МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Система антивірусного захисту комп'ютерної мережі малого підприємства»

Завідувач
випускаючої кафедри **А. С. Довбиш**

Керівник роботи **В.В. Кальченко**

Студент групи КБ-71 **М.А. Чорненький**

СУМИ 2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

"_____" _____2021 г.

ЗАВДАННЯ
до випускної роботи

Студента четвертого курсу, групи КБ-71 спеціальності "Кібербезпека" денної форми навчання Чорненького Микити Анатолійовича.

Тема: "**Система антивірусного захисту комп'ютерної мережі малого підприємства**"

Затверджена наказом по СумДУ

№_____ от _____2021 г.

Зміст пояснювальної записки: 1) Аналіз предметної області. Огляд загроз і ризиків комп'ютерної мережі малого підприємства, Постановка задачі. 2) Огляд існуючих рішень, Zillya, Bitdefender,Інші способи захисту ПК.ESET. MCAfee, Avast. 3) Інформаційний огляд програми. Завантаження, Встановлення, Використання. 4) Розгортання та налагодження серверної частини антивірусної системи, Розгортання клієнтської частини антивірусної системи, Розробка і впровадження налаштувань антивірусної системи, Результати розробки.

Дата видачі завдання "_____"_____2021 г.

Керівник випускної роботи _____ Кальченко В.В.

Завдання приняв до виконання _____ Чорненький М.А.

РЕФЕРАТ

Записка: 91 стр., 70 рис., 14 джерел., 8 таблиць

Об’єкт дослідження – антивірусні програми та антивірусний захист корпоративної мережі від компанії Eset.

Мета роботи – дослідити антивіруси, їх призначення та можливості.

Методи дослідження – спрощення та пришвидшення процесу встановлення антивірусів.

Результати – В ході виконання роботи було досліджено методи швидкого розгортання антивірусних систем за допомогою вбудованих інструментів Windows Server та антивірусного забезпечення Eset Remote Administrator.

Зміст

Вступ

В світі в котрому електронні пристрої займають більшу частину нашого життя, тоді коли вони перестали бути простими засобами для розваг, а перетворилися на потужні машини котрі проводять багато різних операцій з даними, а також можуть зберігати на своїх накопичувачах данні котрі люди або компанія не хотіла б втратити.

Важливість цього ми й так знаємо. Тому їм на допомогу приходять розробники так званих антивірусів.

Антивірус це спеціальна програма створена для сканування електронних пристроїв на предмет шкідливого ПО. І таких спеціальних програм існує багато різних видів, котрі мають різний функціонал, різну вартість, різну направленість.

Які види антивірусів існують?

Існують декілька видів антивірусних програм, такі як антивірусні сканери, антивірусні монітори, поліфаги, монітори, ревізори та блокувальники.

Антивірусні сканери це програми які одразу ж після запуску перевіряють файли та оперативну пам’ять комп’ютера на наявність можливих вірусних загроз та забезпечують нейтралізацію знайденого вірусу.

Антивірусні монітори це програми які постійно знаходяться в операційній системі та забезпечують постійну перевірку файлів в процесі їх загрузки в операційну систему.

Поліфаги це універсальне та ефективне антивірусне ПО. Перевіряє файли, завантажувальні сектора жорсткого диску і операційної системи на наявність нових та невідомих вірусів. Із мінусів займають багато місця на жорсткому диску та повільна робота.

Ревізори програма яка провіряє зміни у файлі, не можуть знайти вірус у нових файлах так як не перевіряли попередню інформацію про файл, але займають зовсім небагато місця.

Блокувальники здатні виявити та зупинити вірус на ранній стадії його розвитку, наприклад при записі в завантажувальний сектор диска, антивірусні програми можуть входити до складу BIOS Setup.

1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Огляд загроз та ризиків комп’ютерних мереж малого підприємства

Основні ризики котрі зустрічаються в мережах малого підприємства. Люди котрі завжди будуть слабкою ланкою в будь якій інформаційній системі. Застарілі технології, які дуже часто використовуються в мережах малого підприємства. Тому через свою застарілість мають багато проблем в захисті. Відсутність компетентних спеціалістів котрі повинні забезпечувати безпеку мережі. Все це може призвести до витоку, викрадення, втрати важливих даних мережі малого підприємства.

1.2 Аналіз сучасного шкідливого програмного забезпечення

Сучасне шкідливе програмне забезпечення поділяється на троянські програми, програми шпигуни, вимагачі, вандали, руткіти, ботнети, кейлогери, бекдори, експлойти, макровіруси.

Троянські віруси – котрі проникають до комп’ютерів під видом безпечних програм, Основний функціонал даних програм це викрадення паролів або збір даних.

Шпигуни це програми котрі відслідковують дії користувача та передають їх зловмиснику також можуть аналізувати дії користувачів в інтернеті та на основі цього можуть демонструвати користувачам рекламу.

Вимагачі повністю блокують доступ до комп’ютеру та потребують гроші за розблокування даних. Мають можливість шифрування заблокованих даних.

Вандали блокують доступи к сайтам антивірусів та доступ к антивірусів та іншим програмам.

Руткіти це віруси гібриди, котрі можуть містити в собі інші віруси. Мають різний функціонал, можуть отримати доступ до ПК, маскуються під інші віруси та збирають данні про комп’ютери та їх процеси.

Ботнети це великі мережі заражених комп’ютерів котрі використовуються для спільних ДДОС та інших кібератак, які через велику кількість комп’ютерів дуже важко відслідкувати.

Кейлогери це такі клавіатурні шпигуни котрі перехоплюють будь який ввід з клавіатури.

Бекдори це утілити для прихованого адміністрування, що дозволяють обійти систему захисту та контролювати комп’ютер, без відому користувача.

Експлойти це скрипт або програма котрі використовують специфічні уразливості ОС для проникнення у систему.

Макровіруси це невеликі програми котрі написанні на макромові, поширюються лише через документи що створені для спеціального додатку котрі використовуються для подальшого запуску.

1.3 Постановка задачі

На основі інформації про шкідливе ПЗ треба про аналізувати існуючи методи захисту та обрати найкраще, після чого створити систему захисту локальної мережі малого підприємства.

2. ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

2.1 Zillya

Почнемо з нашого вітчизняного антивірусу з назвою Zillya! від українського розробника “Лабораторія Zillya!” створений був у 2009 році, остання версія вийшла 26 травня 2015р. Має декілька варіантів поширення для дому та бізнесу, для бізнесу та держави, смартфону і планшету, та безкоштовна версія. Також версія для дому та бізнесу має декілька різних варіантів розповсюдження.

Zillya! Антивірус найдешевший варіант та найменша кількість можливостей

Zillya! Internet Security середній варіант між ціною та кількістю можливостей

Zillya! Total Security максимальна кількість можливостей для комплексного захисту ПК.[1]

Таблиця 2.1. Варіанти розповсюдження антивірусу Zillya!

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

Віртуальна клавіатура Зберігає пароль від крадіжки зловмисниками		Так	Так
Оптимізатор Виявляє сміттєві файли системи та звільнити місце на диску		Так	Так
Файл-шредер Забезпечує видалення інформації без можливості відновлення		Так	Так
Батьківський контроль Надає ефективний інструмент контролю батькам за активністю дитини за ПК			Так
Менеджер процесів Дозволяє контролювати та управляти запущеними програмами/процесами.			Так
Менеджер автозапуску Дає можливість переглянути список програм, котрі завантажуються автоматично із запуском операційної системи та відключити програми з автозапуску.			Так

Приватність даних Дозволяє очистити дані профілів користувача в браузерах та забезпечити таким чином приватність роботи в мережі.			Так

Таблиця 2.2 Варіанти розповсюдження антивірусу Zillya для мобільних пристроїв

	Zillya! Mobile Antivirus	Zillya! Internet Security for Android 2.0
Антивірус Має повноцінний антивірусний функціонал.	Так	Так
Сканер Знаходить та видаляє шкідливі програми.	Так	Так
Автопілот Здійснює перевірку нових додатків одразу в момент встановлення.	Так	Так
Планувальник Можливість назначити регулярне сканування.	Так	Так
Оптимізатор Дозволяє очистити тимчасові файли із диску та звільнити необхідне місце на пристрої.	Так	Так
Прискорювач Допомагає вивантажити додатки із оперативної пам’яті для прискорення роботи системи та подовження роботи батареї.	Так	Так
Антикрадій Захист даних на телефоні при втраті або крадіжці.		Так
Веб-фільтр Блокування доступу до фішингових та інших шкідливих сайтів.		Так
Батьківський контроль Дозволяє контролювати активність дитини в мережі Інтернет.		Так

Версія для планшету Доступна повноцінна версія для планшету	Так	Так

2.2 Bitdefender

Наступним у списку буде один з найпопулярніших антивірусів це румунський Bitdefender котрий стоїть на захисті у 500 мільйонів користувачів на протязі 18 років. Як і всі інші антивіруси має декілька рішень для різних потреб а також різних платформ. Із незвичайного це те що всі рішення можуть бути встановлені на декілька різних пристроїв незалежно від того які вони – ПК, Mac, Android, IOS, купуючи спеціальний набір можна забути про те який антивірус встановити на тому чи іншому пристрої. Також в продажі існує спеціальний Bitdefender BOX це екосистема кібербезпеки яка підключається до шлюзу інтернет провайдера або до персонального маршрутизатора, використовувати як автономну систему захисту для усіх потреб в інтернеті. В комплекті також йде антивірус Bitdefender Total Security та сам Box Network Security Hub. [2]

Таблиця 2.3 Варіанти розповсюдження антивірусу Bitdefender

Можливості	Bitdefender Internet Security	Bitdefender Total Security	Bitdefender Family Pack
Повний захист даних у режимі реального часу. (Windows\MacOs)	Так (Тільки Windows)	Так	Так
Bitdefender VPN Захищає вашу інтернет-присутність, шифруючи весь інтернет-трафік. 200 МБ щоденного трафіку включено на кожен пристрій.	Так (Тільки Windows)	Так	Так

Захисник файлів Запобігає несанкціонованим змінам ваших найважливіших файлів. (Windows\MacOs)	Так (Тільки Windows)	Так	Так
Батьківський контроль Пропонує цифрову допомогу батькам та додаткову безпеку в Інтернеті для дітей. Увійдіть віддалено в Bitdefender Central, щоб не відставати від них. (Windows\MacOs\Android\IOS)	Так (Тільки Windows)	Так	Так
Профілактика веб-атак Наша технологія веб-фільтрації гарантує, що ви ніколи не потрапляєте на шкідливий веб-сайт. (Windows\MacOs)	Так (Тільки Windows)	Так	Так
Вдосконалений захист від загроз Вдосконалена технологія, орієнтована на поведінку, виявляє та блокує розширені загрози та програм вимагачів. (Windows)	Так	Так	Так
Багатошаровий захист від програм вимагачів	Так	Так	Так

Кілька шарів захисту від програм вимагачів захищають ваші файли від шифрування. (Windows)			
Антитрекер Зберігає приватний перегляд і дозволяє керувати трекерами, які збирають ваші дані. (Windows)	Так	Так	Так
Мікрофонний контроль Допомагає вам відновити контроль над власними пристроями. Використовуйте його, і ви зможете побачити, які програми мають доступ до мікрофона вашого пристрою та коли. (Windows)	Так	Так	Так
Радник з безпеки Wi-Fi Отримайте доступ до своєї мережі Wi-Fi та безпеки маршрутизатора, незалежно від того, звідки ви підключаєтесь. (Windows)	Так	Так	Так

Безпечний Інтернет-банкінг Користуйтеся банками та здійснюйте покупки із Safepay, нашим унікальним Спеціалізованим браузером, Який забезпечує безпеку ваших транзакцій. (Windows)	Так	Так	Так
Менеджер паролів Захищає ваші паролі, інформацію про кредитні картки та інші конфіденційні дані в кібер-сховищі для легкого доступу, коли вони вам знадобляться. (Windows)	Так	Так	Так
Антифішинг та боротьба з шахрайством Запобігає фішинг чи шахрайство в Інтернеті, коли ви купуєте, купуєте чи просто користуєтесь браузером. (Windows)	Так	Так	Так
Оцінка вразливості Перевірте наявність на наявність “дірок” у безпеці та вразливості однією миттю. (Windows)	Так	Так	Так
File Shredder Видаліть файл назавжди і не залишайте слідів, які він коли-небудь існував на вашому ПК. (Windows)	Так	Так	Так

Захист веб-камери Повідомляє вас, коли додатки намагаються отримати доступ до вашої веб-камери та дозволяє блокувати несанкціонований доступ. (Windows)	Так	Так	Так
Брандмауер конфіденційності Блокує вторгнення та фільтрує ваш мережевий трафік. (Windows)	Так	Так	Так
Безпечні файли Запобігає несанкціонованим змінам ваших найважливіших файлів.(Windows)	Так	Так	Так
Батьківський контроль Пропонує цифрову допомогу батькам та додаткову безпеку в Інтернеті для дітей. Увійдіть віддалено в Bitdefender Central, щоб не відставати від них. (Windows\MacOs\Android\IOS)	Так (Тільки Windows)	Так	Так
Шифрування файлів Створює на комп'ютері зашифровані, захищені паролем сховища для конфіденційних та конфіденційних документів. (Windows)	Так	Так	Так

Мережева профілактика загроз Нові технології розвідувальної інформації про кіберзагрози можуть аналізувати та виявляти підозрілі заходи на рівні мережі, а також блокувати складні подвиги, URL-адреси, пов'язані із зловмисним програмним забезпеченням чи ботнетом, та жорстокі атаки. (Windows)	Так	Так	Так
Захисту від угону Упаковує ефективні засоби проти втрат і проти крадіжок, і це доступно віддалено. (Windows\Android)		Так	Так
Прискорювач пристроїв Підвищує швидкість та продуктивність ваших пристроїв за допомогою оптимізатора OneClick. (Windows)		Так	Так
Захист "машини часу" Запобігає шифруванню чи знищенню резервних копій складних зловмисних програм. (Mac)		Так	Так
Adware Blocker Звільніть свій Mac від рекламного ПЗ, програм викрадачів, небажаних панелей інструментів та інших додатків браузера. (Mac)		Так	Так
Економія акумулятора та продуктивність Захищає ваш мобільний досвід практично не впливаючи на швидкість або час автономної роботи. (Android)		Так	Так

Захист веб-сторінок Повідомляє вас про веб-сторінки, які містять зловмисне програмне забезпечення, фішинг або шахрайський вміст. (Android\IOS)		Так	Так
Конфіденційність аккаунту Перевіряє,чи ваші онлайн-акаунти були причетні до будь-якого порушення даних. (Android\IOS)		Так	Так

2.3 Інші способи захисту ПК

Якщо ми не хочемо використовувати повноцінні антивіруси, але хочемо захисту нашої системи на допомогу нам приходить Microsoft з їх вбудованим антивірусом Windows Defender[5] це безкоштовний антивірус який встановлюється разом з Windows та надає захист комп’ютера на початковому етапі, та після. Його використання не впливає на продуктивність комп’ютера тому може підійти як альтернатива звичайному антивірусу. Наступним захисником нашого комп’ютеру може виступити Malwarebytes та Malwarebytes AdwCleaner.[4] На відмінну від інших антивірусів вони можуть боротися з вірусами але основне напрямлення це знешкодження рекламних вірусів.

2.4 ESET

Наступним антивірусом у списку, це словацький ESET, за офіційними даними їм користуються 110 мільйонів користувачів. В своєму розпорядженні має багата різних варіантів розповсюдження від майже усіх відомих платформ до декількох варіантів на платформ або ж універсальний варіант для всього. А також заготовлені спеціальні бізнес пакети. Для мікробізнесу з їх ESET SMALL OFFICE PACK(Захист робочих станцій та захист мобільних пристроїв), ESET SMALL OFFICE PACK СТАНДАРТНИЙ(Централізоване управління, захист робочих станцій, розширений захист робочих станцій, захист мобільних пристроїв, захист файлових серверів), ESET NOD32 SMALL BUSINESS PACK(Централізоване управління, захист робочих станцій та захист мобільних пристроїв).

Для малого та середнього бізнесу ESET NOD32 ANTIVIRUS BUSINESS EDITION(Централізоване управління, захист робочих станцій та захист мобільних пристроїв, захист файлових серверів), ESET NOD32 SMART SECURITY BUSINESS EDITION(Централізоване управління, захист робочих станцій, розширений захист робочих станцій, захист мобільних пристроїв, захист файлових серверів), ESET NOD32 SECURE ENTERPRISE(Централізоване управління, захист робочих станцій, розширений захист робочих станцій, захист мобільних пристроїв, захист файлових серверів, захист почтових серверів, захист шлюзів).

Та великого ESET DYNAMIC MAIL PROTECTION(Централізоване управління, захист почтових серверів, вбудована пісочниця), ESET ENDPOINT PROTECTION PLUS(Централізоване управління, захист робочих станцій, розширений захист робочих станцій, захист мобільних пристроїв, захист файлових серверів, вбудована пісочниця), ESET DYNAMIC ENDPOINT PROTECTION(Централізоване управління, захист робочих станцій, розширений захист робочих станцій, захист мобільних пристроїв, захист файлових серверів, вбудована пісочниця, розширений захист робочих станцій), ESET ENTERPRISE THREAT DEFENSE(Централізоване управління, захист робочих станцій, розширений захист робочих станцій,

захист мобільних пристроїв, захист файлових серверів, захист почтових серверів, захист шлюзів, вбудована пісочниця).[6]

Таблиця 2.4 Варіанти розповсюдження антивірусу Eset NOD32

	ESET NOD32 Антивиру с (Windows)	ESET NOD32 Internet Security (Windows, Android, MacOs, Linux)	ESET NOD32 Mobile Securit y (Androi d)	ESET NOD32 Cyber Security (MacOs)	ESET NOD32 Cyber Security Pro (MacOs)	ESET NOD32 Антиві рус для Linux Deskto p (Linux)
Захист від вірусів і програм-вимагачів	Так	Так	Так	Так	Так	Так
Захист від інтернет-шахраїв	Так	Так		Так	Так	Так
Розширен е машинне навчання	Так	Так				
Захист он-лайн-п латежів		Так				
Захист домашній мережі і веб-камер и		Так				
Захист від хакерів		Так		Так	Так	Так
Антивор		Так				
Батьківсь кий контроль для ПК		Так				

Батьківський контроль для Android		Так				
Кросплатформенная захист	Так	Так				
Захист мобільних пристроїв і Smart TV		Так				
Захист особистих даних		Так	Так	Так	Так	
Захист SIM-карти		Так	Так			
Пошук зниклого пристрою		Так	Так			
Захист веб-камери		Так				
Безпека дітей		Так			Так	
Ігровий режим		Так		Так	Так	

2.5 MCAfee

Наступним буде антивірус від американської компанії MCAfee, Був створений в 1988 році, до даного часу мав декілька неприємних моментів в 2010 році після одного з оновлень антивірус почав видаляти системний файл svhost.exe після чого комп’ютери втрачали доступ до інтернету а в деяких випадках починали нескінченне перезавантаження комп’ютера. В 2012 знову з’явилася помилка яка відключала користувачам інтернет. На даний момент антивірус має більш 500 мільйонів активних користувачів. Має декілька варіантів розповсюдження це McAfee® Total Protection, McAfee® Safe Connect VPN(надає захист при використанні загально доступних мережах Wi-Fi, захищає конфіденційність скриваючи нашу IP адресу, ваше фізичне розташування, банківські реквізити і дані кредитної картки будуть захищені під час роботи в Інтернеті та при підключенні через віртуальний сервер по всьому світу ви можете отримати доступ до вмісту, додатків і веб-сайтів, використання яких обмежено по регіону), McAfee® Safe Family (відслідковує те як ваші діти користуються своїми пристроями, має можливість обмежувати екранний час для користування пристроями та можливість блокування додатків і фільтрацією веб-сайтів), McAfee® WebAdvisor (блокує шкідливі та фішингові сайти, навіть якщо ви випадково натиснете на посилання, повідомляє вас при неправильному введені адреси веб-сайту та безпечне завантаження що перевіряє файли перед завантаженням і попереджає про загрозу) та McAfee® Mobile Security для Android.[7]

Таблиця 2.5 Варіанти розповсюдження антивірусу McAfee

McAfee® Total Protection
Антивірусна програма
Оптимізація швидкодії
Онлайн підтримка від кваліфікованих спеціалістів служби підтримки
Диспетчер паролів
Безпечний перегляд веб-сторінок
McAfee® Shredder
Зашифроване сховище

Таблиця 2.6 Варіанти розповсюдження антивірусу мобільної версії McAfee

McAfee® Security Mobile Starter (IOS та Android)	McAfee® Security Mobile Standard (IOS та Android)	McAfee® Security Mobile PLUS (IOS та Android)
Перевірка безпеки	Перевірка безпеки	Перевірка безпеки
Перевірка конфіденційності	Перевірка конфіденційності	Перевірка конфіденційності
Захист від крадіжок	Захист від крадіжок	Захист від крадіжок
Безпечна мережа Wi-Fi	Безпечна мережа Wi-Fi	Безпечна мережа Wi-Fi
Оптимізація батареї	Оптимізація батареї	Оптимізація батареї
Оптимізація пам'яті	Оптимізація пам'яті	Оптимізація пам'яті
Засіб очищення сховища	Засіб очищення сховища	Засіб очищення сховища
Відстеження обсягу трафіку	Відстеження обсягу трафіку	Відстеження обсягу трафіку
	Резервне копіювання мультимедійних даних	Резервне копіювання мультимедійних даних
	Підтримка по телефону	Підтримка по телефону
	Без вбудованої реклами	Без вбудованої реклами
	Надійне блокування додатків	Надійне блокування додатків
	Гостьовий режим	Гостьовий режим
	Безпечний веб-перегляд	Безпечний веб-перегляд
		VPN для захисту Wi-Fi

2.6 Avast

Наступним у списку антивірусів буде чеський Avast Antivirus від однойменної Avast Software існує дві версії антивірусу для усіх платформ це Avast Free Antivirus та Avast Premium Security, а також набір окремих утиліт котрі мають вузько напрямлені можливості це Avast AntiTrack котрий допомагає дізнатися які сайти ведуть спостереження за вашими діями, скриває дії котрі ви робили на сайті, скриває данні про покупки в інтернеті для того щоб не було реклами подібних товарів, а також дозволяє збирати данні про ваш ПК. Avast Secure Browser це браузер від Avast котрий забезпечує швидкий перегляд сайтів без реклами, безпека будь яких дій в інтернеті, захищає данні від викрадення, блокування шкідливих сайтів та завантажень, автоматичний примус сайтів до використання шифрування, приховування електронних особових даних за допомогою унікального профілю браузера, отримання сповіщень при виток облікових даних. А також програми котрі допомагають з підвищенням продуктивності ПК це Avast Cleanup Premium допомагає підвищити продуктивність ПК за рахунок своїх інструментів це сплячий режим це запатентований метод настройки переводить всі ресурсомісткі програми в сплячий режим, Shortcut Cleaner для видалення старих ярликів, автоматичне обслуговування ПК, очистка диску, Registry Cleaner що видаляє непотрібні дані з реєстру, очистка браузеру для видалення непотрібних файлів та файлів cookie, панель налаштувань та центр підтримки для огляду стану вашого ПК, видалення непотрібного ресурсномісткого ПО, дефрагментація і оптимізація диска, Disk Doctor що допомагає перевіри диск на наявність помилок на диску та виправляє їх або попереджає про їх появлення, Avast Driver Updater що допомагає з вирішенням проблем з драйверами, з їх встановленням або виправляє їх. Avast Battery Saver допомагає зменшити використання батареї та підвищити час роботи ноутбука. Повернемося до повноцінного антивірусу Avast Premium Security має два варіанти розповсюдження для ПК, та версія для смартфонів Mobile Security. Безкоштовна версія передбачає тільки блокування вірусів, шпигунських програм, та інших загроз в реальному часі. Преміум версія має більший

функціонал такий як миттєве попередження через вразливості Wi-Fi мережі та спробах злому їх, захист від переходу на фішингові сайти, захист веб-камери, захист паролів в браузері від їх крадіжки, пісочниця що дозволить відкривати небезпечні файли в безпечній середі, знищення конфеденційних даних без можливості відновлення, можливість використовувати ще один антивірус, та режим не турбувати що відключити повідомлення від Windows та інших додатків. Все це мають версії для Windows та MacOs. Мобільні версії мають інший функціонал такі як звичайний антивірус, веб захист, сховище фотографій, блокування додатків, безпека Wi-Fi, Anti-Theft що допомагає відслідкувати викрадений телефон, заблокувати телефон та видалення даних, останнє відоме місце розташування у випадку розрядження пристрою, захист SIM-карти що автоматично реєструє телефон як втрачений в випадку зміни SIM-карти, блокування дзвінків, енергозбереження. Все це мають версії для Android та IOS.[8]

2.7 Norton

Останнім у списку антивірус буде від американської компанії NortonLifeLock з їх антивірусом Norton AntiVirus що дуже часто піддавався критиці, через свої помилки та помилки керівництва через свою кооперацію з ФБР через те що в антивірус, була додана до білого списку програма кейлогер Magic Lantem котрий й був розроблений ФБР. Наступним буде помилка котра після одного з оновлень почала помічати програму Spotify як троянський вірус. Наступне за що був розкритикований це те що після видалення антивірусу на комп'ютері залишались його файли. Останнім буде те що в 2009 році, деякі користувачі антивіруси знайшли файл який асоціюється з антивірусом з назвою Pifts.exe та постійно намагається підключитись до мережі. Хоч цей файл і вважався діагностичним патчем але чомусь на форумі антивірусу пости з цим файлом постійно видалялись. Функціонал майже нічим не відрізняється від інших, із цікавого це спеціальна хмара для резервного копіювання даних комп'ютера та відновленні при втраті доступу до комп'ютеру, жорсткого диску, або після шифрування даних через програму вимагач, а також можливість зв'язатися з експертами з лабораторії Norton котрі допоможуть у видаленні вірусу, і якщо вірус не буде видалено то гроші за підписку будуть повернені. Існують також версії для IOS та Android котрі не відрізняються від інших описаних вище. А також версії від Norton 360 Standard до Norton 360 Premium мають можливість встановлення на всі види пристроїв.[9]

Таблиці 2.7 Варіанти розповсюдження антивірусу Norton AntiVirus

	Norton AntiVirus Plus	Norton 360 Standard	Norton 360 Deluxe	Norton 360 Premium
Кількість пристроїв	Norton Antivirus Plus забезпечує захист для 1 пристрою ПК або Mac.	Norton 360 Standard забезпечує захист одного пристрою PC, Mac®, смартфона або планшета.	Norton 360 Deluxe забезпечує захист до 5 ПК, Mac®, смартфонів або планшетів.	Norton 360 Premium забезпечує захист до 10 ПК, Mac®, смартфонів або планшетів
Захист від Програм шпигунів, шкідливих програм і програм-вима гачів і антивірусна програма	Так	Так	Так	Так
Резервне копіювання в хмарі для ПК	2GB	10GB	75GB	100GB
Брандмауер для PC і Mac	Так	Так	Так	Так
Password Manager	Так	Так	Так	Так
«Обіцяємо захистити від вірусів»	Так	Так	Так	Так
Батьківський контроль			Так	Так
SafeCam для ПК		Так	Так	Так

2.8 Порівняльний аналіз сучасних антивірусних програмних засобів

Для того щоб вирішити який антивірус обрати, треба створити наглядну таблицю порівняння де на основі важливих параметрів буде обраний антивірус для подальшої роботи. За наданими даними від компанії AV-Test, кращі антивіруси будуть проаналізовані за спеціальними параметрами.

Таблиця 2.8 Порівняльний аналіз антивірусних програм

	Zillya! Total Security	Bitdefender Total Security	ESET NOD32 Endpoint Security	McAfee Total Protection	Avast Ultimate	Norton 360 Premium
Швидкодія	3\6	5\6	6\6	4\6	3\6	3\6
Захист	3\6	5\6	6\6	4\6	4\6	4\6
Зручність використання	4\6	5\6	6\6	4\6	4\6	3\6
Наявність експертного висновку	Ні	Ні	Так	Ні	Ні	Ні

За даною таблицею а також за попереднім аналізом можливостей антивірусного захисту. Найкращім варіантом антивірусного захисту через свою ефективність, кількість можливостей та наявністю потрібного ПЗ для захисту локальних мереж, є антивірус від словацької компанії Eset з їх антивірусом ESET NOD32 Endpoint Security та їх програмним забезпеченням Eset Remote Administrator.

3. ІНФОРМАЦІЙНИЙ ОГЛЯД ПРОГРАМИ

3.1 Завантаження

Все починається з офіціального сайту ESET.UA перейшовши до вкладки для бізнесу, усі продукти, всі продукти для бізнесу, шукаємо захист комп’ютерів та мобільних пристроїв після розгортаємо вкладку захист комп’ютеру шукаємо ESET Endpoint Security та тиснемо на кнопку завантажити, після почнеться завантаження де потрібно обрати потрібну версію Windows та тип інсталятора.(Рис.3.1)

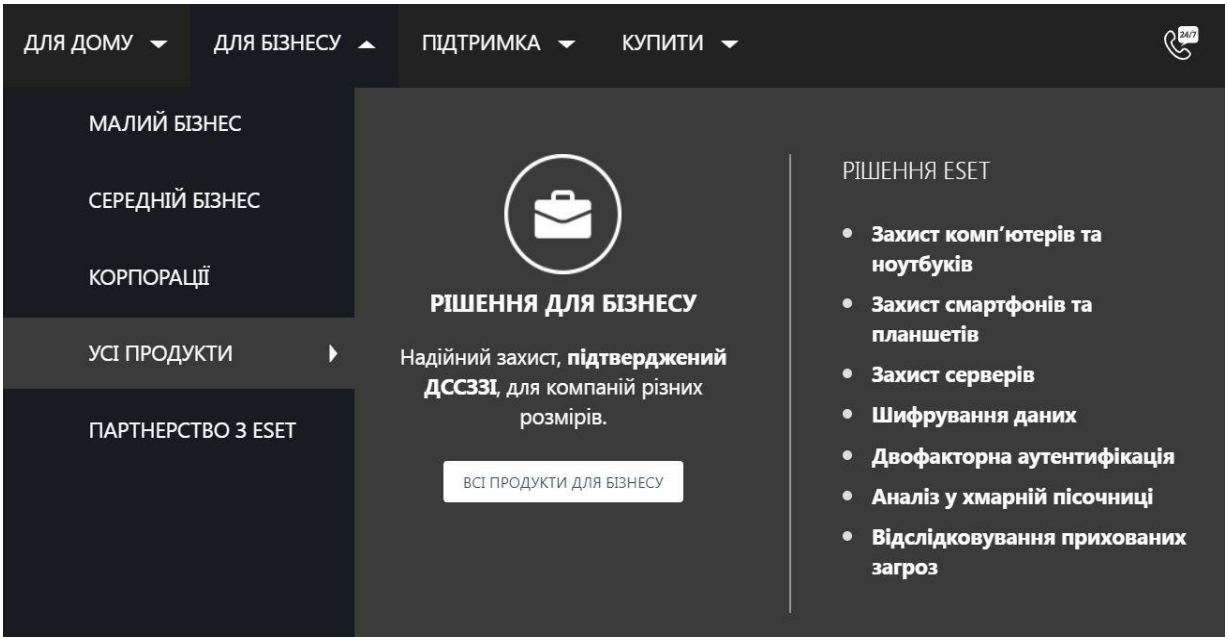


Рис. 3.1 – Вкладка для бізнесу та усі продукті

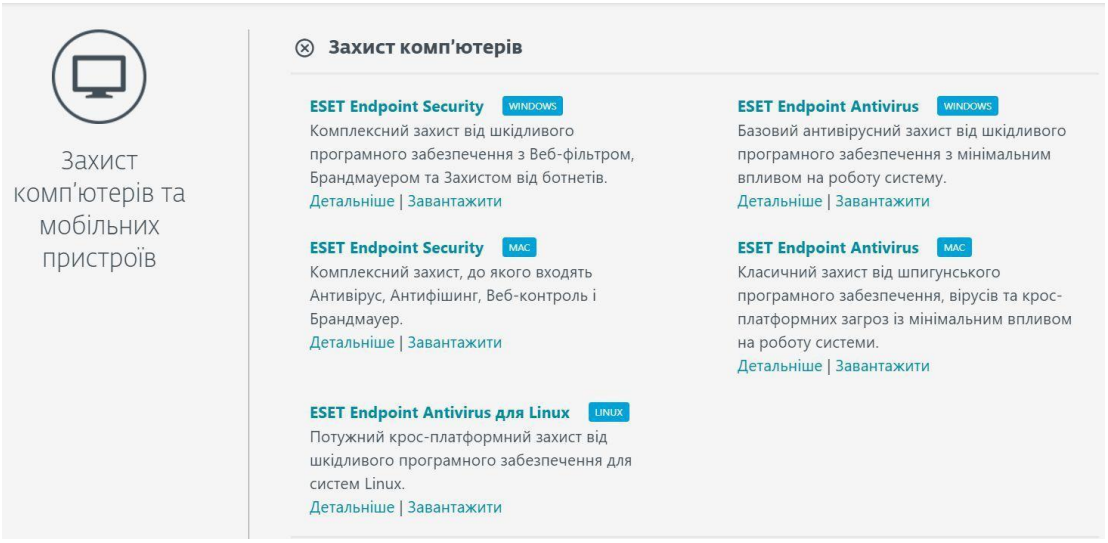


Рис. 3.2 – Обираємо ESET Endpoint Security

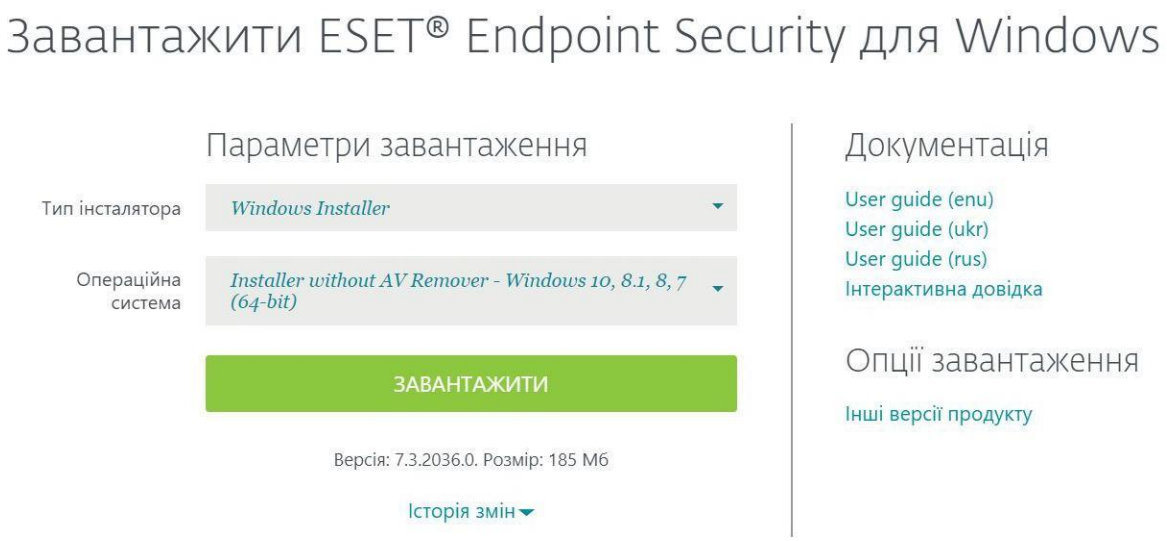


Рис. 3.3 – Обираємо версію для Windows та розрядність нашої системи

3.2 Встановлення

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

Рис 3.4 – Екран інсталяції антивірусу

Ліцензійна угода котру обов’язково потрібно прочитати та погодитись.(Рис 3.5)

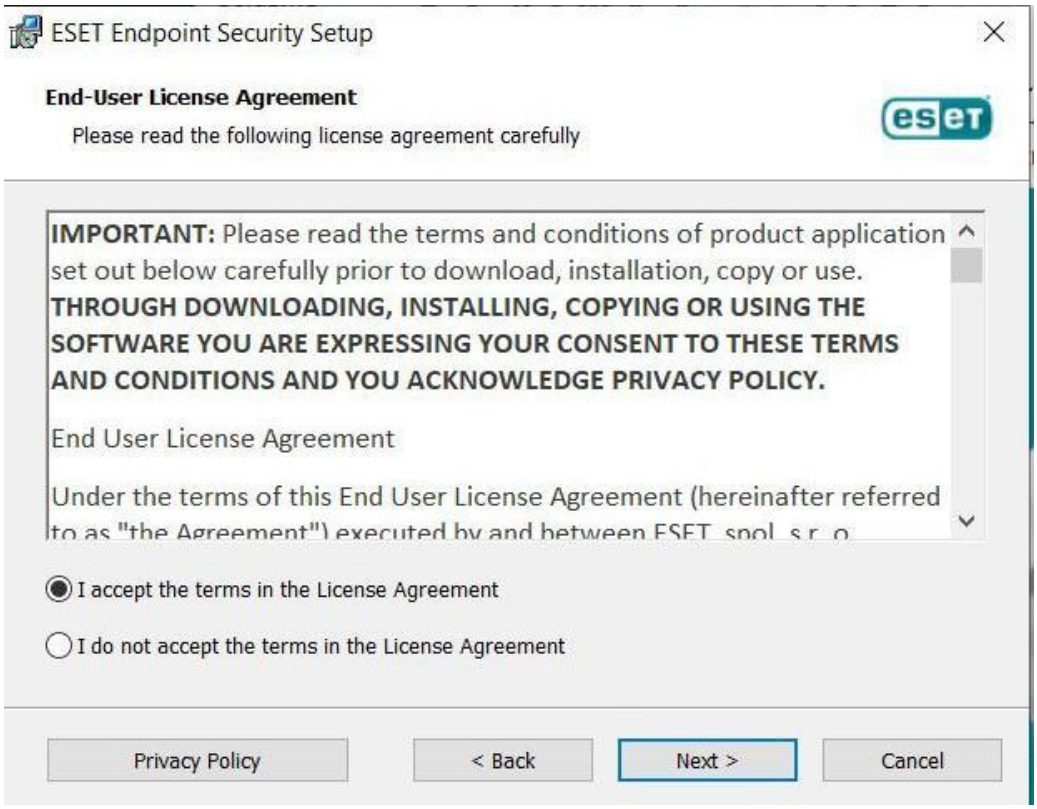


Рис 3.5 – Екран з ліцензійною угодою

Обираємо встановлювати чи ні систему LiveGrid котра дозволяє антивірусу постійно отримувати інформацію про нові зараження, її можна відключити функціонал програми не зміниться, але ця система дозволяє компанії відправляти данні для докладного аналізу що пришвидшує оновлення бази даних та покращує засоби їх виявлення.(Рис 3.6)

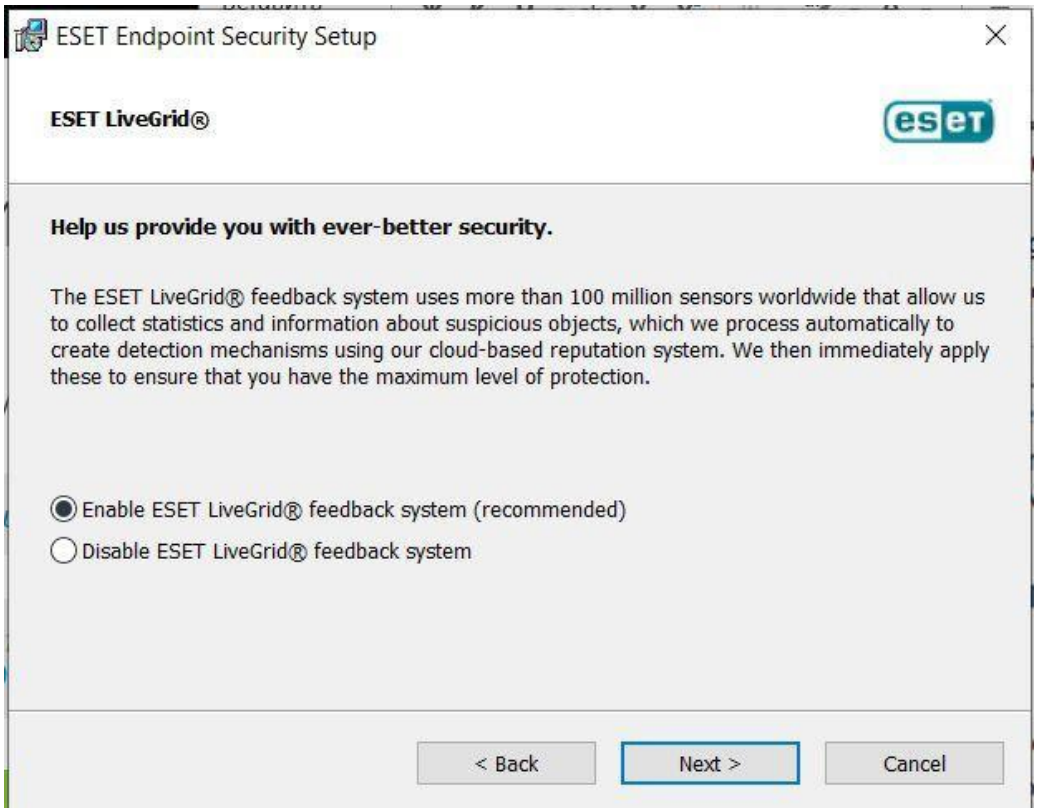


Рис 3.6 – Екран вибору встановлення LiveGrid

Обираємо чи може антивірус виявляти потенційно не бажані програми на думку антивірусу.(Рис 3.7)

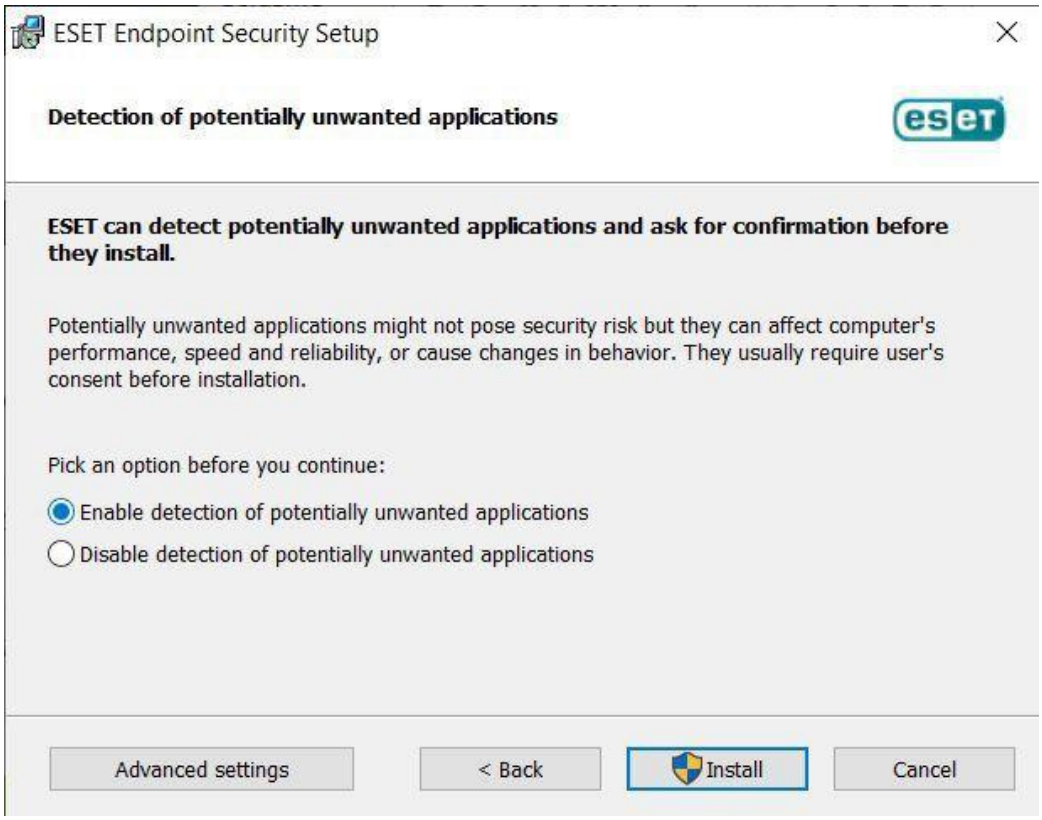


Рис 3.7 – Екран вибору виявлення потенційно не бажаних програм

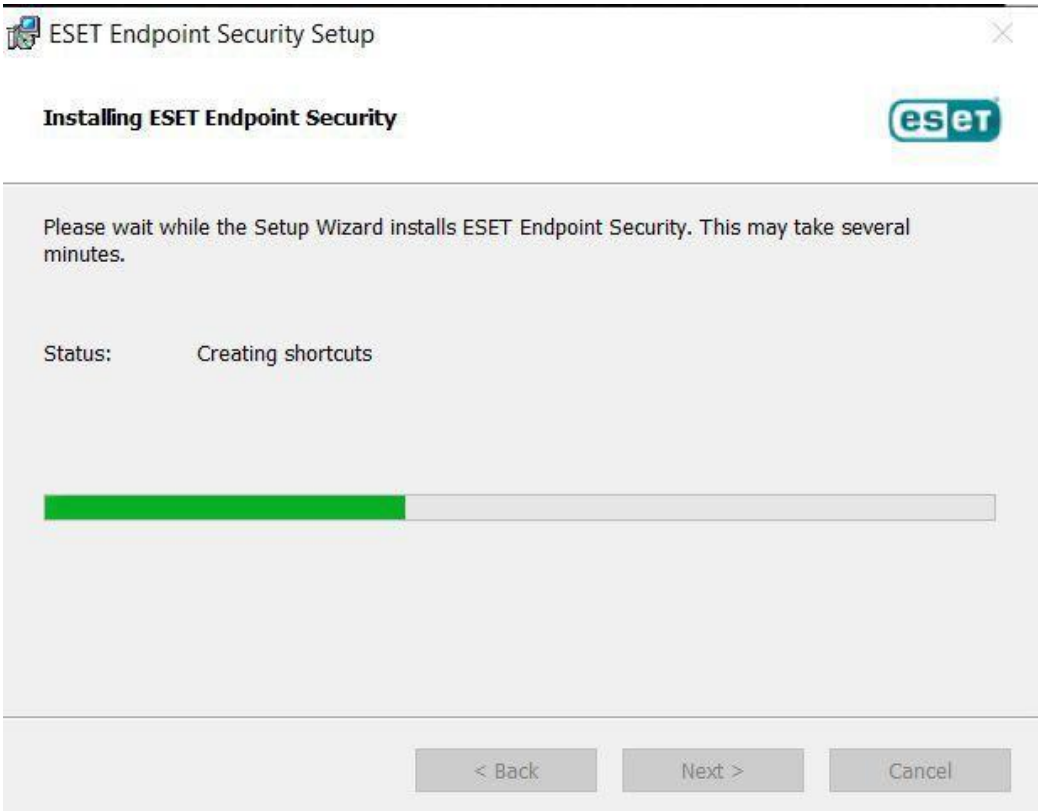


Рис 3.8 – Процес встановлення

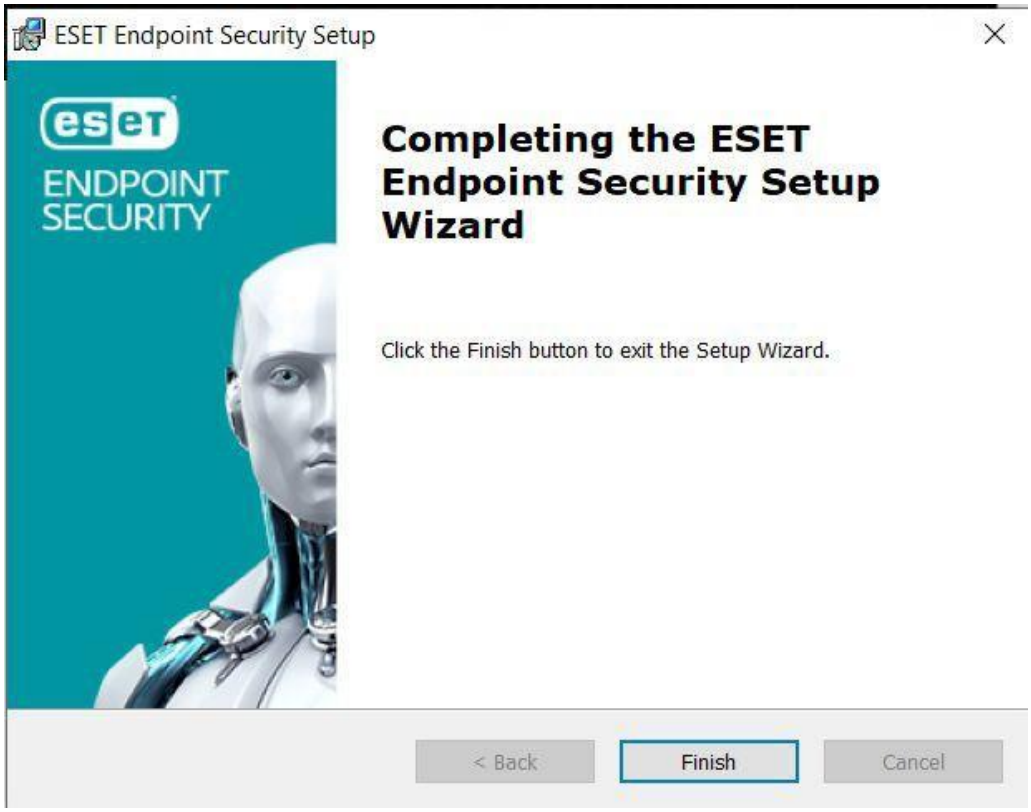


Рис. 3.9 – Інформація про успішне встановлення програми

3.3 Використання

Рис 3.10 – Екран завантаження антивірусу

Одразу ж пропонують активувати ліцензію, якщо ми маємо ліцензійний ключ, або якщо компанія в котрій ви працюєте може надати вам ліцензію. Та можливість використати файл ліцензії при відсутності інтернету. В нашому випадку ми просто закриваємо вікно та користуємося пробною версією програми. (Рис 3.11)

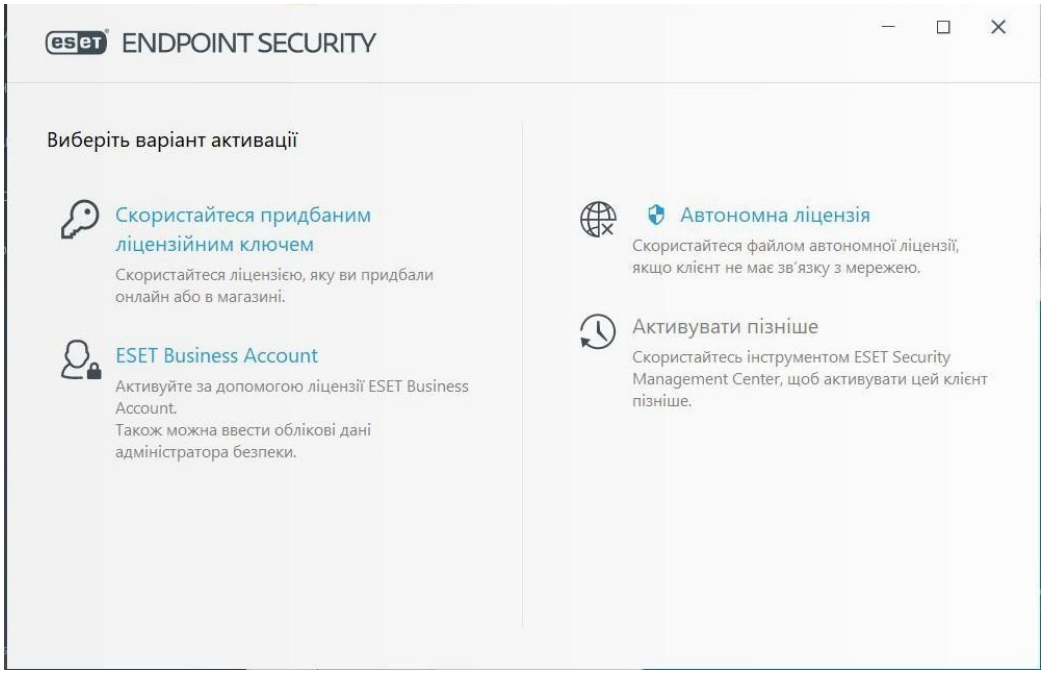


Рис 3.11 – Екран з пропозицією встановлення ліцензії

Основне вікно, де ми можемо подивитись статус нашого захисту, та обрати інші вкладки, такі як сканування комп’ютера, оновлення, параметри, інструменти, довідка та підтримка.

На екрані статус захисту ми повинні бачити статус нашого захисту ПК, але через те що наш продукт не активований ми не бачимо цього статусу. (Рис 3.12)

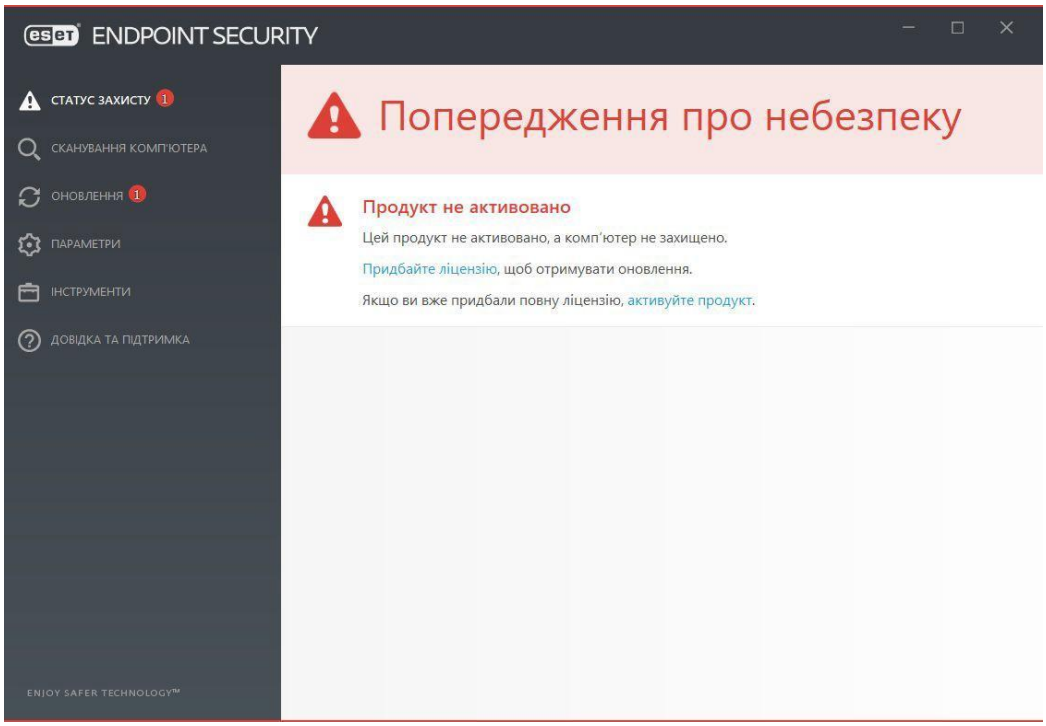


Рис 3.12 – Основний екран

Наступне вікно це сканування комп’ютера, де одразу почалося перше сканування, але перед цим проходить оновлення ядра. Сканування змінних носіїв дозволяє сканувати різні змінні носії. А також сканування файлу через просте перетягування в спеціальне вікно. Справа вгорі є кнопка з знаком питання котра відправить нас на сайт з допомогою де можливо знайти відповіді на питання про різні пункти меню. (Рис 3.13)

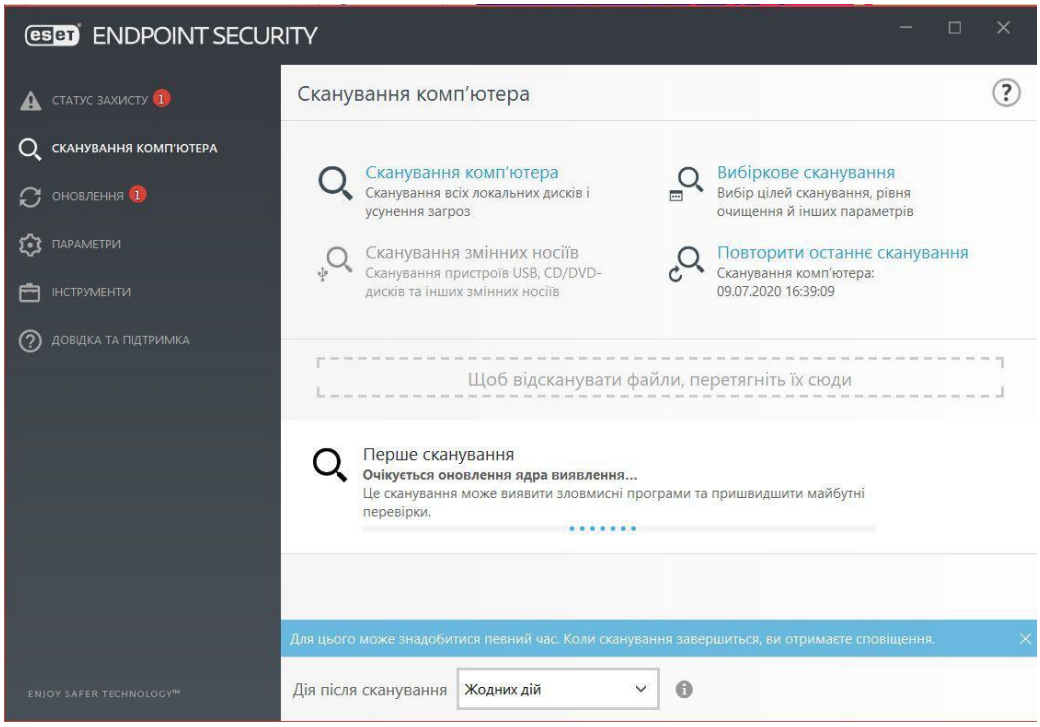


Рис 3.13 – Екран сканування комп’ютера

Вибіркове сканування дозволяє обрати тільки один диск, або папку та навіть оперативну пам’ять з завантажувальним сектором. Також ми можемо написати шлях до файлу що може пришвидшити сканування. (Рис 3.14)

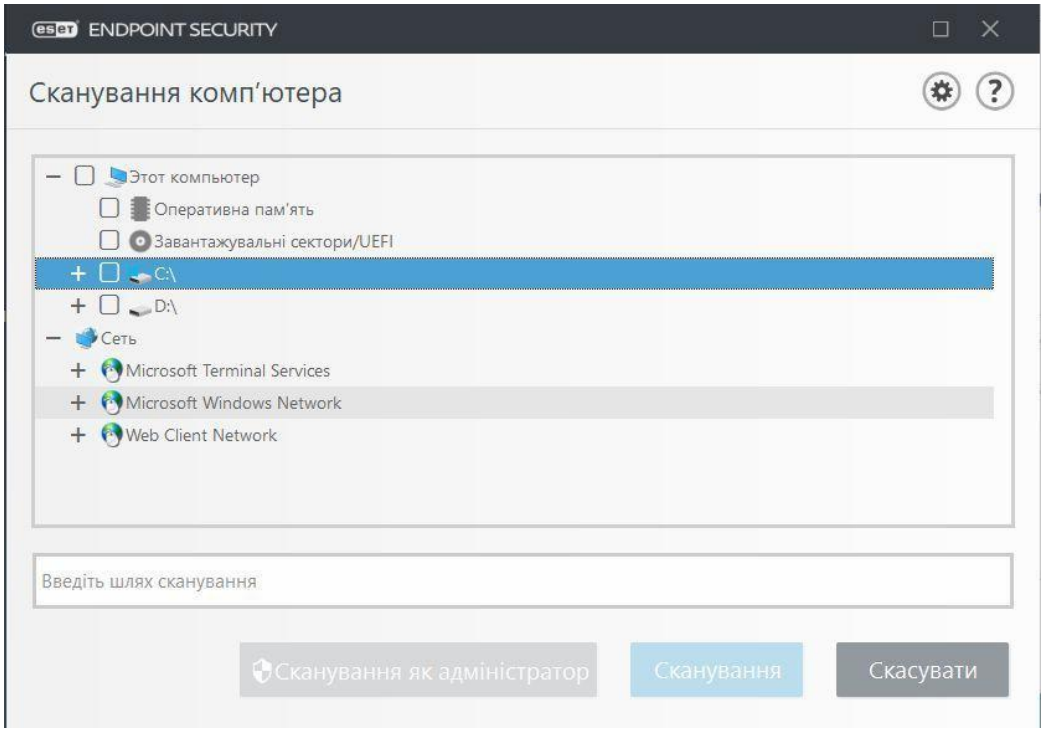


Рис 3.14 – Екран вибіркового сканування

Наступним буде вкладка оновлення де ми можемо провірити версію програми, останнє оновлення та дата останньої перевірки. Також за допомогою пунктів перевірити наявність оновлень можемо примусово перевірити оновлення та змінити частоту оновлень або додати нове завдання. (Рис 3.15)

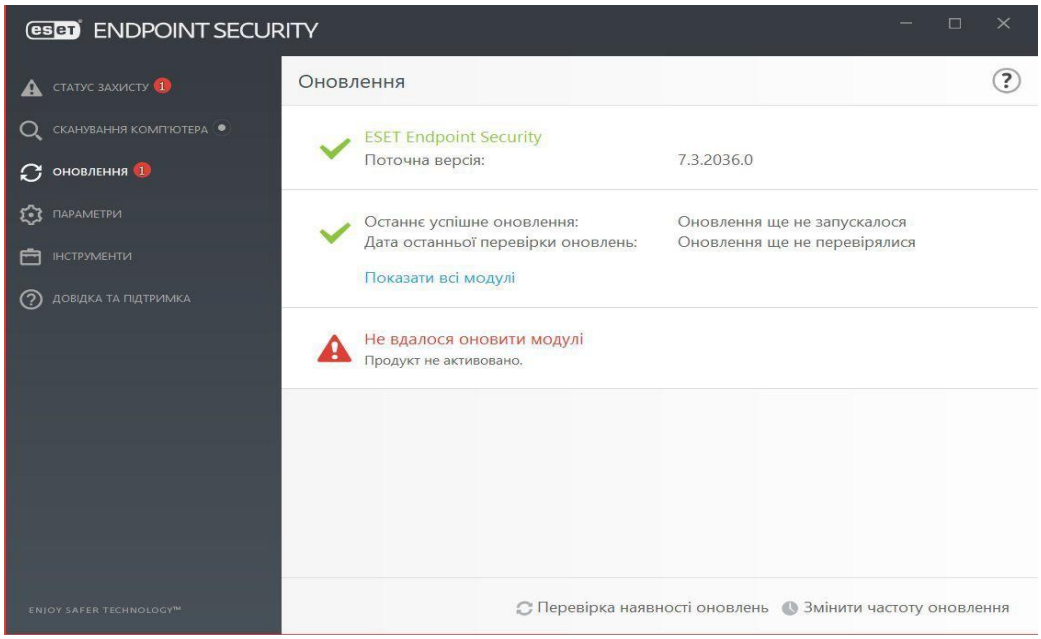


Рис 3.15 – Екран оновлення

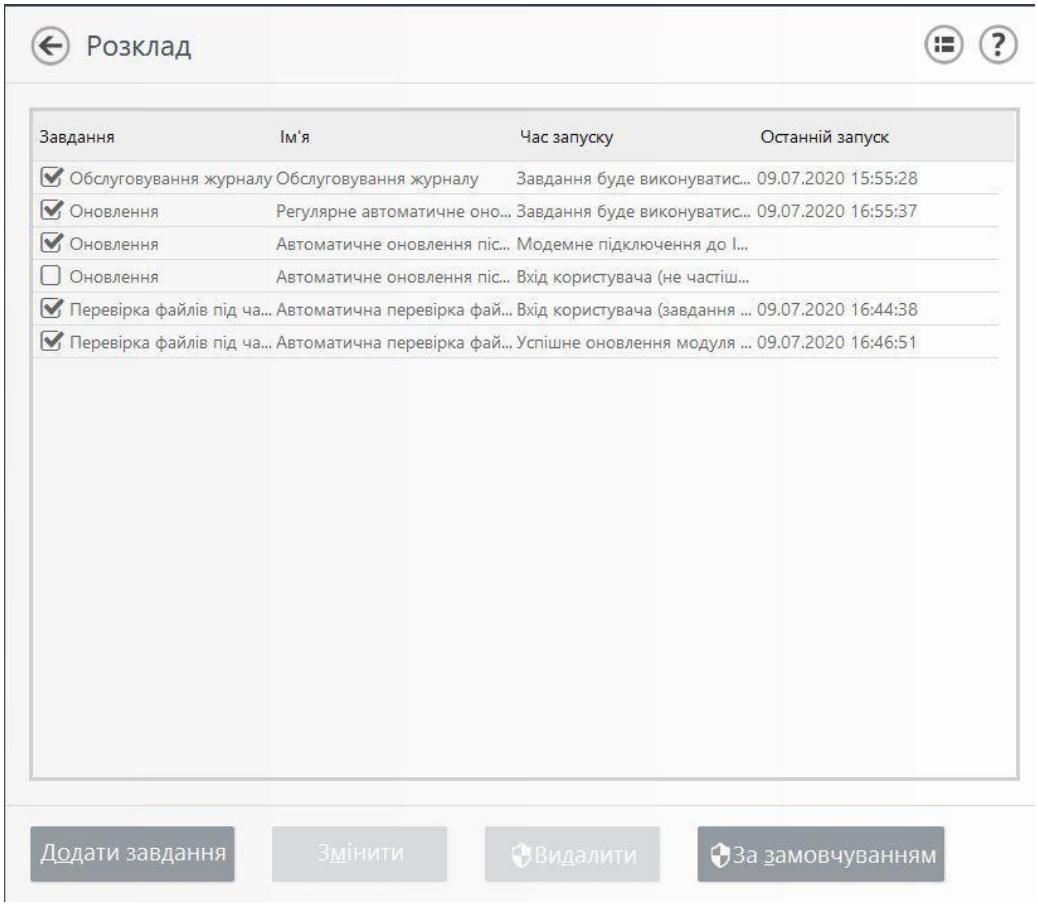


Рис 3.16 – Екран розкладу перевірок та оновлень

Наступним буде вікно з параметрами. Де є 3 варіанти параметрів а також можливість імпортувати або експортувати параметри. А також додаткові параметри.(Рис 3.17)

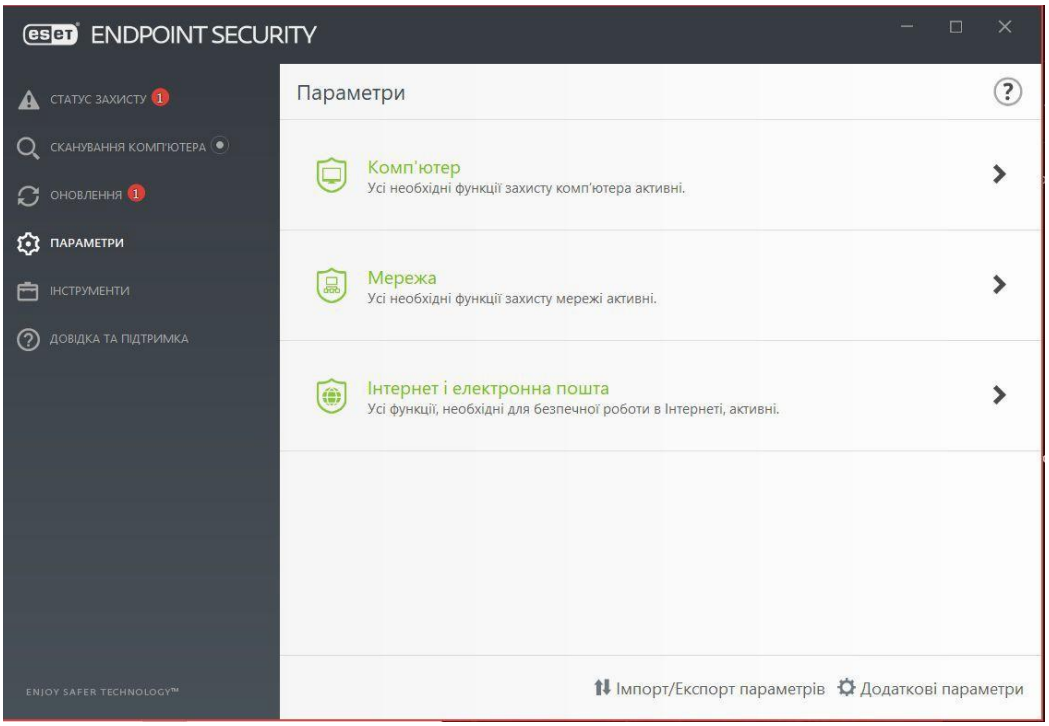


Рис 3.17 – Екран з параметрами

В вкладці комп’ютер ми можемо налаштувати основні параметри для захисту ПК. Захист файлової системи допомагає виявляти шкідливе ПЗ на комп’ютері та контроль пристроїв допомагає знешкодити віруси на різних флешках, дисках та інших пристроїв нажаль це не працює через неактивований антивірус. Звідси ми можемо одразу перейти до додаткових параметрів цих параметрів натиснувши на шестерню. (Рис 3.18)

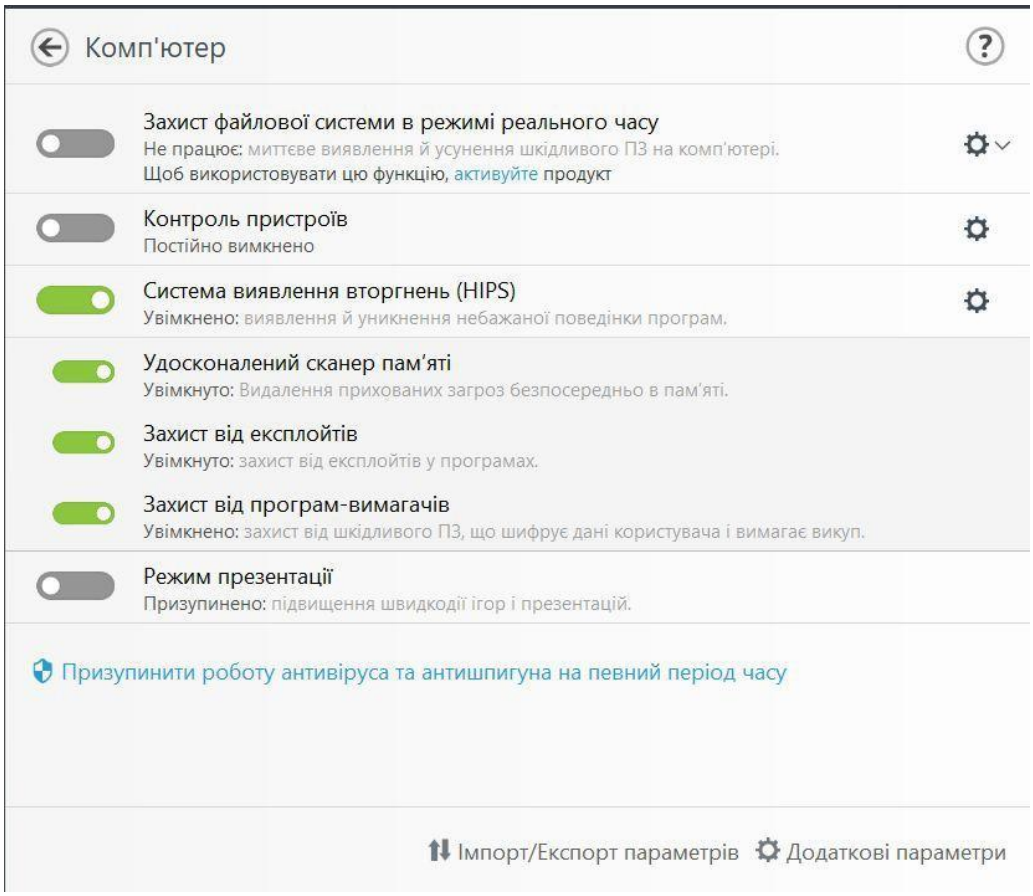


Рис 3.18 – Екран вкладки параметрів комп’ютеру

Наступним є налаштування захисту мережі. Брандмауер що буде фільтрувати мережевий трафік. захист мережі від атак дозволяє захиститися від мережевих атак, захист від ботнетів. (Рис 3.19)

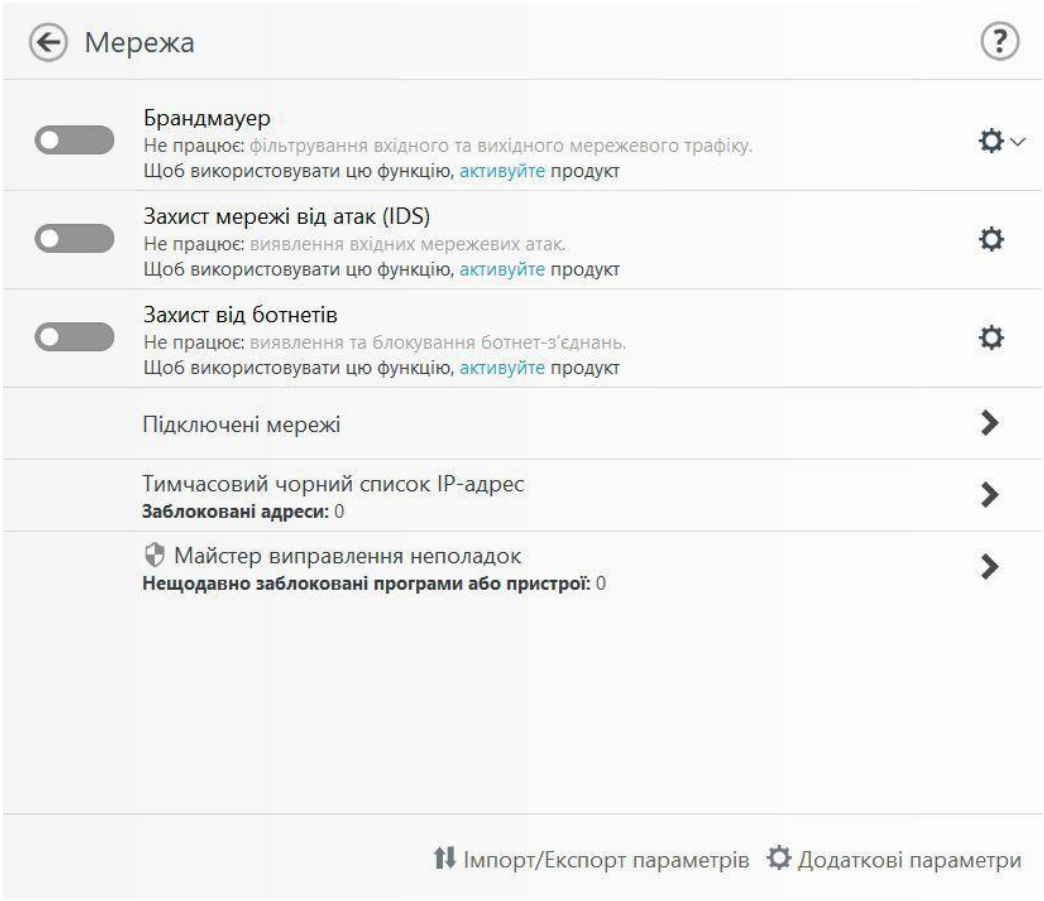


Рис 3.19 – Екран параметрів мережі

В пункті підключені мережі ми можемо подивитися параметри мережі к котрій ми підключені, змінити тип захисту, отримання попереджень через слабке шифрування та інші параметри нашою мережі.(Рис 3.20)

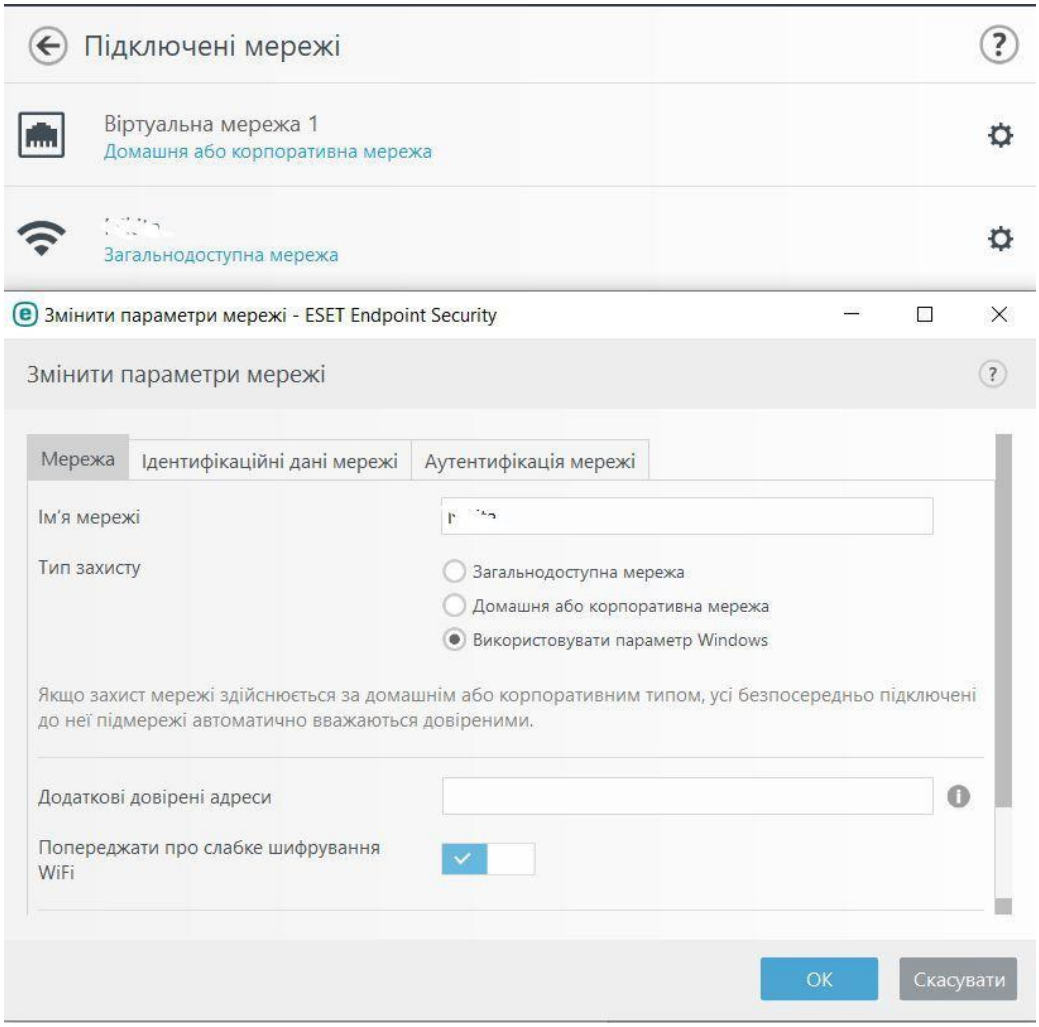


Рис 3.20 – Екран підключень до мережи

Тимчасовий чорний список IP-адрес дозволяє додати до чорного списку IP-адрес котрий ми хочемо заблокувати. (Рис 3.21)

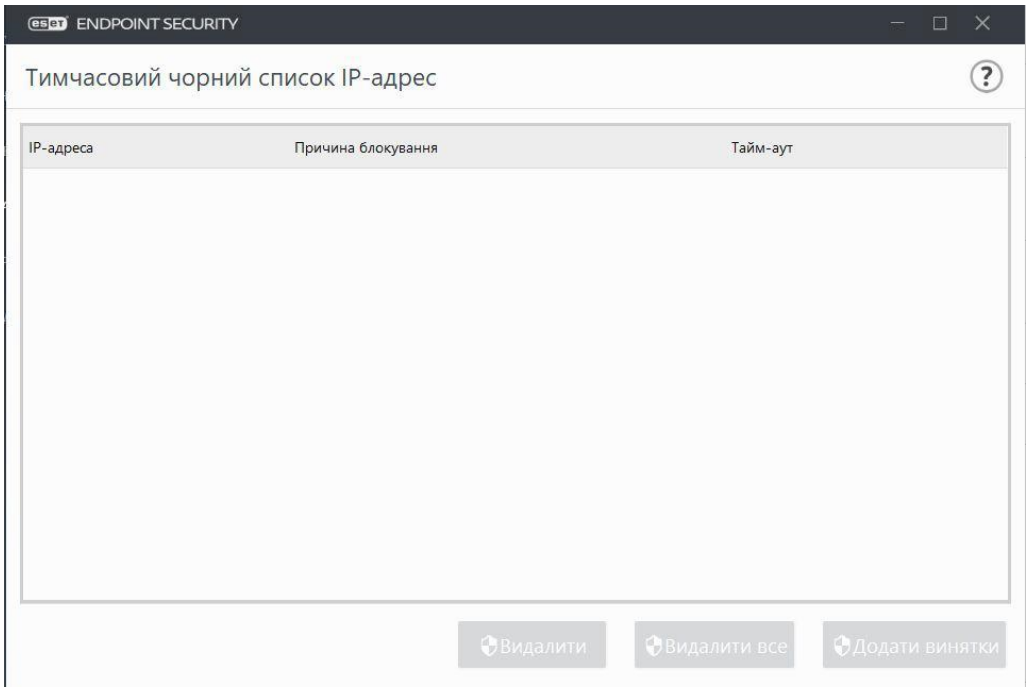


Рис 3.21 – Чорний список IP-адрес

Майстер виправлення неполадок допомагає вирішувати різні проблеми з захистом мережі. (Рис 3.22)

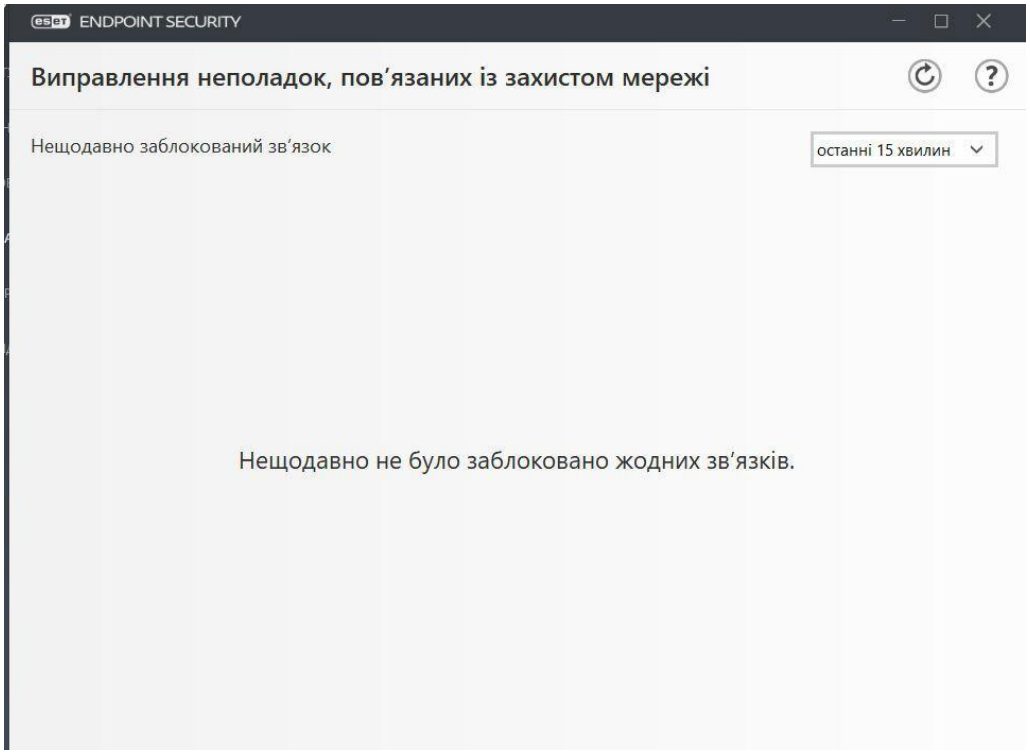


Рис 3.22 – Екран виправлення неполадок

Додаткові параметри дозволяють детальніше настроїти всі параметри антивірусу. Має дуже велику кількість пунктів для гнучкою настройкою параметрів антивірусу. (Рис 3.23)

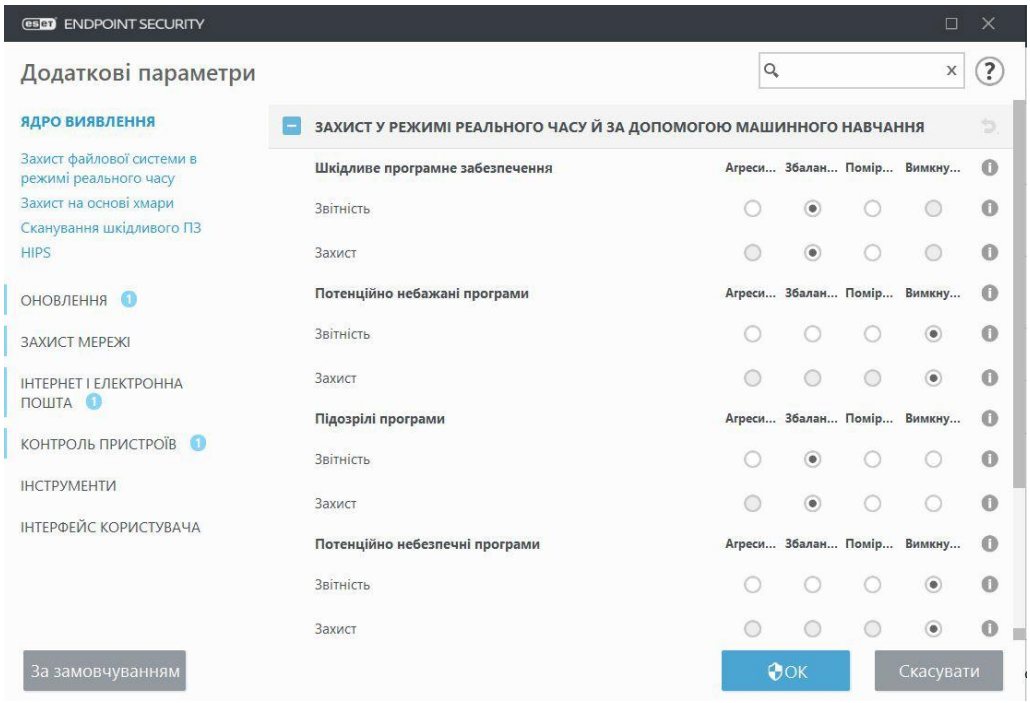


Рис 3.23 – Екран додаткових параметрів

Наступним пунктом є інструменти де є набір невеликих інструментів що забезпечують контроль за нашим ПК. В пункті файли журналу маємо змогу подивитися на події що коїлися на нашому ПК. (Рис 3.24)

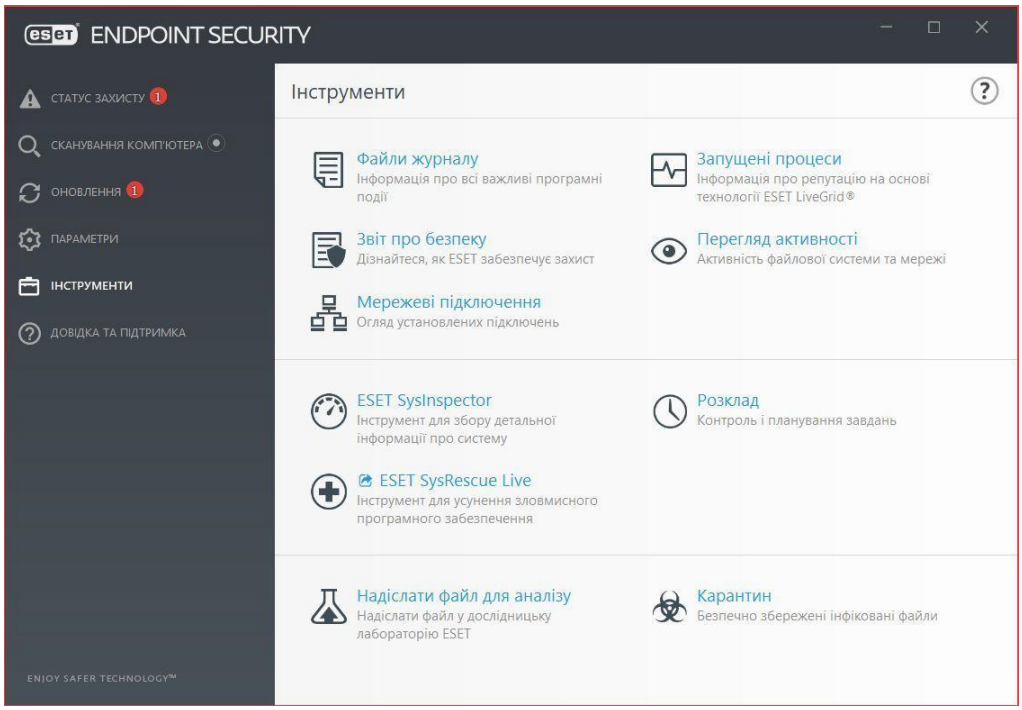


Рис 3.24 – Екран інструментів

Запущені процеси дозволяють подивитися на файли з додатковою інформацією від ESET та подивитись репутацію кількість користувачів та час першого виявлення вірусу в процесі. (Рис 3.25)

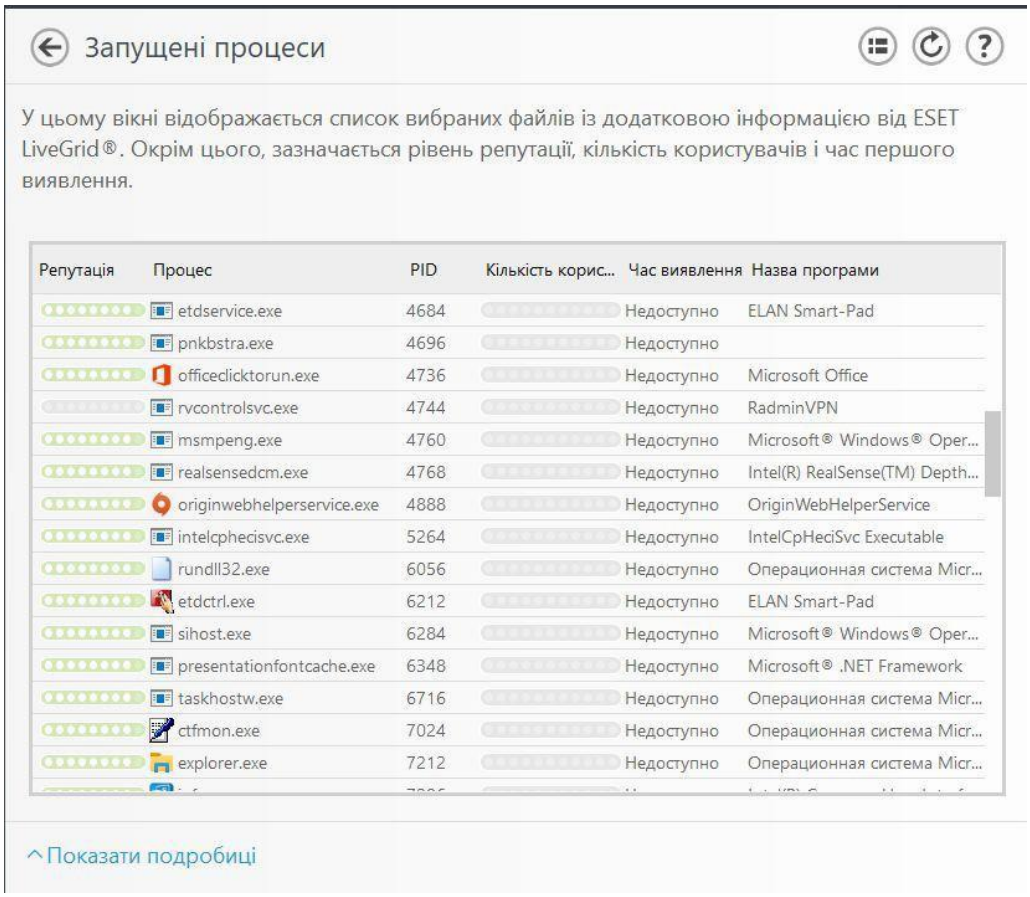


Рис 3.25 – Екран запущених процесів

Вкладка звіт про безпеку дає можливість подивитись інформацію про те що перевірив антивірус та про розповсюдженість шкідливого ПЗ в світі. (Рис 3.26)

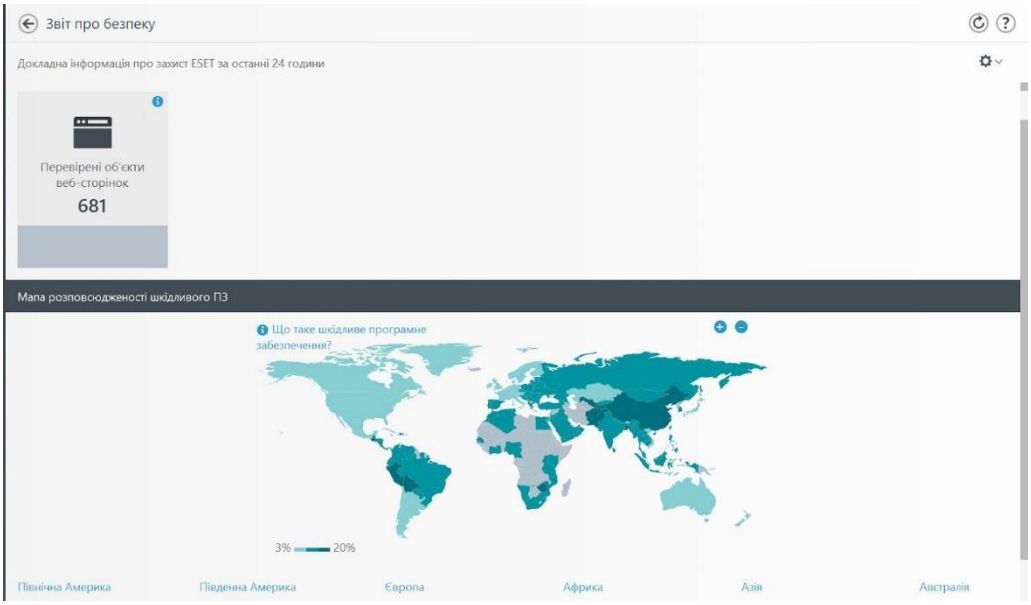


Рис 3.26 – Екран звіту про безпеку

Перегляд активності дозволяє продивитися скільки даних проходить через наш ПК. (Рис 3.27)

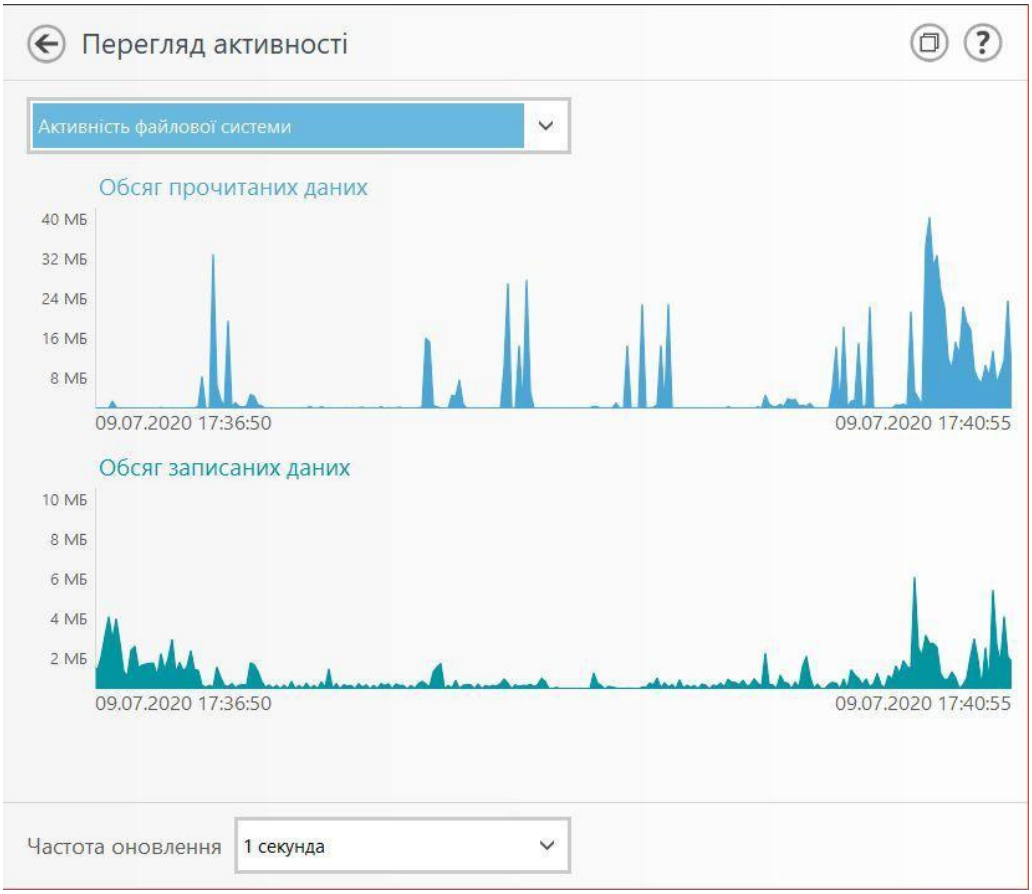
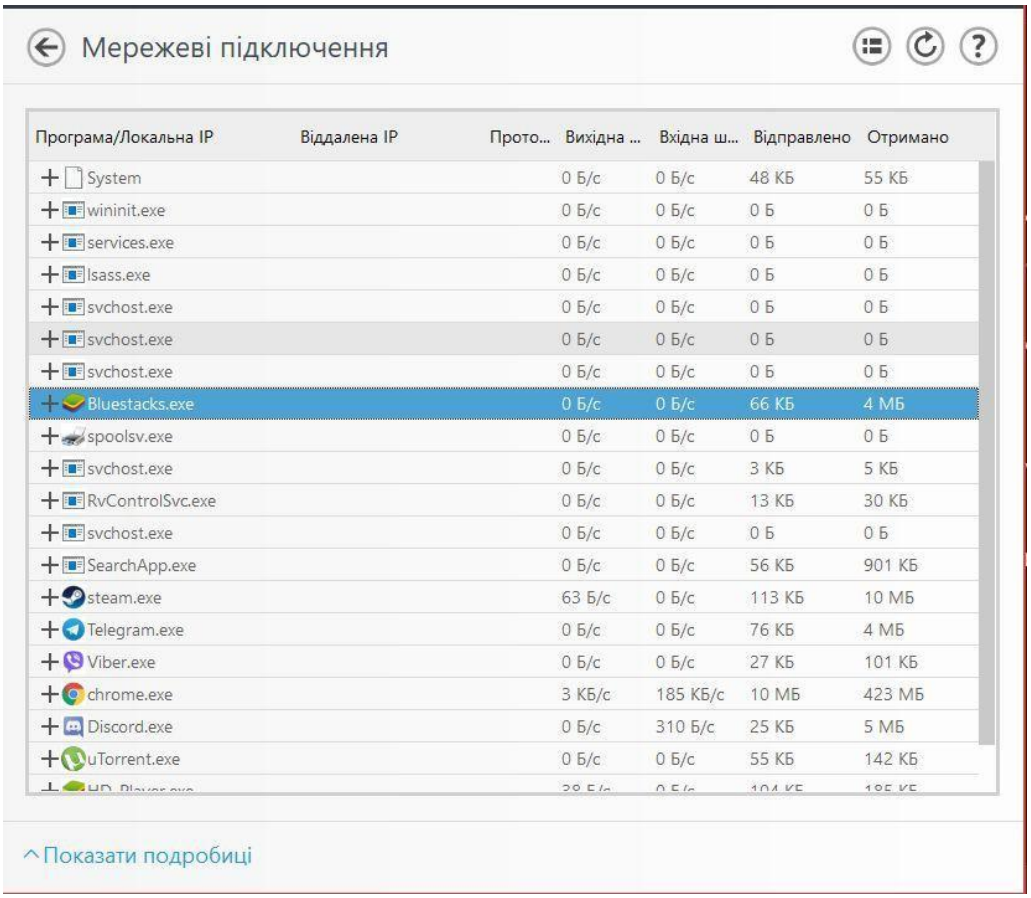


Рис 3.27 – Екран активності антивірусу

Мережеві підключення дозволяють продивитися які програми використовують наш трафік, скільки трафіку використовуються, швидкість яку використовує програма та IP-адреси з протоколами підключення до мережі. (Рис 3.28)



Рису 3.28 – Екран мережевих підключень

ESET SysInspector дозволяє більш детальніше зібрати інформацію про комп’ютер та відсортувати за рівнем безпеки програми та файли від безпечних до небезпечних. (Рис 3.29)

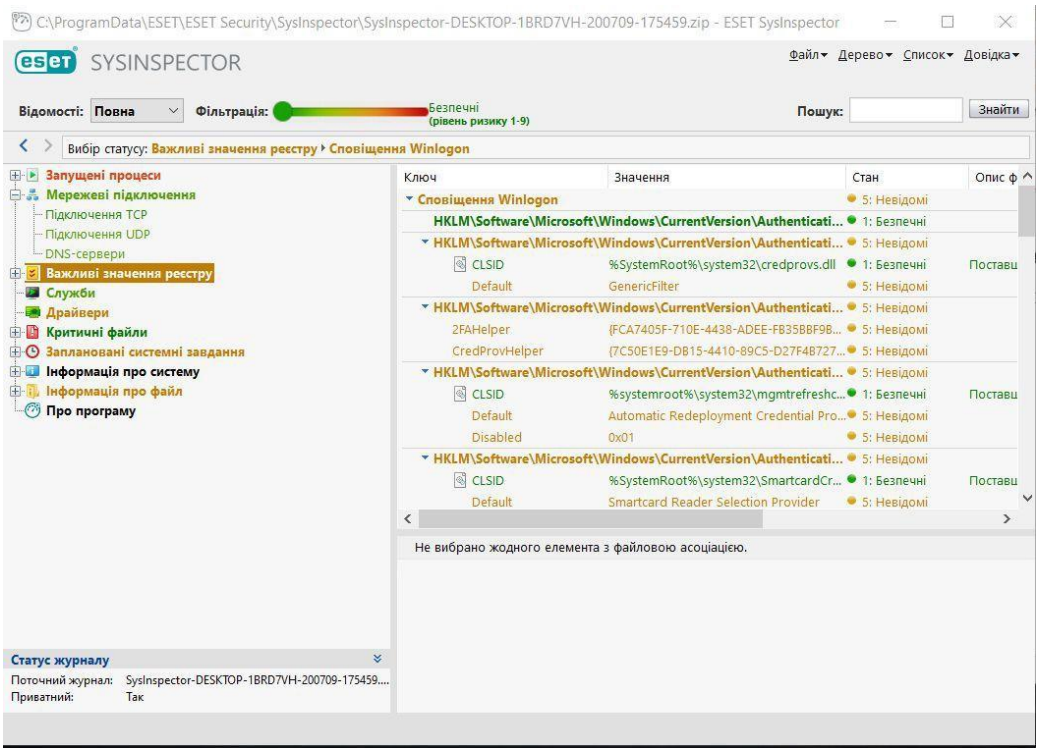


Рис 3.29 – Екран SYSINPECTOR

Екран відправки зразків дозволяє відправити файл на аналіз в лабораторію ESET. (Рис 3.30)

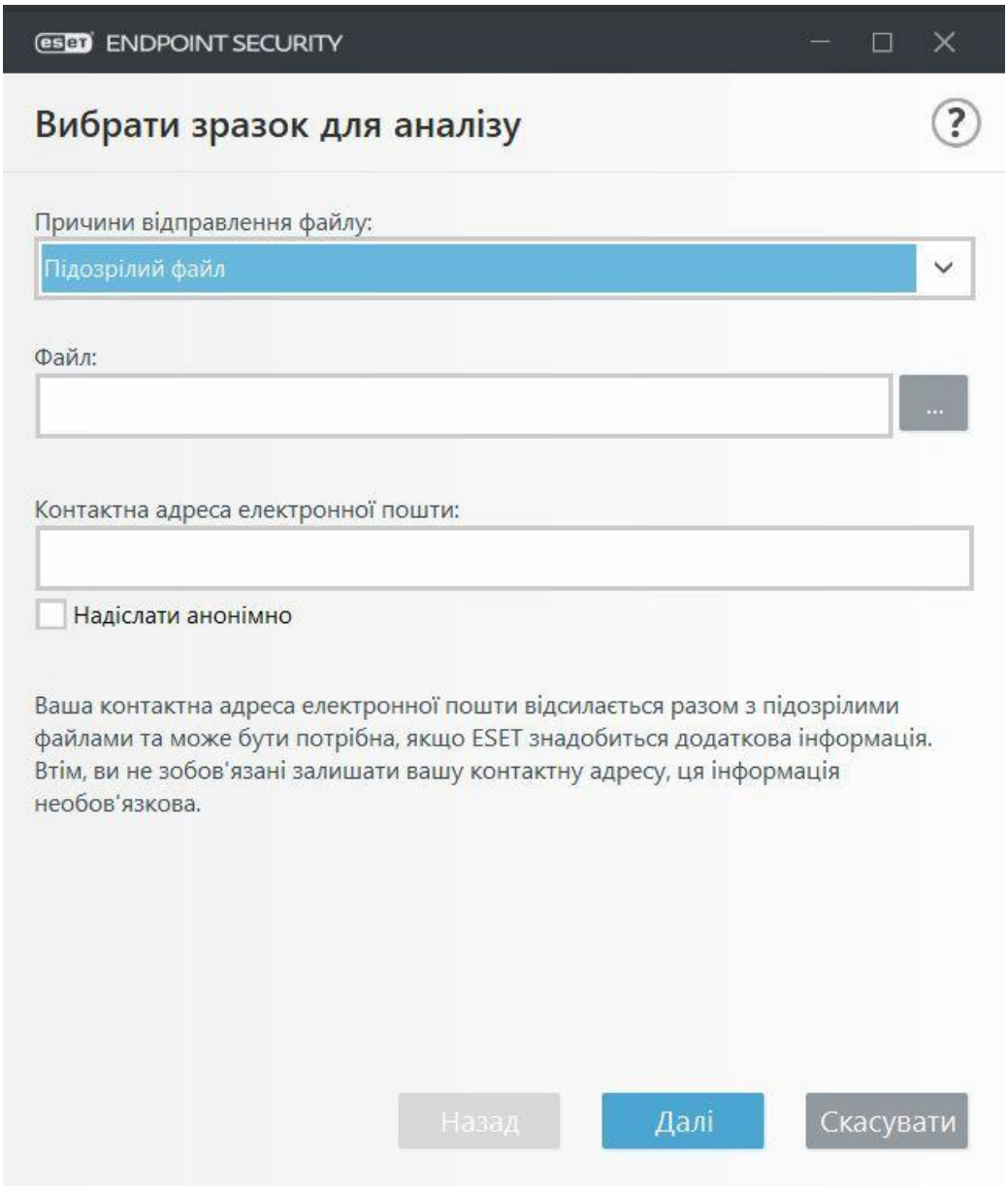


Рис 3.30 – Екран відправки зразку

Карантин де можливо продивитися які файли були додані до карантину через загрозу. (Рис 3.31)

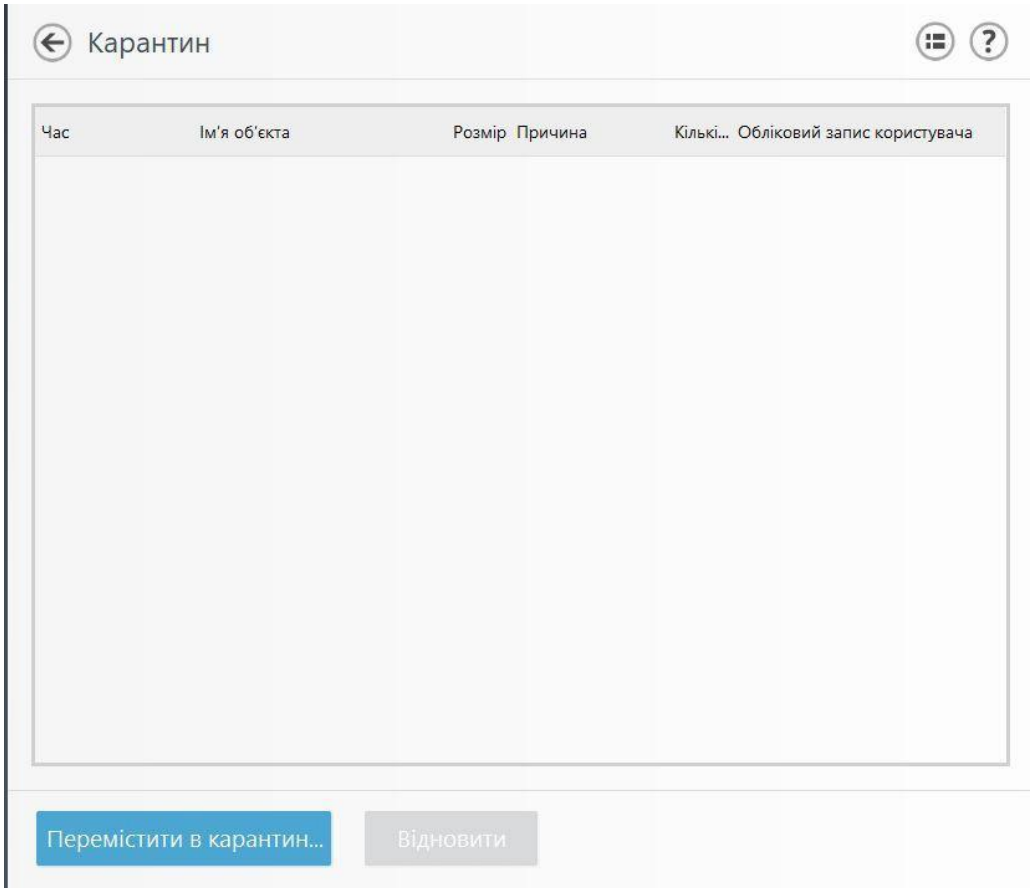


Рис 3.31 – Екран карантину

Довідка та підтримка дозволяє продивитися різну інформацію про антивірус, керівництво користувача, звернутися до служби підтримки, подивитися енциклопедію загроз, а також дізнатися версію програми та активувати продукт. (Рис 3.32)

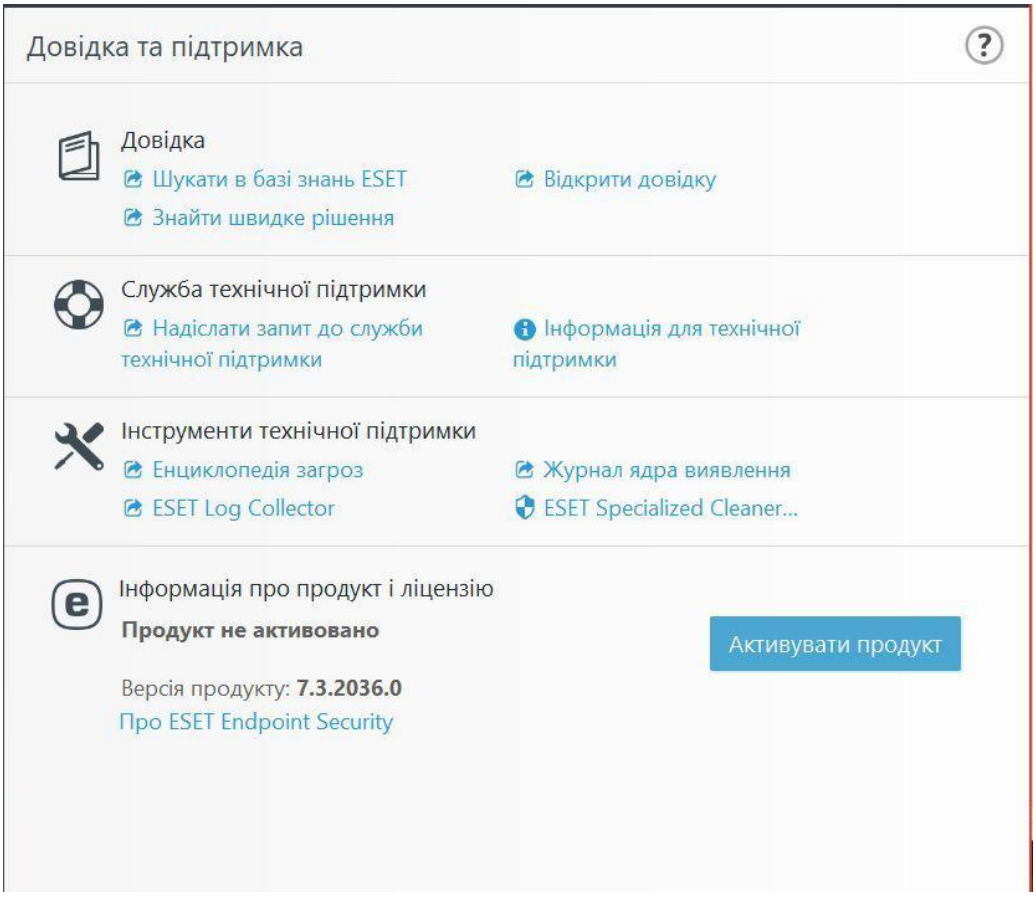


Рис 3.32 – Екран з довідкою та підтримкою

4. РОЗГОРТАННЯ АНТИВІРУСНОЇ СИСТЕМИ ЗАХИСТУ

В сучасному світі, захист на підприємстві дуже важлива річь, через велику кількість важливих даних в мережі, тому антивірусний захист корпоративної мережі невід'ємна частина будь якого підприємства. Через те що в малому підприємстві присутні декілька ПК, тому встановлення антивірусів на кожну машину було б дуже довго. Тому для пришвидшення розгортання антивірусів ми можемо використовувати використати вбудовану функцію Windows Server таку як Управління Груповими Політиками, де за допомогою деяких налаштувань можливо зробити автоматичне розгортання будь яких програм при завантаженні ПК, без будь якої взаємодії з іншими комп'ютерами.

Для того щоб імітувати мале підприємство, буде використована Windows Server для імітування основного ПК з котрого будуть проводитися налаштовування антивірусу на інших комп'ютерах, що за допомогою віртуальних машин, налаштованих в одну локальну мережу, буде з імітована локальна мережа малого підприємства. [13]

4.1 Розгортання та налагодження серверної частини антивірусної системи

Спочатку потрібно встановити основну програму з котрої можливо буде відслідковувати стан наших ПК, без взаємодії з ними. (Рис 4.1)

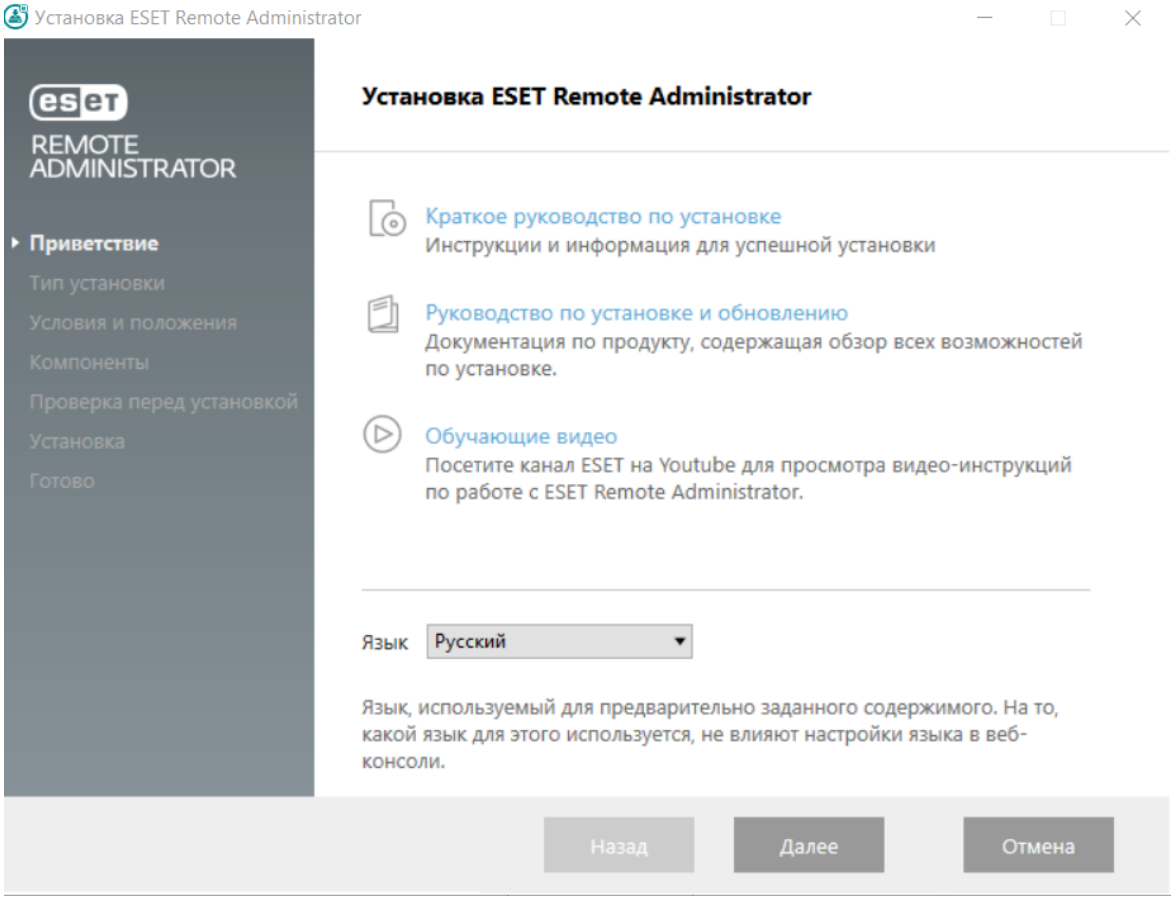


Рис 4.1 Екран привітання встановлення Eset Remote Administrator

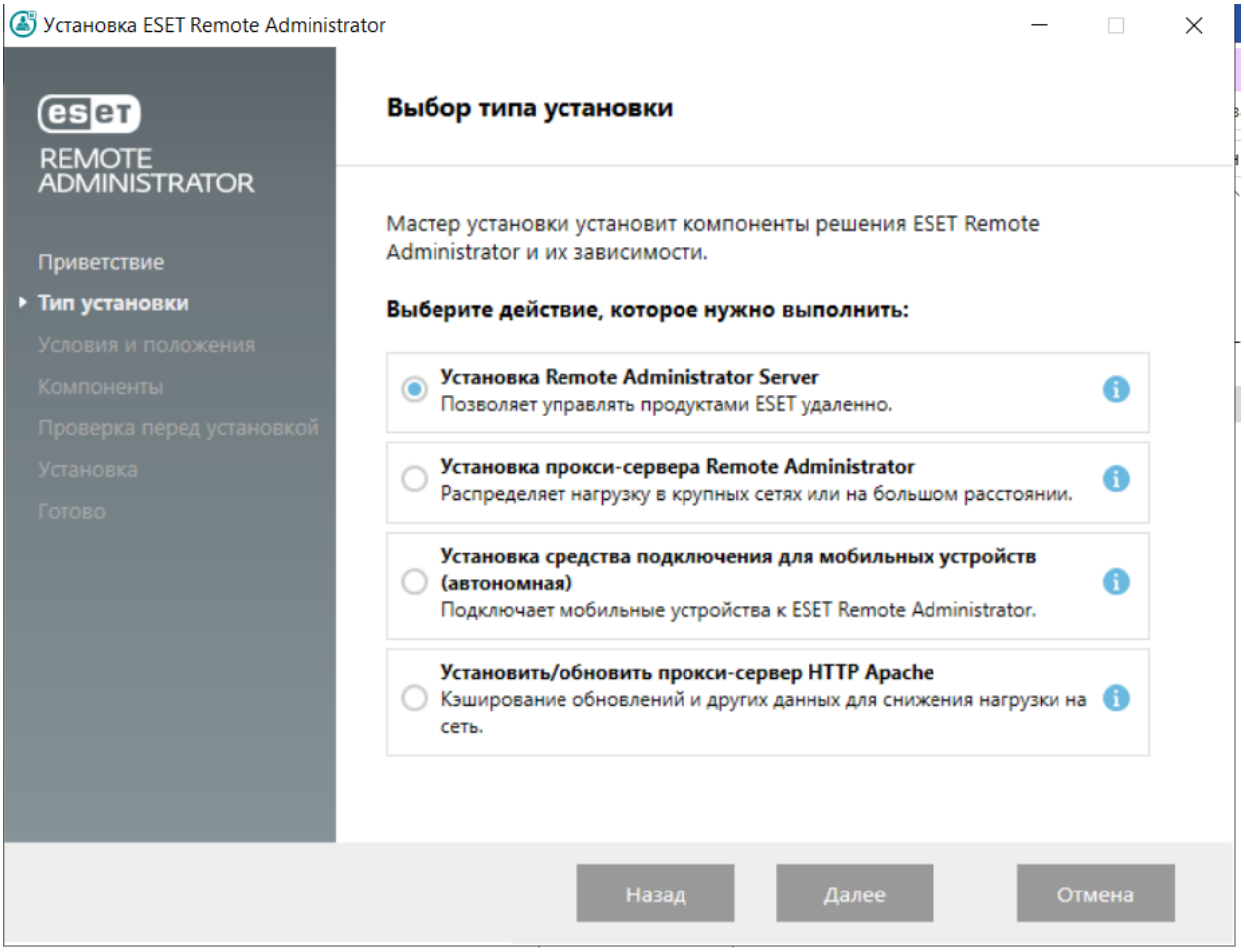


Рис 4.2 Обираємо лише встановлення нашого Remote Administrator Server

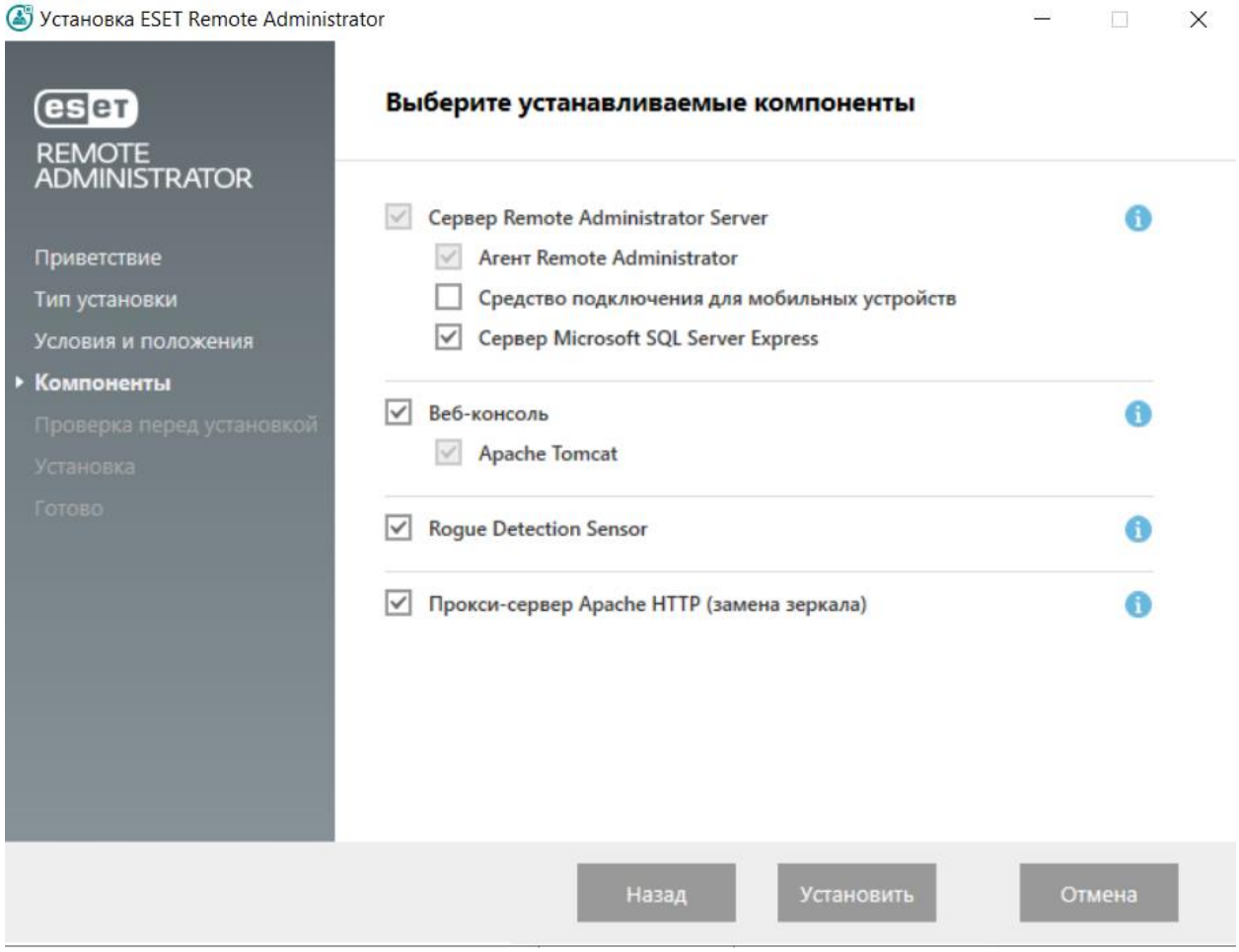


Рис 4.3 Обираємо повний комплект інструментів

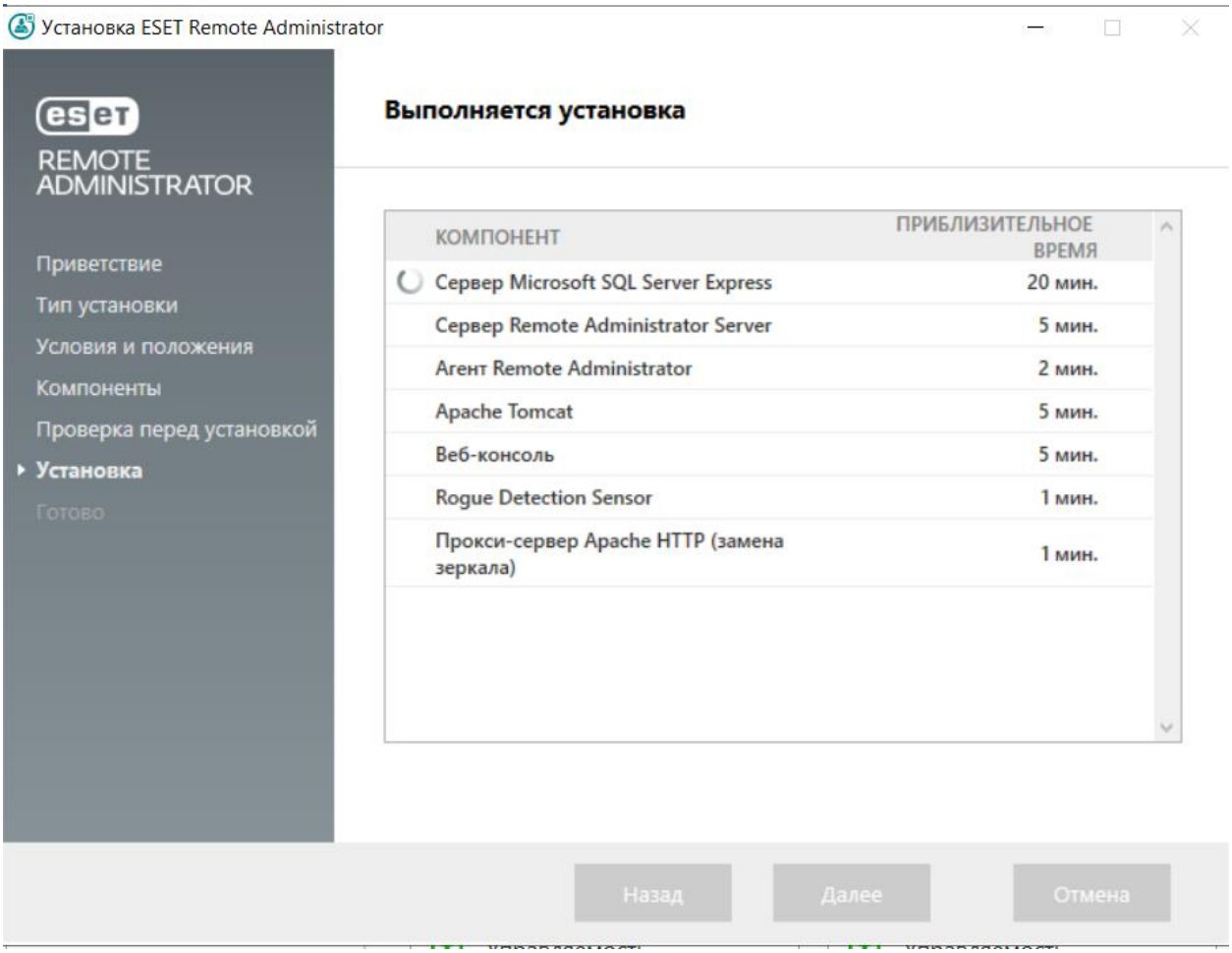


Рис 4.4 Процес встановлення

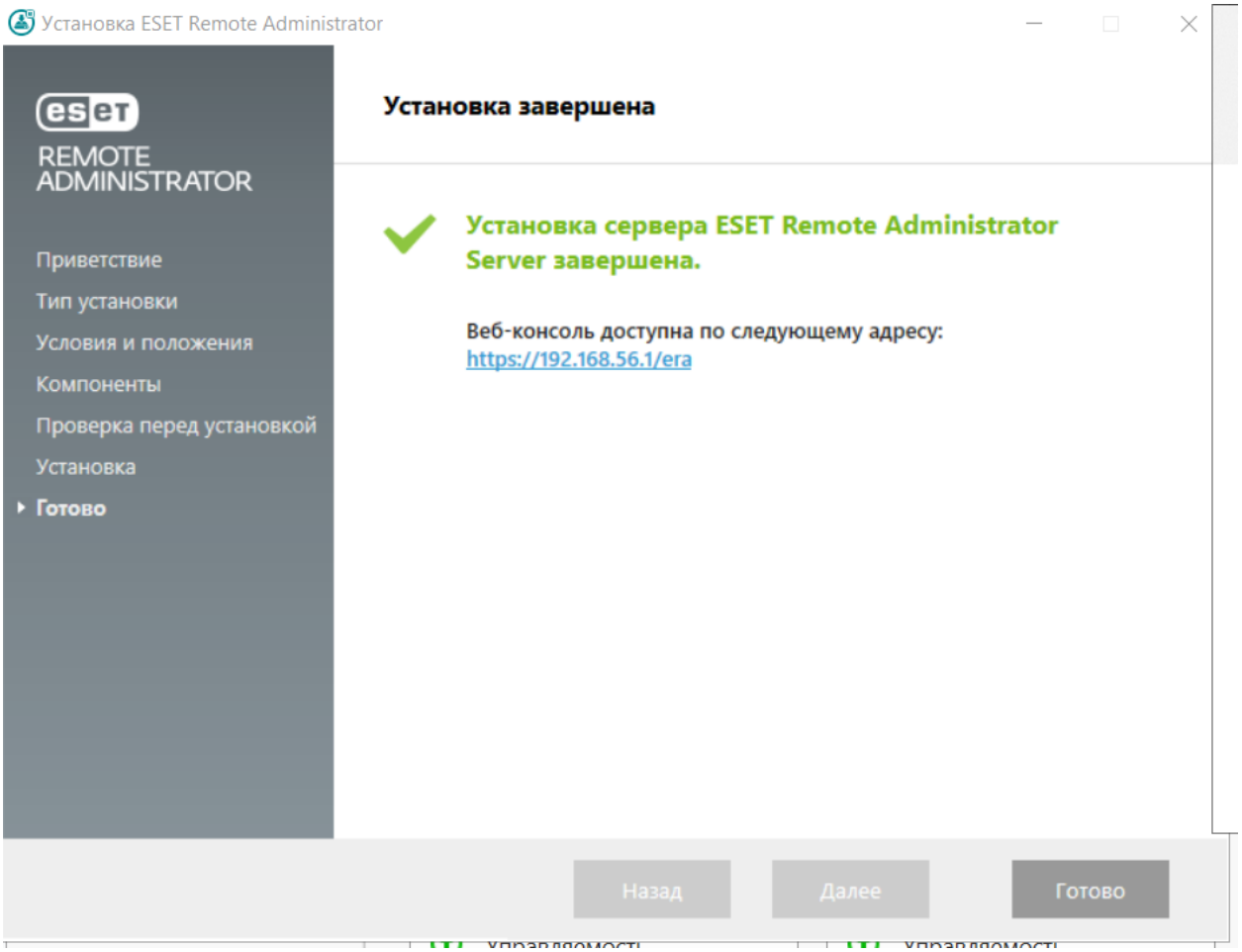


Рис 4.5 Інформація про успішне встановлення Remote Administrator Server

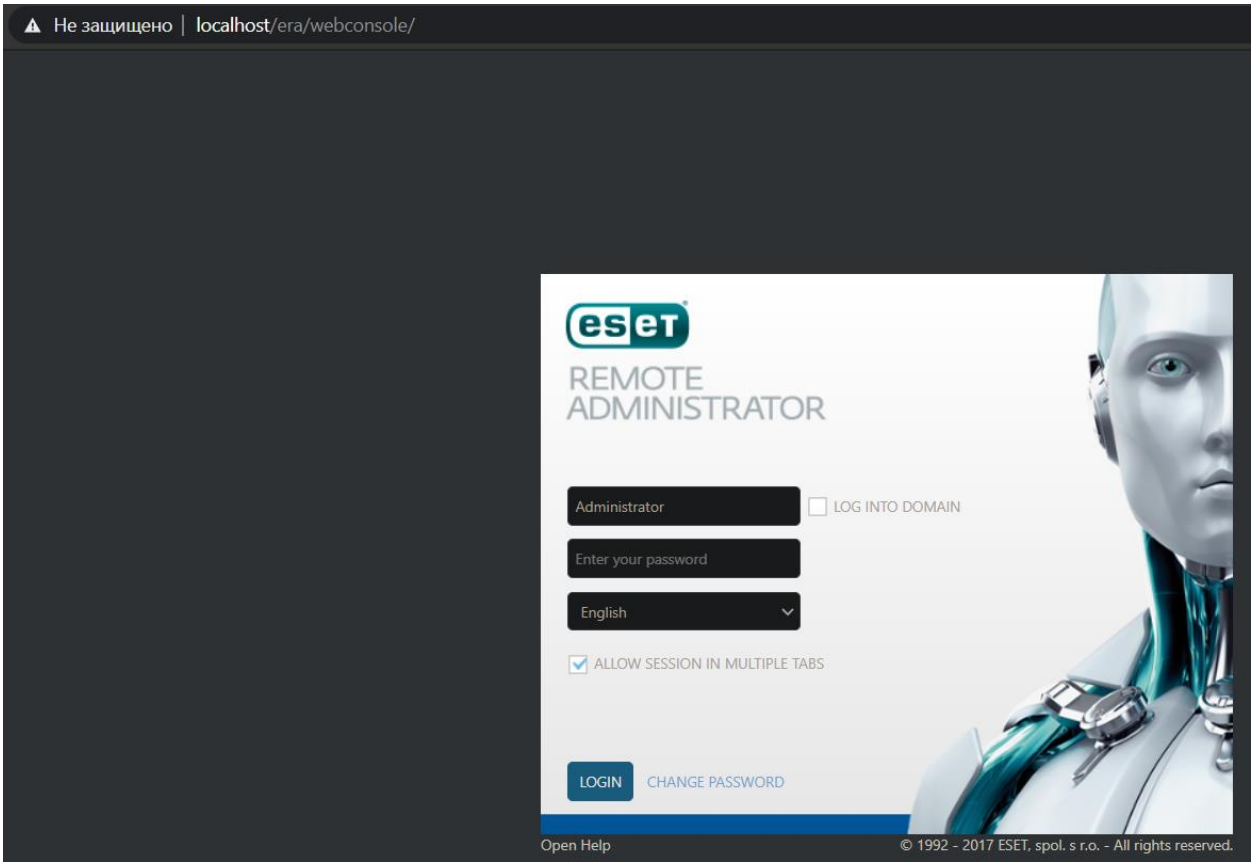


Рис 4.6 Для того щоб почати користуватися нашою програмою треба перейти на сайт Localhost, де нас зустріне екран входу до нашої системи

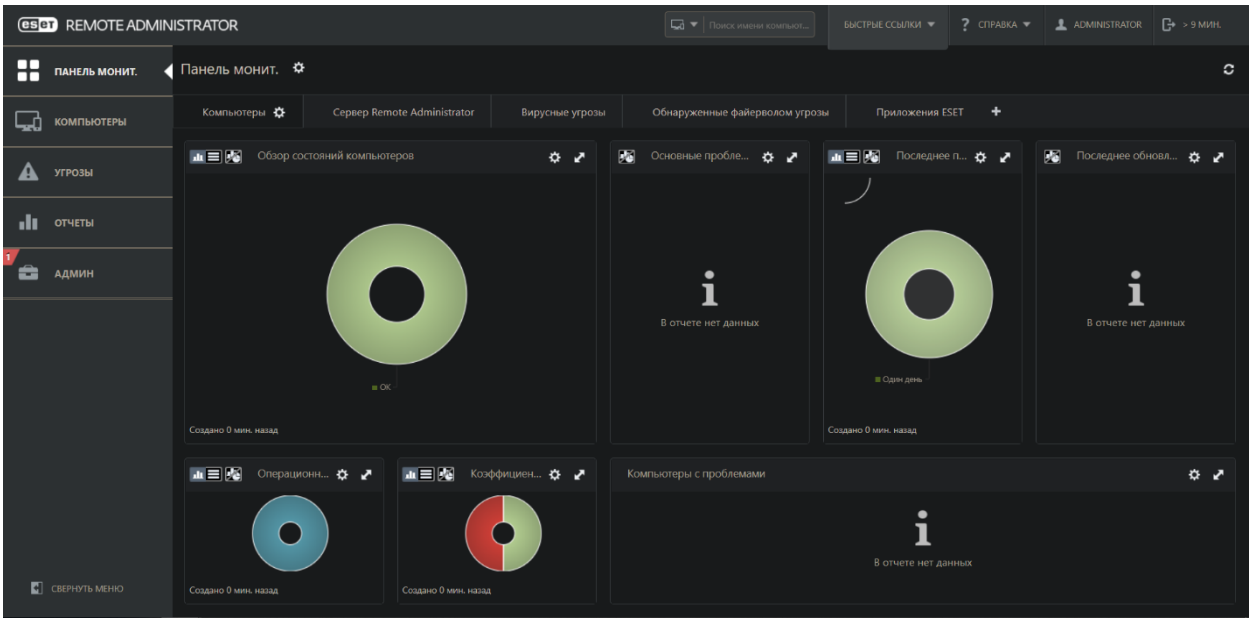


Рис 4.7 Основний екран де ми можемо відслідкувати всю інформацію про наші комп’ютери на даний момент

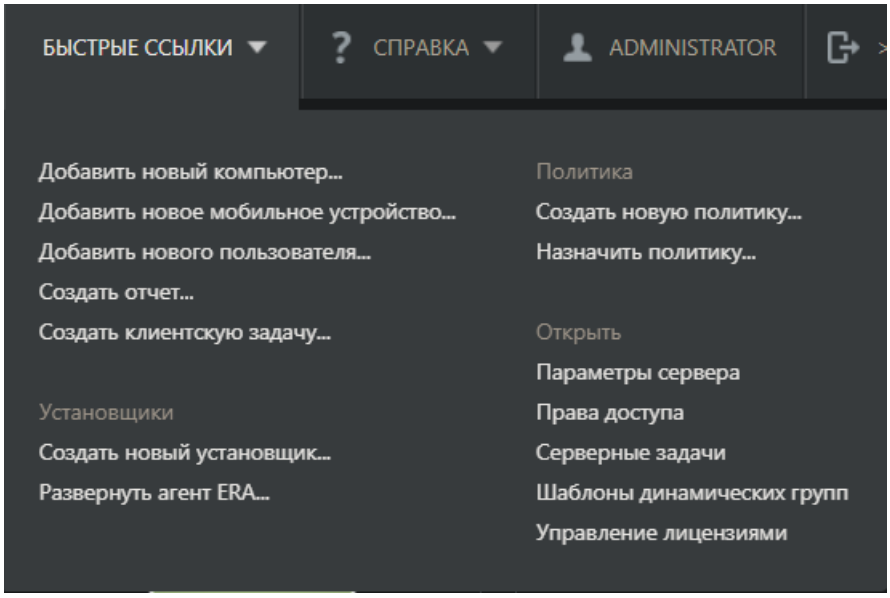


Рис 4.8 Для того щоб створити файл автоматичного встановлення антивірусів, на нашому основному екрані переходимо до швидких посилань обираємо створити нову політику

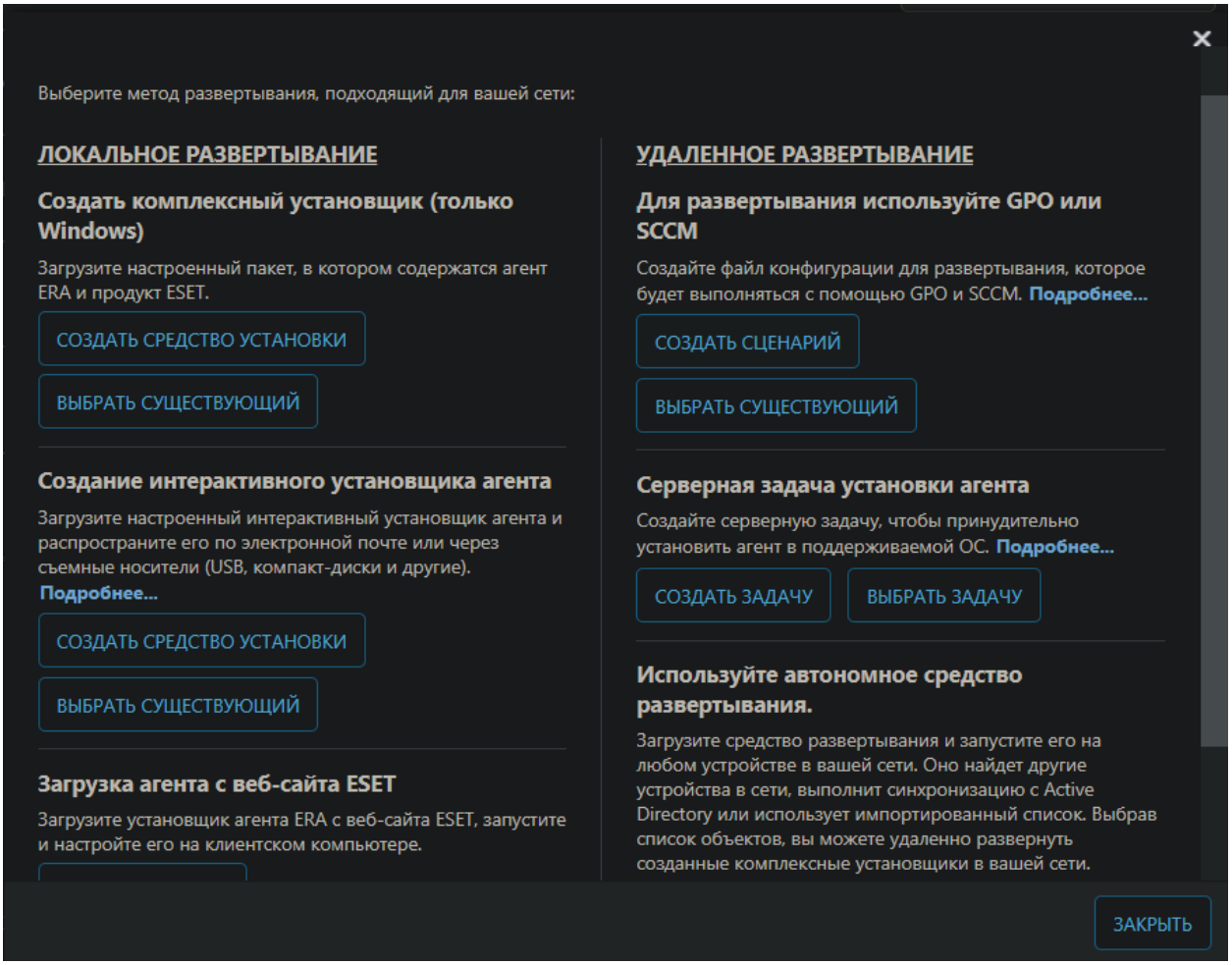


Рис. 4.9 Обираємо дистанційне розгортання, та тиснемо на створити сценарій.

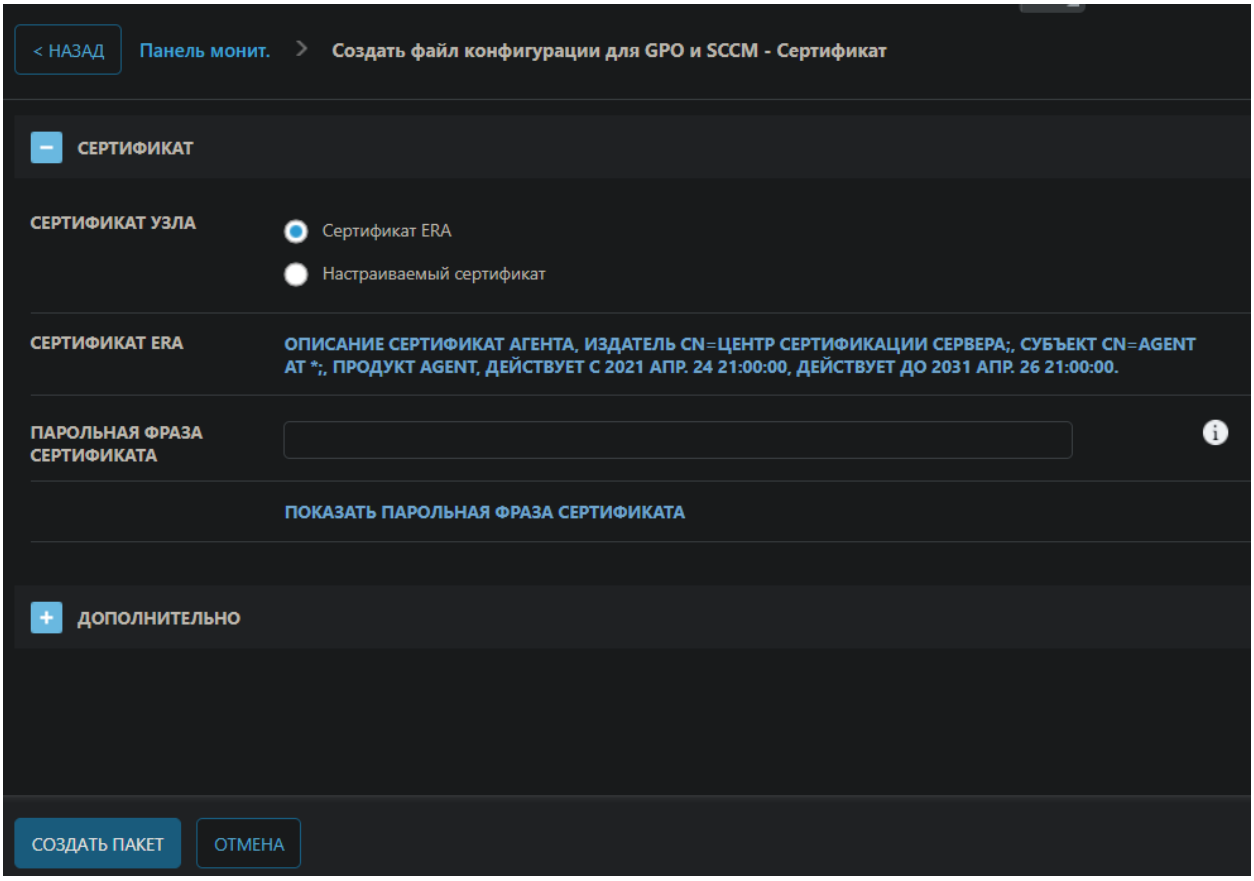


Рис 4.10 Встановлюємо такі параметри та тиснемо створити пакет

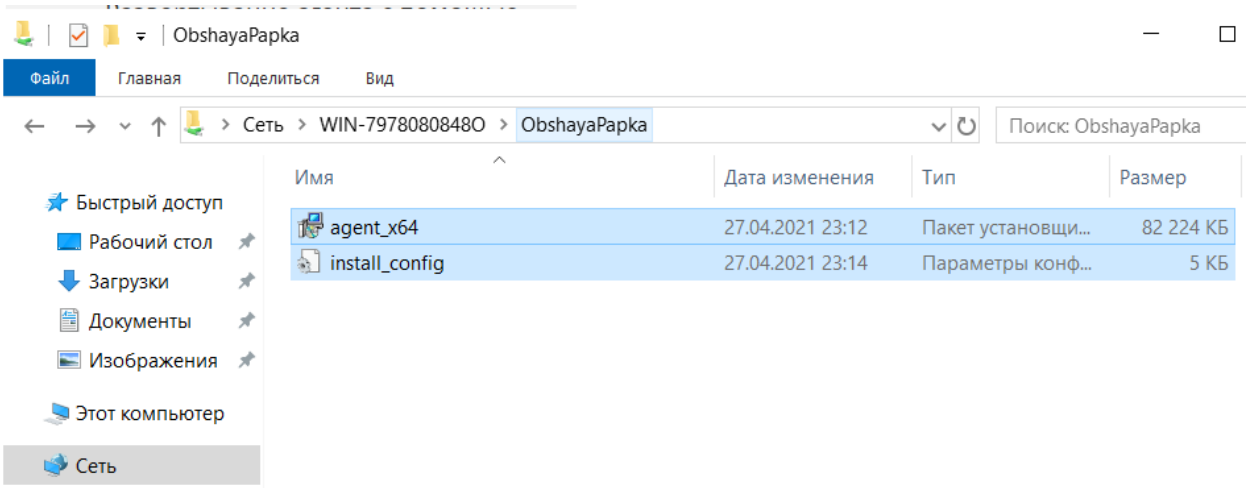


Рис 4.11 Після цього до нашого ПК, завантажиться 2 файли котрі в майбутньому будуть використовуватися для швидкого розгортання.

4.2 Розгортання клієнтської частини антивірусної системи

На цьому первинні налаштування закінчилися далі буде налаштування нашої віртуальної машини для того щоб ми могли розгорнути наші антивіруси.

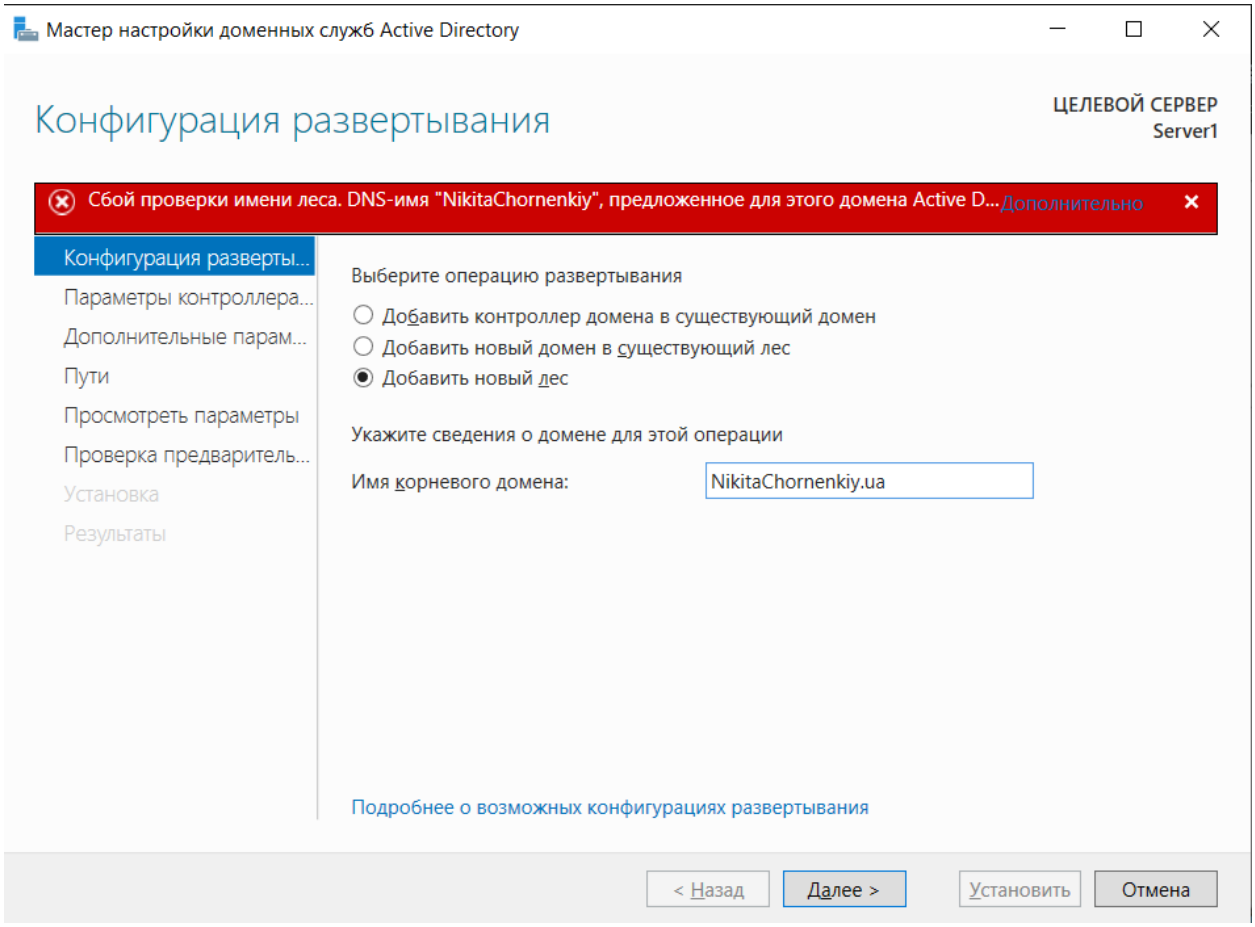


Рис 4.12 Для цього за допомогою вбудованого функціоналу Windows Server, ми повинні налаштувати доменні служби Active Directory.

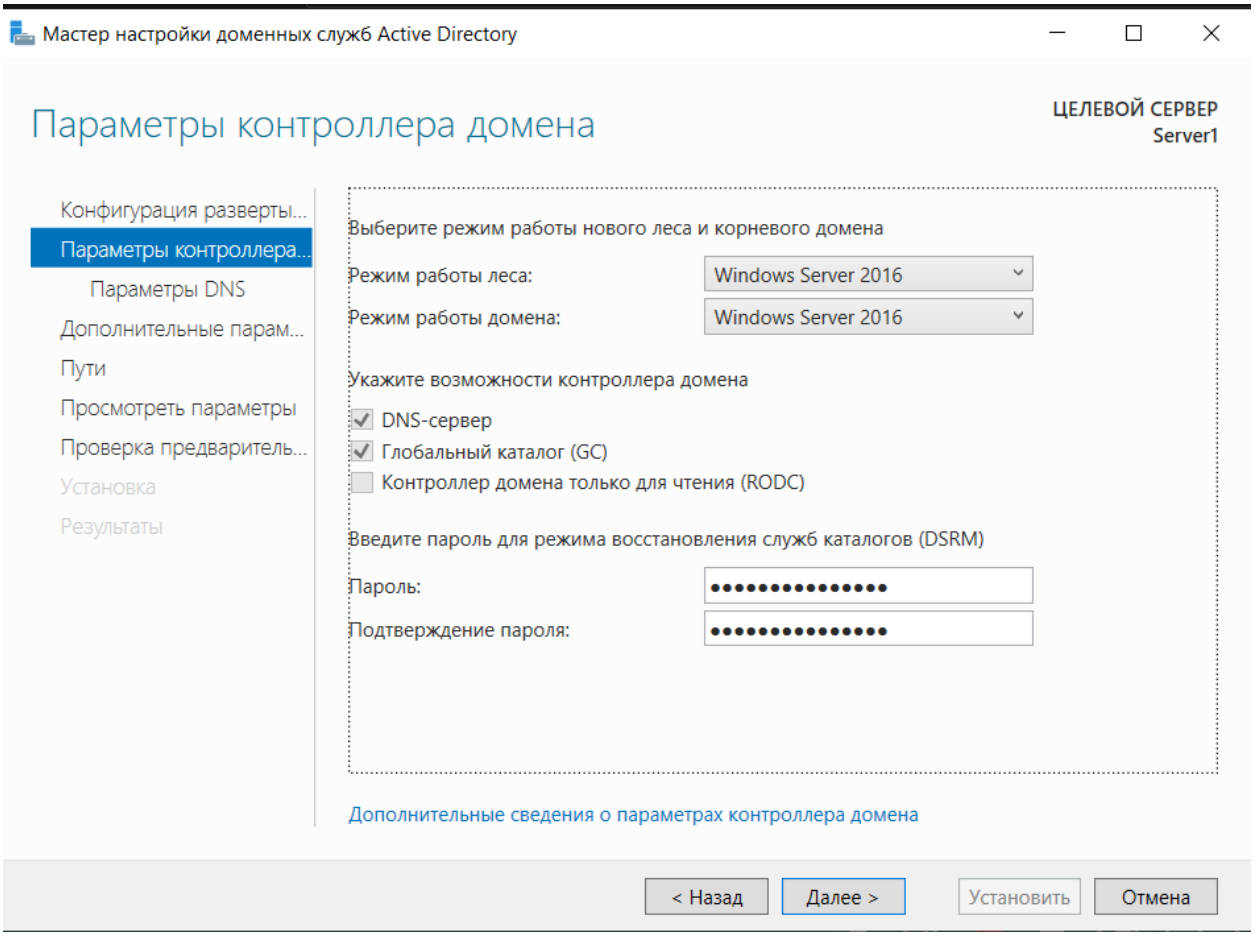


Рис 4.13 Встановлюємо параметри домену, встановлюємо DNS сервер, та налаштовуємо пароль.

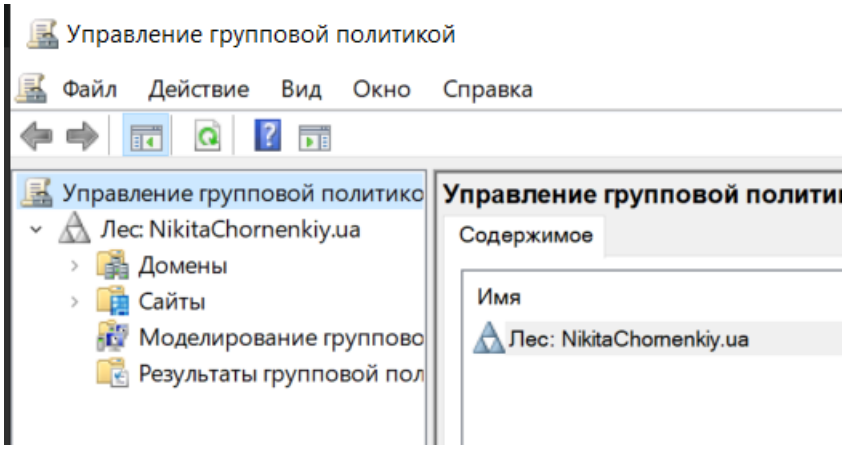


Рис 4.14 Після того як ми все правильно налаштували в нашій груповій політиці створиться наш домен котрий в майбутньому буде використовуватися для розгортання.

Для того щоб додати наші доменні ПК до мережі так званого лісу нам потрібно налаштувати DNS та DHCP. (Рис 4.15)

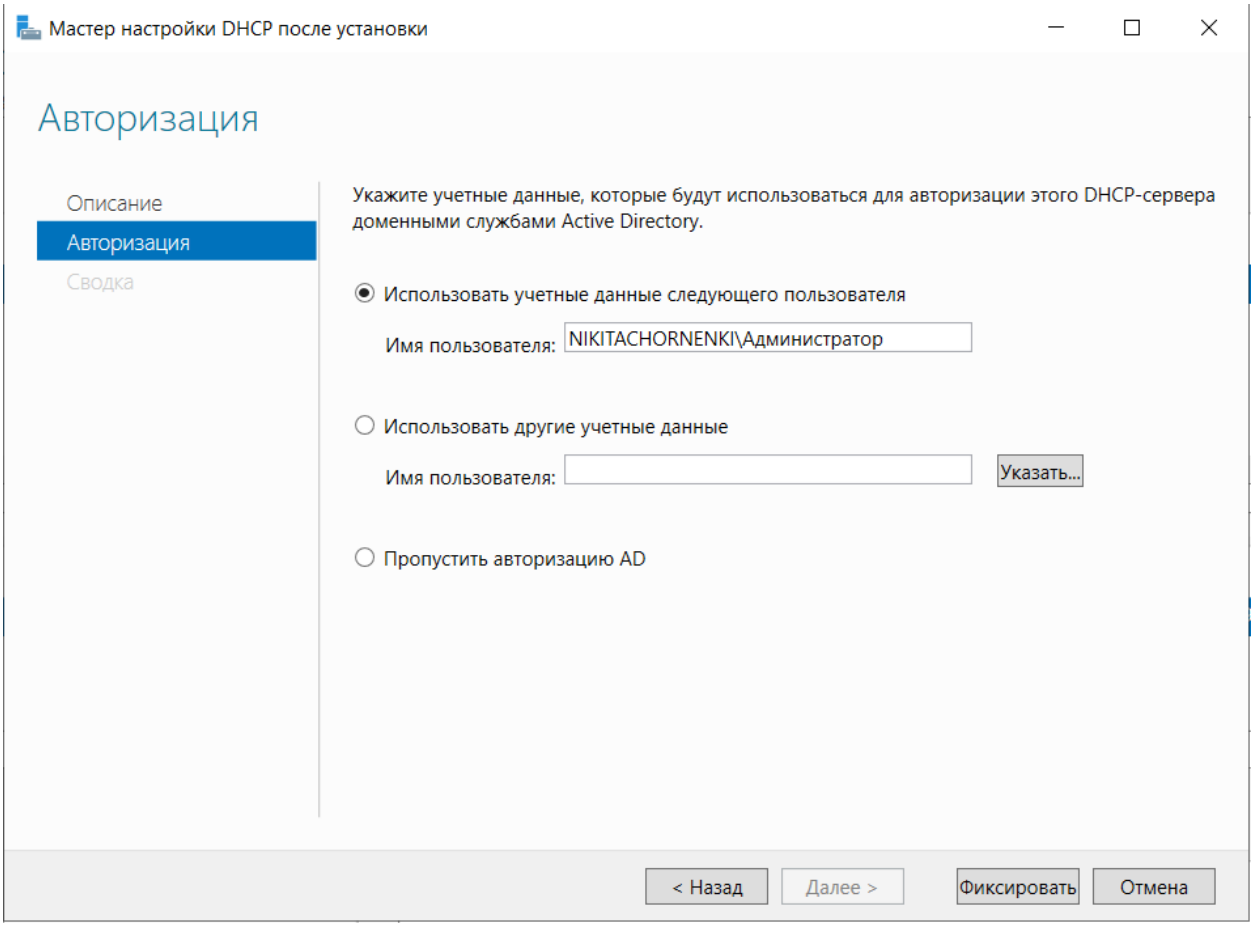


Рис 4.15 Встановлення DHCP серверу

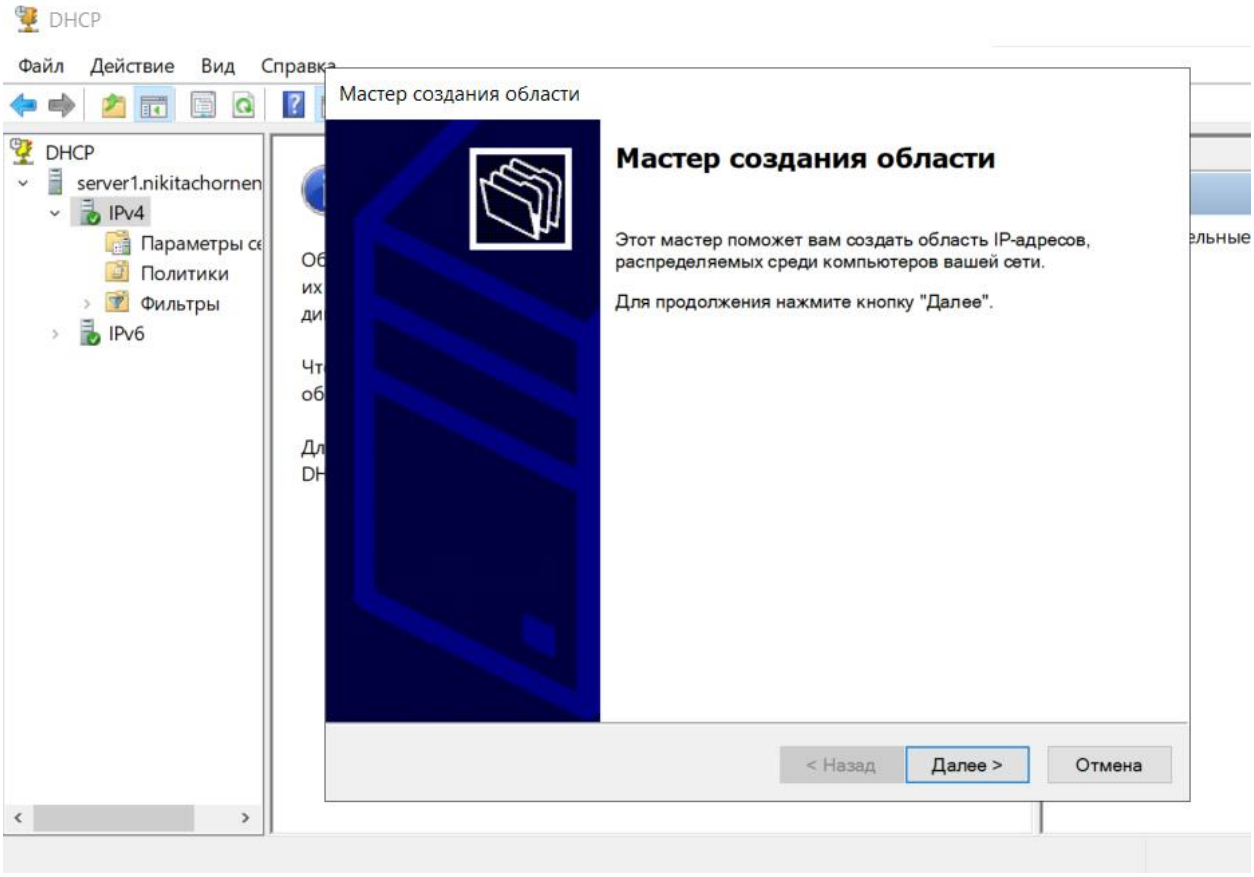


Рис 4.16 Створюємо спеціальну область IP адресів для того щоб наші ПК змогли об’єднатися в одну мережу

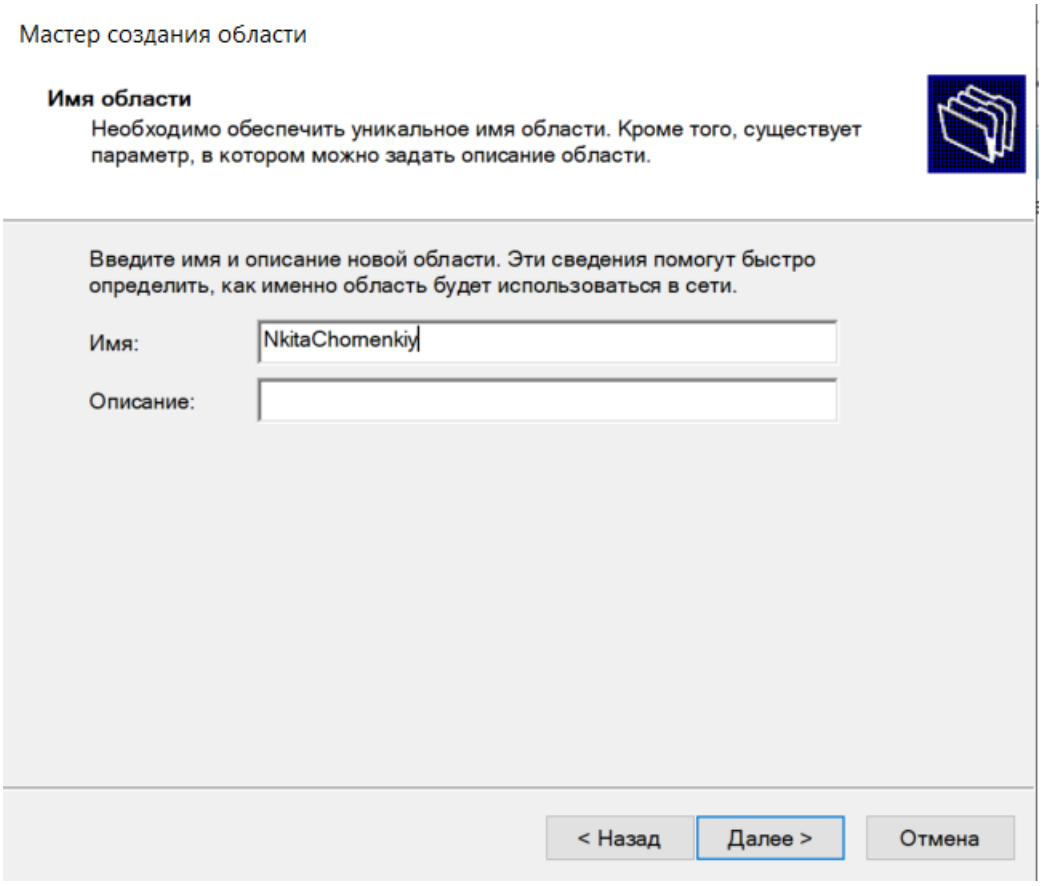


Рис 4.17 Додаємо ім’я для нашої області

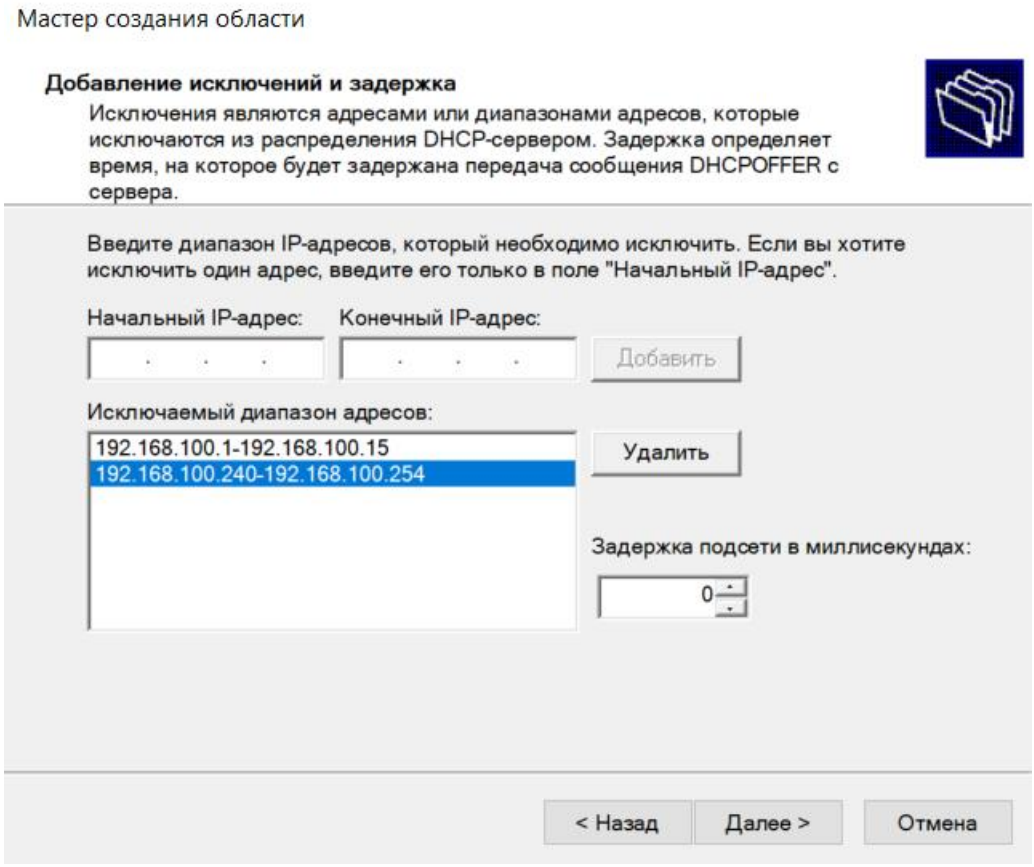


Рис 4.18 Додаємо діапазон адресів для того щоб наші ПК змогли автоматично обрати один з адресів

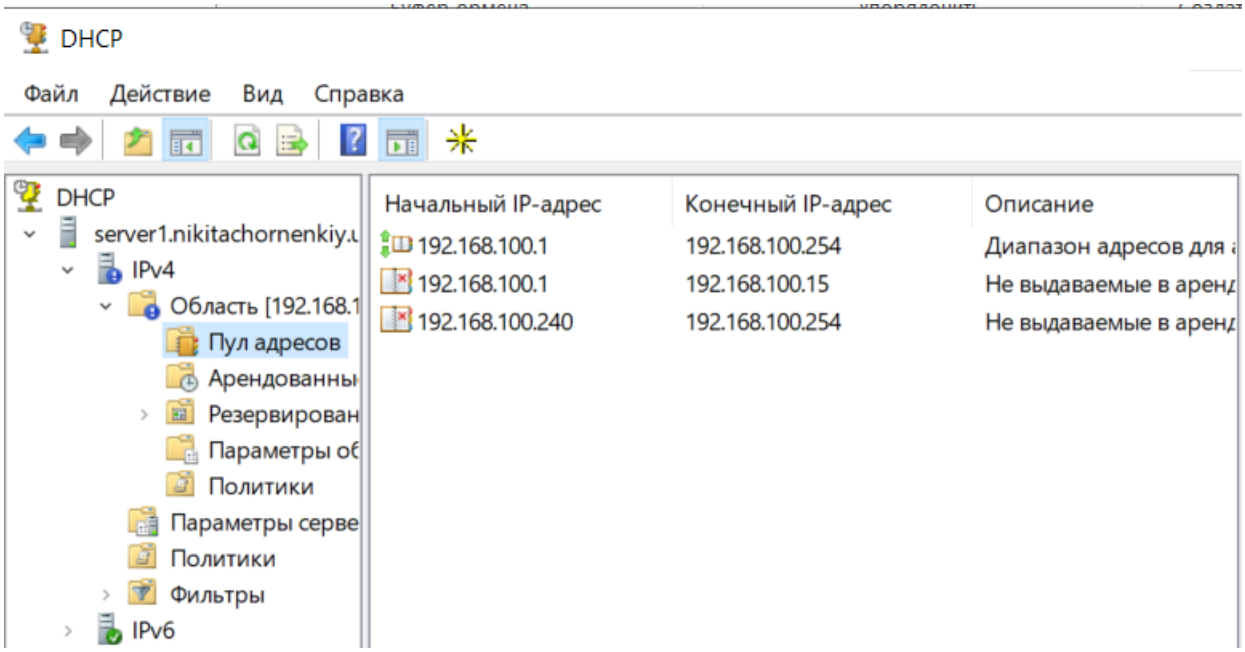


Рис 4.19 Після всіх налаштувань ми зможемо побачити наш пул адресів котрі в майбутньому наші комп'ютери використають для автоматичного налаштування локальної мережі.

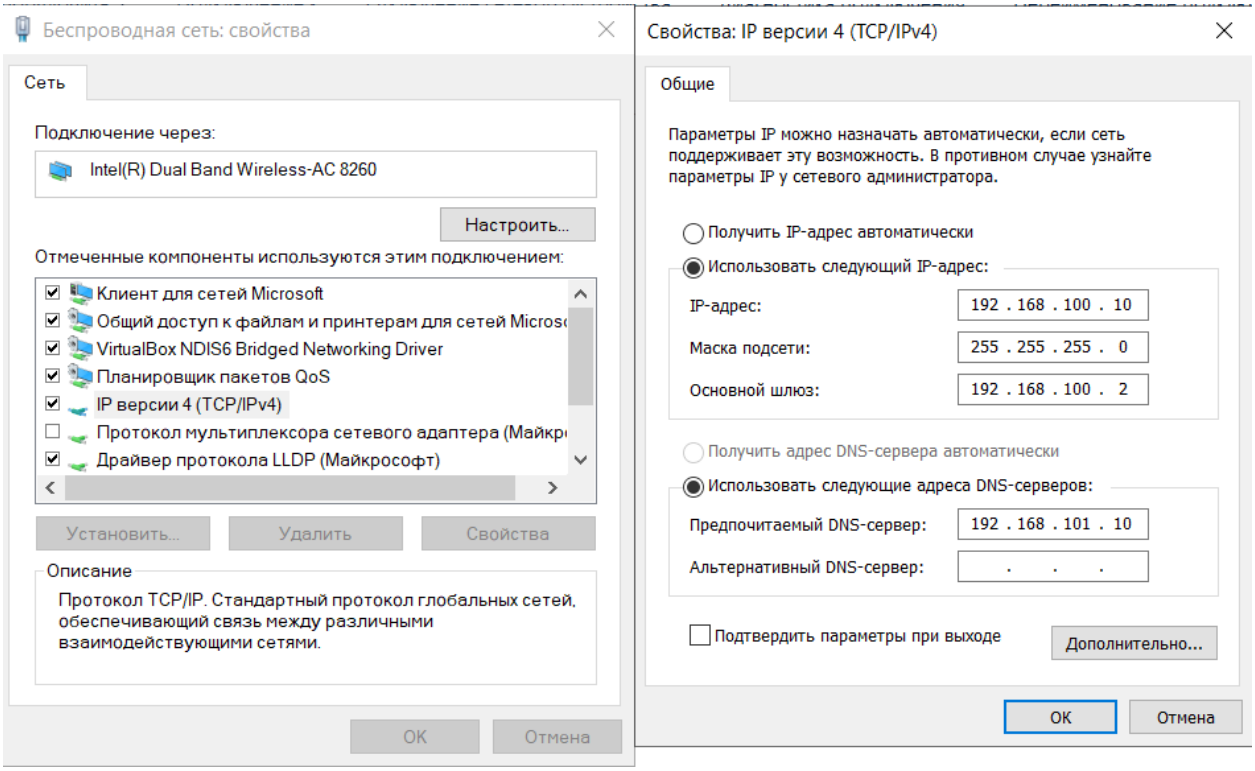


Рис 4.20 Налаштовуємо DNS сервер на нашому основному ПК

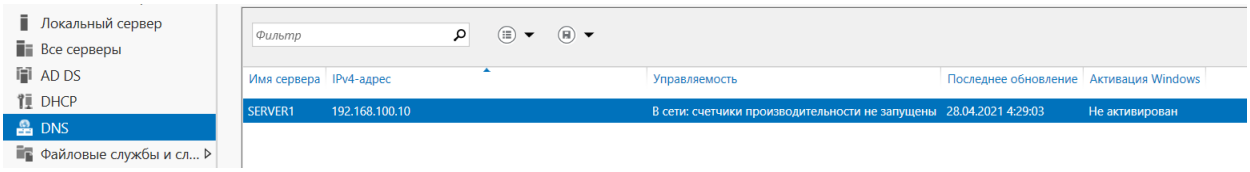


Рис. 4.21 Після успішного налаштування ми можемо побачити в меню нашого Windows серверу.

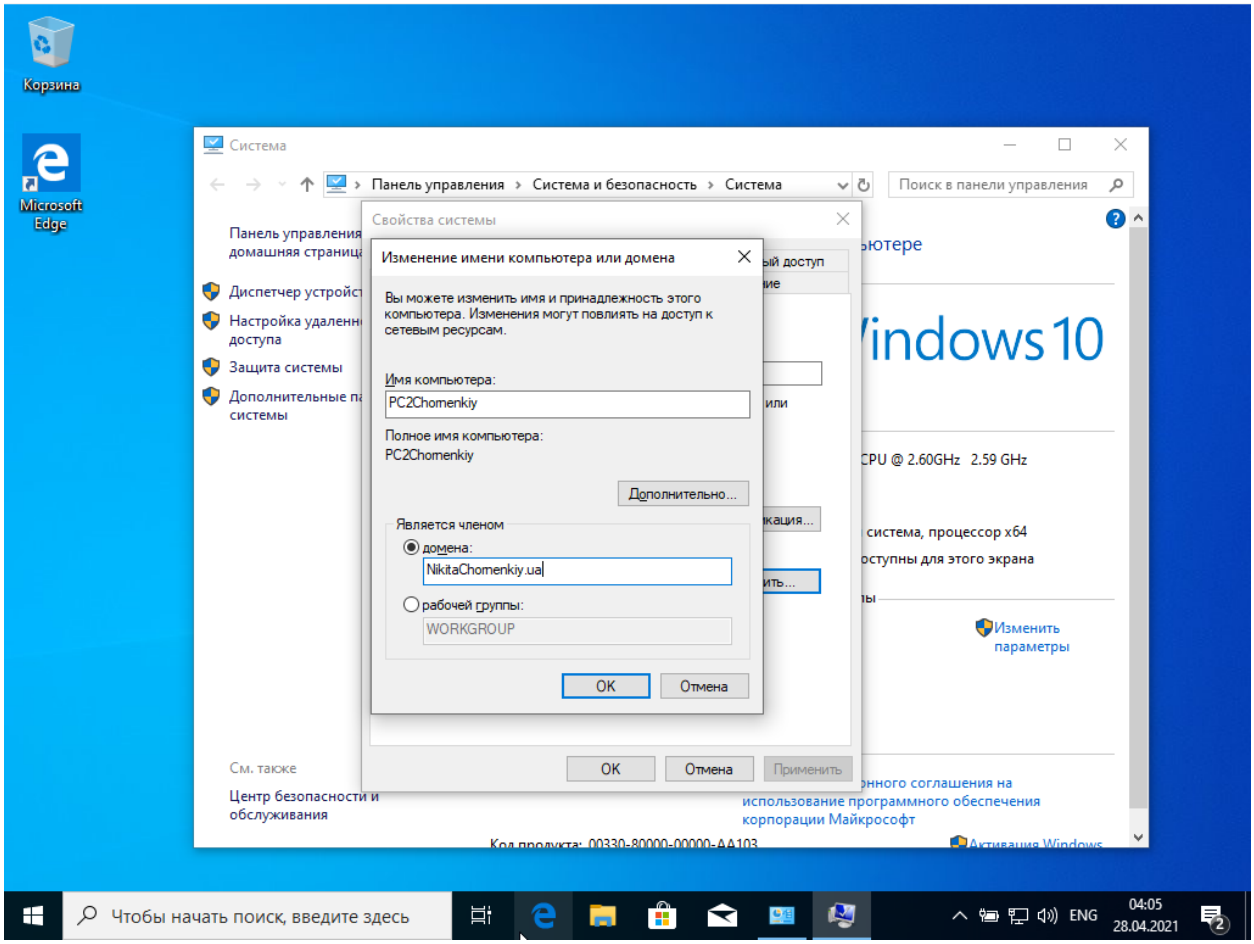


Рис. 4.22 Після всіх налаштувань на нашій віртуальній машині ми зможемо додати його до нашого створеного домену основного ПК.

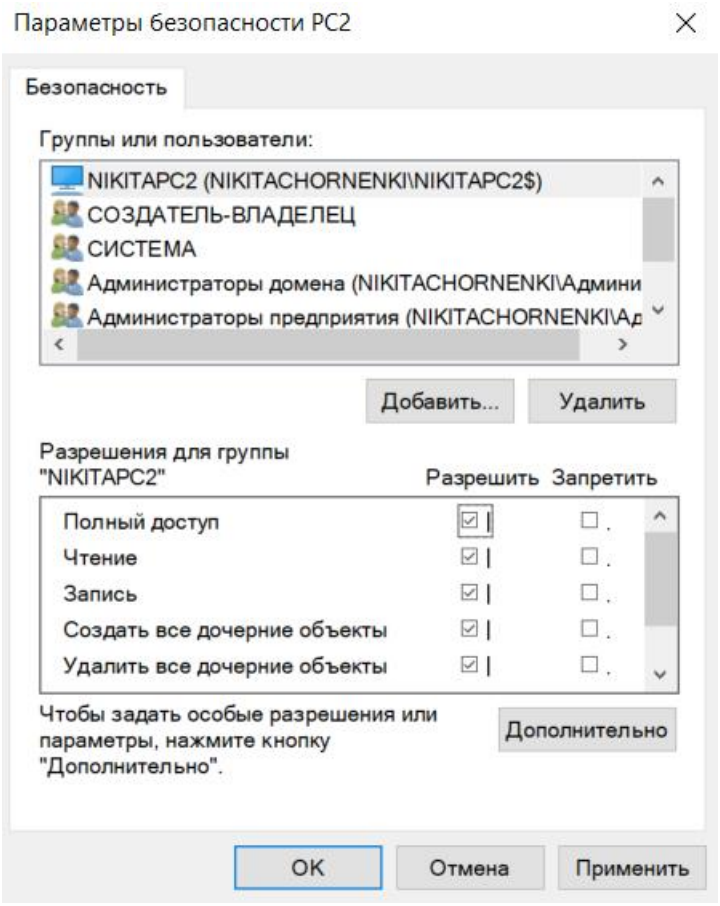


Рис 4.23 Надаємо нашому ПК максимальні привілеї, для того щоб наш віртуальний ПК мав повний функціонал.

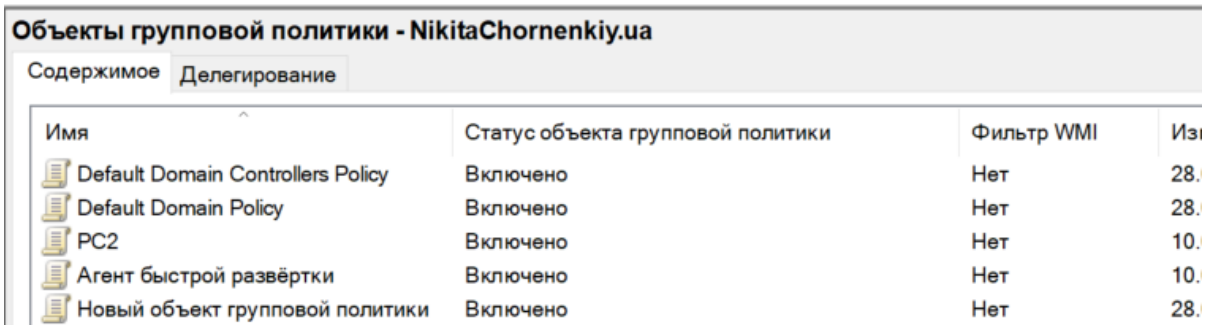


Рис 4.24 Після ми додаємо наш новий ПК до групової політики, після цього ми зможемо взаємодіяти з ним з нашого основного ПК. А також створюємо новий об’єкт Агент швидкої розгортки для того щоб здійснити розгортання нашого антивірусу.

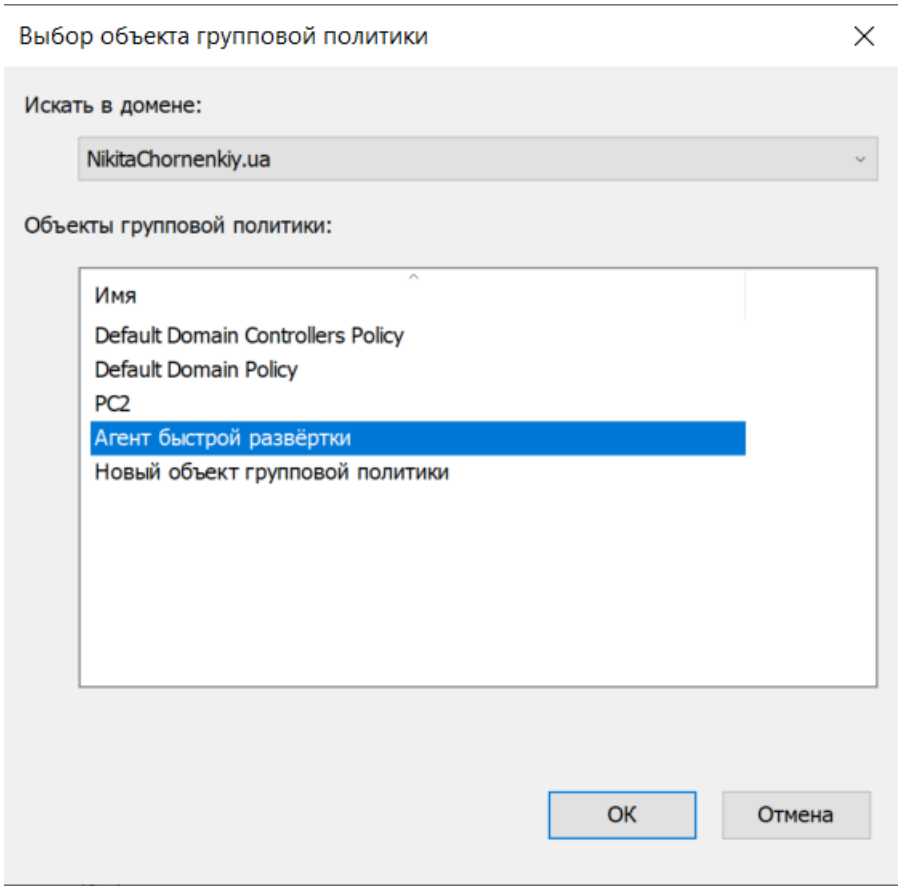


Рис 4.25 Робимо наш об’єкт основним для того щоб дати можливість розгорнути наш антивірус

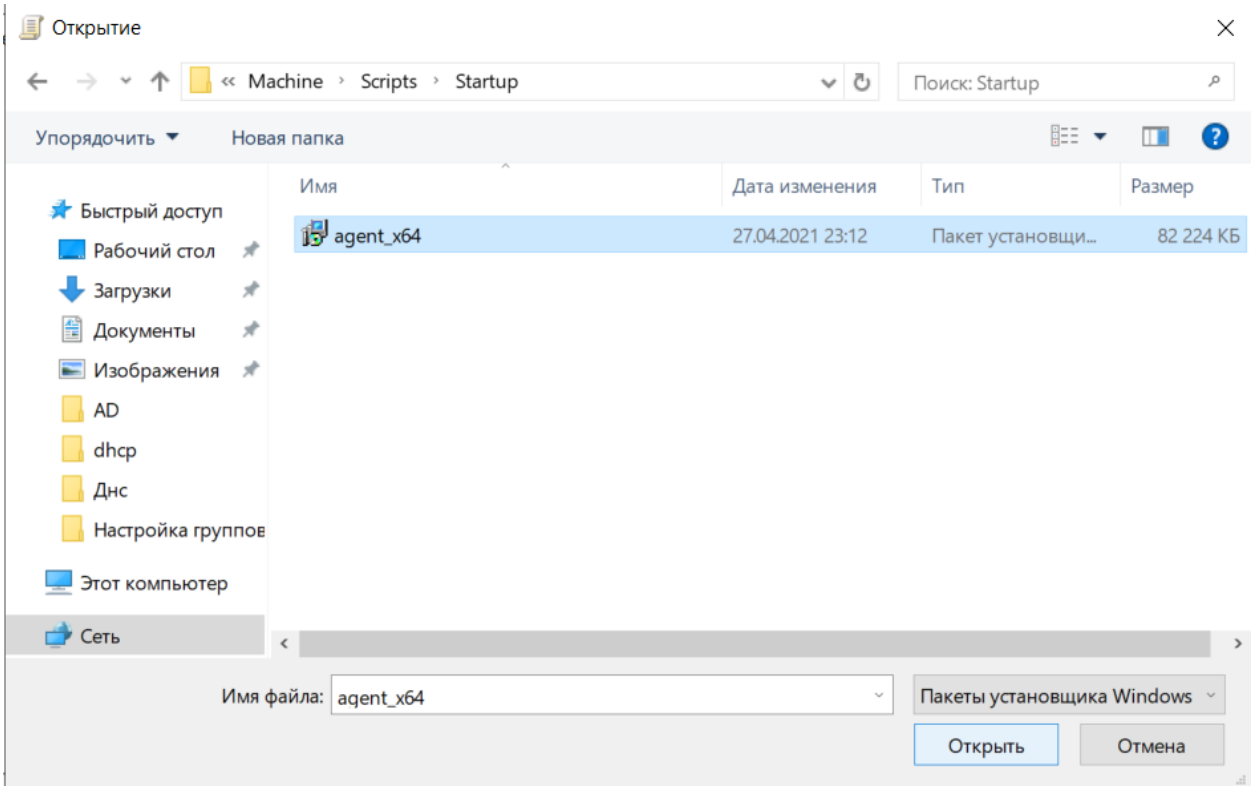


Рис 4.26 Обираємо наш інсталятор антивірусу для подальшого встановлення.

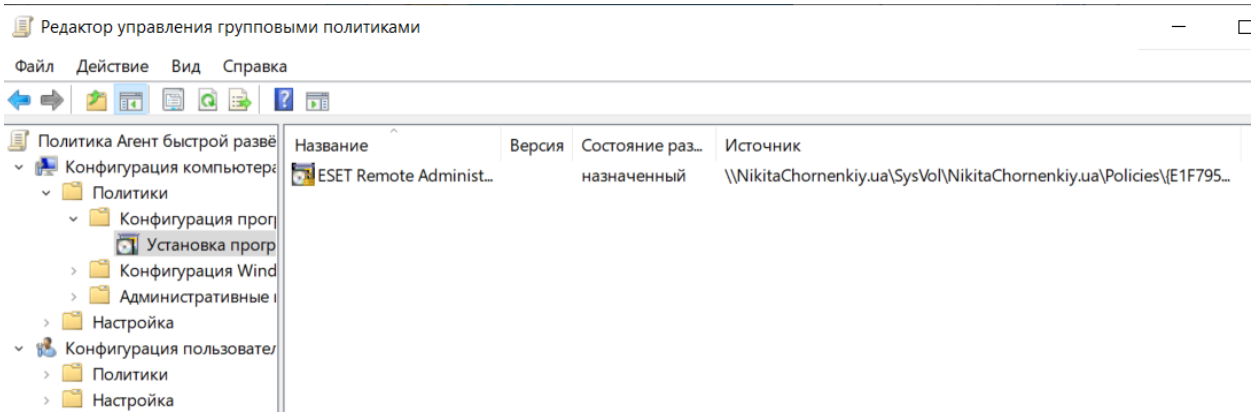


Рис 4.27 Після успішного додавання нашого антивірусу, він відобразиться в цьому меню.

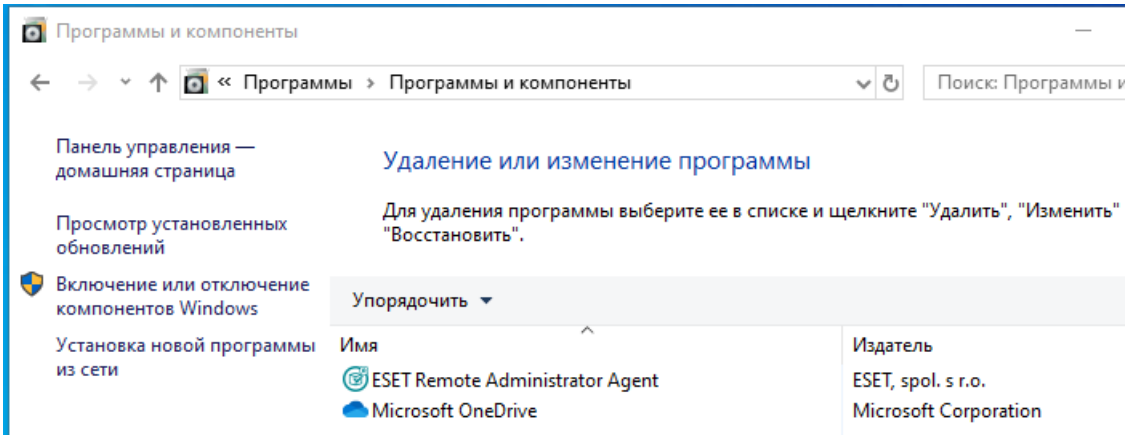


Рис 4.28 Після цього ми завантажуємо наш віртуальний ПК, і після завантаження ми можемо побачити успішне встановлення антивірусу на наш віртуальний ПК.

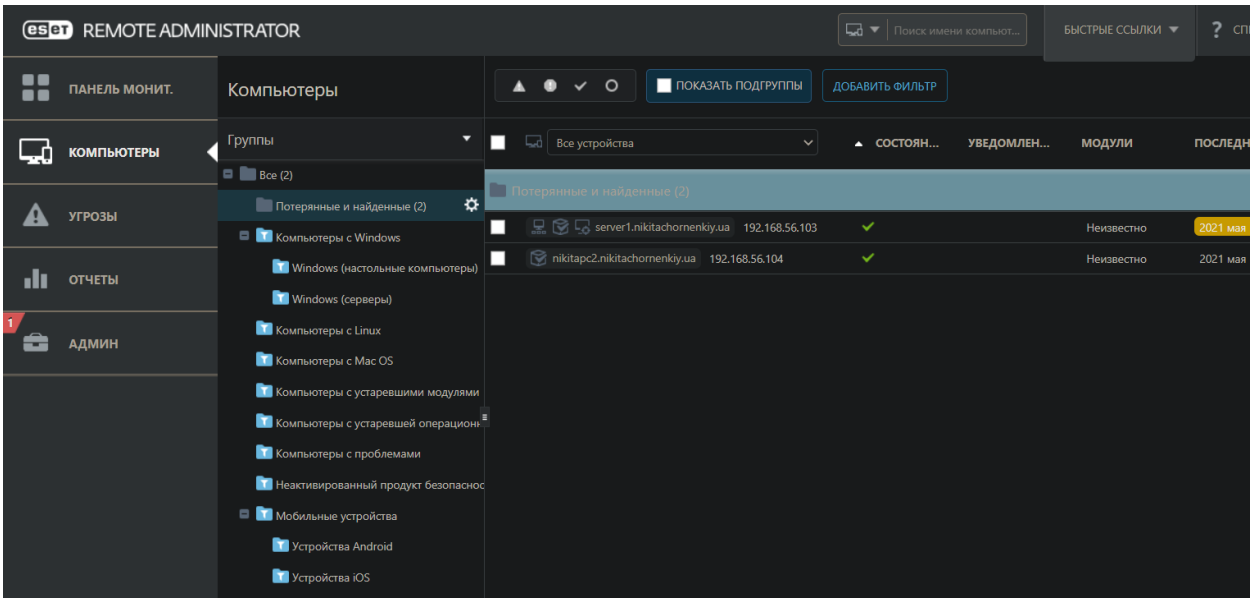


Рис 4.29 А також успішне встановлення антивірусу можна побачити в адміністративній панелі нашого антивірусу.

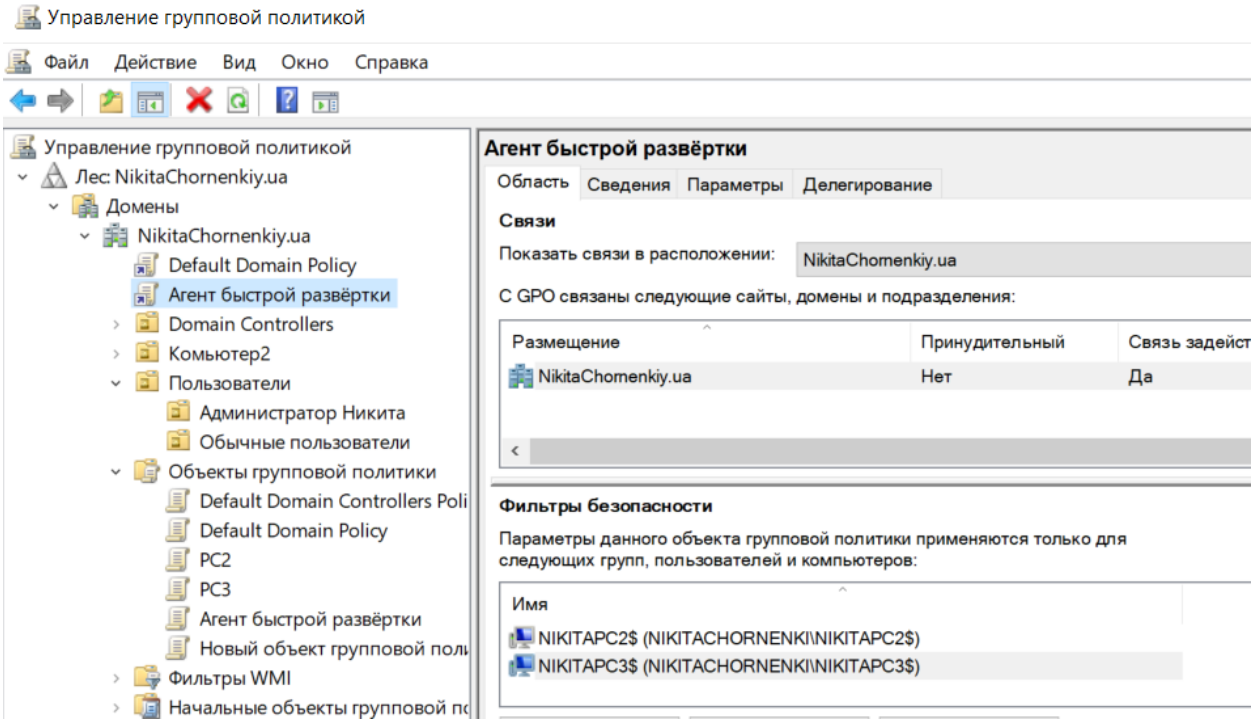


Рис 4.30 Для швидкого розгортання антивірусу на інші ПК, треба додати їх до фільтру безпеки, після цього всі ПК котрі були додані до фільтру автоматично розгорнуть антивірус.

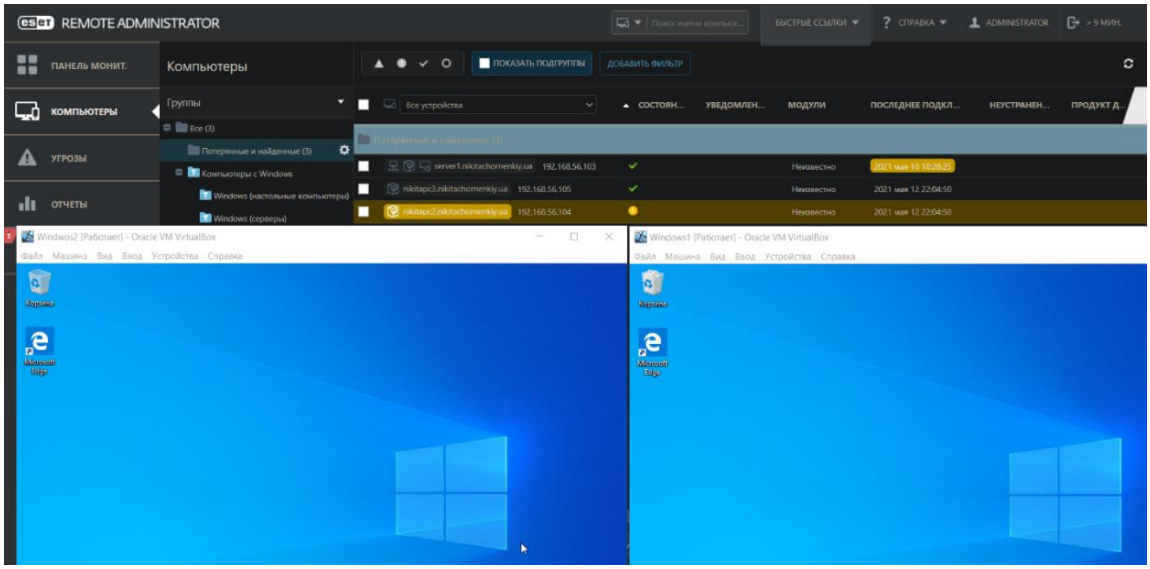


Рис 4.31 В адміністративній панелі ми бачимо основний ПК та 2 віртуальні машини на котрих розгорнуті антивіруси.

4.3 Розробка і впровадження налаштувань антивірусної системи

Наступним буде продемонстровано як за допомогою політик Eset Remote Administrator, зробити сканування системи та блокування зовнішніх USB накопичувачів. (Рис 4.32)

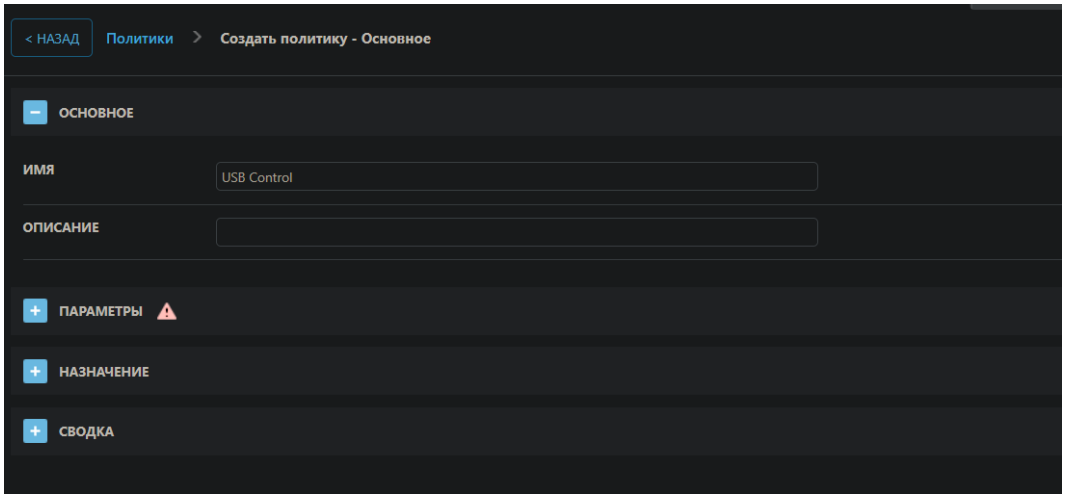


Рис 4.32 Створюємо політику контролю зовнішніх пристроїв

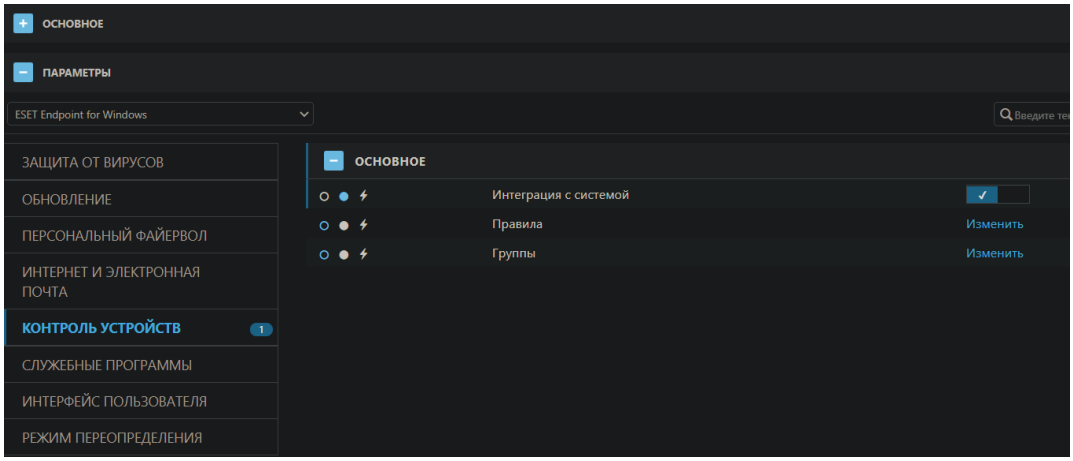


Рис 4.33 Міняємо нашу політику під свої потреби

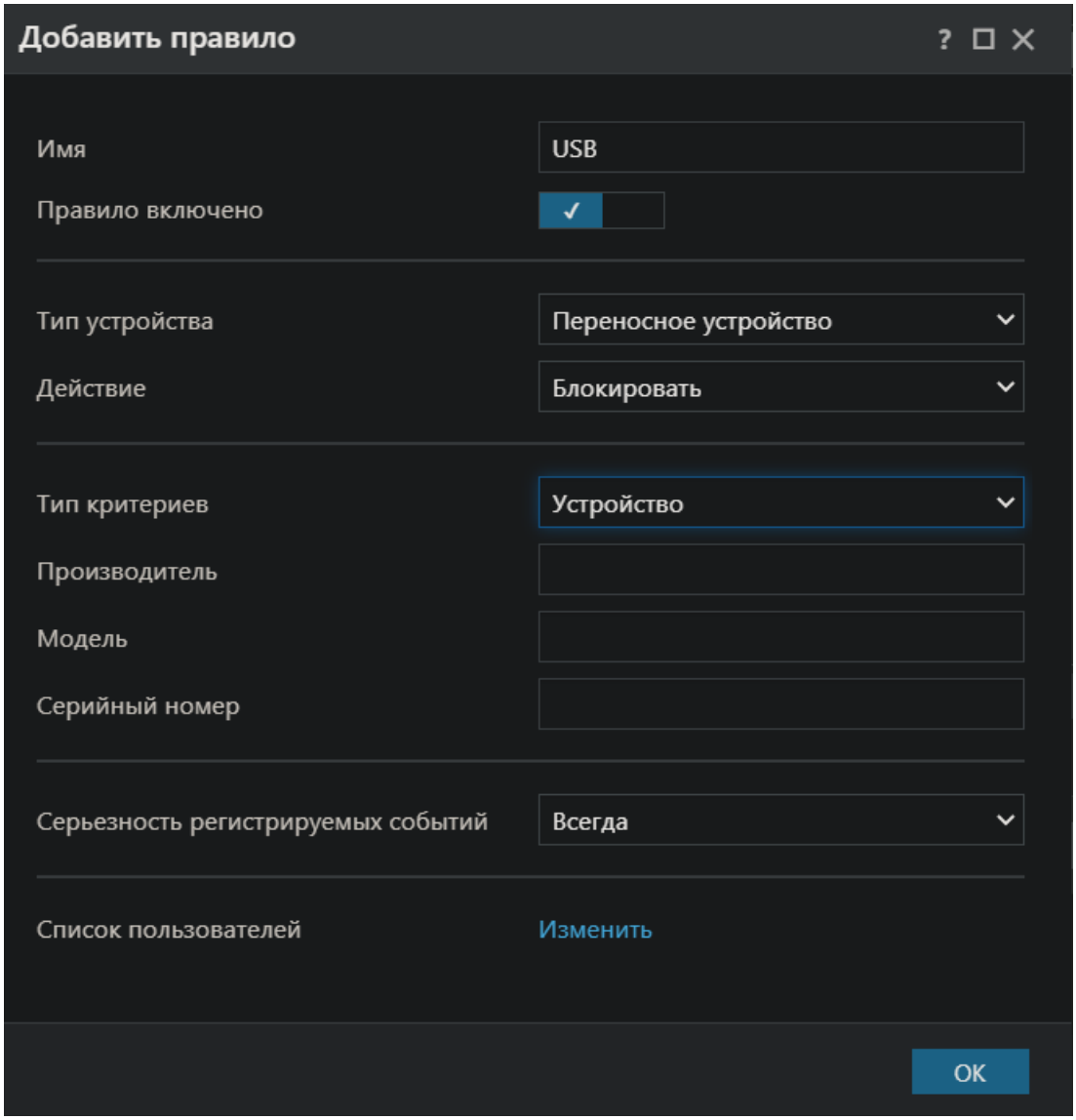


Рис 4.34 Додаємо правила нашій політиці

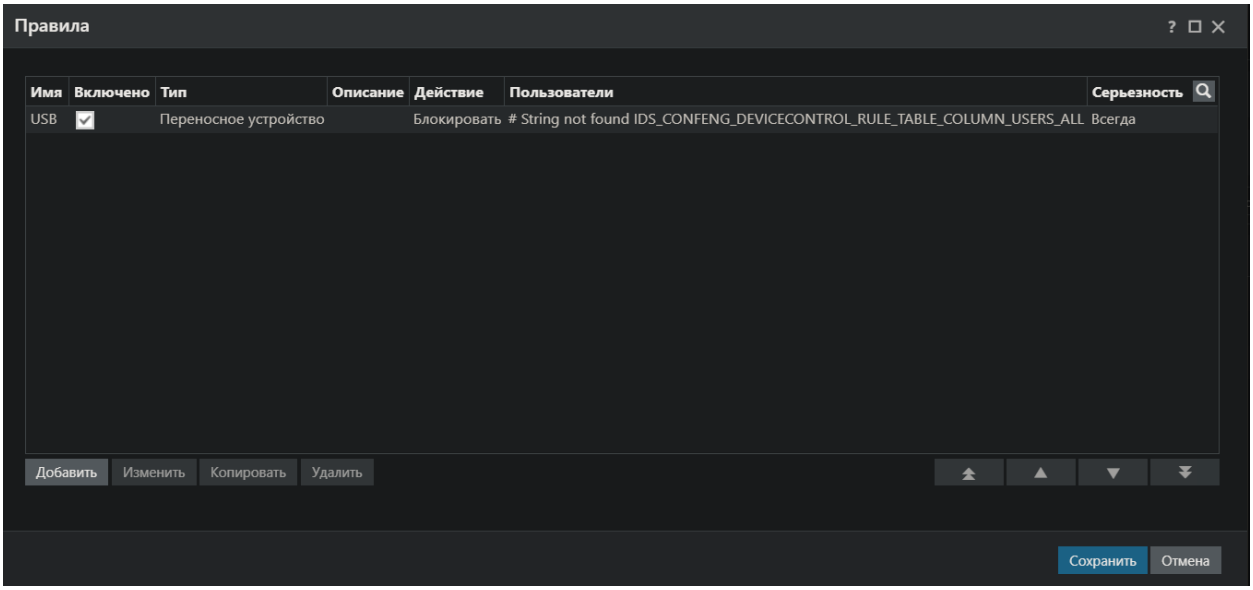


Рис 4.35 Зберігаємо наші правила

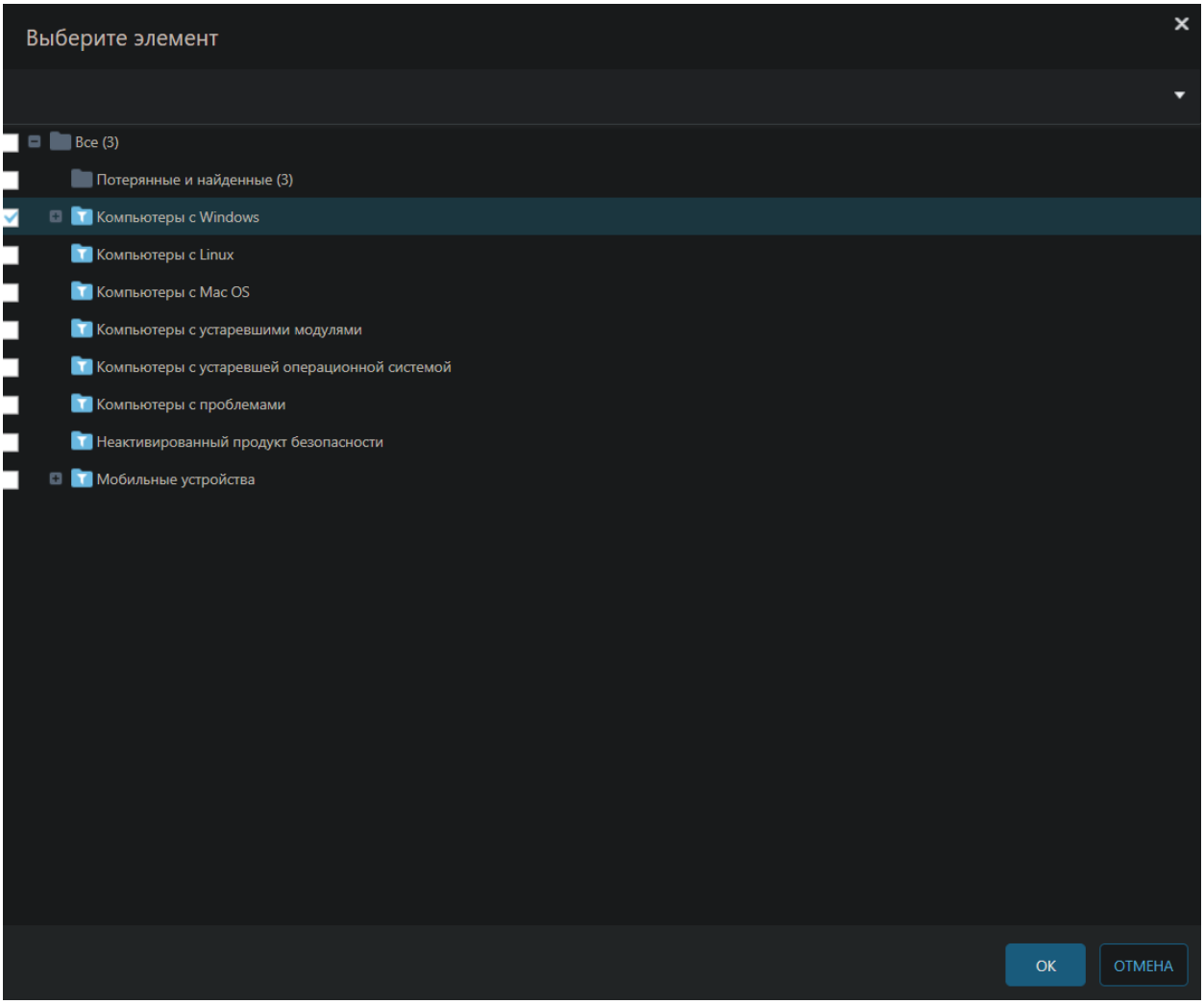


Рис 4.36 Додаємо наші правила до наших ПК

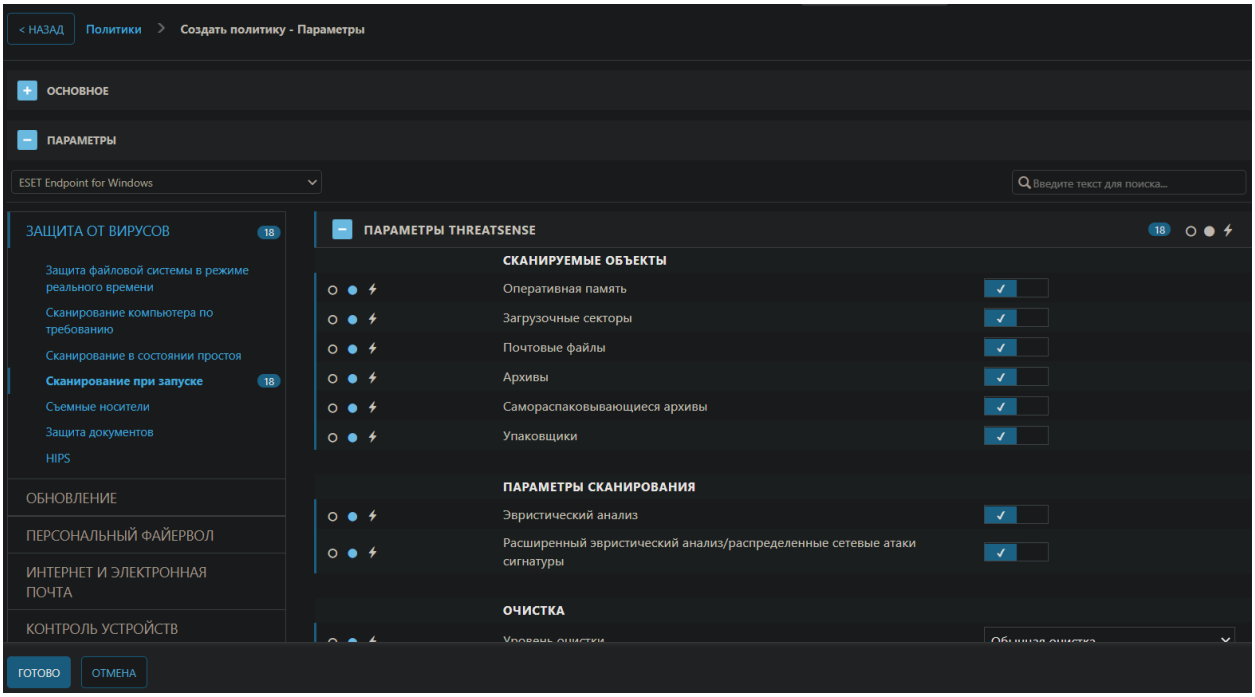


Рис 4.37 За аналогією робимо сканування наших комп'ютерів при запуску систем

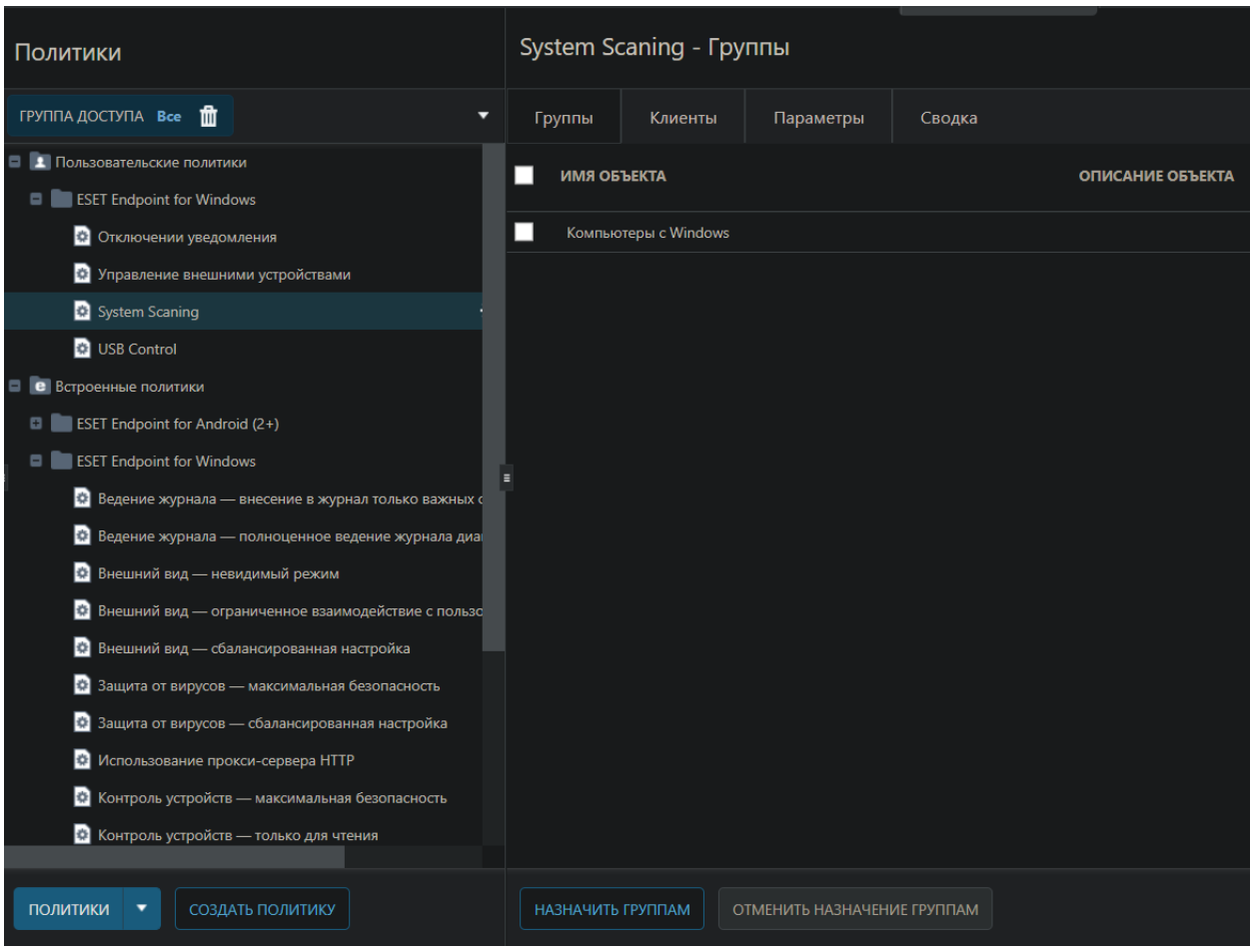


Рис 4.38 Прикріпляємо наші комп'ютери до цих політик

4.4 Результати розробки

В результаті розробки нашої системи антивірусного захисту ми отримали налаштовану систему захисту локальної мережі в котрій за нашими потребами були обмеження для збільшеного захисту від зовнішніх загроз.

Висновки

У кваліфікаційній бакалаврській роботі було проаналізоване програмне забезпечення для захисту персональних ПК. Проаналізований та визначений оптимальний варіант для розгортання антивірусних систем. Після чого був обраний варіант в котрому за допомогою вбудованих можливостей Windows Server під назвою Управління Груповими Політиками за допомогою котрого ми досягли своєї мети та змогли встановити захист на наших комп’ютерах в локальній мережі. Були детально розглянуті варіанти антивірусного захисту від усіх відомих виробників антивірусного програмного забезпечення. А також на власному прикладі розглянуто роботу одного з них.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Офіційний сайт Zillya – https://zillya.ua/
2. Офіційний сайт BitDefender – https://www.bitdefender.com/
3. Офіційний сайт MalwareBytes – https://ru.malwarebytes.com/
4. Офіційний сайт Microsoft – https://support.microsoft.com/en-us/windows/help-protect-my-pc-with-microsoft-defender-offline-9306d528-64bf-4668-5b80-ff533f183d6c
5. Офіційний сайт ESET – https://www.eset.com/us/
6. Офіційний сайт MCAfee – https://www.mcafee.com/ru-ru/index.html
7. Офіційний сайт Avast – https://www.avast.ua/
8. Офіційний сайт Norton – https://us.norton.com/
9. Антивирус – для чего он нужен [Електронний ресурс] – https://www.softmaker.com/ru/blog/bytes-and-beyond/anti-virus-why-bother
10. Для чего нужен антивирус [Електронний ресурс] – https://habr.com/ru/post/266789/
11. Види антивирусов, Действительно ли он необходим, этот антивирус [Електронний ресурс] – http://pc-information-guide.ru/bezopasnost/vidy-antivirusov-dejstvitelno-li-on-n%20eobxodim-etot-antivirus.html
12. Этапы развертывания — GPO [Електронний ресурс] – https://help.eset.com/era_admin/65/ru-RU/fs_agent_deploy_gpo.html
13. Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats – Quinn Kiser (Author) – 5 September 2020 – С.240
14. Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks – Tim Rains (Author) – 29 May 2020 –С.428