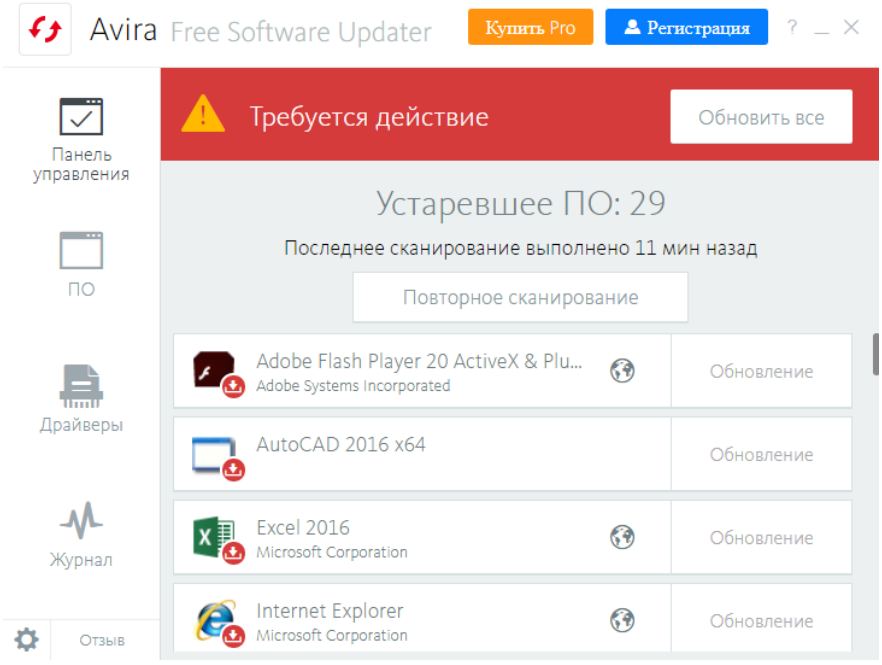
Наступний пункт це додаткові функції захисту які можна ввімкнути та вимкнути за бажанням.



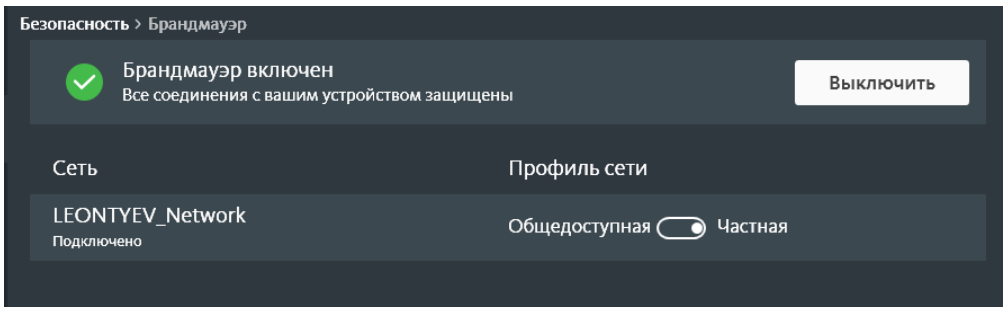
Далі йде карантин – функція тимчасової ізоляції файлу до якого виникли підозри



Модуль оновлення ПО визначає програми які необхідно оновити для оптимізації

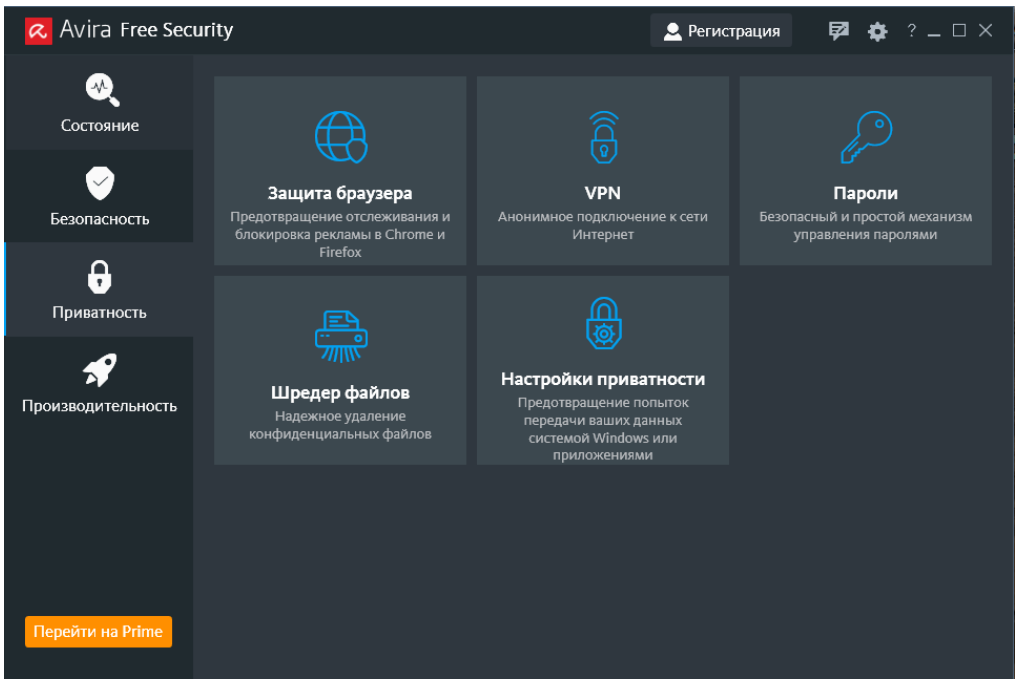


Брандмауер- функція яка дозволяє змінити статус мережі



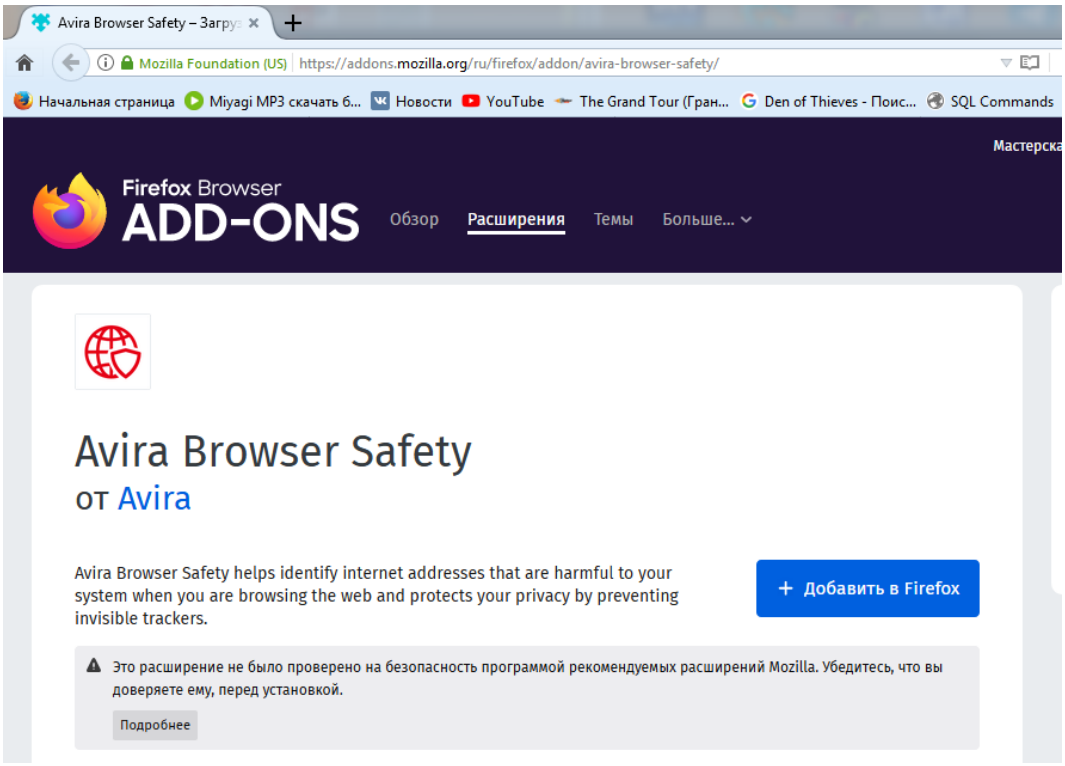
Приватність

Переходимо до вкладинки приватність

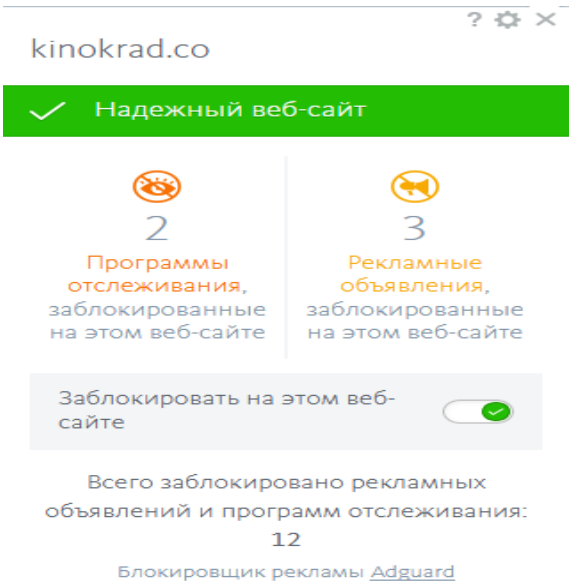


В цій вкладинці також 5 пунктів

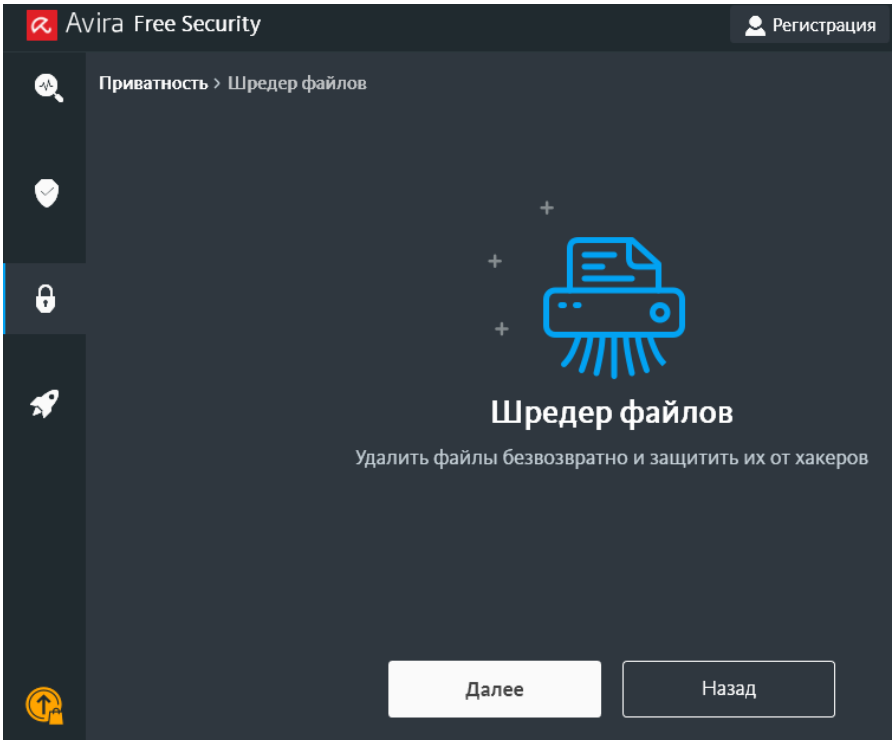
Першим йде захист браузеру. Переходимо і нас перекидає на сторінку ознайомлення



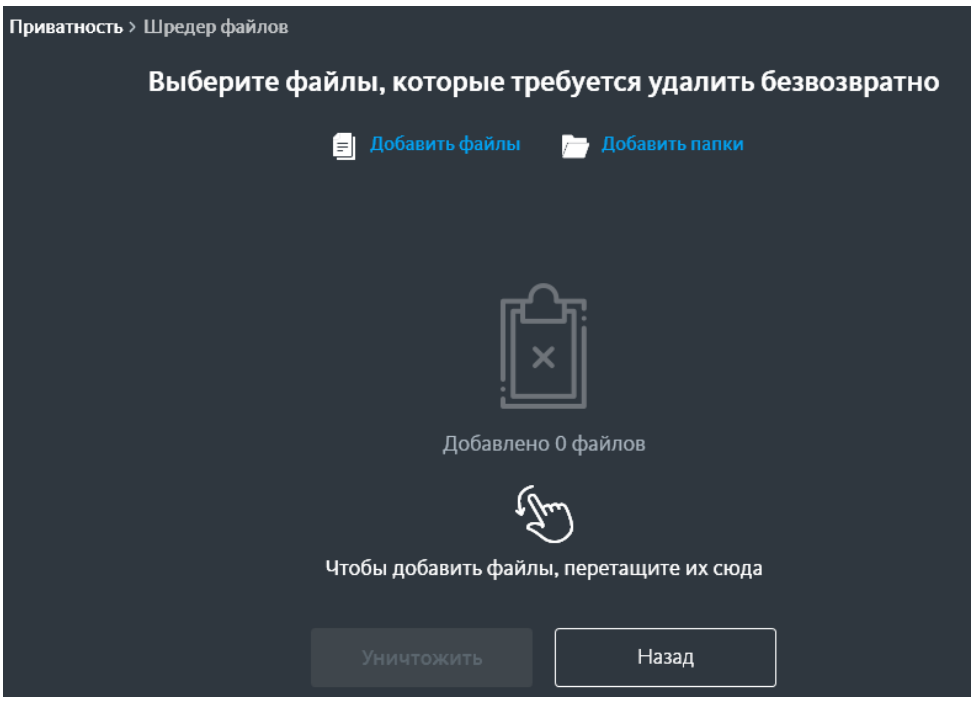
Додаємо захист, після чого проводимо перевірку на сайті де є спливаючі рекламні вікна.

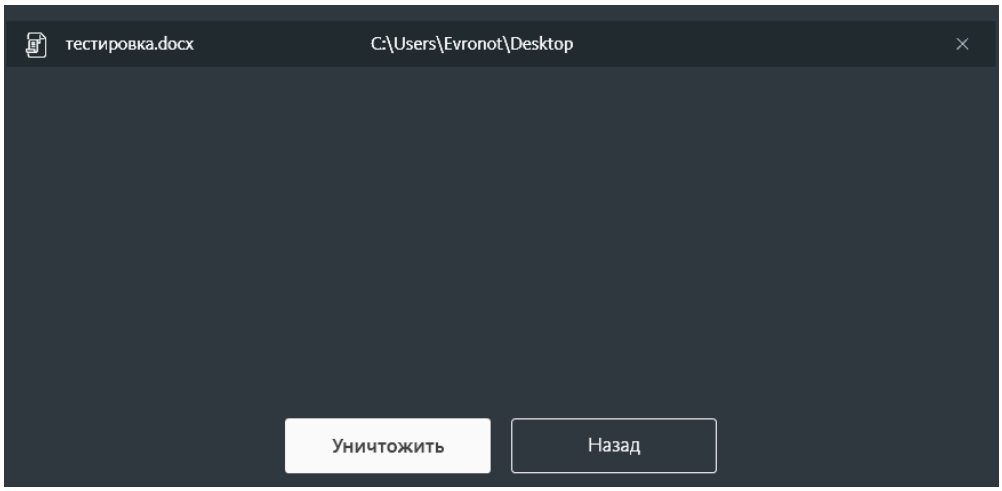


Захист показує результат на якому видно що було заблоковано 3 рекламних об’яви а також 2 програми відстеження(в данному випадку місцезнаходження)
Можна зручно та обов’язковим пунктом конфіденційно зберігати паролі без необхідності кожен раз згадувати їх.
Шредер файлів це зручний спосіб знищити файл без можливості його відновлення

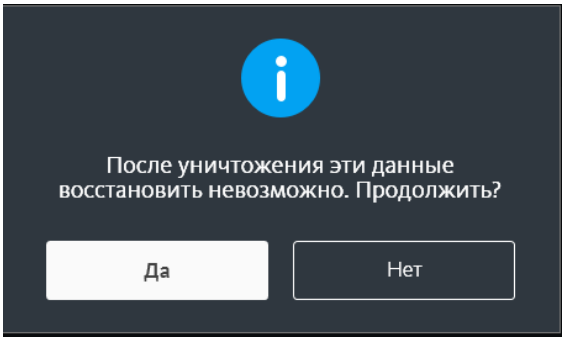


Для роботи з ним потрібно обрати файл який необхідно знищити. Для цього я створив тестовий документ, обрав та знищив його.

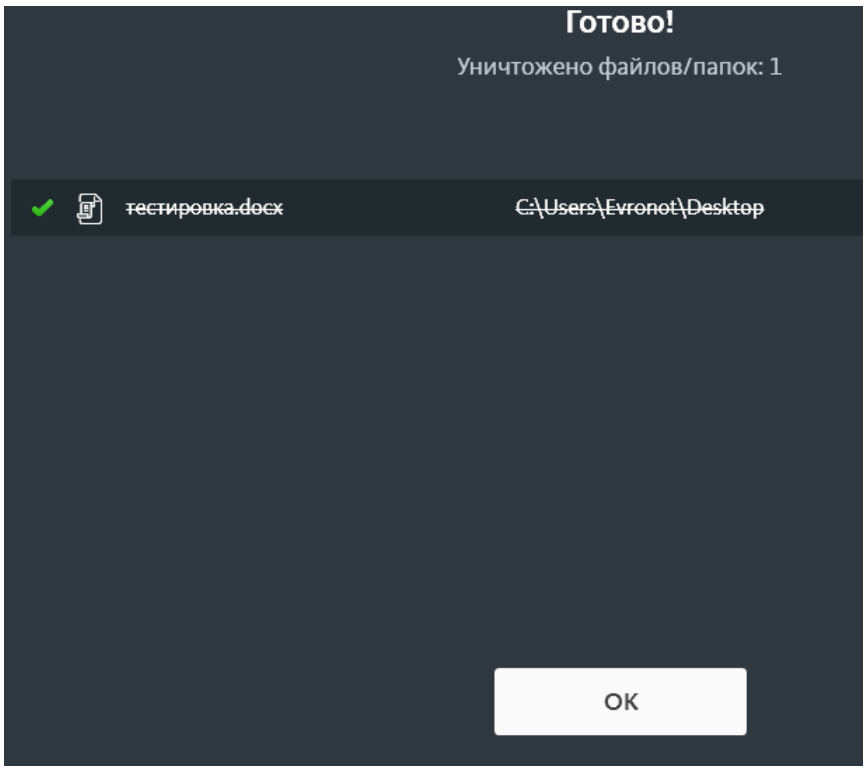




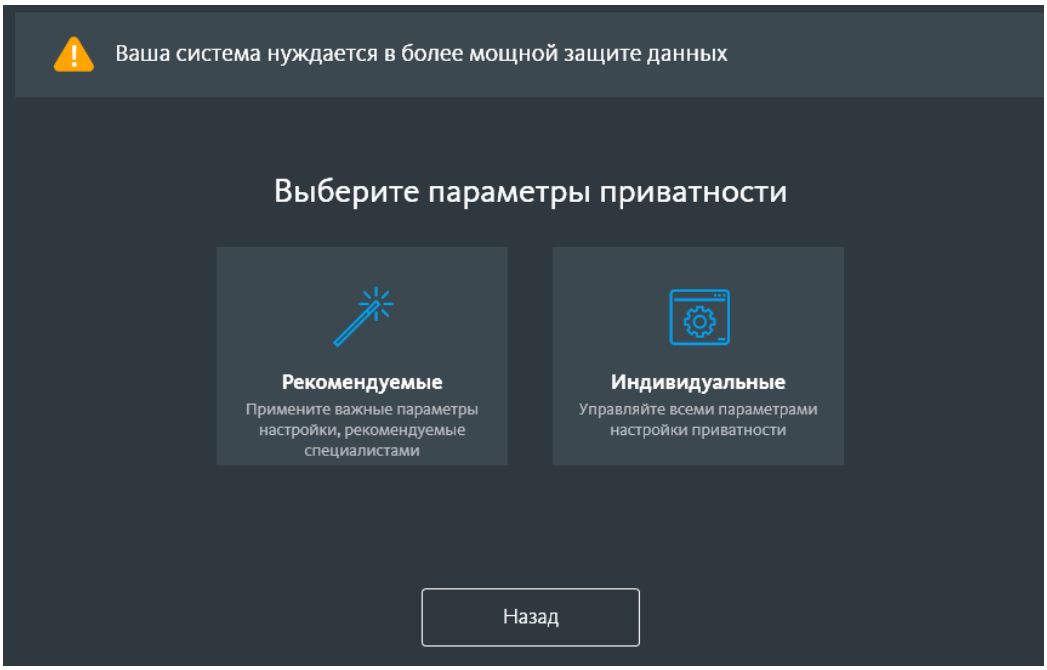
Програма на всяк випадок перепитує та переконується в необхідності знищення, та попереджую про неможливість віновлення:



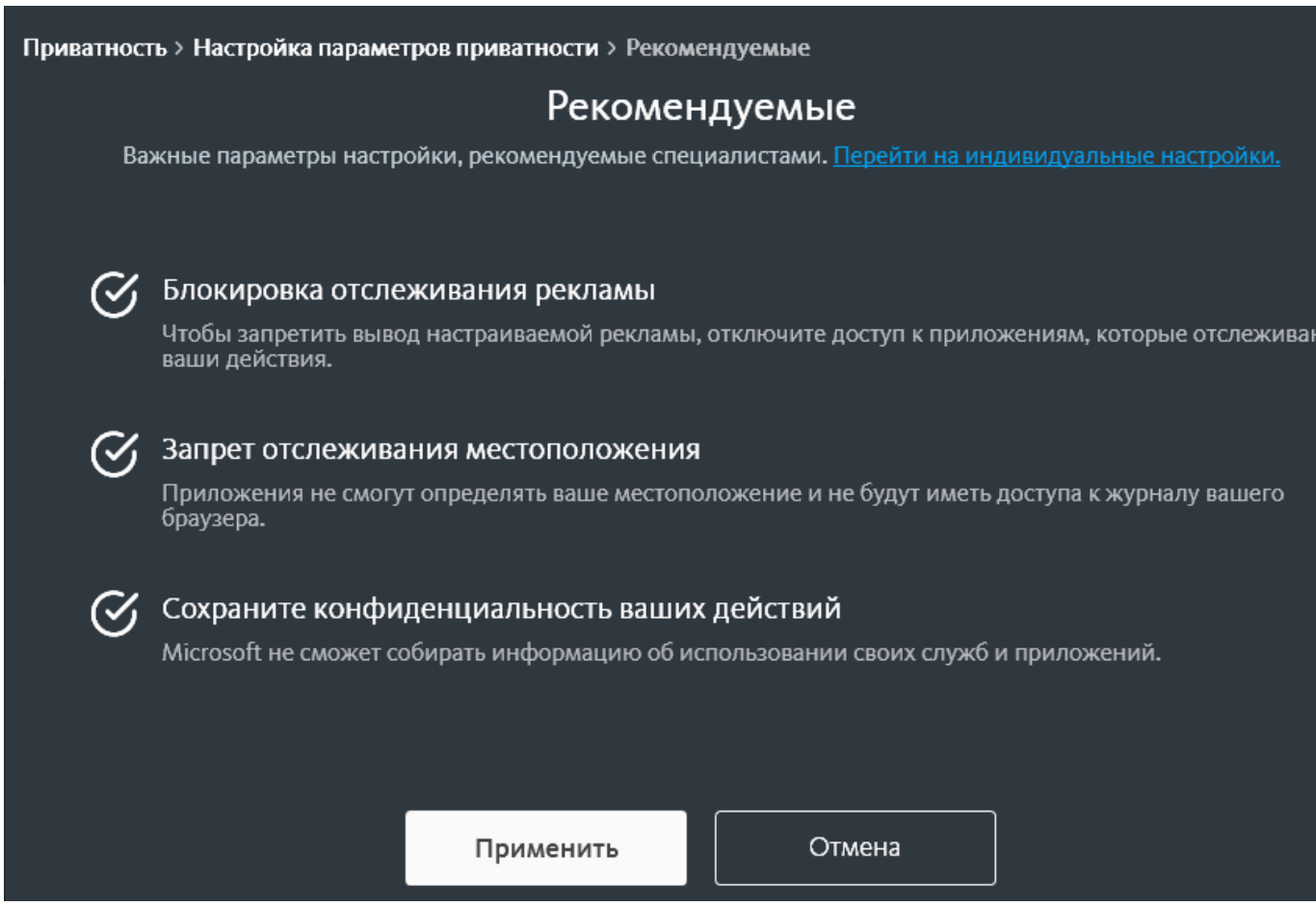
Після цього видає результат



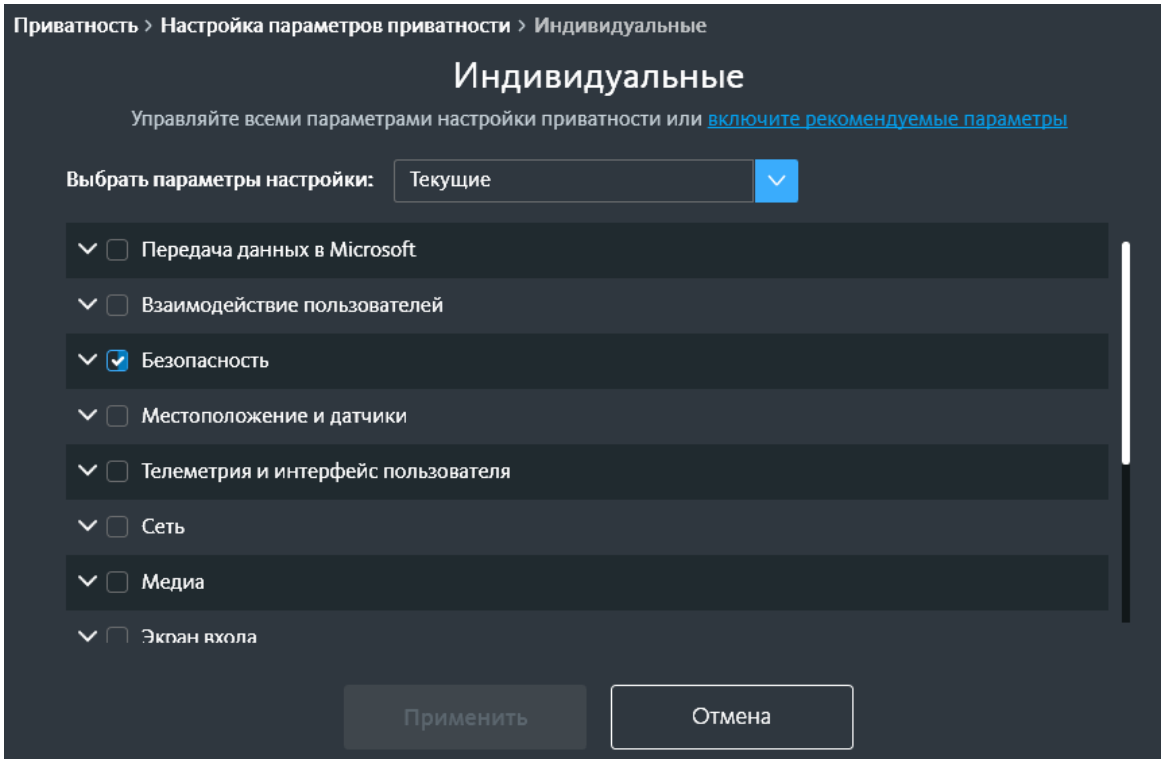
Останнім пунктом є настройки приватності



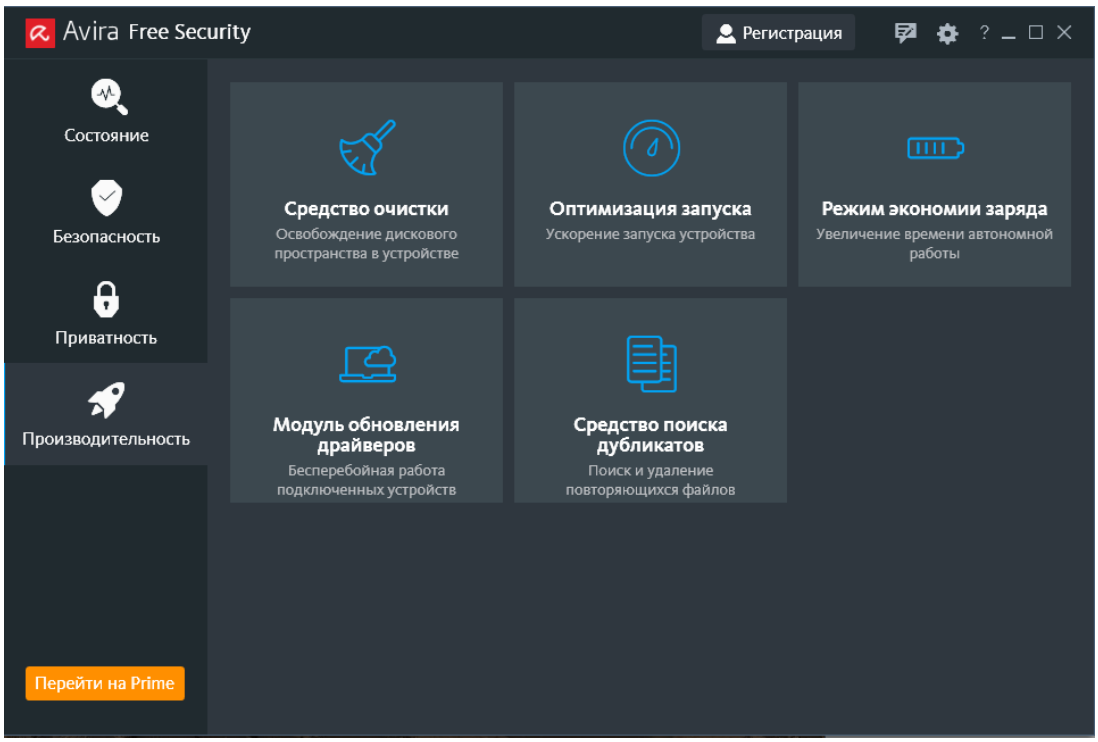
Які поділяються на рекомендовані



Та індивідуальні:

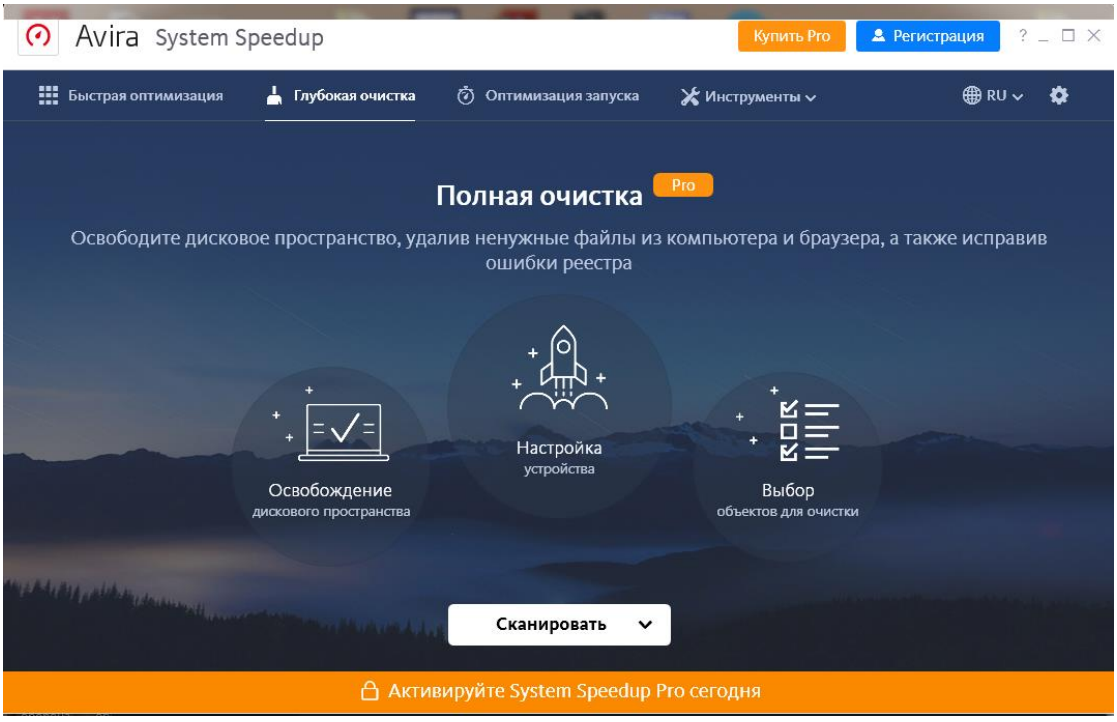


Продуктивність

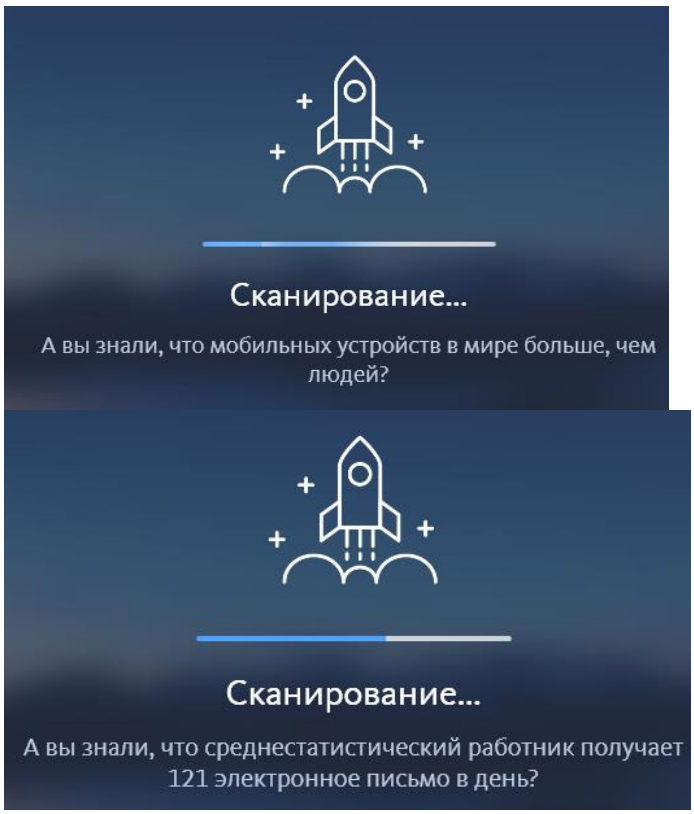


Також поділяється на 5 інструментів які направлені на підвищення продуктивності ПК.

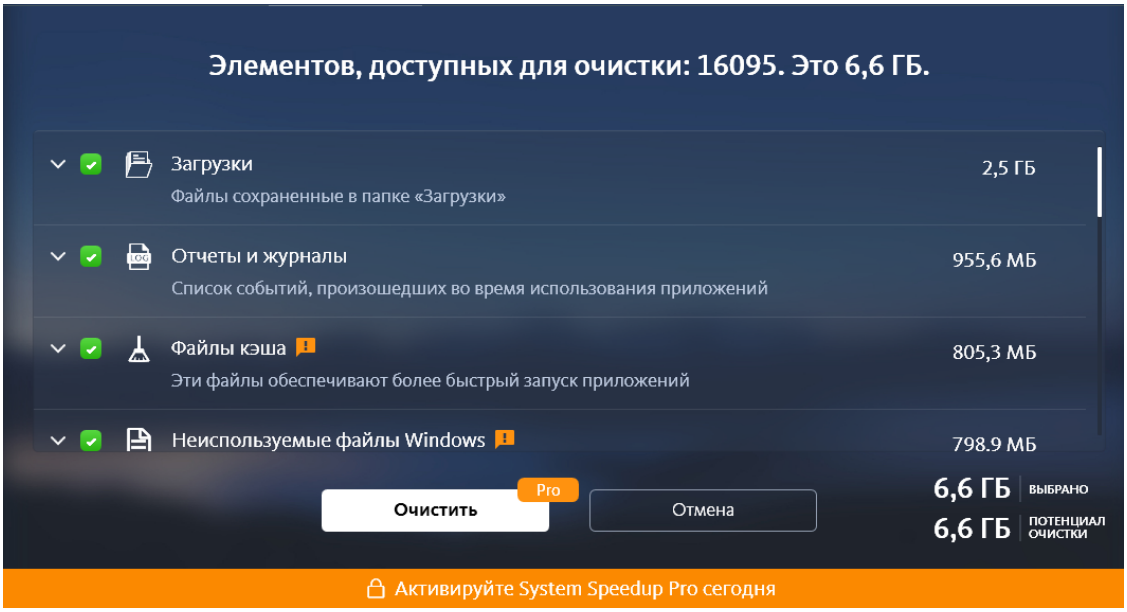
Засіб очищення це засіб який визначає непотрібні файли та пропонує їх видалити.



Тестуємо дану функцію. До речі приємним бонусом є цікаві факти які періодично змінюються під час аналізу.

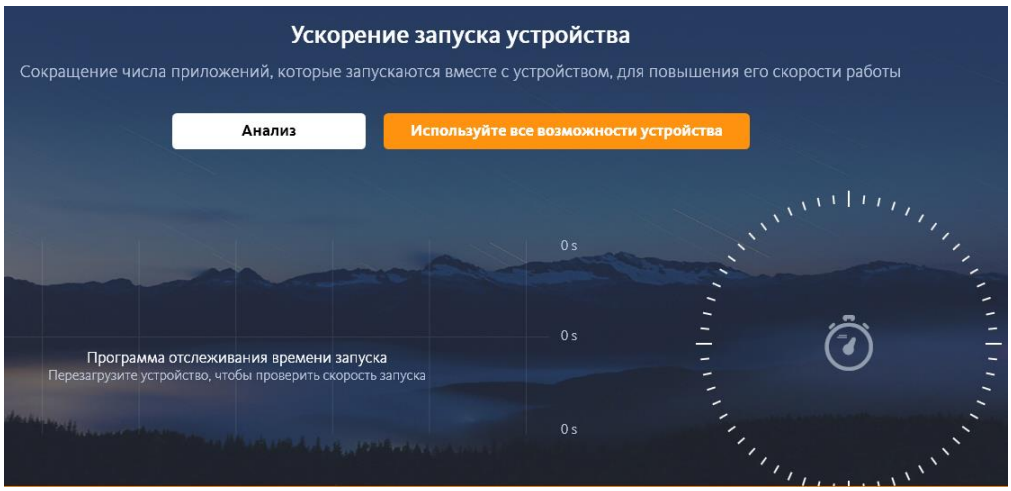


Після аналізу, програма видає результат та пропонує видалити файли.

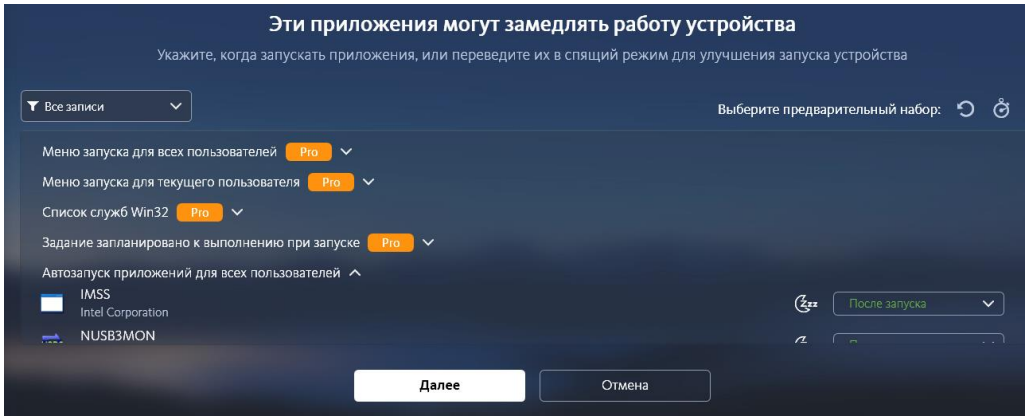


Оптимізацію процесів з метою прискорення роботи

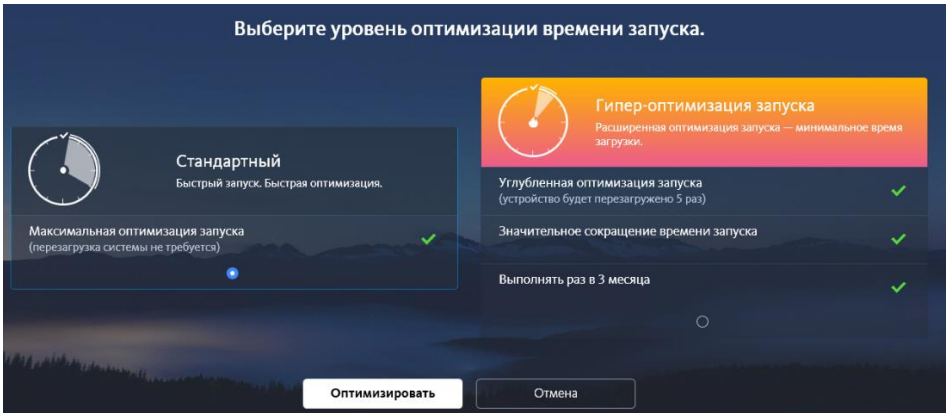
Функція яка скорочує число працюющих прогмам, які запускаються разом з системою для підвищення швидкості роботи.



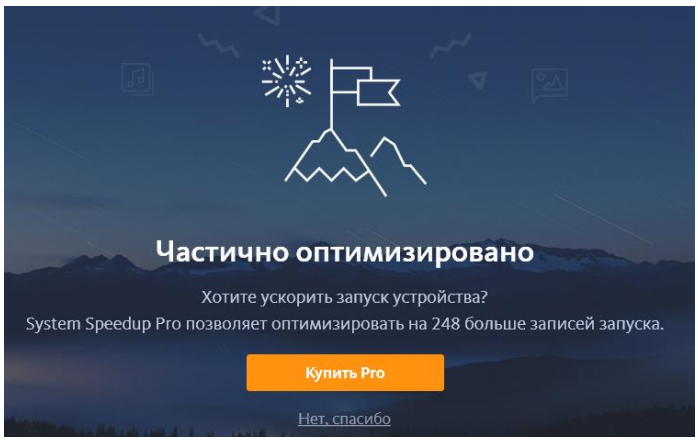
Після натискання кнопки аналіз, програма видає список додатків які потенційно сповільнюють роботу комп’ютера.



Далі програма пропонує самостійно оптимізувати процес двома способами, обираємо перший, так як для безкоштовної версії доступний тільки він

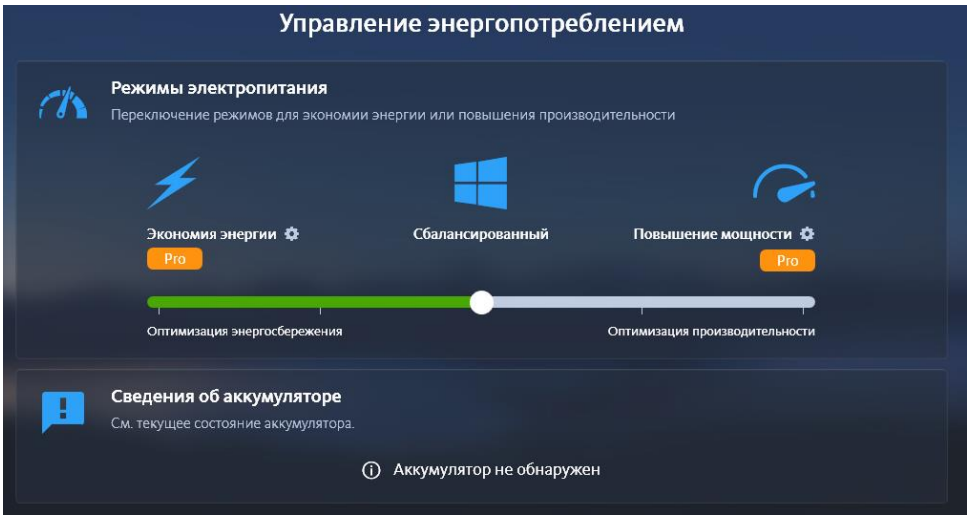


Натискаємо клавішу оптимізувати, після чого програма нам видає результат



Управління енергоспоживанням

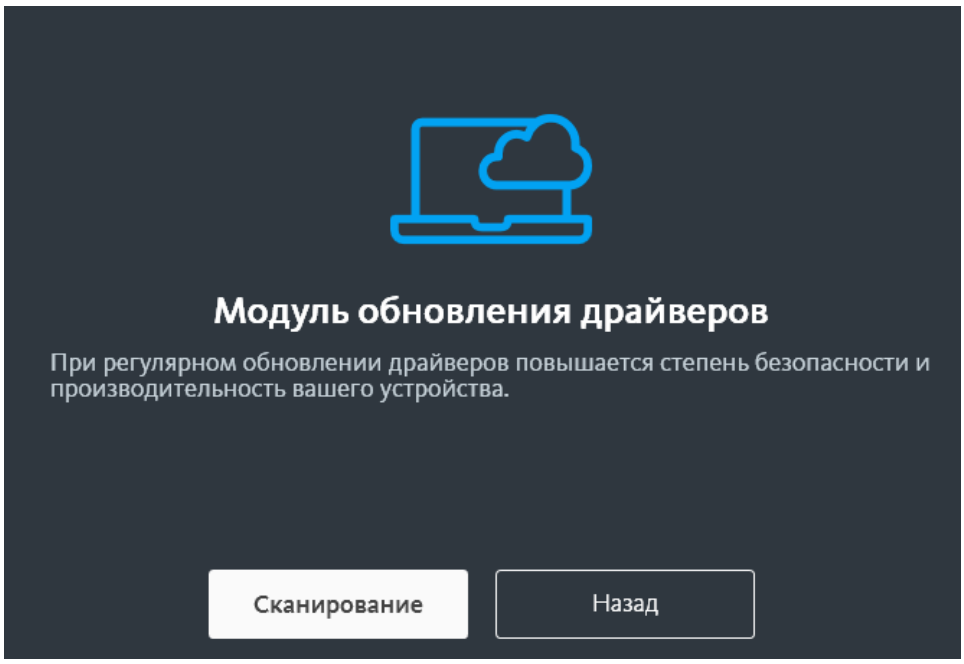
Інструмент який може перенаправляти енергію або на сповільнення процесів з метою подовження автономної роботи або на пришвидшення процесів, жертвуючи часом автономності пристрою.



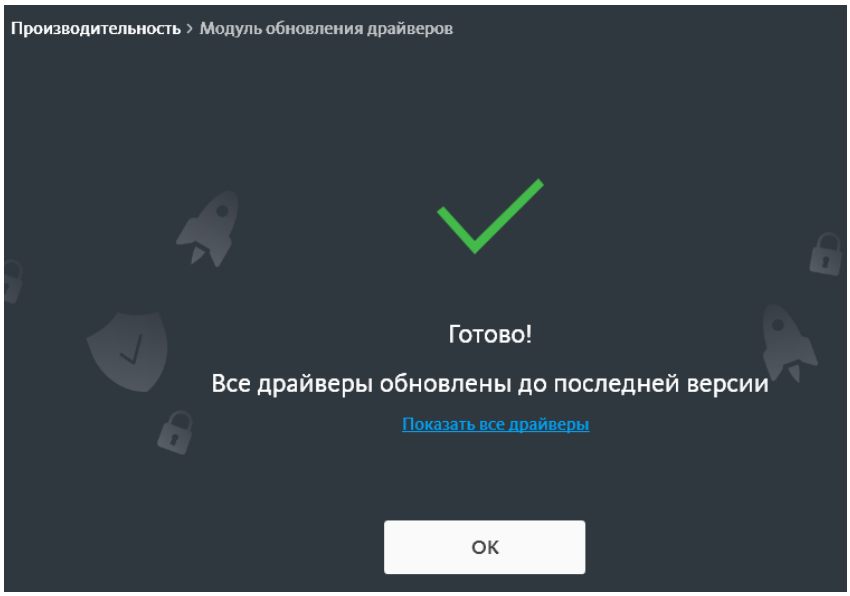
Цю функцію я не маю змоги протестувати через відсутність акумулятора в пристрої.

Модуль оновлення драйверів, це модуль який пропоную підвищити продуктивність та безпеку шляхом оновлення застарілих драйверів.

Інструмент спочатку сканує ПЗ якому потрібен апгрейд.



Після цього проводить оновлення



Та виводить список оновлених драйверів з їх версією.

Для того щоб визначитись з фаєрволом який буде встановлений у нас в системі заисту. Я також вирішив порівняти з іншим фаєрволом.

Сильні сторони керування Kerio

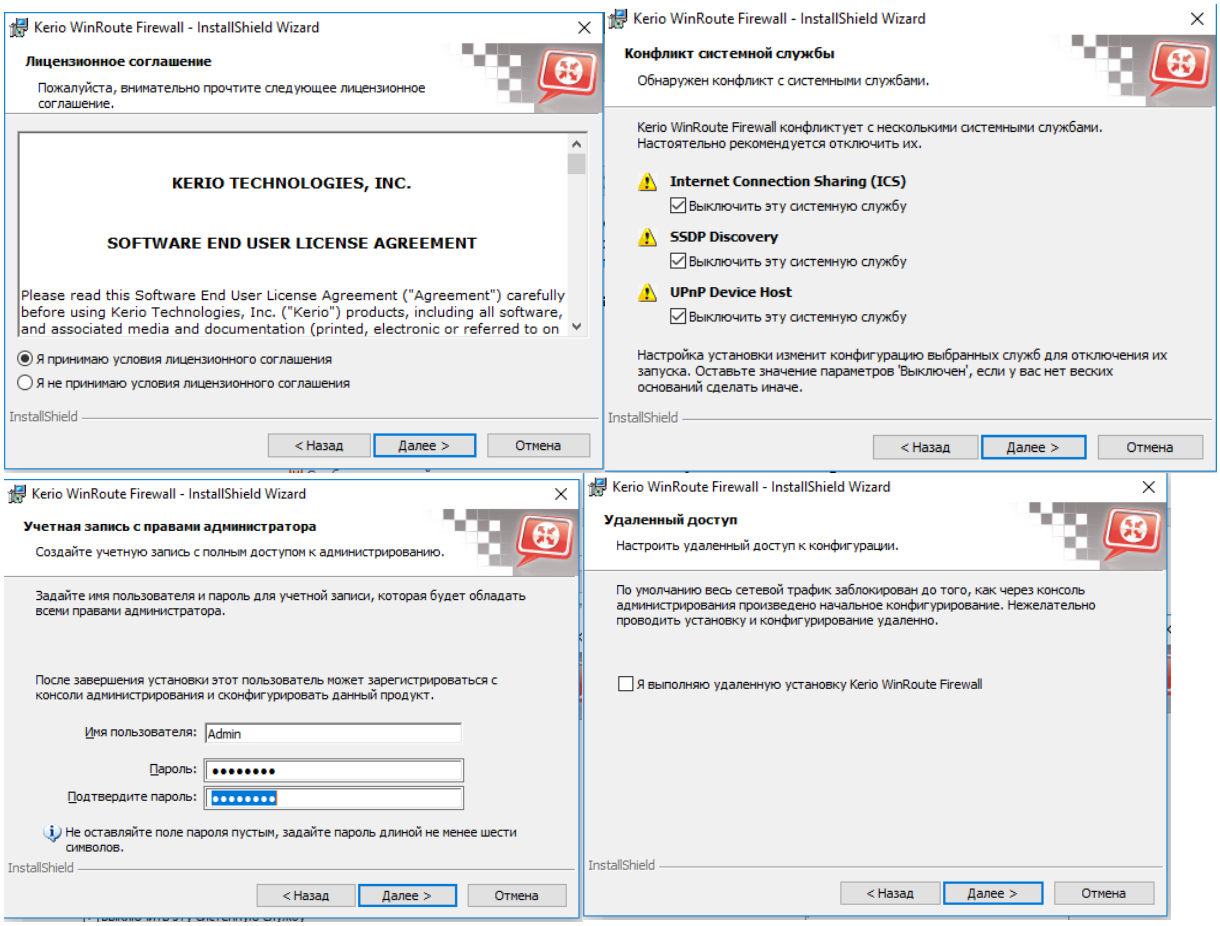
- Простий та інтуїтивно зрозумілий інтерфейс.
- Програмне забезпечення Kerio Control можна встановити на комп’ютері за допомогою методу програмного забезпечення ISO або як віртуальну машину, що дозволяє налаштувати апаратне забезпечення відповідно до розміру мережі.
- Програмне забезпечення Kerio Control включає засоби мережевої безпеки, виявлення та запобігання вторгненню, балансування навантаження та звітування за базовою ціною ліцензії, можна підключити Sophos AV та Kerio Control Web Filter
- Створюйте звіти в режимі реального часу та чіткіше зберігайте історію звітів та надайте точнішу інформацію.
- Kerio Control підтримує IPSec VPN та Kerio VPN (клієнт-сервер та сервер-сервер).
- На думку клієнтів, клієнт Kerio Control VPN - найшвидший і найпростіший в управлінні, налаштуванні та використанні.

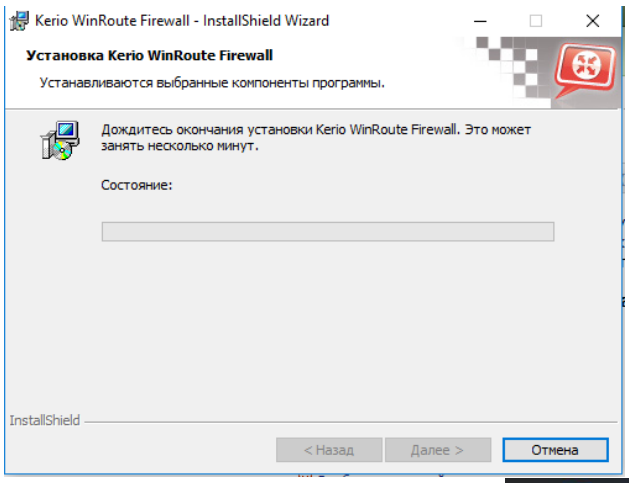
	Kerio control	Entensys userfate
Запобігання вторгнень	+	+
Антивір сканування	+	+
Фільтр інтернет –ресур	+	-
Робота з Ipv6	+	-
Vlan	+	-
Глибокий аналіз пакетів	+	+
VPN	+	-

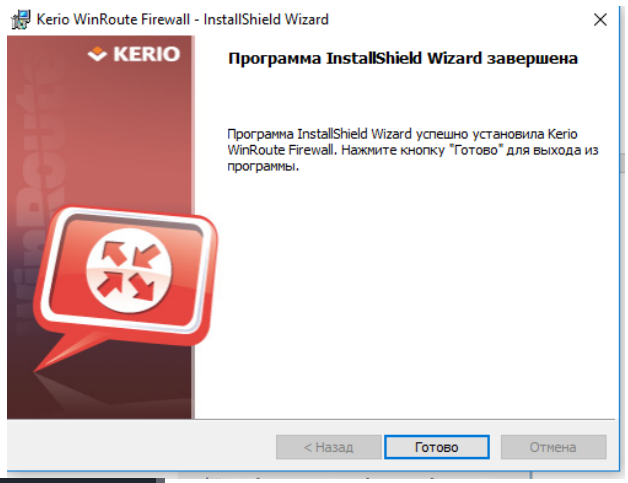
Обравши кращий брандмауер переходимо до налаштувань його

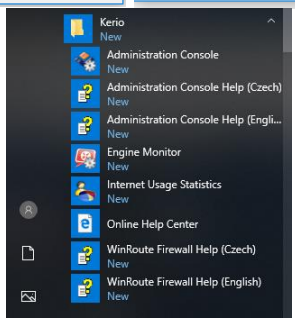
Установка програми

Встановлюємо Kerio WinRoute Firewall 6.7.1.6544



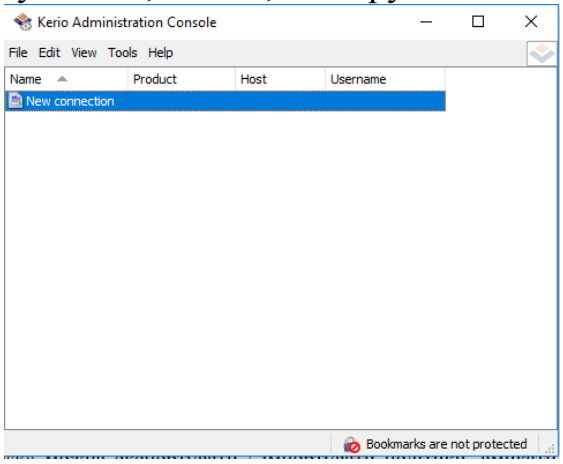


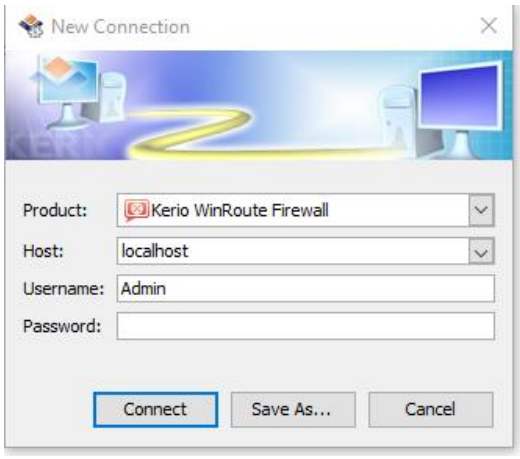




Інтерфейс програми

У головному вікні консолі адміністратора є 5 вкладок: «Файл», «Редагування», «Вид», «Інструменти» та «Довідка».



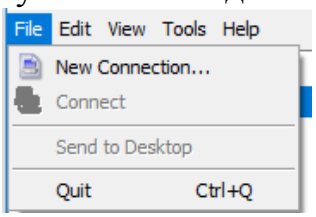


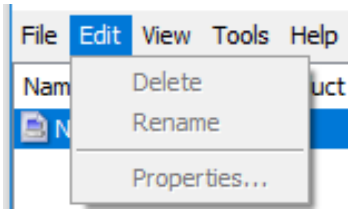
У вкладці «Файл» ми можемо додати нове з’єднання, з’єднатися з вже існуючим доменом, зберігти на робочий стіл та вийти.

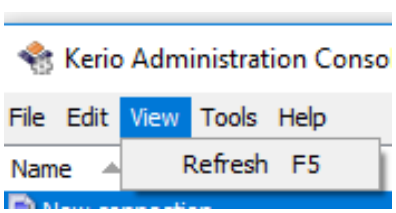
У вкладці «Редагування» ми можемо видалити або переіменувати з’єднання та подивитись його властивості.

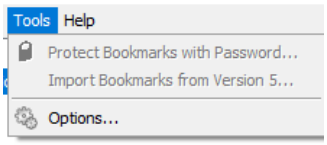
У вкладці «Вид» ми можемо обновити сторінку.

У вкладці «Інструменти» ми можемо захистити закладку поролем або імпортувати її та подивитись опції.







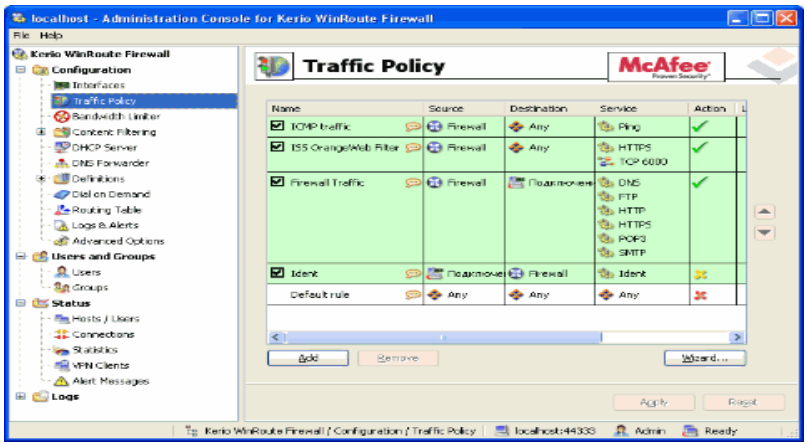


Технічне завдання та програма випробувань

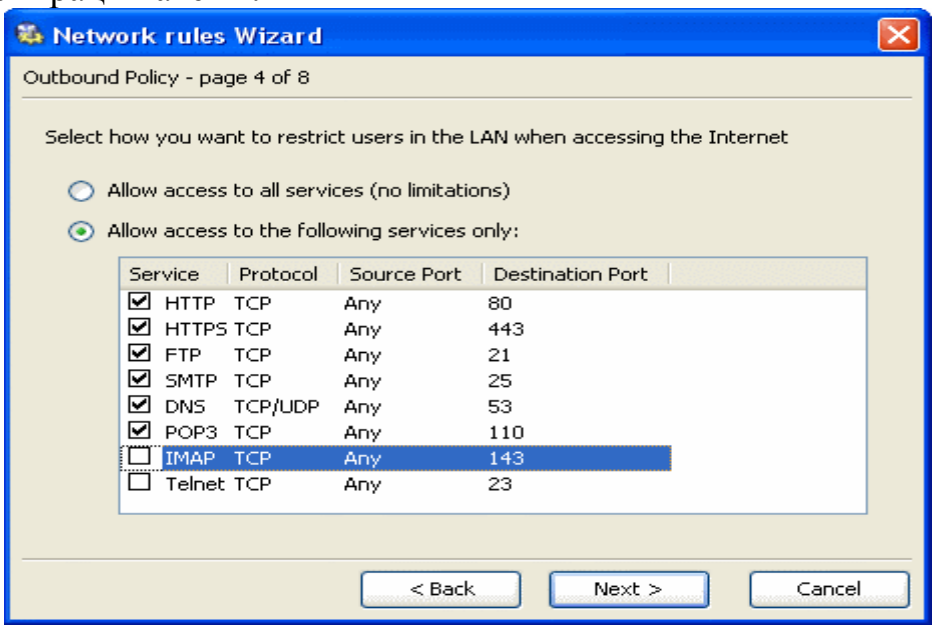
Налаштування стандартних опцій фаєрволу

Встановлюємо фаєрвол, та проводимо його швидке налаштування.

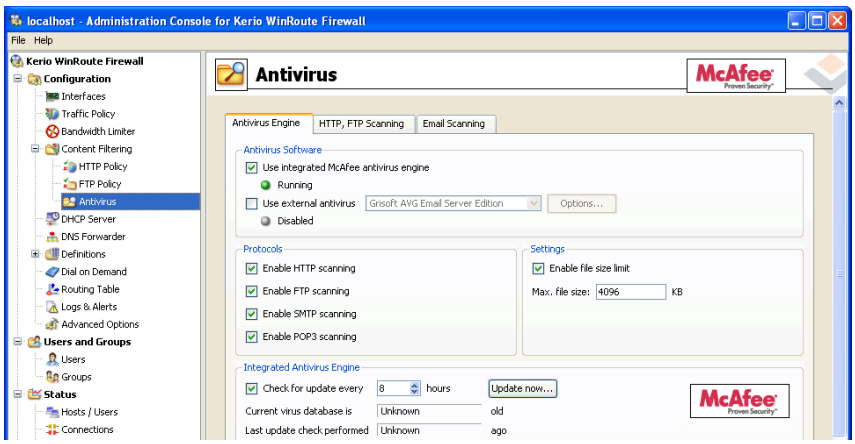
Після встановлення, нам необхідно перезавантажити систему, та ознайомитись з інтерфейсом програми. Після того, як ми установимо нове з'єднання відкриваємо вікно налаштування самого фаєрволу. У основному робочому просторі програми ми бачимо розділи «налаштування», а також «користувачі та групи», «статус», та «логи». У даному випадку нам необхідно переглянути налаштування розділу «налаштування», а саме налаштування трафіку:



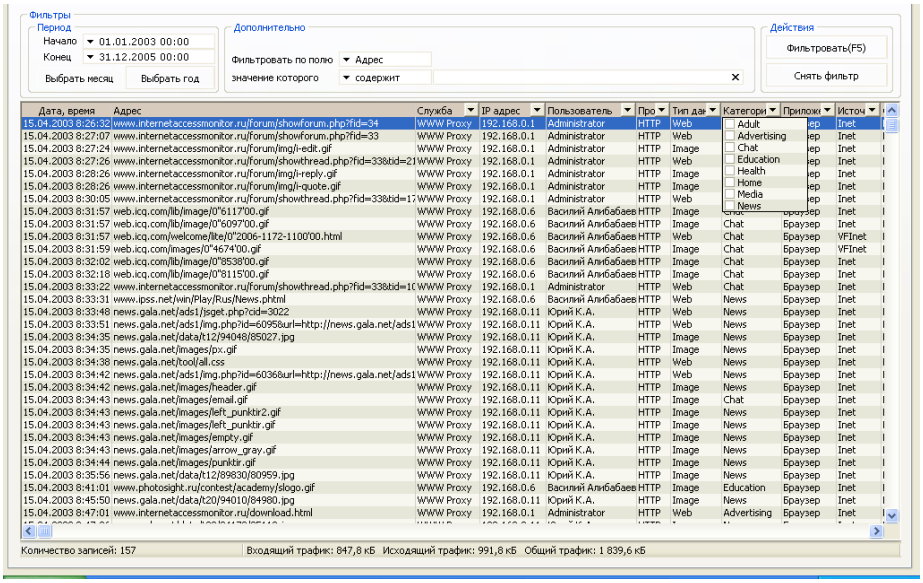
Перейшли до налаштування брандмауера. Переглянули та налаштували правила фільтрації пакетів:



Також у даній програмі є вбудований антивірус, що здатен сканувати саму систему на встановлені віруси.



Internet Access Monitor для Kerio WinRoute - програма, основним завданням якої є облік і контроль Інтернет трафіку.



2.4 Реалізація захисту системи

Проведемо тестування нашої програмної реалізації – в результаті ми повинні отримати стан захищеності банку

Для випробування обираємо утиліту AWFT 5.1 – це демонстративний зразок, який використовує технології троянів в умовах наближених до реальних.

Тестуємим фаєрволом , встановлений на віртуальну машину разом з утилітою AWFT 5.1

Технічні вимоги для запуску AWFT 5.1.

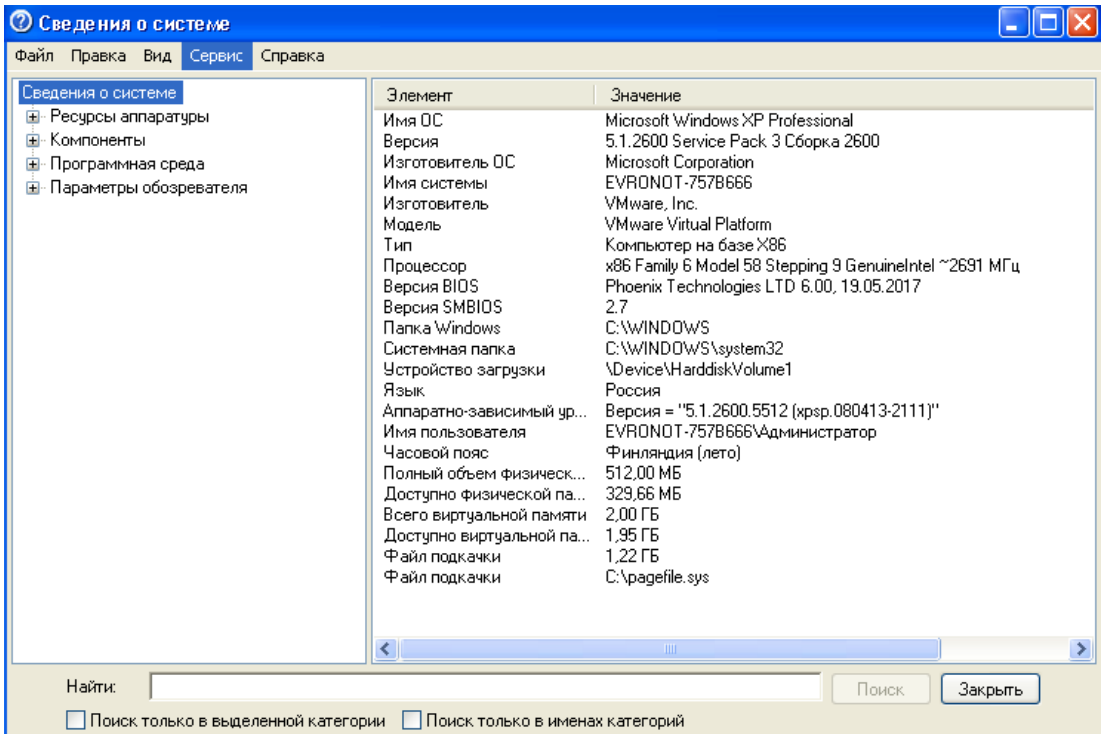
- ПК сумісний з Pentium 250 або вище, 32 або більш ніж мегабайт оперативної пам'яті.

- Windows NT (SP4 або пізнішої версії), Windows 2000, Windows XP або Windows Server 2003.

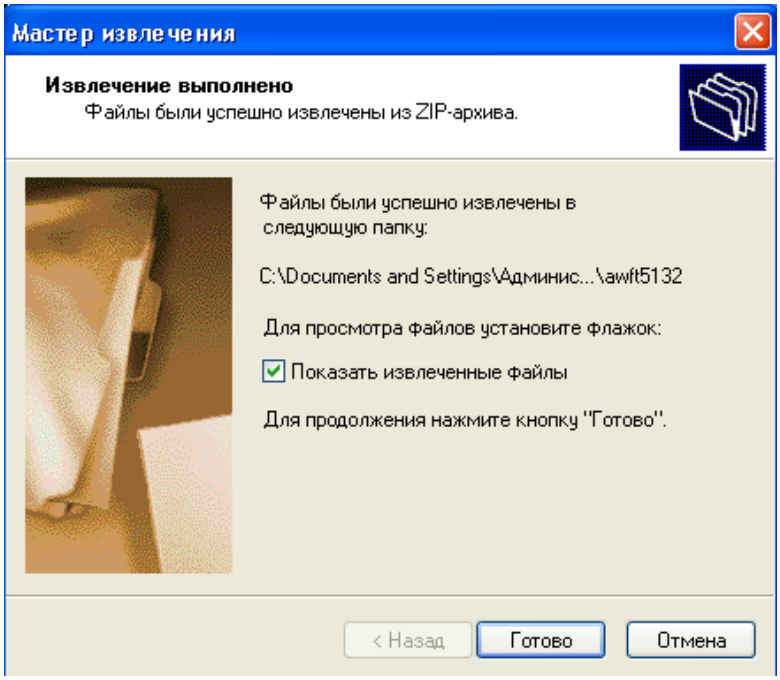
- активне підключення до Інтернету.

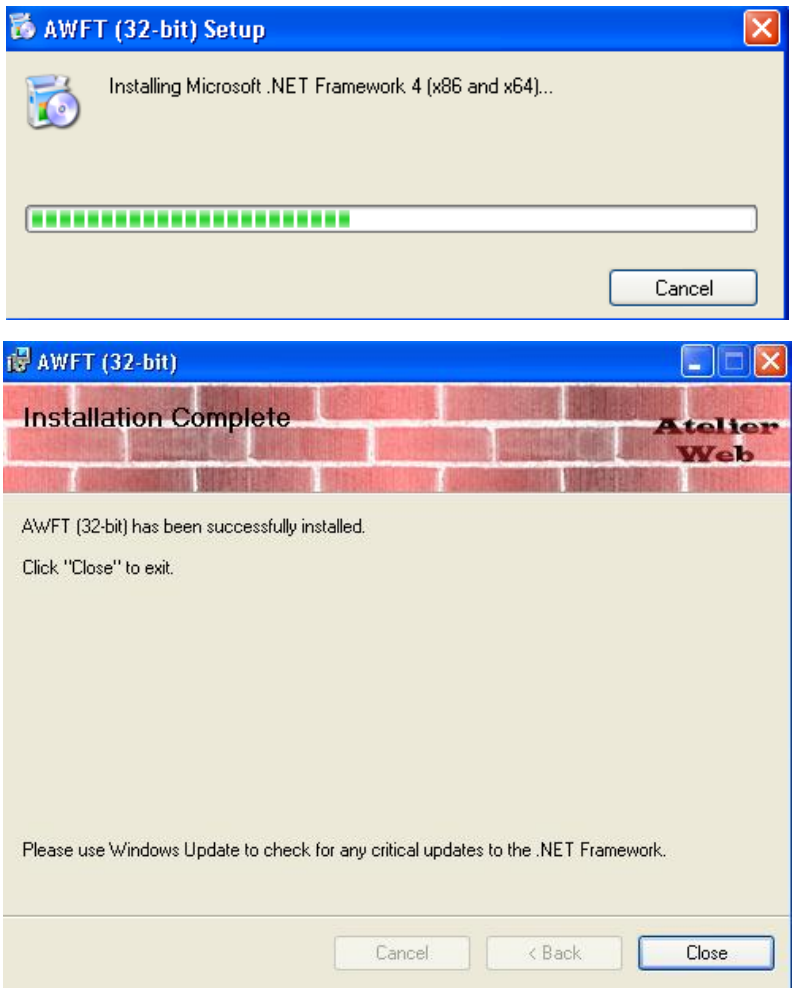
У якості дослідницького полігону буде використаний встановлений на віртуальну машину Windows XP.

Дані наводжу інформацію про використану систему:



Завантажуємо архів з утилітою, фаервол на файл не відреагував.





AWFT 5.1 пропонує 6 тестів для перевірки фаєрвола на якість захисту зсередини.

Тест 1: AWFT 5.1 намагається завантажити копію браузера за замовчуванням і патч в пам'яті перед виконанням. Поразки слабкими фаєрволами.

Тест 2: AWFT 5.1 створює теми на завантаженій копії браузера за замовчуванням. Старий метод, який ефективний для більшості старих антивірусів.

Тест 3: AWFT 5.1 створює теми на Windows Explorer. Інший метод, але більшість брандмауерів провалює тест.

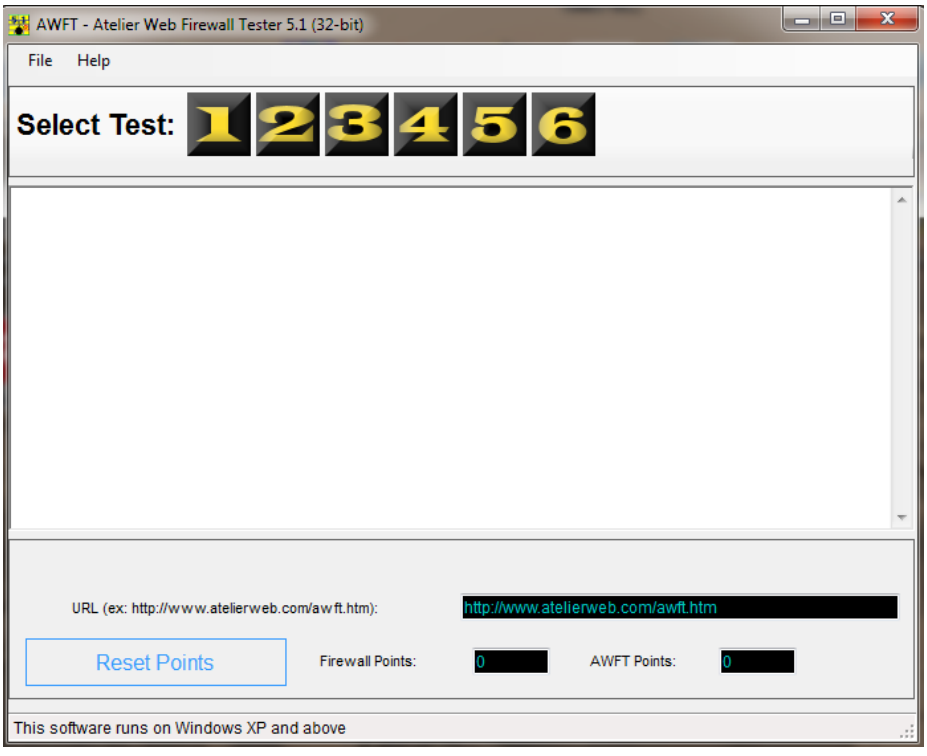
Тест 4: AWFT 5.1 намагається завантажити копію браузера за замовчуванням внутрішнього Windows Explorer і патч в пам'яті перед виконанням. Поразки фаєрволів, які вимагають дозволу на застосування для завантаження іншої копії браузера - Windows Explorer, як правило, дозволяється. Цей тест зазвичай

успішний, якщо браузером заблокований доступ до Інтернету, за замовчуванням.

Тест 5: AWFT 5.1 виконує евристичний пошук(У процесі пошуку в програмі використовується деяка оцінна функція, за допомогою якої можна грубо оцінити, наскільки "гарним" (чи "поганим") є поточний стан) для проксі-серверів і іншого програмного забезпечення з дозволеним доступом в Інтернет на порт 80, завантажує копію і парчі в пам'яті до виконання зсередини теми на Windows Explorer. Цей тест вкрай важкий для фаєрволів.

Тест 6: AWFT 5.1 виконує евристичний пошук проксі-серверів і іншого програмного забезпечення з доступом в Інтернет на порт 80, запитів користувачеві вибрати один з них, то створює нитку на вибір процесу.

Встановлюю та запускаю AWFT 5.1, фаервол та інтернет також запущені. Після запуску AWFT 5.1 бачимо таке вікно:



На головній панелі ми бачмо список із 6 тестів(які є діючими кнопками, в першому полі навпроти URL нам показують сайт для перевірки який наразі буде використовуватися з можливістю зміни, кнопка Reset Points обнуляє бали які набирає або фаєрвол або AWFT 5.1 після кожного тесту.

Суть тестів: утиліта намагається обійти фаєрвол і надіслати запит в інтернет і завантажити на комп'ютер інформацію, в даному випадку тестову веб-сторінку. Намагатися обманювати фаєрвол, утиліта буде шістьма різними способами. Тут будуть як старі, так і більш сучасні методи обходу фаєрволів.

Змінюю адресу завантажувальної сторінки на http://www.google.com/ та розпочинаю тестування.

Тест 1

Фаєрвол негайно реагує. Дія блокується.

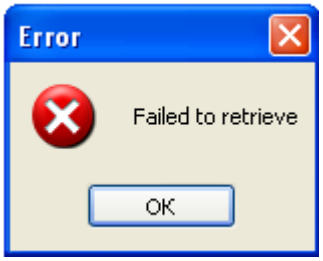
Тест 2

Фаєрвол негайно реагує. Дія відповідно також блокується.

Тест 3

Навіть на третьому тесті фаєрвол блокує атаку.

Тест 4



Більш нові методи також не можуть обійти фаєрвол, який відразу реагує та блокує атаку.

Тест 5

Утиліта AWFT намагатиметься обійти фаєрвол в режимі реального часу, під час серфінгу. Для тестування я запускаю браузер, відкриваю будь-який сайт і виконую рухи курсором миші. Після маніпуляцій натискаю у вікні AWFT кнопку п'ятого тесту.

Проте фаєрвол успішно блокує атаку та проходить перевірку.

Тест 6

Останній тест AWFT є аналогією попередньому. Використовується метод з пошуком встановленого софта, що має право виходити назовні через порт 80. Даний спосіб був змінений на використовування користувальницького запиту. Разом із цим AWFT намагається додати до браузеру хіджек, тобто власну таємну панель інструментів.

Для проходження тесту я знову запускаю браузер, відкриваю будь-який сайт і виконую рухи курсором миші. Після маніпуляцій натискаю у вікні AWFT кнопку шостого тесту.

Висновок: Вдало проведених атак у AWFT 0, а вдало відбитих атак у фаєрвола 6. Це я вважаю за ідеальний результат для фаєрволу

2.5 Висновки до розділу 2

В другому розділі ми розібрали більш детальний захист інформації

Системи та підсистеми захисту. Провели оцінку ризиків ІББ. Дослідили можливості небезпек та вивели все на діаграму. Спроектували систему захисту банку та показали систему захисту інформації

Висновок

У даній роботі було досліджено систему захисту системи банку, можливі загрози, ризики оцінка ризиків та система.

Дослідили загрози інформаційній безпеці банкую, тим самим, як ми могли помітити що у структурі захисту даних банківської установи, виділяють основні компоненти- безпека ресурсів та інфраструктури.

Так як, основним етапом при захисті інформації в інформаційних системах є аналіз ризиків. Імовірність того, що загроза реалізується, визначається наступними основними факторами - привабливістю ресурсу (цей показник враховується при розгляді загрози навмисного впливу з боку людини), та можливістю використання ресурсу для отримання доходу (показник враховується при розгляді загрози навмисного впливу з боку людини) а також простотою використання уразливості при проведенні атаки.

І класифікація може бути класифіковані за різними ознаками : «За аспектом інформаційної безпеки, на який спрямовані загрози: є Загрози конфіденційності (неправомірний доступ до інформації).

З цього можемо зробити висновок, що на сьогоднішній день важливо розвивати всі напрями інформаційної безпеки, адже дані які використовують люди, банки, та інші установи є важливою частиною нашого життя і впливають на подальше життя. На підставі «Критеріїв оцінки захищеності інформації в комп'ютерних системах (НСД) НДТЗ 2.5-004-99 проаналізував міжмережевий екран на предмет функціональності і захищеності, склав технічне завдання випробувань

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Казмірчук С.В. Дослідження методик оцінки ризиків / С.В. Казмірчук, В.В. Волянська // Сучасні проблеми захисту інформації з обмеженим доступом: міжвідомча науково-практ. конф., тези доп. – К., 2008. С.67-69.

2. НД-ТЗІ-2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах – А.2.1.8 Звіт за результатами проведення аналізу ризиків та формування завдань на створення КСЗІ

3. НД-ТЗІ-2.5-008-2002 – Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу

4. Казмирчук С.В. Базовые параметры риска в области информационной безопасности / С.В. Казмирчук // «АВІА-2011»: X міжнар. наук.-техн. конф. : матер. конф. – К. : НАУ, 2011. Том 1 – С. 2.68-2.71.

Закони та нормативні документи

5. Про основні засади державного нагляду (контролю) у сфері господарської діяльності [Текст] : Закон України №877-V від 5 квітня 2007 р. / Верховна Рада України // Відомості Верховної Ради України. – 2007. – №36. – Ст. 389.

6. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст] : НД ТЗІ 1.1-003 – 1999. – Чин. 1999. 04.28. – К. : ДСТСЗІ СБ України, 1999. – 12 с.

7. Типове положення про службу захисту інформації в автоматизованій системі [Текст] : НД ТЗІ 1.4-001 – 2000. – Чин. 2000.12.04. – К. : ДСТСЗІ СБ України, 2000. – 32 с.

8. Security of Information Systems in Organization: A Bank Model - **2013 – 47стр**

9. Securing Information Technology for Banks and Accounting Information Systems - (2018) pp. 3291-3300

10. Information Security in Banks and Financial Institutions – 2016 – 34

11. Information Security Risk Assessment Checklist

12. Типове положення про службу захисту інформації в автоматизованій системі [Текст] : НД ТЗІ 1.4-001 – 2000. – Чин. 2000.12.04. – К. : ДСТСЗІ СБ України, 2000. – 32 с.

13. Руководство по управлению рисками безопасности [Электронный ресурс] / Группа разработки решений Майкрософт по безопасности и соответствию, регулятивным нормам ; Центр Microsoft security center of excellence // TechNet. – Электрон. дан. – Редмонд, США : Корпорация Майкрософт, 2006. – Режим доступа: World Wide Web. – URL: http://technet.microsoft.com/ru-ru/library/ cc163143.aspx. – Загл. с экрана (просмотрено 29 декабря 2011).

14. Казмирчук С.В. Система выбора средств анализа и оценки риска / С.В. Казмирчук, А.Ю. Гололобов, К.В. Никитина // Безпека інформації. – 2012. – №1. – С 15-18.

15. Корченко А.Г. Методы анализа и оценки рисков потерь государственных информационных ресурсов / А.Г. Корченко, В.П. Щербина, С.В. Казмирчук // Захист інформації – 2012. – №1. – С. 126-139.

16. Скулыш Е.Д. Средства анализа и оценки риска информационной безопасности / Е.Д. Скулыш, А.Г. Корченко, Ю.И. Горбенко, С.В. Казмирчук // Інформаційна безпека. Людина, суспільство, держава – 2011. – №3 (7). – С.31-48.

17. Peltier T.R. Information security risk analysis / Thomas R. Peltier. – London : Auerbach Publications, 2001. – 281 p

18. Типове положення про службу захисту інформації в автоматизованій системі [Текст] : НД ТЗІ 1.4-001 – 2000. – Чин. 2000.12.04. – К. : ДСТСЗІ СБ України, 2000. – 32 с

19. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст] : НД ТЗІ 1.1-003 – 1999. – Чин. 1999. 04.28. – К. : ДСТСЗІ СБ України, 1999. – 12 с.

20. Про основні засади державного нагляду (контролю) у сфері господарської діяльності [Текст] : Закон України №877-V від 5 квітня 2007 р. / Верховна Рада України // Відомості Верховної Ради України. – 2007. – №36. – Ст. 389.

21. Риск [Электронный ресурс] / [Авторы Википедии]. – Версия 44986537 // Википедия : Свободная энциклопедия. – Электрон. дан. – Сан-Франциско : Фонд Викимедиа, 2012. – Режим доступа: World Wide Web. – URL: http://ru.wikipedia.org/?oldid=44986537. – Загл. с титул. экрана. – Описание на основе версии, датированной 3 июня 2012 08:54 UTC

22. НОРМАТИВНИЙ ДОКУМЕНТ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від " 28 " квітня 1999 р. № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806- https://tzi.com.ua/downloads/1.1-002-99.pdf

23. Охорона банківської таємниці – правові засади - http://obt.inf.ua/page10.html#q2

24. Загрози інформаційній безпеці у банківських установах- https://essuir.sumdu.edu.ua/bitstream-download/123456789/34067/1/Borysova_banking%20establishment.pdf;jsessionid=AFB4D4F374D21E374F4A4CDCCDC976DE

25. Є.М. Бодюл, канд. юрид. наук, начальник відділу з організації науково-дослідної роботи Національної академії внутрішніх справ ІНФОРМАЦІЙНА БЕЗПЕКА БАНКУ - http://obt.inf.ua/user-files/tezy_konf.pdf#page=53

26. ОСНОВНІ ЗАСОБИ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА ТА ІНФОРМАЦІЙНОЇ ВІЙНИ ЯК ЯВИЩА СУЧАСНОГО МІЖНАРОДНОГО ПОЛІТИЧНОГО ПРОЦЕСУ -http://kul-lib.narod.ru/bibl.files/NBU/metod_01_03011.pdf

27. Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків - https://zakon.rada.gov.ua/laws/show/v0365500-11#Text

28. Information Technology for Banks- https://www.ripublication.com/ijaer18/ijaerv13n6_21.pdf

29. Астахов А.М. Искусство управления информационными рисками / А.М. Астахов – М : ДМК Пресс, 2010. – 314 с.

30. Thomas A.P. Information security risk analysis / John M. Palmer. – London : Publications, 2001. – 281 p.