МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

«Комплексна система захисту інформації автоматизованої системи класу "1" 4-ї категорії комерційного підприємства»

Завідувач

випускаючої кафедри Любчак В.О.

Керівник роботи Ободяк В.К.

Студент групи КБ-81 Медведєв Д.О.

Суми 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

Затверджую_____

Зав. кафедрою Любчак В.О.

“_____” _____2022 р.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи КБ-81 спеціальності «Кібербезпека» денної форми навчання Медведєва Дмитра Олександровича.

Тема: «Комплексна система захисту інформації автоматизованої системи класу "1" 4-ї категорії комерційного підприємства»

Затверджена наказом по СумДУ

№_____ від _____2022 р.

Зміст пояснювальної записки: 1) Аналіз предметної області і існуючих рішень. 2) Вибір середовища програмної реалізації поставленої задачі. 3) Реалізація процесу спрощеного проектування. 4) Оцінка ризиків інформаційної безпеки.

Дата видачі завдання “_____” _____2022 р.

Керівник випускної роботи _____ Ободяк В.К.

Завдання прийняв до виконання _____ Медведєв Д.О.

РЕФЕРАТ

Записка: 84 стор., 30 рис., 2 табл., 8 додатків, 21 джерел.

Мета роботи — спрощення проектування комплексної системи захисту інформації автоматизованої системи класу "1" 4-ї категорії комерційного підприємства.

Об'єкт дослідження — процес проектування автоматизованої системи класу «1» 4-ї категорії комерційного підприємства.

Предмет дослідження – сукупність методів та заходів, які дозволять спростити проектування комплексної системи захисту інформації автоматизованої системи класу "1" 4-ї категорії комерційного підприємства.

Методи дослідження — метод аналітичного огляду, порівняння.

Результати — спрощено проектування КСЗІ автоматизованої системи класу "1" 4-ї категорії за рахунок створеного алгоритму дій, в основі якого лежить програмна реалізації процесу налаштування КСЗІ АС класу «1» 4-ї категорії.

ПРОЕКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, КСЗІ, АВТОМАТИЗОВАНА СИСТЕМА, ISE POWESHELL, СКРИПТОВИЙ СЦЕНАРІЙ, ОЦІНКА РИЗИКІВ, АНТИВІРУСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЛОКАЛЬНА ПОЛІТИКИ БЕЗПЕКИ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 4
ВСТУП 5
РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ І ІСНУЮЧИХ РІШЕНЬ 6
1.1 Класифікація автоматизованих систем 6
1.2 Проектування КСЗІ АС класу «1» 4-ї категорії 9
1.3 Аналіз проектування 32
1.4 Методологія оцінки ризику інформаційних систем 33
1.5 Постановка задачі 36
РОЗДІЛ 2. ВИБІР СЕРЕДОВИЩА ПРОГРАМНОЇ РЕАЛІЗАЦІЇ 37
2.1 Аналіз програмних продуктів 37
2.2 Використання ISE PowerShell 38
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПРОЦЕСУ СПРОЩЕНОГО ПРОЕКТУВАННЯ 40
3.1 Використання скриптового сценарію 40
3.2 Імпорт попередньо налаштованої політики безпеки 43
3.3 Імпорт конфігурації роботи антивірусного ПЗ 45
РОЗДІЛ 4. ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 47
4.1 Процес оцінки ризиків інформаційної безпеки 47
4.2 Результат оцінки ризиків 47
ВИСНОВОК 56
СПИСОК ЛІТЕРАТУРИ 58
ДОДАТОК А 61
ДОДАТОК Б 62
ДОДАТОК В 63
ДОДАТОК Г 65
ДОДАТОК Ґ 73
ДОДАТОК Д 79

ДОДАТОК Е 83
ДОДАТОК Є 84

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АС – автоматизована система

КЗЗ – комплекс засобів захисту

ІБ – інформаційної безпеки

КС – комп’ютерна система

КСЗІ – комплексна система захисту інформації

ОС – операційна система

ПЗ – програмне забезпечення

ММС – Microsoft Management Console

ВСТУП

Операційна система Windows 10 використовується для обробки конфіденційної інформації, але за стандартом ОС використовуються стандартні параметри системи та виділених компонентів, що не відповідає критеріям безпеки, встановленим багатьма організаціями та комерційними підприємствами.

Використання системи з неправильними налаштуваннями може призвести до критичних порушень безпеки, дозволяючи зловмисникам витікати конфіденційну інформацію або викликати збій системного обладнання.

Не менш важливим критерієм є загальна кількість витраченого часу на ручне проектування комплексної системи захисту інформації згідно документації, в якій виділені параметри роботи системного обладнання, згідно регламенту роботи комерційного підприємства.

В ході даної роботи розглядається предметна область, до якої входить аналізування автоматизованої системи, компонентів, які входять в їх склад, можливі класифікації та принципи проектування комплексної системи захисту інформації автоматизованої системи класу 1 4-ї категорії з критеріями, які відповідають вимогам для використання спроектованої системи в комерційних підприємствах.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ І ІСНУЮЧИХ РІШЕНЬ

1.1 Класифікація автоматизованих систем

Відповідно до Закону України «Про захист інформації в автоматизованих системах» автоматизована система – апаратно-програмний комплекс, за допомогою якого здійснюється автоматизована обробка конфіденційної інформації, відповідно до принципів роботи комерційного підприємства [1]. Головним призначенням АС являється формування вимог щодо комплексів засобів захисту, відповідно до характеристик інформації, якою оперує відповідна система.

До складу автоматизованої системи входить:

- операційна система, за допомогою якої виконується робота системи;
- фізичне середовище, в якому розташовується відповідна система;
- персонал, котрий виконує роль наглядача та виконує моніторинг системи, під час її функціонування та проводить регламентні роботи [1].

Вимоги до функціонального складу комплексу засобів захисту залежать від:

- характеристик інформації, якою оперує відповідна система (відкрита або інформація з закритим доступом);
- операційної системи;
- фізичного середовища (будівля/кабінет, де знаходиться система);
- персоналу і організаційних мір, які кожна організація формулює відповідно до своїх потреб.

Відповідно до нормативно-правових актів, що встановлюються законодавством - всі наведені компоненти визначають класифікацію та необхідні правила, за допомогою яких проектується та вводиться в експлуатацію АС.

За сукупністю характеристик АС (конфігурація апаратних засобів ОС, фізичне розміщення комплексу, категорії оброблюваної інформації, кількості користувачів) виділено три основних класи АС, в кожному класі приписуються різні вимоги щодо принципу проектування комплексної системи захисту інформації [2].

Існують наступні категорії автоматизованих систем:

1. **Клас «1»** — апаратно-програмний комплекс, який складається з однієї системи та обробляє інформацію однієї або декількох категорій конфіденційності.

До особливостей даної класифікації відносяться:

- можливість працювати одному користувачу з повноваженнями на доступ та редагування конфіденційної інформації , яка оброблюється;
- технічні засоби (відповідні носії інформації) з точки зору захищеності відносяться до однієї категорії і можуть використовуватись для збереження інформації.

2. **Клас «2»** — апаратно-програмний комплекс, який складається з декількох системи та одночасно обробляє інформацію різних категорій конфіденційності.

До особливостей даної класифікації відносяться:

- можливість працювати одразу декільком користувачам, маються однакові повноваження щодо доступу до інформації, яка оброблюється;
- призначення різних повноважень щодо редагування конфіденційної інформації;
- технічні засоби з точки зору захищеності відносяться до різних категорій які можуть одночасно здійснювати обробку інформації.

3. **Клас «3»** — розподілений апаратно-програмний комплекс, який складається з багатьох системи та одночасно обробляє інформацію різних категорій конфіденційності.

До особливостей даної класифікації відносяться:

- можливість працювати певною кількістю користувачів, до яких можуть застосовуватись різні повноваження щодо доступу до інформації, яка оброблюється;
- технічні засоби з точки зору захищеності відносяться до різних категорій які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності;
- можливість здійснення передачі інформації через різні вузли, що реалізують різну політику безпеки.

Згідно вимогам з реалізації інформаційної безпеки - в кожній автоматизованій системі реалізовується необхідний стан захищеності інформаційних ресурсів, що надає змогу визначити критерії, згідно яких проектується КСЗІ для АС [2].

Виконуючи подальшу роботу розглядається процес проектування комплексної системи захисту інформації АС класу «1» 4-ї категорії.

Автоматизована система класу «1» 4-ї категорії має особливості, які притаманні звичайній АС класу «1», а саме:

- з комплексом може працювати один користувач, з повноваженнями на доступ та редагування конфіденційної інформації;
- технічні засоби (носії інформації) з точки зору захищеності відносяться до однієї категорії та використовуються для збереження інформації.

В той же час АС класу «1» 4-ї категорії висуває додаткові вимоги, серед яких:

- можливість використання системи декількома користувачами з різними повноваженнями щодо доступу до конфіденційної інформації, що оброблюється (адміністратор має всі привілеї на доступ до будь-якої інформації, що знаходиться в АС, інші користувачі можуть зчитувати інформацію тільки в рамках визначених

адміністратором прав на доступ до певних директорій, де знаходяться дані);

- установка різних привілеїв щодо редагування конфіденційної інформації, що оброблюється (адміністратор має всі привілеї на редагування будь-якої інформації, що знаходиться в АС, інші користувачі можуть редагувати інформацію тільки в рамках визначених адміністратором прав на доступ до певних директорій, де знаходяться дані);
- за допомогою контролю за зовнішніми пристроями використання обраних носіїв інформації для збереження конфіденційних даних (всі інші носії, за винятком попередньо обраних, блокуються та доступ до них стає неможливим).

Після аналізу предметної області, у якій розглядається визначення автоматизованих систем та їх класифікація, наступним кроком є вирішення поставленої задачі, відповідно до теми кваліфікаційної роботи бакалавра. Основним вирішенням поставленої задачі є процес ручного проектування комплексної системи захисту інформації автоматизованої системи класу «1» 4-ї категорії.

1.2 Проектування КСЗІ АС класу «1» 4-ї категорії

В основі проектування КСЗІ АС є ручне налаштування всіх необхідних параметрів, після чого спроектована система працює, відповідно до вимог зазначеними в документації. До параметрів, котрим необхідне редагування входить:

- параметри конфіденційності;
- облікові записи;
- шаблон локальної політики безпеки;
- файлова система;
- реєстру ОС.

Кожний з наведених вище параметрів редагується за допомогою інструментарію операційної системи, що дає змогу провести налаштування без задіяння пропрієтарного програмного забезпечення. Але коли процес доходить до налаштування контролю роботи зовнішніх пристроїв, то редагування параметрів системи стає недостатньо [3].

Створення правил доступу до зовнішніх пристроїв (до яких входять зовнішні накопичувачі даних, USB-девайси, принтери та ін.), що регламентується принципом роботи АС класу «1» 4-ї категорії можливе тільки за допомогою спеціалізованого програмного забезпечення, у якому можливе включення оснастки, де відповідно конфігурується сценарії роботи з накопичувачами даних (до цих сценаріїв входить блокування роботи накопичувачів, дозвіл роботи всіх підключених зовнішніх пристроїв, або робота певного пристрою з подальшим блокуванням інших).

В даному випадку використовується антивірусне програмне забезпечення - ESET Endpoint Security.

1.2.1 Використання інструментарію ОС

Операційна система Windows 10 має вбудований в систему інструментарій для налаштування:

- параметрів конфіденційності;
- роботи облікових записів;
- параметрів безпеки ОС;
- параметрів файлової системи;
- конфігурації реєстру ОС [3].

Редагування параметрів конфіденційності

Основним вирішенням даної проблеми є налаштування кожного параметру, який відповідає за можливе розповсюдження будь-якої інформації та відключення служб/утиліт які дають можливість дистанційно використовувати систему та змінювати важливі для роботи системи параметри [3, 4].

Основні функції для налаштування конфіденційності приведені в ***«Параметрах системи» → «Конфіденційність»*** (Рис. 1.1).

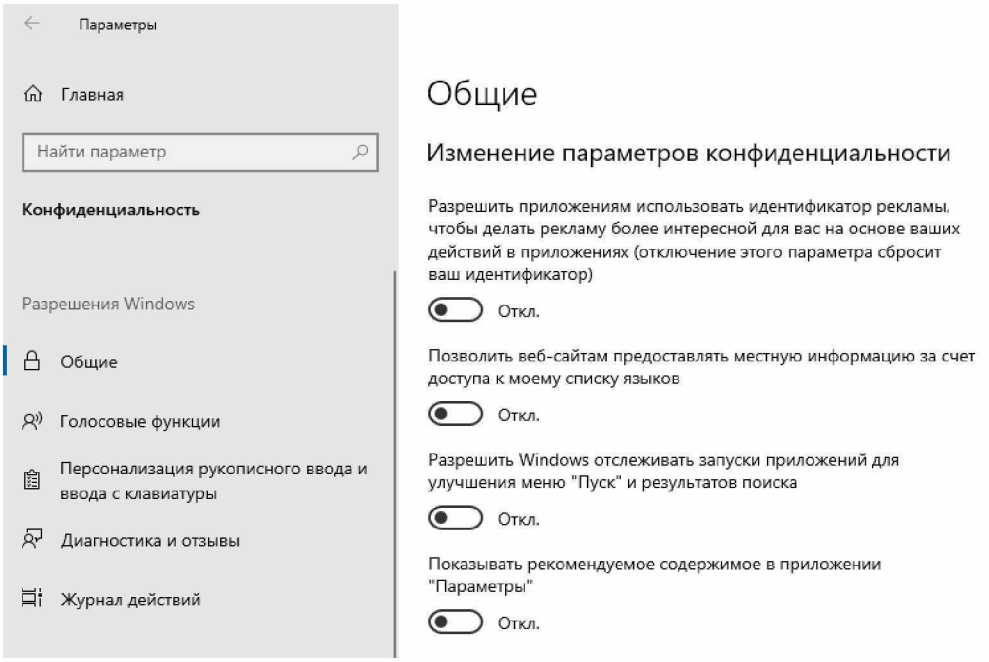

Рисунок 1.1 – Редагування параметрів, відповідальних за конфіденційність

Далі потрібно заборонити використання дозволу на збір інформації та відстежування місцезнаходження, роботи фонових програм та використання програм, які здатні використовувати дані інших програм (Рис.1.2) [4].

Рисунок 1.2 – Редагування параметрів, відповідальних за конфіденційність

Ці функції наведені в ***«Параметрах системи»*** → ***«Конфіденційність»*** → ***«Місцезнаходження»*** → ***«Фонові додатки»*** → ***«Діагностика додатків»*** (Рис. 1.3).

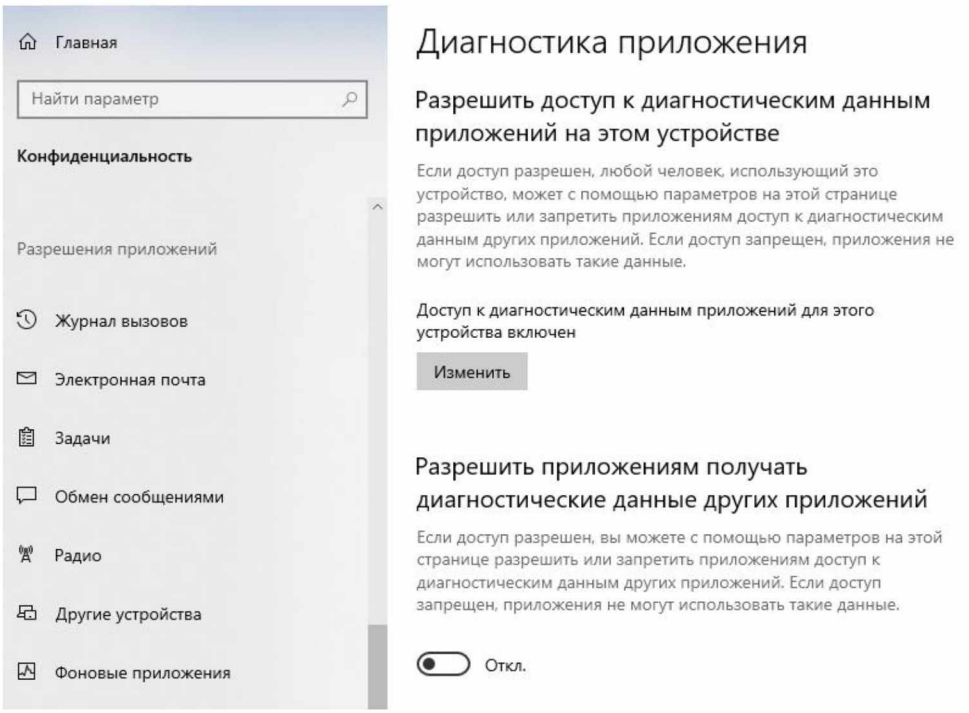

Рисунок 1.3 – Редагування параметрів, відповідальних за конфіденційність

Створення нового облікового запису

Створення облікового запису надає можливість займатись адмініструванням системи та розподілити рівень допуску до файлової системи

між декількома користувачами. Завдяки цьому можливо надати допуск до певної папки/диску/файлу певному користувачеві та адміністратору (всі інші мають вводити пароль для можливості відкрити та переглянути вміст певної папки або робити редагування файлів) [5].

Створення нового користувача відбувається в «***Керування комп'ютером»*** → ***«Локальні користувачі та групи»*** → ***«Користувачі»*** → ***«Новий користувач»*** (Рис. 1.4) та потрібно ввести ім'я користувача та пароль (за необхідністю також ввести повне ім'я, опис та вимагати зміну паролю з першим входом нового користувача)

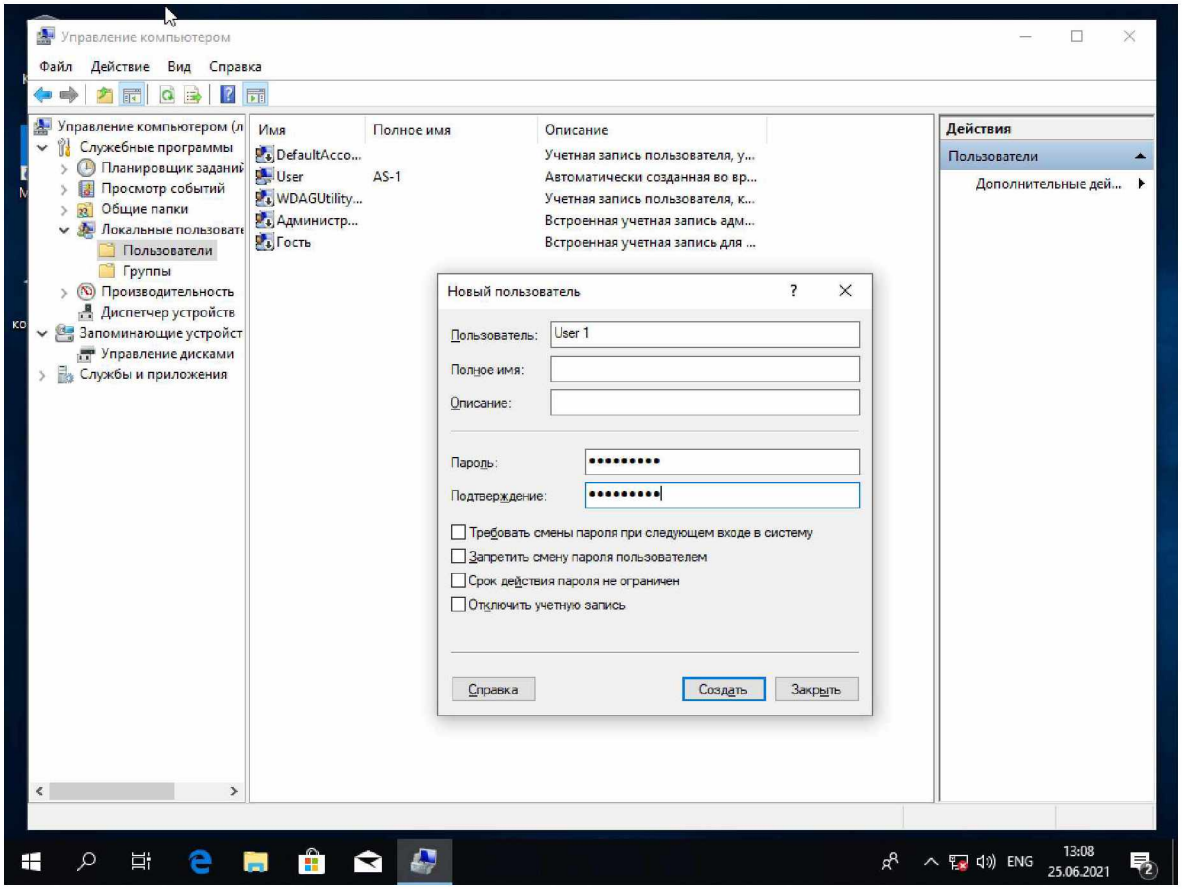

Рисунок 1.4 – Процес створення облікового запису

Після створення нового користувача потрібно задати відповідні привілеї доступу шляхом:

- виключення із списку доступу всіх облікових записів та груп користувачів,

- додавання в список користувача, який матиме змогу використовувати дану папку на свій розсуд.

Надання привілеїв відбувається в ***«Властивості»*** → ***«Безпека»*** , далі ми видаляємо всі групи/користувачів та залишаємо ***«Адміністратор»*** та певного користувача, який буде використовувати цю папку, в нашому випадку – **«User 1»** та виставляємо параметр ***«Повний доступ»*** (Рис. 1.5) [5].

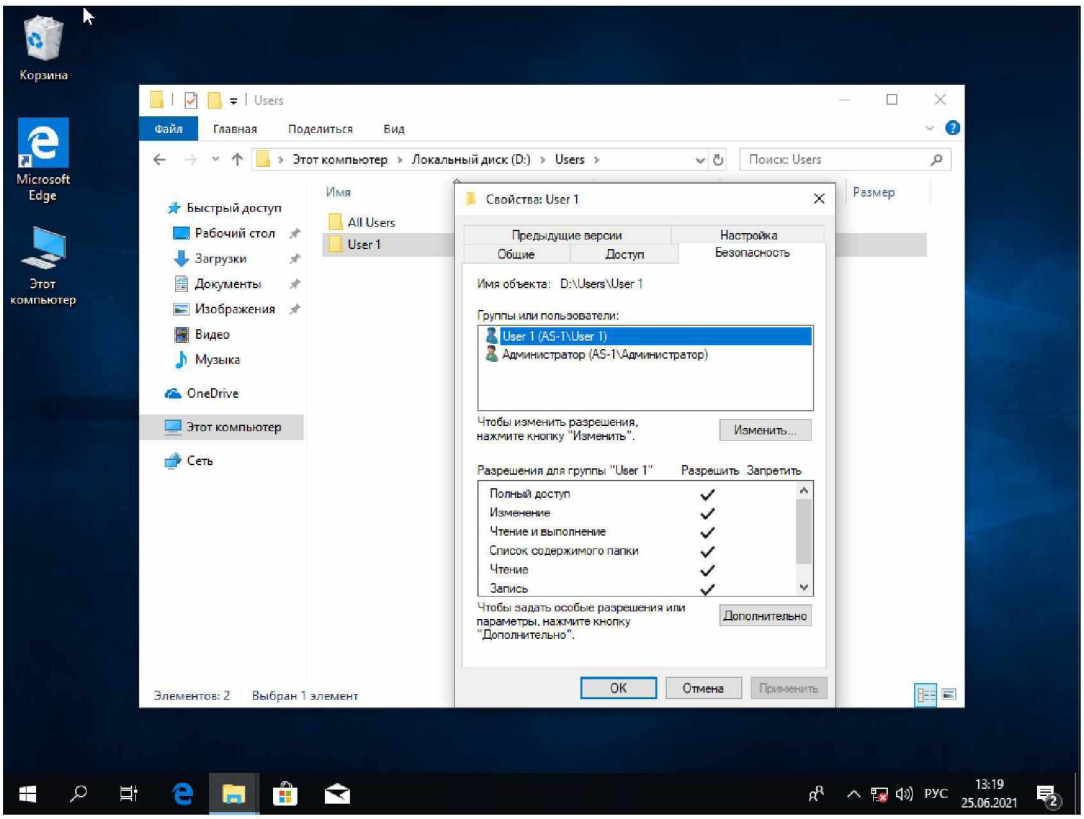

Рисунок 1.5 – Надання привілеїв доступу

Після виконання наведених вище дій процес створення нового облікового запису та надання привілеїв доступу вважається закінченим [5,6].

Створення та налаштування шаблону безпеки

Після створення та налаштування привілеїв доступу нових облікових записів, наступним кроком настає створення шаблону безпеки.

Шаблон безпеки - це текстовий файл з розширенням ***.inf***, який містить набір параметрів конфігурації безпеки. За допомогою шаблону безпеки

надається можливість централізовано керувати параметрами безпеки на робочих станціях або серверах. Шаблон використовується для застосування до окремих комп'ютерів заданих наборів параметрів групової політики, пов'язаних з безпекою, також за допомогою шаблонів безпеки надається можливість провести аналіз відповідності поточних налаштувань комп'ютера, що містяться в створених шаблонах безпеки [10].

Параметри шаблону безпеки зачіпають, в основному, такі політики:

- політики облікових записів «Безпека паролів», блокування облікових записів;
- локальні політики Аудиту , призначення прав користувачів і інші параметрів безпеки;
- політики журналу подій «Безпека журналу подій»;
- політики груп з обмеженим доступом «Адміністрування членства в локальних групах»;
- політики системних служб «Безпека» і режим запуску локальних служб.

Кожний з наведених вище параметрів надає змогу тонко налаштувати систему, завдяки чому можливо підібрати конфігурацію, яка унеможливить створення пролому в безпеці.

Створення шаблону можливе з використанням ***Microsoft Management Console, MMC*** (***Консоль Управління Microsoft)***. ***MMC*** - компонент операційної системи, завдяки якому надаються більш широкі можливості для управління системою. Основний принцип дії полягає в ***оснастках*** - певних програмах, що дозволяють налаштувати різні параметри роботи операційної системи та виконувати процеси адміністрування [5, 6].

Для редагування локальної політики безпеки, шляхом налаштування шаблону безпеки, необхідно в командному рядку ввести «mmc» для запуску консолі редагування, після чого відкривається консоль редагування, де

потрібно перейти в ***«Файл» → «Додавання та видалення оснастки»***, після чого знайти та обрати ***«Шаблони безпеки»*** (Рис. 1.6).

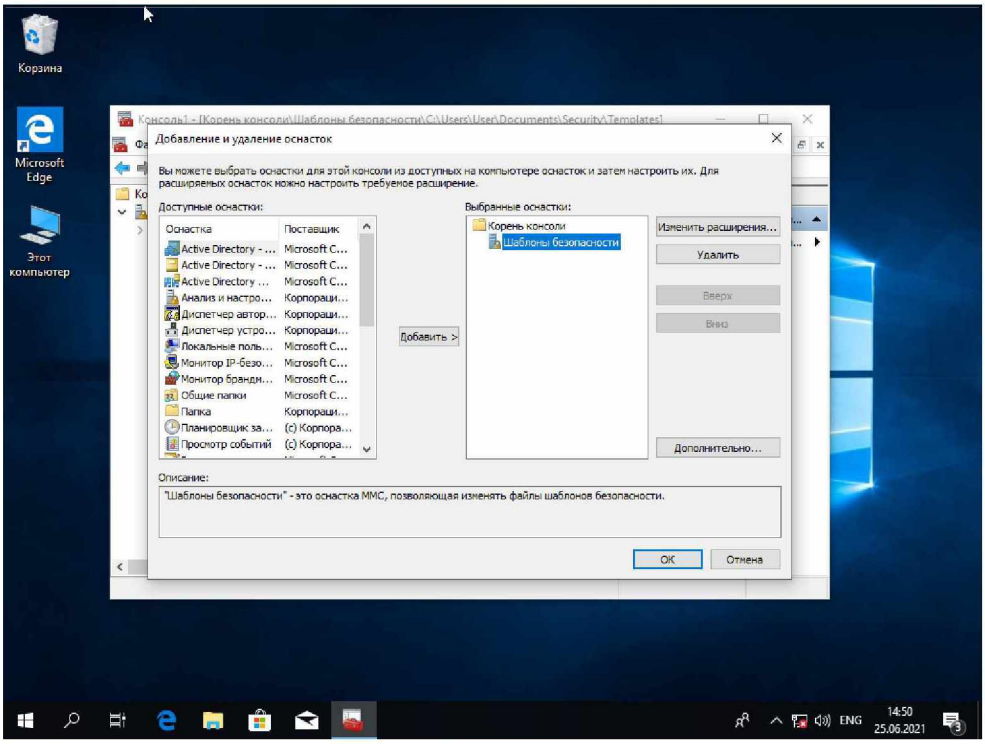

Рисунок 1.6 – Додавання оснастки «Шаблони безпеки»

Далі потрібно перейти до відповідного розділу та створити шаблон безпеки (Рис. 1.7).

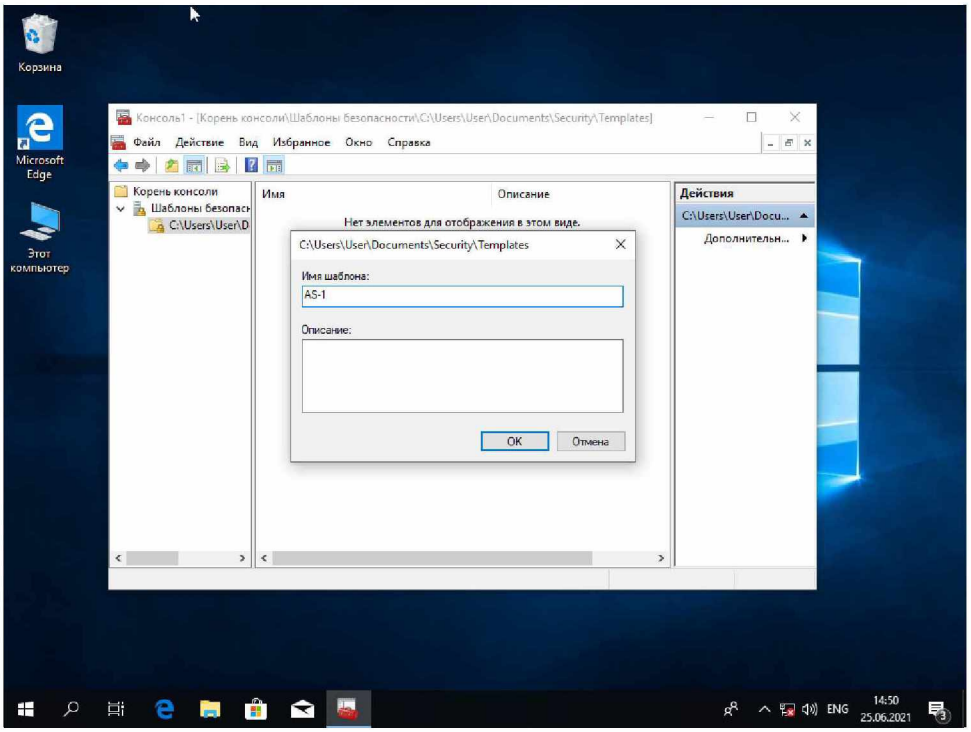

Рисунок 1.7 – Створення шаблону

Після цього відкривається доступ до налаштування параметрів локальної політики (Рис. 1.8).

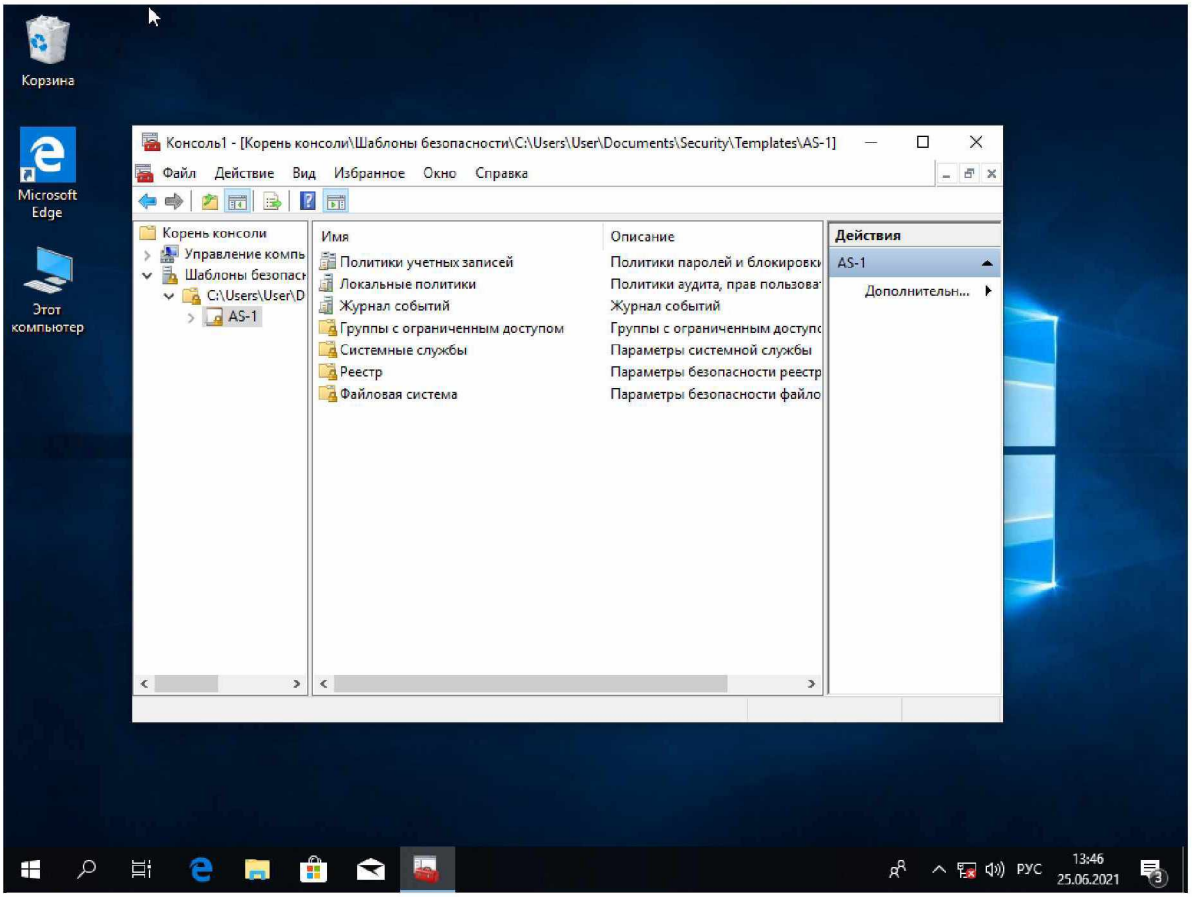

Рисунок 1.8 – Параметри локальної політики

Першим пунктом відбувається налаштування політики облікових записів, яка містить параметри безпеки для паролів і блокування облікових записів.

Налаштування політики паролів

Політика паролів необхідна для призначення рівня складності паролів та їх тривалості. Дане налаштування унеможливлює зловмиснику здійснити атаку на систему завдяки нестійкому паролю.

Відповідні параметри налаштовуються за допомогою редактора політики виключно через консоль керування Майкрософт («***MMC***») за посиланням: ***«Шаблони безпеки → «Диск» → «Шлях до шаблону» → «Ім'я шаблону» → «Політика паролів»*** (Рис. 1.9).

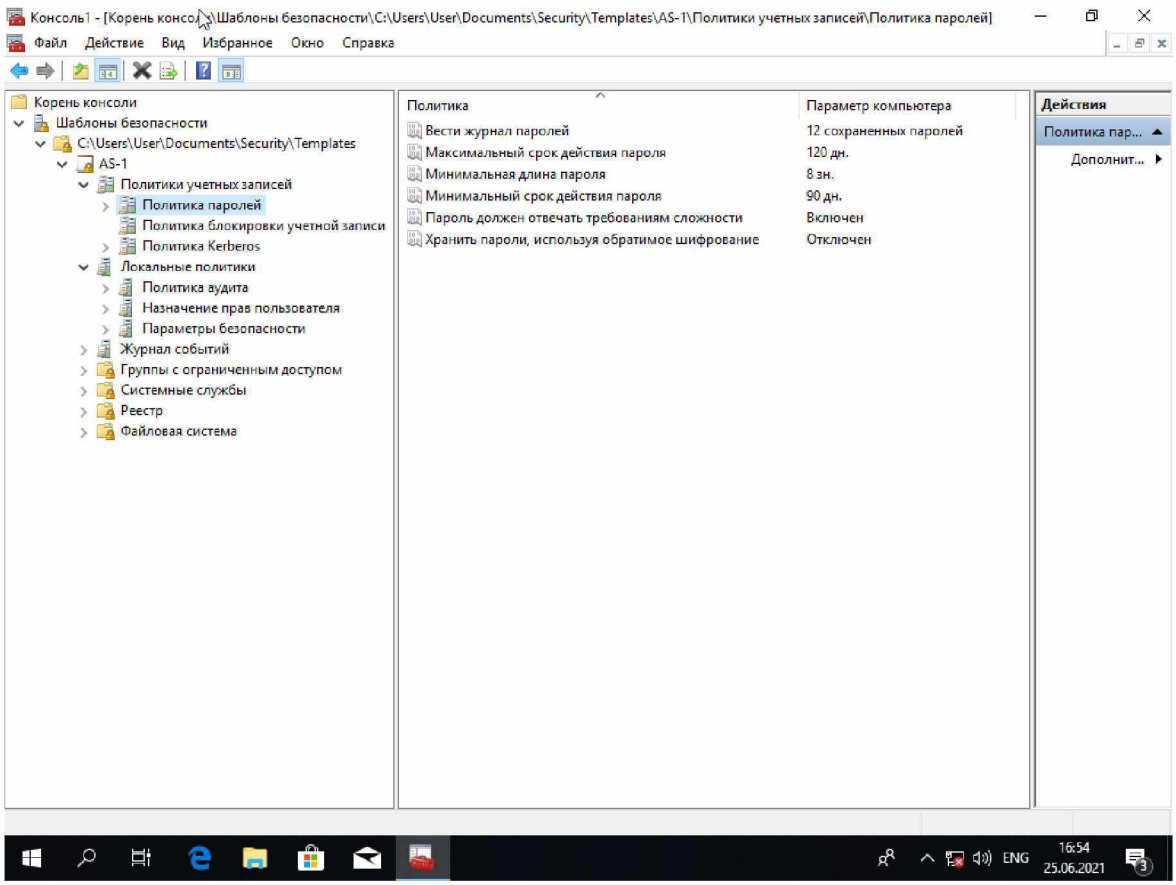

Рисунок 1.9 – Встановлення політики паролів

В додатку А наведені рекомендовані параметри політики паролів.

Налаштування політики блокування облікових записів

Політика блокування облікового запису використовується для налаштування параметрів, які впливають на можливість подальшої роботи облікового запису. За допомогою даних параметрів встановлюється кількість спроб та інтервал часу, на який блокується користувач.

Відповідні параметри налаштовуються за допомогою редактора політики виключно через консоль керування Майкрософт («***ММС***») за посиланням: ***«Шаблони безпеки → «Диск» → «Шлях до шаблону» → «Ім'я шаблону» → «Політика блокування облікових записів»*** (Рис. 1.10) [6,7].

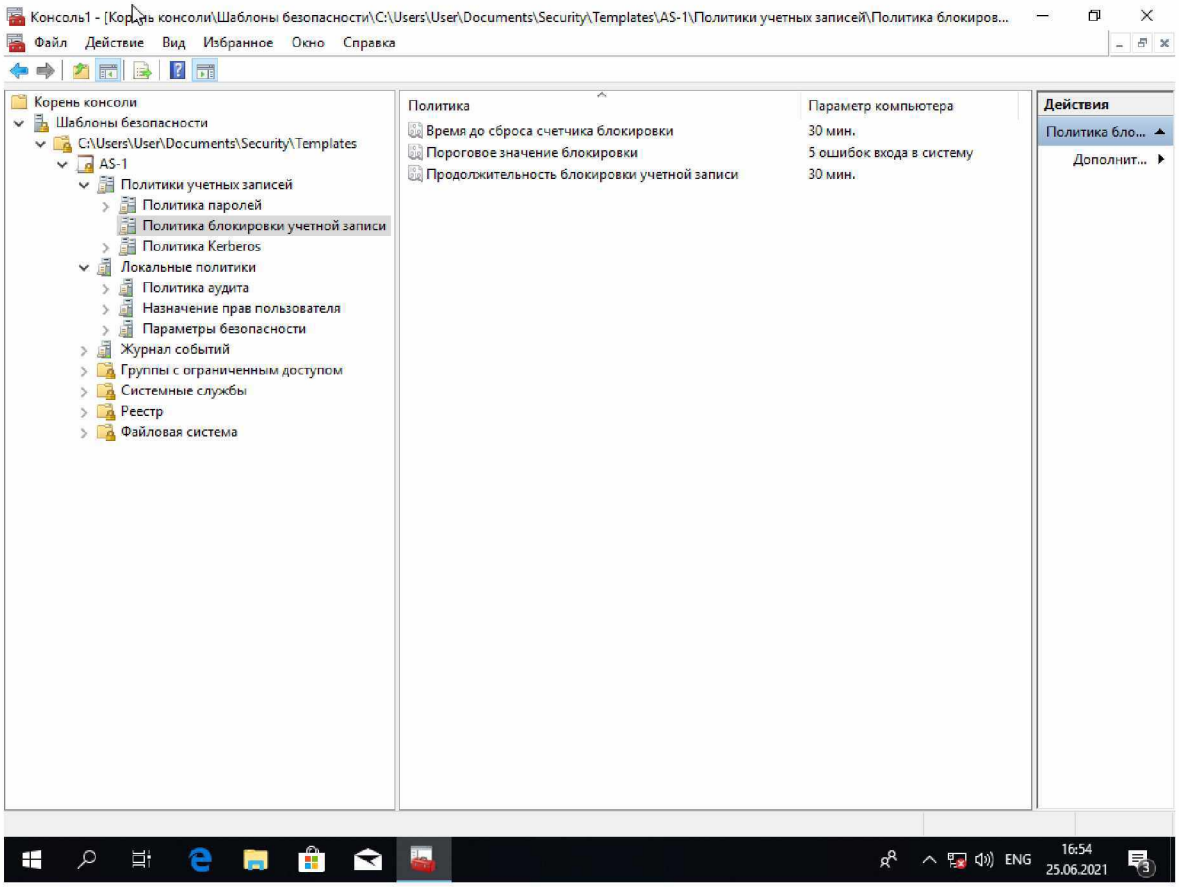

Рисунок 1.10 – Налаштування політики блокування облікових записів

В додатку Б наведені рекомендовані параметри політики блокування облікових записів.

Призначення прав користувачів

Призначення прав користувачів дає можливість конфігурувати привілеї на виконання певних дій користувачам та групам.

Необхідні параметри налаштовуються за допомогою редактора політики прав користувачів за посиланням: ***«Шаблони безпеки → «Диск» → «Шлях до шаблону» → «Ім'я шаблону» → «Призначення прав користувача»*** (Рис. 1.11).

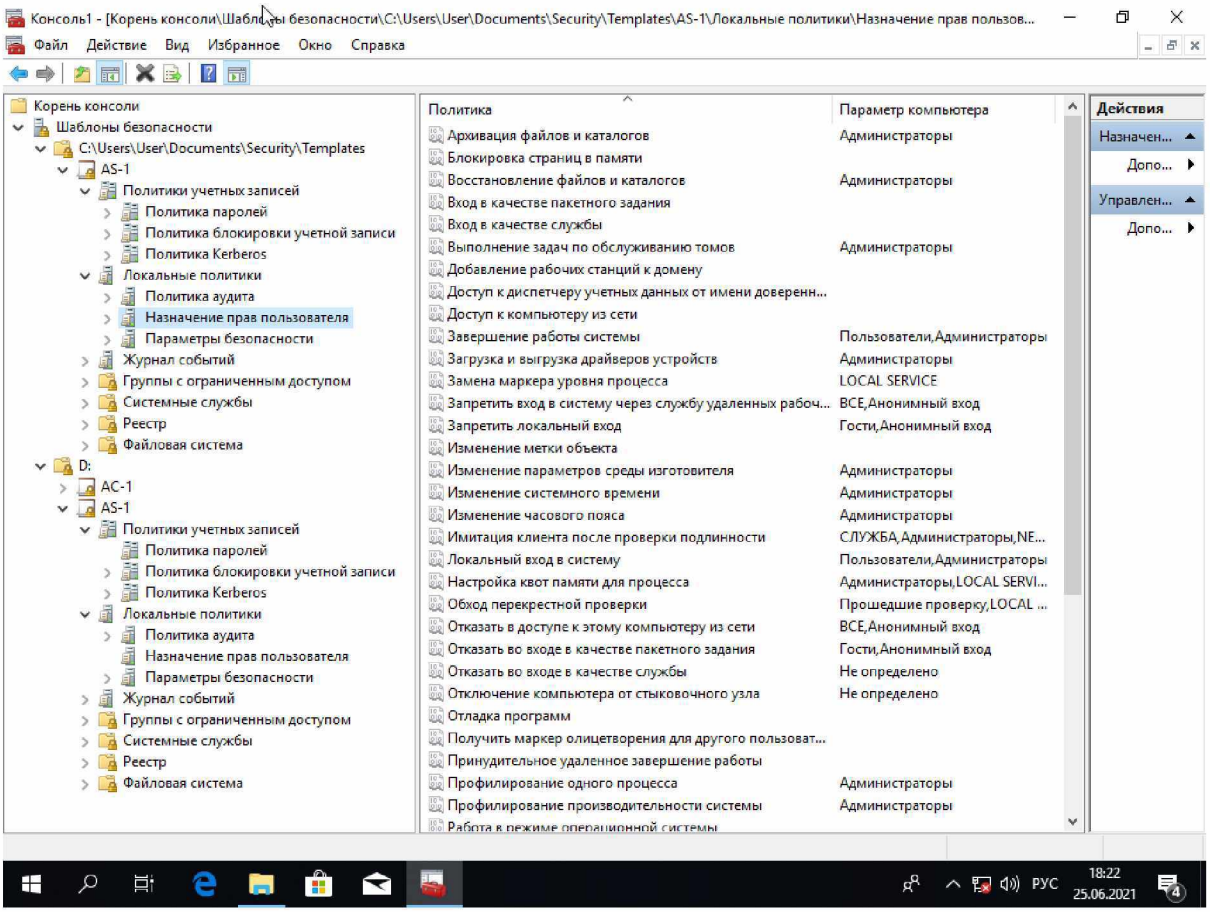

Рисунок 1.11 – Призначення прав користувачів

В додатку В наведені рекомендовані параметри реєстру прав користувачів.

Налаштування параметрів безпеки

Пункт ***«Параметри безпеки»*** дозволяє редагувати роботу специфічних функцій системи наприклад, установку драйверів, дозвіл до пристроям читання та іншим компонентам системи.

Необхідні параметри налаштовуються за допомогою редактора політики безпеки за посиланням: ***«Шаблони безпеки → «Диск» → «Шлях до шаблону» → «Ім'я шаблону» → «Параметри безпеки»*** (Рис. 1.12).

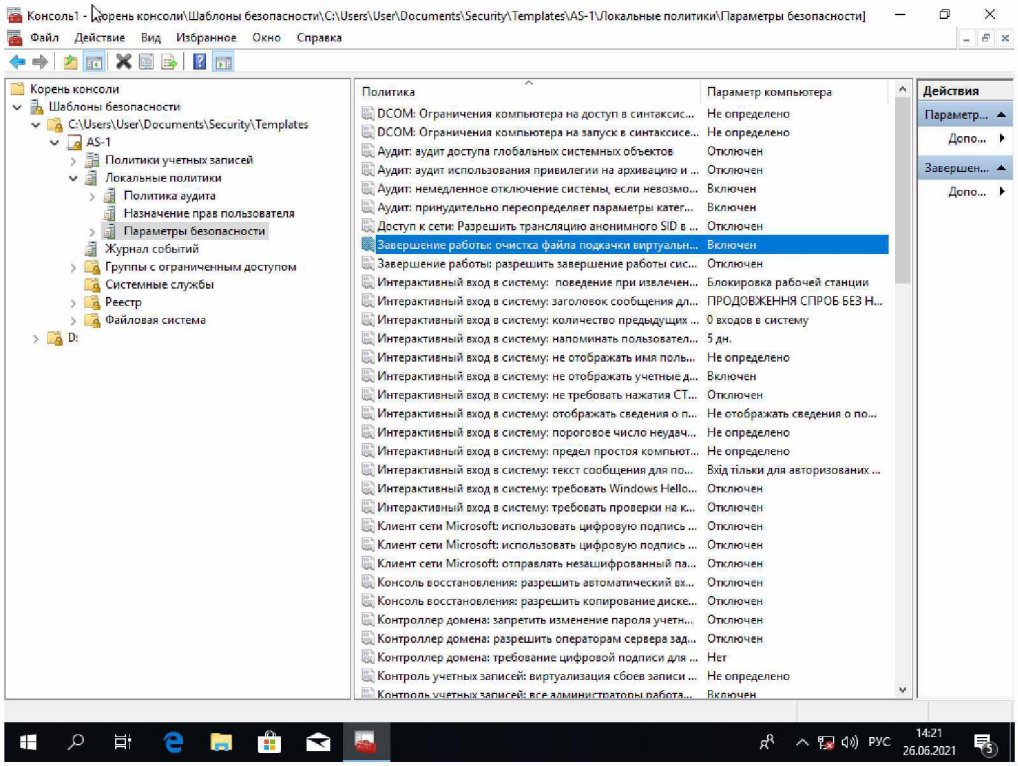

Рисунок 1.12 – Призначення параметрів безпеки

В додатку Г наведені рекомендовані параметри безпеки ОС.

Налаштування параметрів системних служб

Важливим етапом налаштування системи є конфігурація системних служб, які починають функціонувати відразу при запуску системи. Важливу роль для безпеки, оптимізації продуктивності і завантаження ОС Windows відіграє налаштування системних служб [7].

Вимикання непотрібних та потенційно небезпечних служб надає можливість присікти можливі атаки зловмисників, але потрібно пам'ятати, що деякі служби тісно залежать від роботи інших, тому для вимикання однієї служби потрібно вимикати 2 або 3 інших (деякі служби можуть бути відсутні в залежності від редакції операційної системи)

Параметри системних служб налаштовуються за посиланням: «***Шаблони***

безпеки → «Диск» → «Шлях до шаблону» → «Ім'я шаблону» → «Системні служби» (Рис. 1.13).

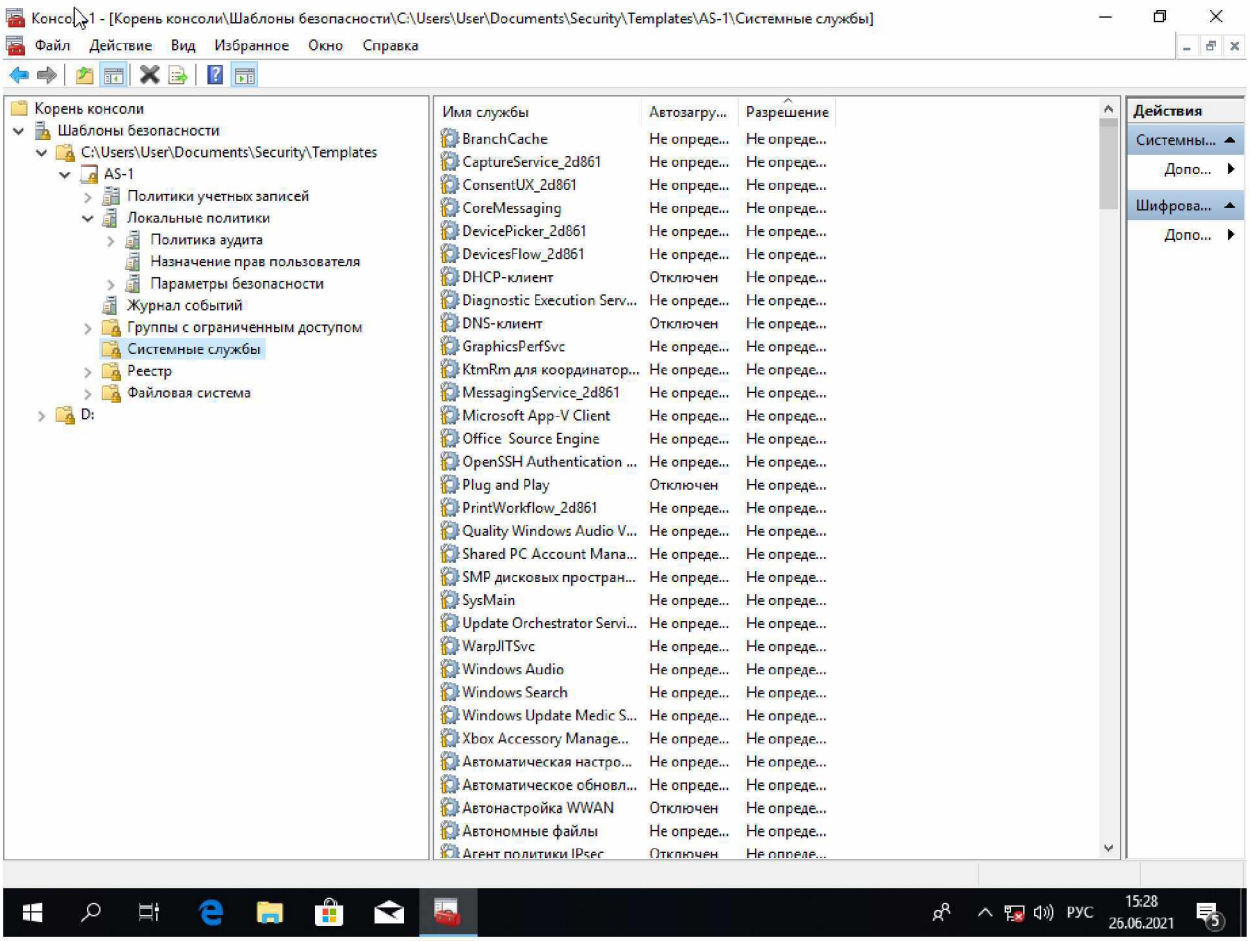

Рисунок 1.13 – Налаштування параметрів системних служб

В додатку Г наведені рекомендовані параметри системних служб ОС. Всі інші параметри встановлюються індивідуально в залежності від прийнятої політики безпеки в системі.

Налаштування параметрів файлової системи

Редагування параметрів файлової системи задає привілеї доступу до файлової системи, що надає змогу тонко налаштувати рівень доступу до певних директорій [7].

Необхідні параметри налаштовуються за посиланням: «***Шаблони безпеки → «Диск» → «Шлях до шаблону» → «Ім'я шаблону» → «Файлова система»***

(Рис. 1.14).

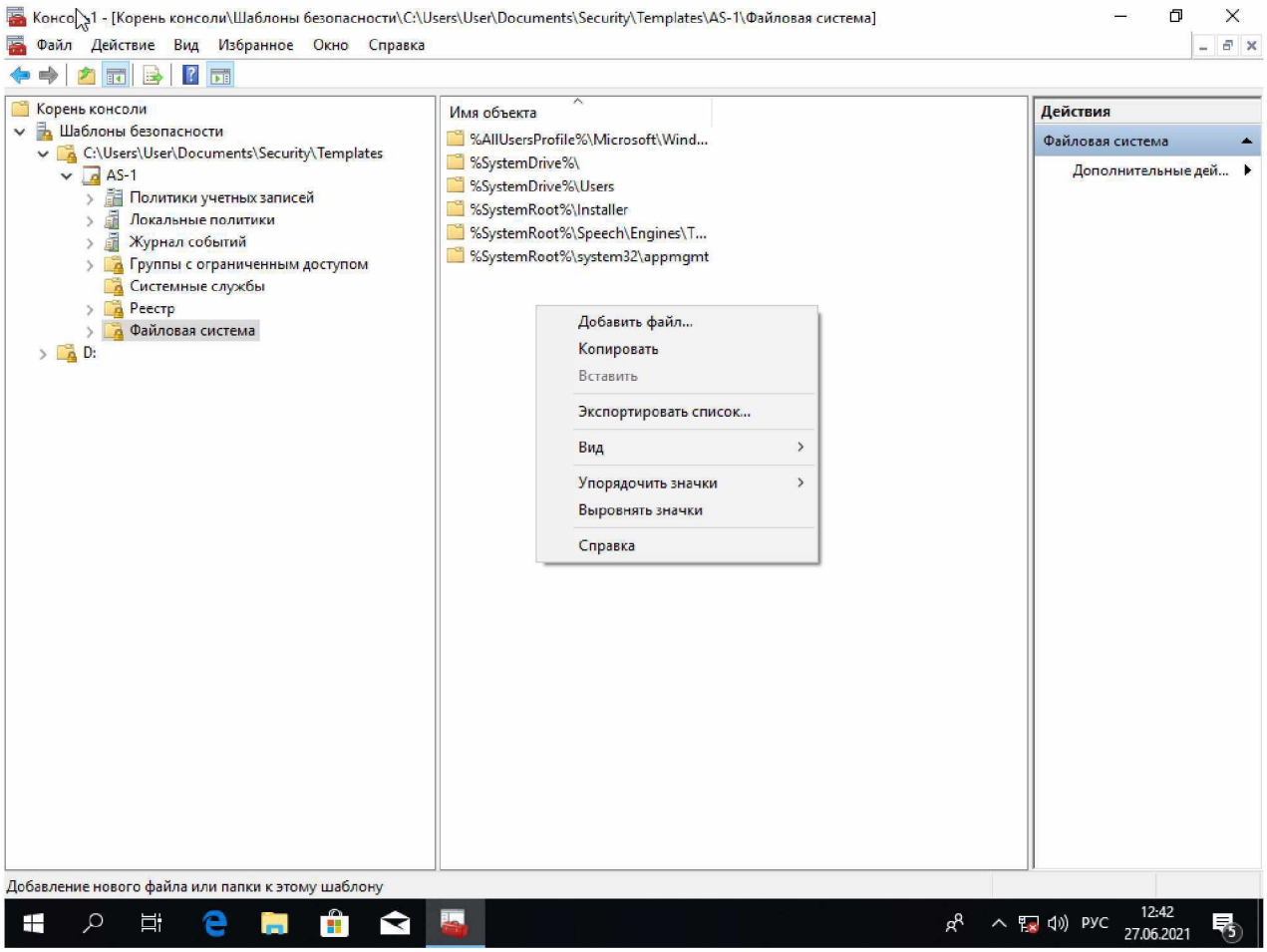

Рисунок 1.14 – Налаштування параметрів файлової системи

В додатку Д наведені основні рекомендовані значення параметрів файлової системи.

Налаштування параметрів реєстру

Наступним етапом після налаштування параметрів файлової системи є налаштування параметрів реєстру, але Microsoft Management Console (MMC) не дає можливості редагувати значення реєстру (параметри реєстру не відображаються представлені в дуже скороченому вигляді), тому в даному випадку використовується консольна команда ***«Regedit»***, яка вмикає вбудований в операційну систему Windows редактор реєстру [7].

Завдяки редактору реєстру можливо редагувати роботу компонентів (Рис. 1.15).

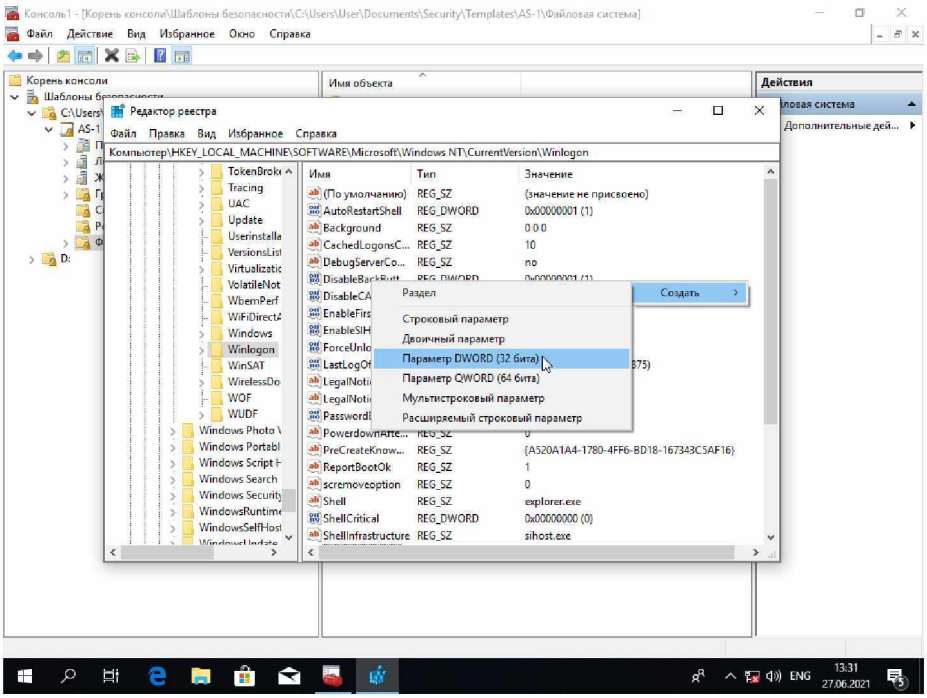

Рисунок 1.15 – Створення параметру реєстру

Ці компоненти відповідають за роботу системних утиліт, сервісів, автоматизованих задач, та дозволів (Рис. 1.16).

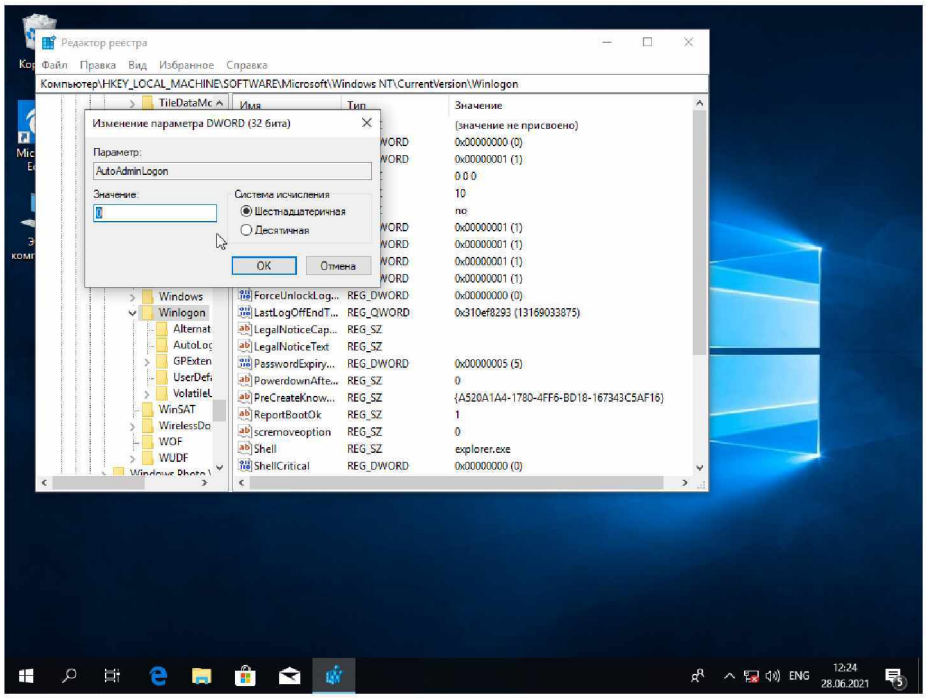

Рисунок 1.16 – Присвоєння значення параметра реєстру

В додатку Е наведені основні рекомендовані значення параметрів реєстру.

1.2.2 Використання пропрієтарного ПЗ

Наступним кроком після редагування параметрів системи є налаштування контролю зовнішніх пристроїв. Через неможливість за допомогою стандартних компонентів операційної системи Windows 10 ініціювати контроль роботи зовнішніх накопичувачів даних - необхідні спеціалізовані програмні забезпечення, у яких можливе включення оснастки, за допомогою яких конфігурується сценарії роботи з накопичувачами даних (до цих сценаріїв входить блокування роботи накопичувачів, дозвіл роботи всіх підключених зовнішніх пристроїв, або робота певного пристрою з подальшим блокуванням інших).

Налаштування контролю пристроїв відбувається за допомогою зазначеного вище антивірусного програмного забезпечення – ESET Endpoint Security (Рис. 1.17) [8].

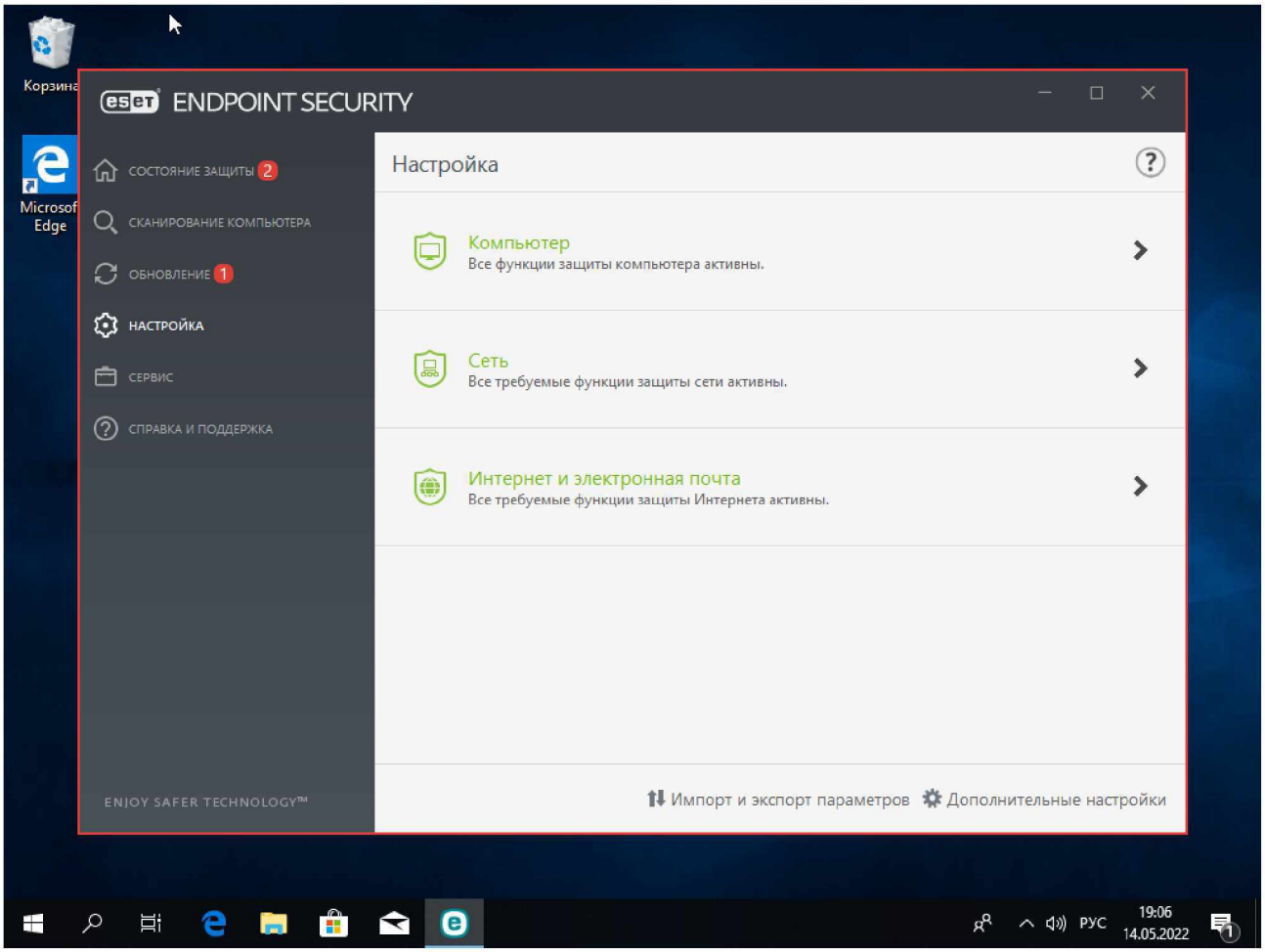

Рисунок 1.17 – Інтерфейс антивірусу ESET Endpoint Security

Для переходу до налаштувань контролю зовнішніх пристроїв потрібно пройти за посиланням: «***Налаштування*** → ***«Додаткові налаштування»*** → ***«Контроль пристроїв»*** (Рис. 1.17). Далі потрібно увімкнути дану оснастку та пройти за наступним посиланням: ***«Правила»*** → ***«Змінити»*** (Рис. 1.18).

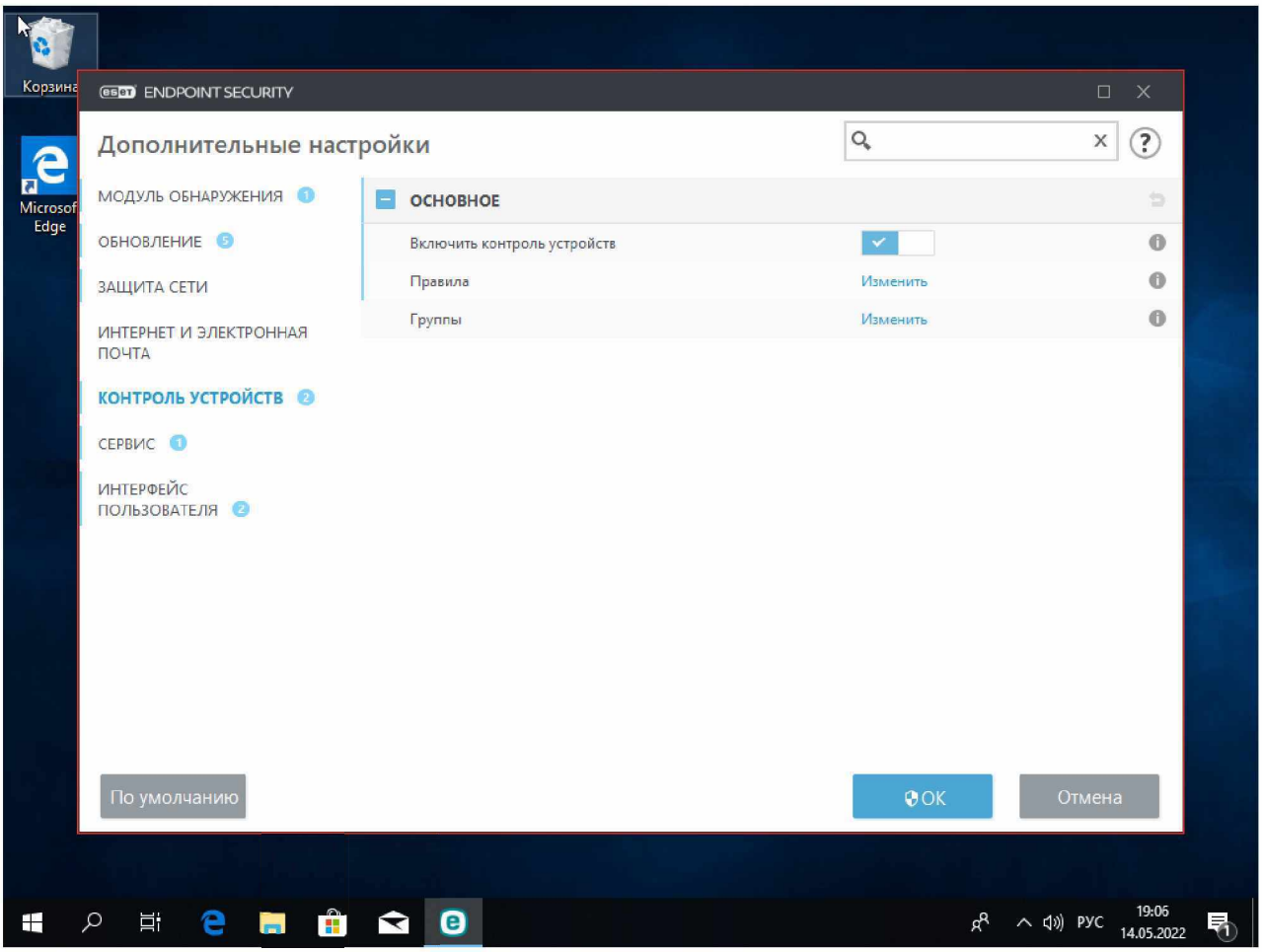

Рисунок 1.18 – Список додаткових параметрів програмного забезпечення

Увімкнення даної оснастки відкриває доступ до подальшого налаштування правил використання зовнішніми пристроями та створенню відповідних сценаріїв роботи з ними (Рис.1.19).

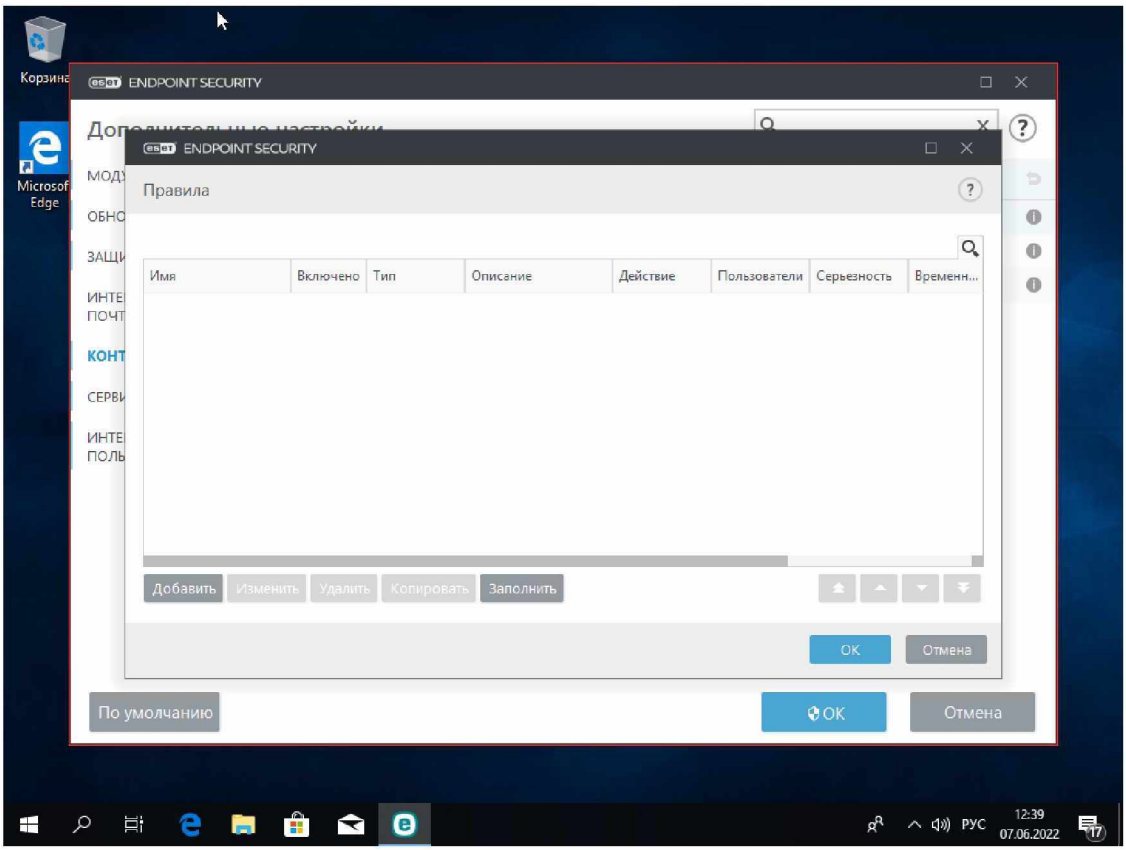

Рисунок 1.19 – Інтерфейс оснастки «Контроль пристроїв»

Після переходів за поданими вище посиланнями ми попадаємо до меню, у якому конфігуруються сценарії роботи з зовнішними пристроями за певними параметрами (Рис.1.20).

Серед параметрів можна виділити:

- ім’я сценарію;
- статус сценарію (включений або виключений);
- сценарій застосування;
- тип пристрою (дисковий накопичувач, CD/DVD, USB-прінтер, модем, портативний пристрій та інші);
- дія (дозвол на роботу, заборона, попередження);
- виробник;
- модель;
- серійний номер;
- список користувачів (яким буде відображатись результат події);

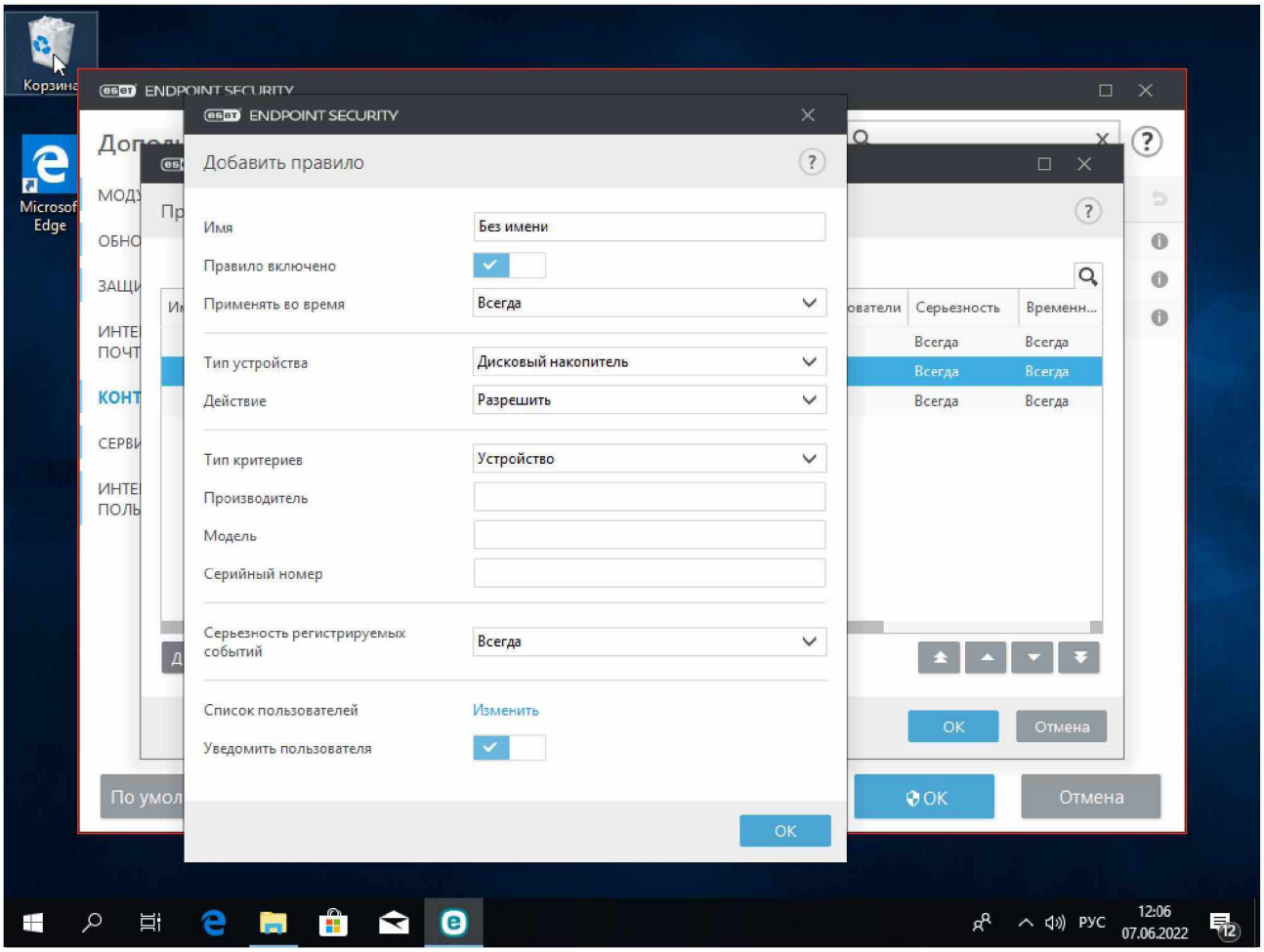

Рисунок 1.20 – Параметри налаштування сценарію роботи

Налаштування сценарію роботи пристрою можливе двома методами:

- ручне введення всієї інформації стосовно пристрою (його тип, виробник, модель, сирійний номер);
- автоматичний пошук всіх підключених приладів та вибір певного з запропанованих (дає змогу автоматично заповнити інформацію стосовно виробника, моделі та сирійного номеру) (Рис.1.21)

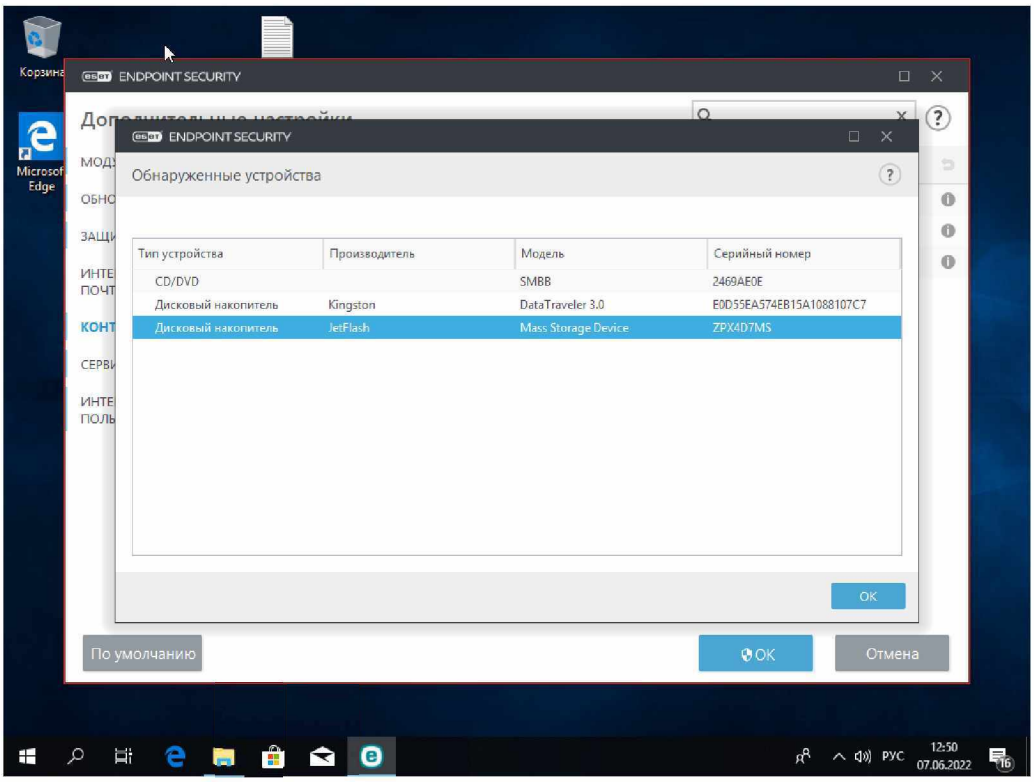

Рисунок 1.21 – Автоматичний пошук приладів

Обираючи один з двох запропонованих варіантів створення конфігурації створюється потрібний сценарій та активується, після чого він з'являється в меню загальному меню правил роботи зовнішніх пристроїв (Рис.1.22) [8].

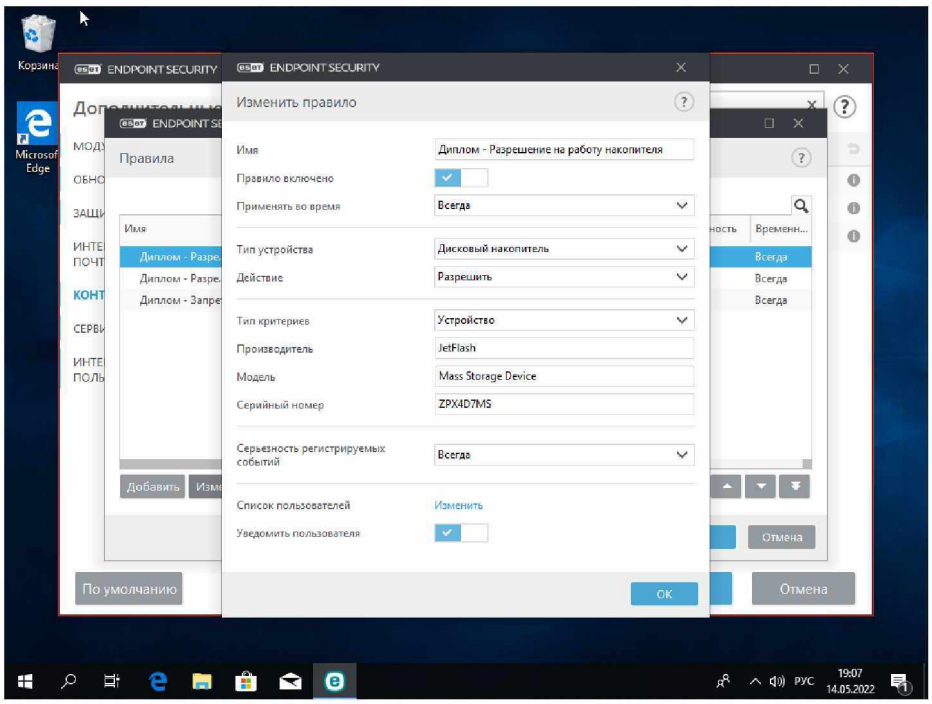

Рисунок 1.22 – Параметри налаштування сценарію роботи (заповнений)

У відповідності до принципу роботи АС класу «1» 4-ї категорії була створена наступна конфігурація, при якій відбувається моніторинг та відслідковування дій пов'язаних з зовнішними накопичувачами даних (USB-флеш носіїв) доступ допускається до двух попередньо обраних пристроїв, інші – при спробі підключення будуть розпізнаватись системою, але будуть попередньо заблоковані що унеможливює створенню вразливостей у безпеці за допомогою копіювання/підміни інформації (Рис.1.23).

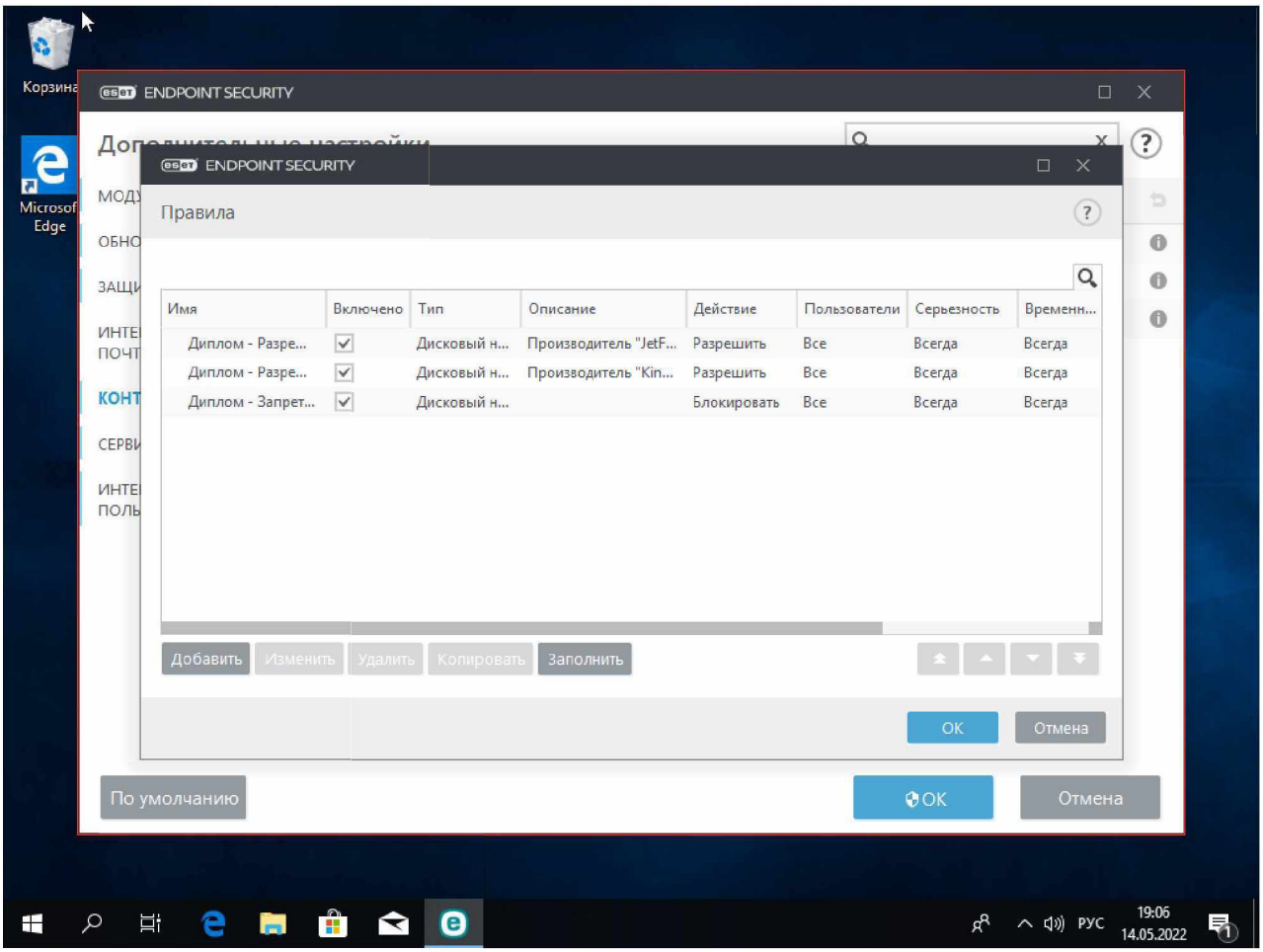

Рисунок 1.23 – Сценарій роботи оснастки

Результатом налаштування контролю зовнішніми пристроями є виконання потрібного сценарію – заборона на доступ до всіх USB-флеш носіїв, окрім двох, які мають права на доступ до них та можливість читання/редагування інформації, яка знаходиться на цих USB-флеш носіях.

1.3 Аналіз проектування

Результатом виконання налаштування системи є стабільна робота системи з повною відповідністю критеріїв автоматизованої системи класу 1 4-ї категорії.

Під час виконання даного процесу був виявлений наступний недолік - в разі якщо користувач буде проводити ручне налаштування системи згідно зазначених вище параметрів, то загальна тривалість налаштування займає від 5 до 6 годин, при умові що потрібно налаштувати тільки одну комп'ютерну систему. При збільшенні кількості КС потребуючих конфігурації передбачувано збільшується загальний час, що витрачається на налаштування.

Альтернативним шляхом є:

1. Написання скрипту, що здійснює:
   - додавання облікових записів у систему;
   - надання привілеїв доступу до певних папок у системі;
   - додавання відповідних параметрів/ключів реєстру та присвоєння цим параметрам певних значень.
2. Імпорт попередньо налаштованого шаблону безпеки, який включає в себе:
   - налаштування політики паролів;
   - налаштування політики облікових записів;
   - призначення прав користувачів;
   - налаштування параметрів безпеки;
   - налаштування параметрів системних служб;
   - налаштування параметрів файлової системи.
3. Імпорт попередньо налаштованої конфігурації роботи антивірусного програмного забезпечення ESET Endpoint Security, до якого входить оснастка «контроль пристроїв».

1.4 Методологія оцінки ризику інформаційних систем

Методологія – це набір стандартних правил, дій та процедур, які реалізуються для перевірки захищеності АС. Процедури передбачають процес тестування системи на предмет виявлення недоліків при первинному проектуванні. В цьому плані передбачаються не лише цілі проведення випробувань, а комплекс дій, які мають бути виконані для оцінки ризиків інформаційної безпеки АС.

Методології будуються на основі галузевих стандартів, які формулюють правила щодо оцінки захищеності АС [9-11].

Дані стандарти вимагають наступний принцип оцінки ІБ для АС:

- розгляд певного активу системи;
- ідентифікація вразливостей, відповідно розглядаємого активу системи;
- розгляд виявлених загроз, по відношенню до ідентифікованих вразливостей;
- виявлення впливу загроз на критерії конфіденційності, цілісності, доступності та спостережності;
- документації дій, які спрямовані на протидію виявленим недолікам АС.

Серед методологій, які відповідають наведеним вище вимогам, можна виділити:

- OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) ;
- Високорівнева оцінка ризиків.

1.4.1 Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) - виконує оцінку ризиків інформаційної безпеки в організації та забезпечує

можливість отримання необхідних результатів з аналізу можливих ризиків витратами часу та ресурсів.

Методологія розглядає людей, технології, інформаційні системи, додатки та інші об'єкти в контексті їх ставлення до інформації та бізнес-процесів та послуг, які вони підтримують. [12]

Процес оцінки ризиків ІБ за методологією OCTAVE складається з наступних етапів:

1. Підбір якісних параметрів, за допомогою яких виробляється опис можливих вразливостей та відповідних ризиків. Ці параметри можуть включати ймовірність реалізації ризику, збиток від нього та інші наслідки для організації.

2. Опис певного активу, що містить його унікальні особливості, якості, характеристики та цінність. Кожний актив фіксується, що дає змогу сформувати подальший процес ідентифікації загроз та ризиків системи.

3. Ідентифікації ризиків шляхом ретельного аналізу спроектованої системи працівниками комерційного підприємства. На даному етапі визначаються можливі вразливості по відношенню до певного активу та ризики, актуальні для аналізованих активів.

4. Визначення загроз за певними критеріями: людський фактор, використання технічних засобів, технічні та інші проблеми. По кожному типу загроз для кожного активу можуть бути визначені сценарії реалізації загроз, що включає опис їхнього впливу на ймовірність реалізації.

5. Використання інформації про найбільш ймовірні сценарії загроз, на даному етапі проводиться аналіз їх впливу на роботу спроектованої системи.

6. Використовуючи інформацію, отриману на попередніх етапах, проводиться оцінка впливу загроз на роботу системи та ранжування виявлених ризиків відповідно до критеріїв, визначених на етапі визначення критеріїв вимірювання ризиків.

7. Визначення ризику визначається та його обробка залежно від його впливу на роботу системи.

Переваги: детальне оцінювання всіх можливих вразливостей та ризиків спроектованої АС;

Недоліки: не даються чіткі інструкцій з організації моніторингу стану ризиків ІС [12].

1.4.2 Високорівнева оцінка ризиків

Високорівнева оцінка ризиків інформаційної безпеки - застосування високорівневої оцінки наслідків, а не систематичного аналізу загроз, вразливостей, активів і наслідків та синхронізація з додатковими планами, пов'язаними з менеджментом змін [13].

До особливостей високорівневого оцінювання ризиків ІБ можливо віднести:

- високорівнева оцінка ризику може мати справу з більш глобальним розглядом організації та її інформаційних систем. В результаті цього аналіз контексту більше зосереджується на бізнес і експлуатаційної середовищі, ніж на технологічних компонентах;
- використання високорівневої оцінки ризику дозволяє розглядати більш обмежений перелік загроз та вразливостей, розподілених по певних сфер, що дозволяє ретельно прорахувати методи позбавлення вразливостей по відношенню до певної системи;

Переваги оцінки ризику високого рівня наступні:

- включення початкового простого підходу, що дозволяє отримати подальше схвалення програми оцінки ризику;

- ресурси і засоби застосовуються там, де вони найбільш корисні, тому системи, які найбільше потребують захисту – мають перший пріоритет для розгляду.

Детальний процес оцінювання інформаційної безпеки включає в себе ретельну ідентифікацію та визначення цінності активів, оцінку загроз цим активам і оцінку вразливостей.

На ймовірність виникнення конкретної загрози впливає:

- привабливість активу;
- простота перетворення, що використовує уразливість активу в винагороду - застосовується при розгляді умисної загрози з боку персоналу;
- технічні можливості чинного фактору загрози - може бути застосовано при розгляді умисної загрози з боку персоналу;
- чутливість уразливості до використання - можна застосувати до технічним і нетехнічних вразливостей [13].

1.5 Постановка задачі

Метою дипломної роботи є спрощення процесу проектування комплексної системи захисту інформації автоматизованої системи класу "1" 4-ї категорії.

Після проведення аналізу предметної області і існуючих методик ручного проектування КСЗІ автоматизованих систем виявлено, що для досягнення поставленої мети необхідно виконати такі завдання:

- розробити алгоритм дій по спрощенню проектування КСЗІ автоматизованої системи класу "1" 4-ї категорії;
- реалізувати спрощення проектування КСЗІ автоматизованої системи класу "1" 4-ї категорії;
- перевірити працездатність розробленої системи;
- провести оцінку ризиків інформаційної безпеки АС класу "1" 4-ї категорії.

РОЗДІЛ 2. ВИБІР СЕРЕДОВИЩА ПРОГРАМНОЇ РЕАЛІЗАЦІЇ

2.1 Аналіз програмних продуктів

Інтегроване середовище сценаріїв – розширення стандартної оболонки командного рядка за допомогою якого створюються сценарії, завдяки яким реалізуються певні операції. Завдяки даним діям можливо отримувати доступ до різних сховищах даних, таких як файлова система або реєстр операційної системи.

Існує декілька інтегрованих середовищ сценаріїв, серед яких можна виділити:

1. **ConEmu** - безкоштовний емулятор консолі Windows з можливість роботи з даними та програмним забезпеченням в ОС. Робота з даним емулятором можлива за допомогою вкладок, які представляють собою кілька консолей і простих графічних програм як одне вікно графічного інтерфейсу [14].

Серед переваг даного інструментарію можна зазначити:

- можливість робити одразу в декількох середовищах, за допомогою роботи в режимі вкладок;
- велика кількість допоміжних розширень;
- можливість гнучкого налаштування.

Серед недоліків можна визначити:

- невеликий функціонал в базовому варіанті;
- неможливість налаштовувати компоненти ОС з початку роботи;
- до кінця не розроблена документація для роботи з даним ISE.

2. **PowerShell** - розширювана оболонка командного рядка і пов'язана з нею мова сценаріїв від Microsoft. Використовується для написання, запуску та тестування скриптових сценаріїв в ОС Windows [15].

До переваг даного інструментарію можна відзначити:

- інтеграція в ОС;

- можливість роботи за допомогою командлетів, що спрощує процес створення необхідних сценаріїв;
- можливість запуску на будь-якій АС, під керування ОС Windows;
- неможливість запуску сценаріїв без надання доступу на виконання.

До недоліків можна віднести:

- необхідність в додаванні модулів, для роботи специфічних функцій;
- необхідність в поглибленому дослідженні документації для використання даного ISE.

3. **Cygwin** – ще один емулятор командної строки для Microsoft Windows, за допомогою якого можлива інтеграція ПЗ, даних та інших системних ресурсів на базі ОС Windows [16].

Переваги даної середовища сценаріїв:

- використання оболонки подібної до UNIX-сімейства операційних систем;
- інтеграція в роботу файлової системи;
- широкий інструментарій для роботи з ОС;

Недоліки даного рішення:

- скромний інструментарій для написання сценаріїв;

Серед запропонованих середовищ найбільш підходящим відповідно до завдання по спрощенню процесу проектування КСЗІ АС класу «1» 4-ї категорії є ISE PowerShell.

2.2 Використання ISE PowerShell

Для програмної реалізації поставленої задачі, до якої входить спрощення процесу проектування КСЗІ автоматизованої системи класу «1» 4-ї категорії було обрано інтегроване середовище сценаріїв (ISE) PowerShell, як інструментарій для написання скрипту, що автоматично виконує потрібні операції з настройки системи, відповідно до документації.

Інтегроване середовище сценаріїв PowerShell є провідним інструментарієм для написання, запуску та тестування скриптових сценаріїв.

Ключова особливість даного середовища розробки – інтеграція в стандартні компоненти операційної системи Windows, що відбиває потребу в пошуку пропрієтарного програмного забезпечення для написання скриптових сценаріїв [17].

Скрипт PowerShell використовує контейнер файлів ***.ps1***, який запускається на будь-якій КС, за умови дозволу на виконання локальних сценаріїв або сценаріїв з спеціальним ідентифікаційним підписом, що є ще одним аргументом для використання даної середи розробки. Дана особливість унеможливлює несанкціоноване використання будь-якого скрипту, який здатен змінити налаштування КС. Виконання сценарію здійснюється моментально, за умови якщо потрібно бачити процес виконання та вивід результату потрібне відкриття даного програмного забезпечення [18].

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПРОЦЕСУ СПРОЩЕНОГО ПРОЕКТУВАННЯ

Продумуючи варіант вирішення даної проблеми було знайдено 3 шляхи подолання даного недоліку, а саме:

1) використання скрипту створеного за допомогою інтегрованого середовища розробки – ISE PowerShell;

2) імпорт попередньо налаштованої локальної політики безпеки;

3) створення конфігурації до антивірусного програмного забезпечення ESET Endpoint Security.

3.1 Використання скриптового сценарію

За допомогою використання скрипту реалізовується спрощення процесу проектування КСЗІ АС класу «1» 4-ї категорії, згідно поставленої задачі.

Даний скрипт має такий алгоритм роботи:

- додавання декількох облікових записів в ОС;
- присвоєння паролю створеним обліковим записам;
- створення особистої папки для кожного з користувачів;
- за допомоги ACL команди зміну NTFS привілеїв доступу до певних директорій в системі [19];
- позбавлення прав на доступ та редагування щодо певної директорії для певного користувача;
- надання прав на повний доступ щодо певної директорії для певного користувача;
- створення ключа у реєстрі та присвоєння йому певного значення [20];

Першим кроком для застосування даного сценарію необхідно додати модуль: ***«NTFSSecurity»***, який дає змогу налаштовувати NTFS привілеї доступу до обраних директорій в системі.

Для додавання даного розширення потрібно скопіювати папку з даною конфігурацією та вставити її за наступним шляхом: «***C:\Windows***» → «***System32***» → «***WindowsPowerShell → v1.0 → «Modules***» (Рис. 3.1).

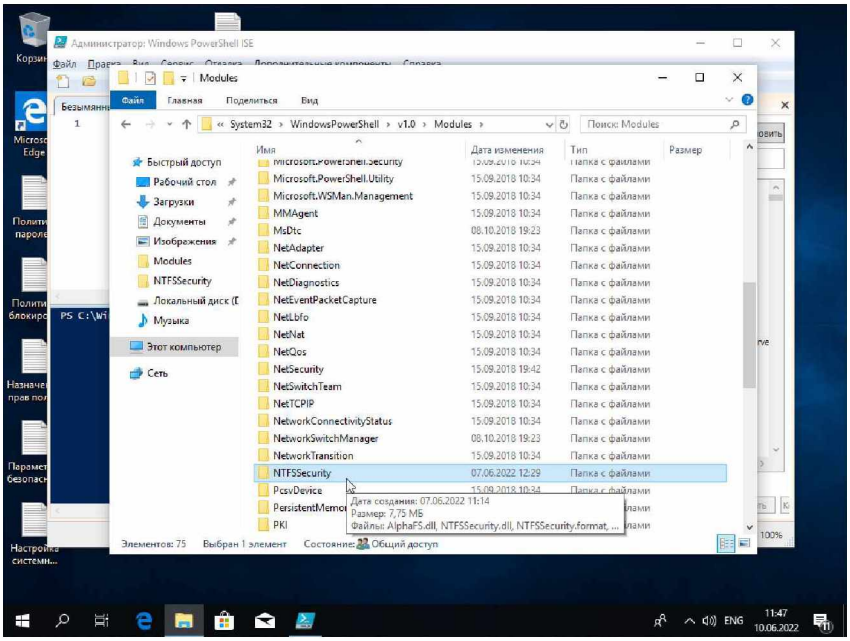

Рисунок 3.1 – Додавання розширення «NTFSSecurity»

Далі для застосування даного скрипту потрібно відкрити ISE PowerShell від імені адміністратора (Рис. 3.2), так як стандартна політика безпеки ОС не дозволяє виконувати сценарії у звичайному режимі.

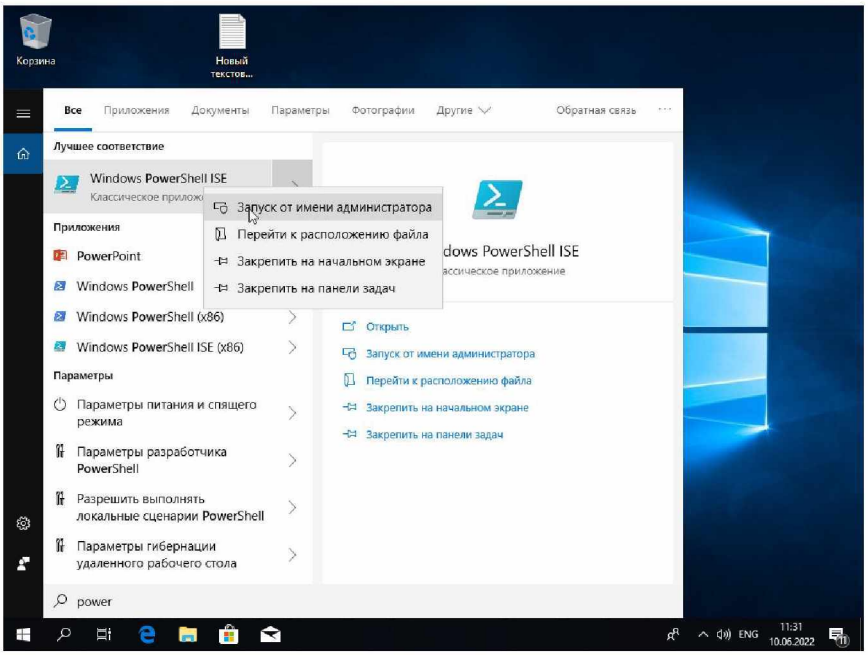

Рисунок 3.2 – Запуск PowerShell від імені адміністратору

Після відкриття даного ISE, потрібно ввести в командну строку (знизу) наступну команду: ***«-Set-ExecutionPolicy RemoteSigned»***. Дана команда дає дозвіл на виконання скриптових сценаріїв з довіреним цифровим підписом або з локальними. Після вводу команди иибираємо варіант «***Так***» та затверджуємо зміни у роботі політики виконання (Рис. 3.3).

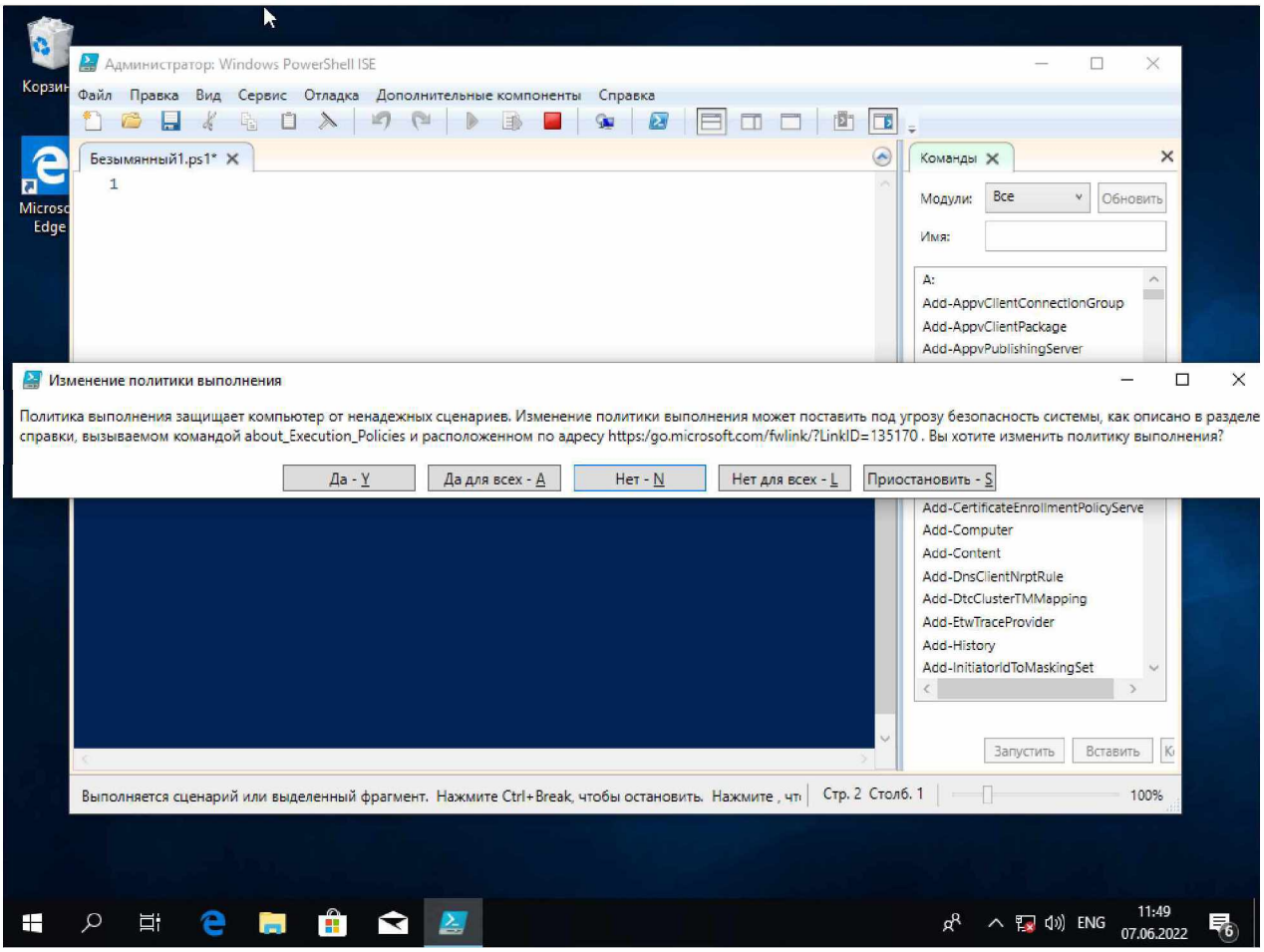

Рисунок 3.3 – Затвердження змін у роботи політики виконання

Після виконання даних маніпуляцій йдемо до: ***«Файл» → «Відкрити»***, обираємо потрібний нам скриптовий файл з контейнером формату .ps1 та натискаємо ***«Виконати»***, за цим розпочинається процес виконання скрипту за описаним вище алгоритму дій (Рис. 3.4).

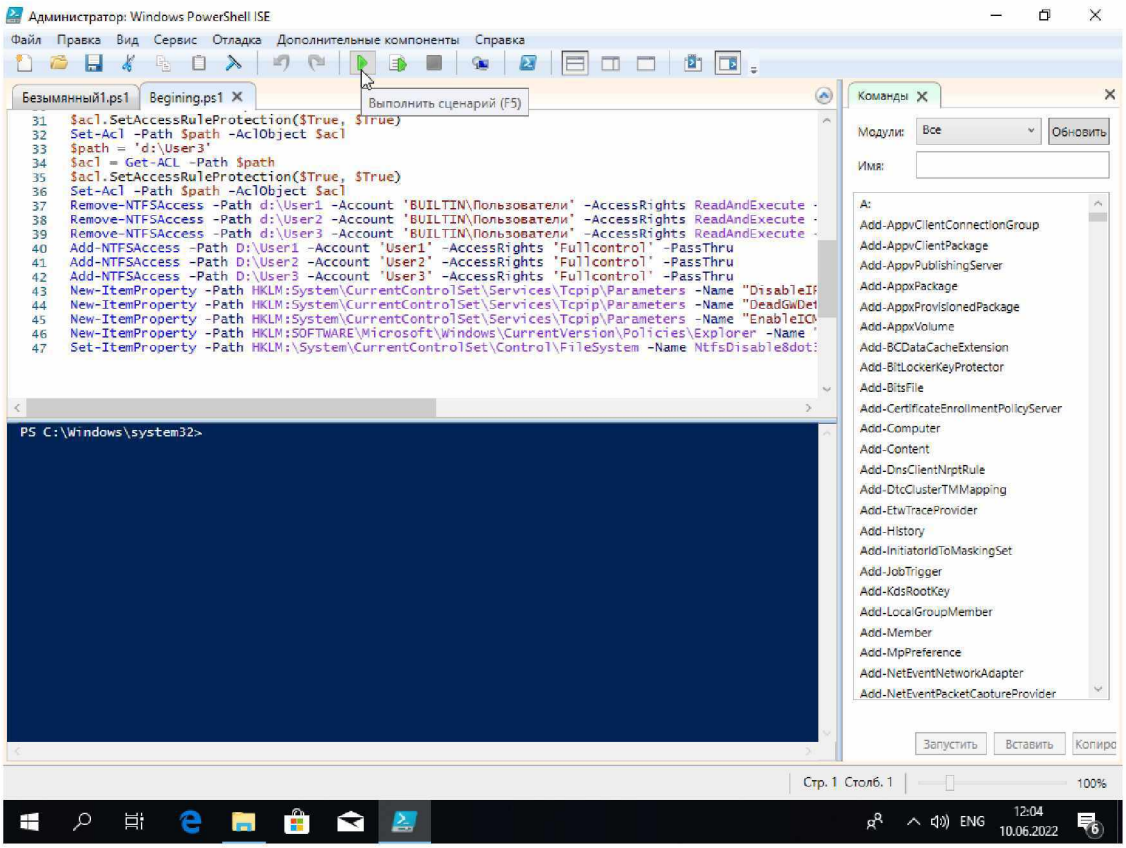

Рисунок 3.4 – Імпорт та початок процесу виконання

Лог виконання буде відображений у командному рядку, розташованому під вкладкою з відображеним кодом.

Текст скрипту, який виконує дії наведені нижче відображений в додатку Є.

3.2 Імпорт попередньо налаштованої політики безпеки

Через специфічність роботи PowerShell виявляється наступна проблема - неможливість роботи з політиками безпеки ОС, що унеможливлює подальший процес автоматизації налаштування КС, через що потребується шукати альтернативні рішення щодо скорочення часу необхідного для проектування системи. Вирішенням даного питання є імпорт налаштованого шаблону політики безпеки за допомогою Microsoft Management Console.

Для застосування попередньо налаштованого шаблону потрібно додати оснастку ***«Шаблони безпеки»*** після чого обрати за допомогою ПКМ – ***«Новий шлях для пошуку шаблонів»*** та обрати директорію, в якій знаходиться

потрібний файл. Далі додається оснастка ***«Аналіз та налаштування безпеки»*** після чого обрати за допомогою ПКМ - ***«Імпорт шаблону»*** та обрати потрібний шаблон безпеки - файл з розширенням ***.inf*** (Рис. 3.5).

Можливо провести аналіз комп'ютера на предмет сумісності параметрів підібраних в шаблоні та після цього натиснути ***«Настроїти комп'ютер»***. Після виконання процесу настройки потребується перезавантаження системи задля застосування змінених параметрів.

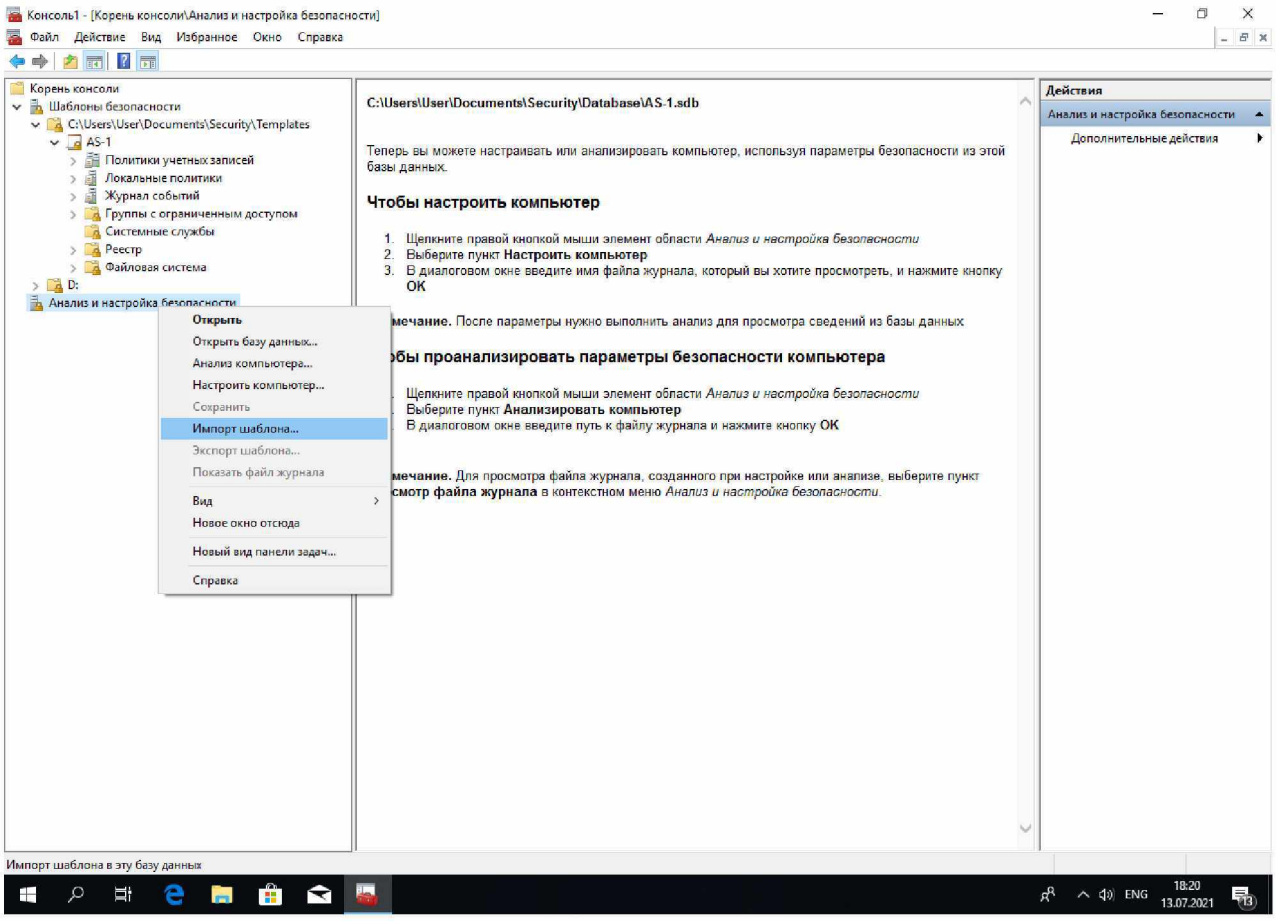

Рисунок 3.5 – Процес імпорту шаблону політики безпеки

Результатом налаштування системи за допомоги імпорту попередньо налаштованого шаблону (Рис. 3.6) безпеки буде завантаження КС з

необхідними параметрами та створення журналу, у якому виводиться процес та результат імплементації даних установок.

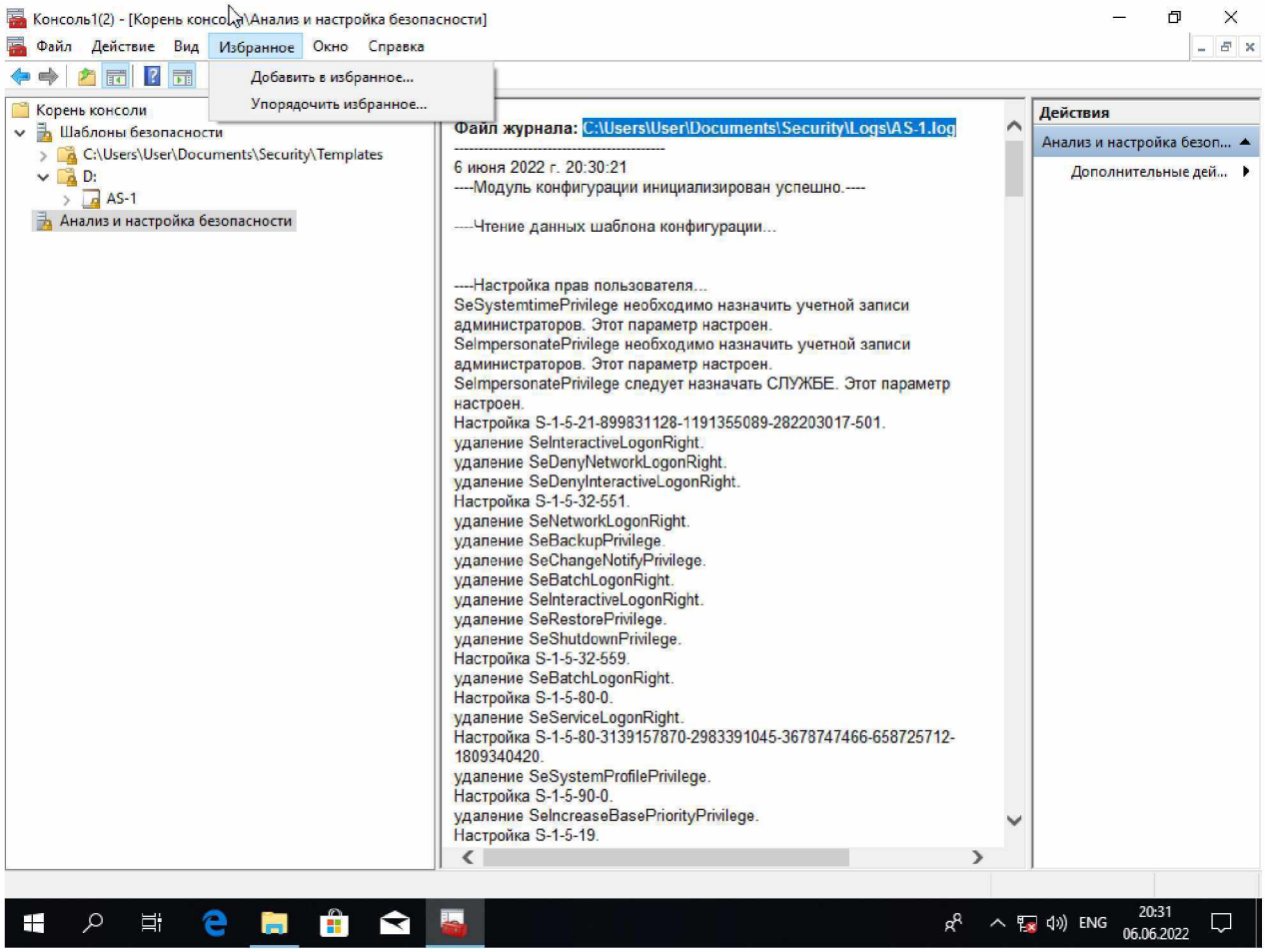

Рисунок 3.6 – Результат виконання налаштування

3.3 Імпорт конфігурації роботи антивірусного ПЗ

Наступним кроком після використання скрипту та імпорту локальної політики безпеки є імпорт конфігурації, яка дає змогу швидко налаштувати контроль пристроїв.

Процес імпортування сценарію (Рис 3.7), відбувається так: «***Імпорт та експорт параметрів»*** → ***«Імпорт параметрів»***, після чого обирається директорія з потрібним ***.xml*** файлом та обирається потрібний об’єкт.

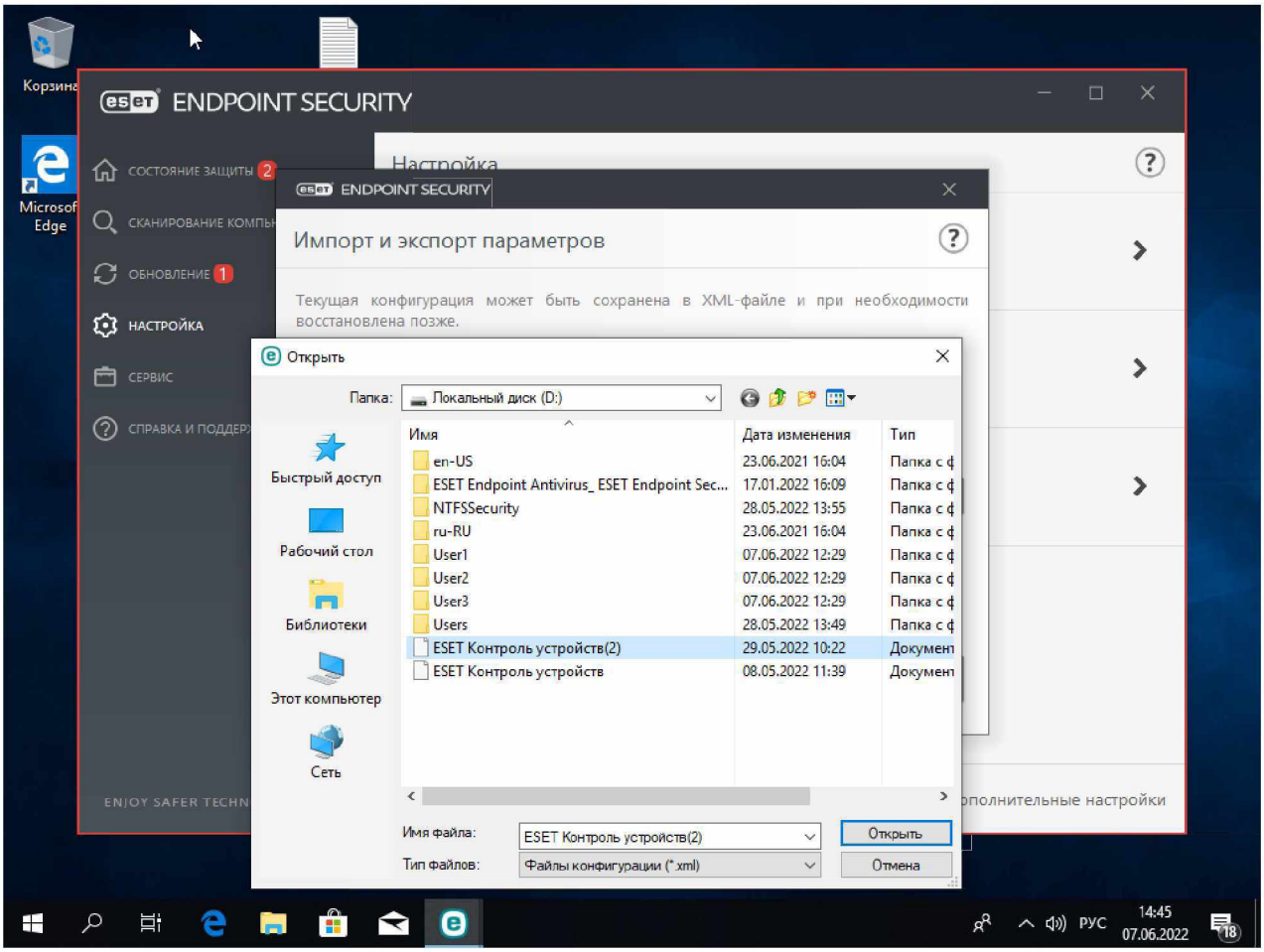

Рисунок 3.7 – Процес імпорту конфігурації роботи антивірусного ПЗ

Результатом налаштування роботи антивірусного програмного забезпечення за допомоги імпорту попередньо налаштованої конфігурації буде робота ПЗ з параметрами відповідними роботі АС класу «1» 4-ї категорії.

РОЗДІЛ 4. ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1 Процес оцінки ризиків інформаційної безпеки

Оцінювання ризиків ІБ автоматизованої системи потребує алгоритмізації, що дає можливість якісно провести експерту оцінку ризиків потрібної системи.

Алгоритм складається з наступних етапів:

- аналіз можливих вразливостей та загроз, відповідно до розглянутих активів системи ;
- оцінка ймовірності реалізації загрози;
- оцінюється вплив, який може вплинути на цілісність, конфіденційність, доступність та спостереженість по відношенню до ресурсів системи;
- документування можливих методів протидії виявленим загрозам.

Подальше оцінювання ризиків ІБ, по відношенню до спроектованої КСЗІ АС класу «1» 4-ї категорії складається з наступних етапів:

1. Визначення активу, який буде розглядатись та по відношенню до якого будуть співвідноситись вразивості та певні ризики. Під «активом» мається на увазі будь який фізичний об’єкт, інформація, яка зберігається та оброблюється в АС класу «1» 4-ї категорії;

2. Створення переліку можливих загроз та вразливостей з урахуванням особливостей роботи АС;

3. Оцінка за умовною шкалою впливу реалізації загрози на цілісність, конфіденційність, доступність та спостереженість оброблюваної інформації.

4. Аналіз впливу виявлених загроз та запропонування методів протидії виявленим загрозам.

4.2 Результат оцінки ризиків

Результатом є розгляд реальних загроз та вразливостей АС класу «1» 4-ї категорії, відповідно до норм прийнятих в галузі інформаційної безпеки. Було проведено попередню конфігурацію за яким визначається вплив на реалізацію

загроз за критеріями цілісності, конфіденційності, доступності та спостережності (Таблиця 4.1).

Таблиця 4.1 - визначення впливу на реалізацію загроз за критеріями цілісності, конфіденційності, доступності та спостережності

Оцінка	**Цілісність**	**Конфіденційність**	**Доступність**	**Спостережність**
1	Малоймовірна втрата інформації	Конфіденційна інформація має низькі шанси на розкриття	Доступність інформації залишається, дуже низька вірогідність порушення доступності до інформації	Повна або майже повна можливість спостерігати за діями працівників
2	Незначна втрата інформації, низька вірогідність суттєвого впливу на роботу системи	Маються помірні шанси на розкриття окремих документів, які не відносяться до інформації з обмеженим доступом	Доступність інформації залишається, але маються певні зміни щодо роботи системи	Залишається можливість слідкувати за діями працівників, але маються певні проблеми з спостережністю
3	Помірні втрати інформації, мається помірний вплив на роботу структури	Маються помірні шанси на розкриття окремих документів, які відносяться до інформації з обмеженим доступом.	Доступність інформації вже не є достатньою задля стабільної роботи системи Доступність до інформації – середня	Неможливість відстежити частину дій працівників. Можливі помірні ризики з компрометацією роботи системи
4	Великі втрати інформації, мається значний вплив на роботу системи. Можлива зупинка роботи системи.	Високі шанси на розкриття документів, які відносяться до інформації з обмеженим доступом.	Доступність інформації дуже важка, робота системи під питанням. Доступність до інформації – низька	Неможливість відстежити значну частину дій працівників. Великі ризики з компрометацією роботи системи
5	Повна інформації. Зупинка роботи системи, відбувається порушення законодавства України	Розкриття документів, які відносяться до інформації з обмеженим доступом. Зупинка роботи системи.	Неможливий доступ до інформації, максимальний ризик зупинки роботи системи.	Неможливість відстежити будь-які дії працівників, порушення законодавства України.

Обчислення величини ризику було реалізовано за допомогою наступної формули:

$MR = (C + I + A + O) \cdot PT$, де MR – величина ризику, C – конфіденційність, I – цілісність, A – доступність, O – спостереженість, PT – ймовірність реалізації загрози. Принцип оцінювання величину ризику реалізується за допомогою виставлення балів від 1 до 5, де:

1 – дуже низька вірогідність загрози по відношенню до розглянутого критерію;

2 – низька вірогідність загрози по відношенню до розглянутого критерію;

3 – середня вірогідність загрози по відношенню до розглянутого критерію;

4 – висока вірогідність загрози по відношенню до розглянутого критерію;

5 – дуже висока вірогідність загрози по відношенню до розглянутого критерію [21].

Відповідно до цього проаналізовані вразливості системи та виявлені ризики, також були запропонований комплекс дій для протидії знайденим загрозам (Таблиця 4.2).

Величина ризику може оцінюватись наступним чином:

81-100 балів – дуже високий ризик. Необхідність в терміновому втручанні та перегляді засобів захисту системи для протидії можливим наслідкам.

61-80 балів – високий ризик. Рекомендоване втручання для запобігання спричиненню відчутних наслідків по відношенню до системи.

41-60 балів – середній ризик. Рекомендоване втручання для запобігання спричиненню помірних наслідки по відношенню до системи.

21-40 балів – незначний ризик. Дані загрози можуть не спричиняти помірних наслідків по відношенню до системи, наслідки з малою шкідливістю для роботи системи.

0-20 – малоймовірний ризик. Актуальні для системи загрози можуть не спричиняти незначних та слабких наслідків з малою шкідливістю для роботи системи [21].

Таблиця 4.2 – Оцінка ризиків ІБ

№	Актив	Вразливість	Загрози	Конфіденційність	Цілісність	Доступність	Спостережність	Імовірність реалізації загроз	Величина ризику	Засоби протидії загрозам
1	2	3	4	5	6	7	8	9	10	11
1.	Апаратні засоби	Недостатнє обслуговування/дефектна інсталяція з носіїв даних	Порушення ремонтопридатності інформаційної системи	3	4	3	3	3	39	Документування правил обслуговування апаратно-програмного комплексу та роботи з носіями даних
2.		Вади схем для періодичних замін	Руйнування обладнання або носіїв	3	5	5	3	3	48	Перегляд схем для періодичних замін та виправлення недоліків при проектуванні схем
3.		Вади ефективного контролю внесення змін конфігурації	Помилка у використанні	3	3	2	3	2	22	Документування правил, згідно якими проводяться зміни конфігурації у роботі апаратно-програмного комплексу
4.		Сприйнятливість до змін напруги	Втрата джерела живлення	1	5	5	2	4	52	Встановлення компонентів, які мають відповідний клас захисту від скачку напруги, використання джерела безперебійного живлення

Продовження Таблиці 4.2

1	2	3	4	5	6	7	8	9	10	11
5.		Неконтрольоване копіювання	Крадіжка носіїв/документів	5	3	3	5	3	48	Встановлення правил, згідно яким копіювати інформацію може лише адміністратор системи
6.		Сприйнятливість до пилу, вологості, забруднення	Пил, корозія, обмерзання	2	4	3	2	3	33	Встановлення правил щодо якості приміщення, у якому знаходиться система
7.	Програмні засоби	Відсутність або недостатнє програмне тестування	Зловживання правами використання ПЗ	2	4	4	3	4	52	Обов’якзове навчання по роботі програмного забезпечення
8.		Відомі недоліки в програмному забезпеченні	Зловживання правами використання ПЗ	3	4	4	3	4	56	Застосування тільки офіціальних версій програмного забезпечення, уникання обновлень до бета-версій
9.		Відсутній 'вихід з системи' при залишенні робочої станції	Зловживання правами використання ПЗ	4	4	3	4	3	45	Обов’язкове внесення до правил перебування за робочою станції параметру «вихід з системи» зі встановлення паролю при вході
10.		Передача або багаторазове використання носіїв даних без належного стирання	Зловживання правами використання ПЗ	4	4	3	4	4	60	Внесення до правил користування системи стирання при багаторазовому використанні носіїв даних

Продовження Таблиці 4.2

1	2	3	4	5	6	7	8	9	10	11
11.		Встановлення неправильного параметру	Помилка при використанні програмного комплексу	3	3	4	2	2	24	Постійна перевірка всіх параметрів системи при запуску згідно документації
12.		Неправильний розподіл прав доступу	Зловживання правами облікових записів	5	4	4	4	4	68	Встановлення відповідних прав доступу до системи, згідно з політикою безпеки організації
13.	Мережа	Вади ідентифікуючих розпізнавальних механізмів для користувальницької аутентифікації	Підроблення прав	5	4	3	5	4	68	Правильне конфігурування обладнання яке виконує роботу ідентифікуючих розпізнавальних механізмів для користувальницької аутентифікації
14.		Незахищені таблиці паролів	Підроблення прав	5	5	5	5	4	80	Встановлення правил щодо паролів, їх складності
15.		Поганий менеджмент паролями	Підроблення прав	5	5	5	5	4	80	Встановлення правил щодо паролів, їх складності
16.		Попереднє або нове програмне забезпечення	Програмний збій	3	5	5	3	4	64	Робота тільки зі стабільними збірками програмного забезпечення

Продовження Таблиці 4.2

1	2	3	4	5	6	7	8	9	10	11
17.		Неконтрольоване завантаження/використання програмного забезпечення	Підробка програмного забезпечення	4	5	5	4	3	54	Встановлення прав доступу, відповідно до яких конкретний користувач системи може використовувати/встановлювати ПЗ
18.		Відмова менеджменту від перевірки звітів	Несанкціоноване використання обладнання	5	4	5	5	4	76	Обов'язкова перевірка звітності щодо роботи апаратно-програмного комплексу
19.		Незахищені лінії зв'язку	Підслуховування	5	5	5	5	4	80	Проектування лінії зв'язку з відповідним захистом від прослуховування (шифрування)
20.		Погана спільна проводка	Відмова телекомунікаційного обладнання	3	5	4	4	4	64	Комплекс мір щодо ліквідації вразливостей в проводці
21.		Небезпечна мережева архітектура	Віддалений шпигунство	5	5	5	5	5	100	Ліквідація вразливостей, спричинених неідеальним налаштуванням мережі
22.	Персонал	Відсутність персоналу	Порушення доступності персоналу	3	3	5	3	4	56	Вербування персоналу за критеріями задовольняючим принципам роботи організації
23.		Невідповідні процедури вербування	Знищення обладнання або носіїв	5	5	5	5	5	100	Створення комплексу мір для тестування майбутніх працівників на предмет наявності необхідних знань.

Продовження Таблиці 4.2

1	2	3	4	5	6	7	8	9	10	11
24.		Недостатнє навчання безпеки	Помилка у використанні	5	4	5	4	4	72	Навчання персоналу правилам безпеки організації
25.		Неправильне використання програмного забезпечення і устаткування	Помилка у використанні	5	5	5	4	3	57	Навчання персоналу правильним користуванням програмним забезпеченням відповідно до заданої документації та політики безпеки організації
26.		Брак механізмів моніторингу	Незаконна обробка даних, подальша компрометація даних	5	5	5	5	4	80	Перевірка журналів, у яких наведені виконані процеси при роботі апаратно-програмного комплексу, документування процесів та подальша доповідь
27.		Неконтрольована робота зовнішнім штатом або персоналом	Крадіжка носіїв/документів	5	5	5	5	5	100	Жорсткій контроль за роботою персоналом: використання камер, охорони, призначення спостерігача, який повідомляє про всі зміни безпосередньо керівництву
28.		Вади політики для правильного використання носіїв передачі даних і обміну повідомленнями	Несанкціоноване використання апаратно-програмного комплексу	5	5	5	5	5	100	Конфігурування локальної політики безпеки згідно наведеної документації, яка складена організацією

ВИСНОВОК

В результаті виконання кваліфікаційної роботи можна відзначити, що поставлена мета була досягнута. В результаті були вирішені такі завдання досліджень:

- проведено аналіз предметної області і існуючих методик ручного проектування КСЗІ автоматизованих систем;
- розроблено алгоритм дій по спрощенню проектування КСЗІ автоматизованої системи класу "1" 4-ї категорії;
- реалізовано спрощення проектування КСЗІ автоматизованої системи класу "1" 4-ї категорії
- перевірена працездатність розробленої системи;
- проведено оцінку ризиків інформаційної безпеки АС класу "1" 4-ї категорії.

Розроблений алгоритм включає три етапи.

1. Використання попередньо написаного скриптового сценарію, який виконує:

- додавання декількох облікових записів в ОС;
- присвоєння паролю створеним обліковим записам;
- створення особистої папки для кожного з користувачів;
- за допомоги ACL команди зміну NTFS привілеїв доступу до певних директорій в системі;
- позбавлення прав на доступ та редагування щодо певної директорії для певного користувача;
- надання прав на повний доступ щодо певної директорії для певного користувача;
- створення ключа у реєстрі та присвоєння йому певного значення.

2. Імпорт попередньо налаштованого шаблону локальної політики безпеки.

3. Імпорт попередньо налаштованої конфігурації роботи антивірусного програмного забезпечення.

Проведена оцінка ризиків інформаційної безпеки по відношенню до спроектованої системи, внаслідок чого були виявлені можливі вразливості, загрози для даної системи та були сформульовані рекомендації для протидії виявленим загрозам.

СПИСОК ЛІТЕРАТУРИ

1. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 31.05.2005 р. № 2594-IV. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text. (дата звернення: 04.05.2022 р.).
2. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу – Зі Зміною №1, затвердженою наказом Адміністрації Держспецзв'язку від 15.10.2008 № 172. – (Серія видань «Нормативний документ»). URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text. (дата звернення: 02.05.2022 р.).
3. Stokes J., Singer M., Diver R., Windows 10 for Enterprise Administrators: Modern Administrators' guide based on Redstone 3 version., 2017 – P. 48-171.
4. Bott E., Windows 10 Inside Out., 2020. – P. 42-51.
5. Rathbone A., Windows 10 For Dummies, 4nd Edition., 2020. – P. 35-71.
6. Knittel B., McPhaedris P., Windows 10 In Depth, 2nd Edition., 2018. – 140 p.
7. Yosifovich P., Solomon D.A., Ionescu A., Windows Internals, Part 1: System architecture, processes, threads, memory management, and more., 2017. – P. 125-230.
8. ESET Endpoint Antivirus User's Guide. URL: https://help.eset.com/eea/8/ru-RU/. (дата звернення: 22.05.2022 р.).
9. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Звід правил для управління інформаційною безпекою – (Серія видань «Видання офіційне»). URL: http://s-byte.com/useful/27002.pdf. (дата звернення: 05.05.2022 р.).
10. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Вимоги щодо системи управління інформаційною безпекою – (Серія видань «Видання офіційне»). URL: http://s-byte.com/useful/27001.pdf. (дата звернення: 05.05.2022 р.).

11. ISO/IEC 27005:2011. Information Security Risk Management. URL: https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf. (дата звернення: 05.05.2022 р.).
12. Пузиренко О. Г. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем / О. Г. Пузиренко, С. О. Івко, О. О. Лаврут // Системи обробки інформації. — Л. : Академія сухопутних військ імені гетьмана Петра Сагайдачного, 2014. — Вип. 8 (124).— ISSN 1681–7710. — С. 128–134.
13. Чунарьова А. В. Аналіз підходів та програмних рішень оцінки і контролю інформаційних ризиків в комп'ютеризованих системах / А. В. Чунарьова, І. І. Пархоменко, І. І. Сащук // Вісник Інженерної академії України. — Х. — 2014. — Вип. 2. — С. 138–142.
14. ConEmu Documentation and User's Guide. URL: https://conemu.github.io/en/TableOfContents.html. (дата звернення: 5.04.2022 р.).
15. Berg C., Windows Powershell and Scripting Made Easy For Sysadmins: A Comprehensive Beginners Guide Windows Powershell And Scripting To Automate Tasks And Environment., 2021. – 71 p.
16. Cygwin User's Guide. URL: https://cygwin.com/cygwin-ug-net/cygwin-ug-net.html. (дата звернення: 1.04.2022 р.).
17. Holmes L., Windows PowerShell Cookbook: The Complete Guide to Scripting Microsoft's Command Shell., 2013. – P. 80-230.
18. Holmes L., PowerShell Cookbook: Your Complete Guide to Scripting the Ubiquitous Object-Based Shell., 2021. – P. 25-105.
19. Bertram A., PowerShell for Sysadmins: Workflow Automation Made Easy., 2020. – P. 45-126.
20. Wilson E., Windows PowerShell Step by Step., 2015. – P. 255-269.
21. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи. URL: file:///C:/Users/User/Downloads/224-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0

%B0%D1%82%D1%82%D1%96-844-1-10-20201224.pdf. (дата звернення: 20.04.2022 р.).

ДОДАТОК А

Таблиця з рекомендованими параметрами політики паролів

№	Назва параметру	Значення параметру
1.	Вести журнал паролів	12 збережених паролів
2.	Максимальний термін дій пароля	120 днів
3.	Мінімальна довжина паролю	8 значний
4.	Мінімальний термін дії паролю	90 днів
5.	Пароль повинен відповідати вимогам складності	Ввімкнена
6.	Зберігати паролі, використовуючи зворотне шифрування	Відключено

ДОДАТОК Б

Таблиця з рекомендованими параметрами політики блокування облікових записів

№	Назва параметру	Значення параметру
1.	Час скидання лічильника блокування.	30 хвилин
2.	Порогове значення блокування	5 помилок входу в систему
3.	Тривалість блокування облікового запису	30 хвилин

ДОДАТОК В

Таблиця з рекомендованими параметрами призначення прав користувачів

№	Назва параметру	Значення параметру
1.	Архівація файлів та каталогів	Адміністратори
2.	Блокування сторінок у пам'яті	
3.	Відновлення файлів та каталогів	Адміністратори
4.	Вхід як пакетне завдання	
5.	Вхід як служба	
6.	Виконання завдань обслуговування томів	Адміністратори
7.	Додавання робочих станцій до домену	
8.	Доступ до диспетчера облікових даних від імені довіреного	
9.	Доступ до комп'ютера з мережі	
10.	Завершення роботи системи	Користувачі,Адміністратори
11.	Завантаження та розвантаження драйверів пристроїв	Адміністратори
12.	Заміна маркера рівня процесу	LOCAL SERVICE
13.	Заборонити вхід до системи через службу віддалених робочих столів	Все,АНОНІМНИЙ ВХІД
14.	Заборонити локальний вхід	
15.	Зміна позначки об'єкта	
16.	Зміна параметрів середовища виробника	Адміністратори
17.	Зміна системного часу	Адміністратори
18.	Зміна часового поясу	Адміністратори
19.	Імітація клієнта після автентифікації	СЛУЖБА, Адміністратори, NETWORK SERVICE, LOCAL SERVICE
20.	Локальний вхід до системи	Адміністратори, Користувачі
21.	Налаштування квот пам'яті для процесу	Адміністратори, LOCAL SERVICE
22.	Обхід перехресної перевірки	Виконавши перевірку, LOCAL SERVICE

Продовження таблиці з рекомендованими параметрами призначення прав користувачів

№	Назва параметру	Значення параметру
23.	Відмовити у доступі до цього комп'ютера з мережі	Все, АНОНІМНИЙ ВХІД
24.	Відмовити у вході як пакетне завдання	Гості, АНОНІМНИЙ ВХІД
25.	Відмовити у вході як служба	Не визначено
26.	Вимкнення комп'ютера від вузла стику	Не визначено
27.	Налагодження програм	
28.	Отримати маркер уособлення для іншого користувача на тому ж сеансі	
29.	Примусове віддалене завершення роботи	
30.	Профілювання одного процесу	Адміністратори
31.	Профілювання продуктивності системи	Адміністратори
32.	Робота в режимі операційної системи	
33.	Дозвіл довіри до облікових записів комп'ютерів та користувачів під час делегування	Не визначено
34.	Дозволити вхід до системи через службу віддалених робочих столів	Не визначено
35.	Синхронізація даних служби каталогів	
36.	Зміна власників файлів та інших об'єктів	Адміністратори
37.	Створення аудитів безпеки	LOCAL SERVICE
38.	Створення глобальних об'єктів	Адміністратори, LOCAL SERVICE
39.	Створення маркерного об'єкту	
40.	Створення постійних спільних об'єктів	
41.	Створення символічних посилань	
42.	Створення файлу підкачки	Адміністратори
43.	Збільшення пріоритету виконання	Адміністратори
44.	Збільшення робочого набору процесу	Адміністратори, LOCAL SERVICE
45.	Управління аудитом та журналом безпеки	Адміністратори

ДОДАТОК Г

Таблиця з рекомендованими параметрами безпеки ОС

№	Назва параметру	Значення параметру
1.	DCOM: Обмеження комп'ютера на доступ до синтаксису SDDL (Security Descriptor Definition Language)	Не визначено
2.	DCOM: Обмеження комп'ютера для запуску в синтаксисі SDDL (Security Descriptor Definition Language)	Не визначено
3.	Аудит: аудит доступу глобальних системних об'єктів	Вимкнено
4.	Аудит: аудит використання привілею на архівацію та відновлення	Вимкнено
5.	Аудит: негайне відключення системи, якщо неможливо внести до журналу записи про аудит безпеки	Вимкнено
6.	Аудит: примусово перевизначає параметри категорії аудиту параметрами підкатегорії політики аудиту (Windows Vista або наступні версії)	Увімкнено
7.	Доступ до мережі: Дозволити трансляцію анонімного SID в ім'я	Вимкнено
8.	Завершення роботи: очищення файлу підкачування віртуальної пам'яті	Увімкнено
9.	Завершення роботи: дозволити завершення роботи системи без виконання входу до системи	Вимкнено
10.	Інтерактивний вхід до системи: поведінка під час вилучення смарт-карти	Блокування робочої станції
11.	Інтерактивний вхід до системи: заголовок повідомлення для користувачів при вході до системи	ПРОДОВЖЕННЯ СПРОБ БЕЗ НАЛЕЖНОЇ АВТОРИЗАЦІЇ Є ЗЛОЧИНОМ

Продовження таблиці з рекомендованими параметрами безпеки ОС

№	Назва параметру	Значення параметру
12.	Інтерактивний вхід до системи: кількість попередніх підключень до кешу (у разі відсутності доступу до контролера домену)	0 входів до системи
13.	Інтерактивний вхід: нагадувати користувачам про закінчення терміну дії пароля заздалегідь	За 5 днів
14.	Інтерактивний вхід до системи: не відображати ім'я користувача під час входу до системи	Не визначено
15.	Інтерактивний вхід до системи: не відображати облікові дані останнього користувача	Увімкнено
16.	Інтерактивний вхід до системи: не вимагати натискання CTRL+ALT+DEL	Вимкнено
17.	Інтерактивний вхід до системи: відображає відомості про користувача, якщо сеанс заблоковано	Не відображати інформацію про користувача
18.	Інтерактивний вхід до системи: гранична кількість невдалих спроб входу	Не визначено
19.	Інтерактивний вхід до системи: межа простою комп'ютера	Не визначено
20.	Інтерактивний вхід: текст повідомлення для користувачів при вході в систему:	Вхід тільки для авторизованих користувачів. Особи, які здійснюють спроби несанкціонованого доступу, порушують законодавство України
21.	Інтерактивний вхід до системи: вимагати Windows Hello для бізнесу або смарт-карту	Вимкнено
22.	Інтерактивний вхід до системи: вимагати перевірки на контролері домену для скасування блокування комп'ютера	Вимкнено

Продовження таблиці з рекомендованими параметрами безпеки ОС

№	Назва параметру	Значення параметру
23.	Клієнт мережі Microsoft: використовувати цифровий підпис (завжди)	Вимкнено
24.	Клієнт мережі Microsoft: використовувати цифровий підпис (за згодою сервера)	Вимкнено
25.	Клієнт мережі Microsoft: надсилати незашифрований пароль стороннім SMB-серверам	Вимкнено
26.	Консоль відновлення: дозволити автоматичний вхід адміністратора	Вимкнено
27.	Консоль відновлення: дозволити копіювання дискет та доступ до всіх дисків та папок	Вимкнено
28.	Контролер домену: заборонити зміну пароля облікових записів комп'ютера	Вимкнено
29.	Контролер домену: дозволити операторам сервера задавати виконання завдань за розкладом	Вимкнено
30.	Контролер домену: вимога цифрового підпису для LDAP-сервера	Ні
31.	Контроль облікових записів: віртуалізація збоїв запису у файл або реєстр на підставі розташування користувача	Не визначено
32.	Контроль облікових записів: всі адміністратори працюють у режимі схвалення адміністратором	Увімкнено
33.	Контроль облікових записів: виявлення установки програм та запит на підвищення прав	Увімкнено
34.	Контроль облікових записів: переключення до безпечного робочого стола під час виконання запиту на підвищення прав	Увімкнено

Продовження таблиці з рекомендованими параметрами безпеки ОС

№	Назва параметру	Значення параметру
35.	Контроль облікових записів: поведінка запиту підвищення прав для адміністраторів в режимі схвалення адміністратором	Запит облікових даних
36.	Контроль облікових записів: поведінка запиту підвищення прав для звичайних користувачів	Запит облікових даних
37.	Контроль облікових записів: підвищення прав для UIAccess-програм лише при встановленні в безпечних місцях	Увімкнено
38.	Контроль облікових записів: підвищення прав тільки для підписаних та перевірених виконуваних файлів	Вимкнено
39.	Контроль облікових записів: дозвіл UIAccess-додатків вимагати підвищення прав, не використовуючи безпечний робочий стіл	Вимкнено
40.	Контроль облікових записів: режим схвалення адміністратором для вбудованого облікового запису адміністратора	Вимкнено
41.	Параметри системи: використовувати правила сертифікатів для файлів Windows, що виконуються, для політик обмеженого використання програм	Вимкнено
42.	Параметри системи: необов'язкові підсистеми	Не визначено
43.	Сервер мережі Microsoft: час бездіяльності до призупинення сеансу:	10 хвилин
44.	Сервер мережі Microsoft: використовувати цифровий підпис (завжди)	Вимкнено
45.	Сервер мережі Microsoft: використовувати	Вимкнено

	цифровий підпис (за згодою клієнта)	
46.	Сервер мережі Microsoft: відключати клієнтів після закінчення дозволеного годинника входу	Вимкнено

Продовження таблиці з рекомендованими параметрами безпеки ОС

№	Назва параметру	Значення параметру
47.	Безпека мережі: мінімальна сеансова безпека для клієнтів на базі NTLM SSP (включаючи безпечний RPC)	Не визначено
48.	Безпека мережі: мінімальна сеансова безпека для серверів на базі NTLM SSP (включаючи безпечний RPC)	Не визначено
49.	Безпека мережі: налаштування типів шифрування, дозволених Kerberos	Не визначено
50.	Безпека мережі: не зберігати хеш-значення LAN Manager при наступній зміні пароля	Вимкнено
51.	Безпека мережі: обмеження NTLM: аудит вхідного трафіку NTLM	Не визначено
52.	Безпека мережі: обмеження NTLM: аудит автентичності NTLM у цьому домені	Не визначено
53.	Безпека мережі: обмеження NTLM: вхідний трафік NTLM	Не визначено
54.	Безпека мережі: обмеження NTLM: додати винятки для серверів у цьому домені	Не визначено
55.	Мережа безпека: обмеження NTLM: додати віддалені сервери у виключення автентичності NTLM	Не визначено
56.	Безпека мережі: обмеження NTLM: вихідний трафік NTLM до віддалених серверів	Не визначено
57.	Безпека мережі: обмеження NTLM: автентифікація NTLM у цьому домені	Не визначено
58.	Мережева безпека: Примусове виведення з сеансу після закінчення допустимих годин	Увімкнено

	роботи	
59.	Безпека мережі: дозволити LocalSystem використовувати нульові сеанси	Не визначено

Продовження таблиці з рекомендованими параметрами безпеки ОС

№	Назва параметру	Значення параметру
60.	Безпека мережі: дозволити використання мережних посвідчень у запитах автентифікації PKU2U до цього комп'ютера	Не визначено
61.	Безпека мережі: дозволити облікового запису локальної системи використовувати посвідчення комп'ютера для NTLM	Не визначено
62.	Безпека мережі: вимога цифрового підпису для LDAP-клієнта	Ні
63.	Безпека мережі: рівень автентифікації LAN Manager	Не визначено
64.	Мережевий доступ: заборонити анонімний доступ до іменованих каналів та загальних ресурсів	Увімкнено
65.	Мережевий доступ: модель спільного доступу та безпеки для локальних облікових записів	Не визначено
66.	Мережевий доступ: не дозволяти перерахування облікових записів SAM анонімними користувачами	Увімкнено
67.	Мережевий доступ: не дозволяти перерахування облікових записів SAM та загальних ресурсів анонімними користувачами	Увімкнено
68.	Мережевий доступ: не дозволяти збереження паролів або облікових даних для автентифікації	Вимкнено
69.	Мережевий доступ: обмежити кількість	Не визначено

	клієнтів, яким дозволено віддалені дзвінки SAM	
70.	Мережевий доступ: дозволяти анонімний доступ до іменованих каналів	Не визначено

Продовження таблиці з рекомендованими параметрами безпеки ОС

№	Назва параметру	Значення параметру
71.	Мережевий доступ: дозволяти анонімний доступ до загальних ресурсів	Не визначено
72.	Мережевий доступ: дозволяти застосування дозволів "Для всіх" до анонімних користувачів	Вимкнено
73.	Мережевий доступ: віддалено доступні шляхи та вкладені шляхи реєстру	Ні
74.	Мережевий доступ: віддалено доступні шляхи реєстру	Ні
75.	Мережевий сервер (Майкрософт): спроба S4U2Self отримати інформацію про затвердження	Не визначено
76.	Мережевий сервер (Майкрософт): рівень перевірки сервером імені учасника служби кінцевого об'єкта	Не визначено
77.	Системна криптографія: використовувати FIPS-сумісні алгоритми для шифрування, хешування та підписування	Вимкнено
78.	Системна криптографія: обов'язкове застосування сильного захисту ключів користувачів, що зберігаються на комп'ютері.	Користувач повинен вводити пароль при кожному використанні ключа
79.	Системні об'єкти: посилити стандартні дозволи для внутрішніх системних об'єктів (наприклад, символічних посилань)	Увімкнено
80.	Системні об'єкти: враховувати регістр для	Увімкнено

	підсистем, відмінних від Windows	
81.	Пристрої: заборонити користувачам інсталяцію драйверів принтера	Увімкнено
82.	Пристрої: дозволити відстиковку без входу до системи	Не визначено

Продовження таблиці з рекомендованими параметрами безпеки ОС

№	Назва параметру	Значення параметру
83.	Пристрої: дозволити доступ до дисководів гнучких дисків лише локальним користувачам	Вимкнено
84.	Пристрої: дозволити доступ до дисків компакт-дисків лише локальним користувачам	Вимкнено
85.	Пристрої: дозволити форматування та вилучення знімних носіїв	Адміністратори
86.	Облікові записи: блокувати облікові записи Майкрософт	Не визначено
87.	Облікові записи: Перейменування облікового запису адміністратора	Рекомендується
88.	Облікові записи: Перейменування облікового запису відвідувача	Рекомендується
89.	Облікові записи: дозволити використання порожніх паролів лише при консольному вході	Увімкнено
90.	Облікові записи: Стан облікового запису 'Адміністратор'	Вимкнено
91.	Облікові записи: Стан облікового запису 'Гість'	Вимкнено
92.	Член домену: завжди потрібний цифровий підпис або шифрування потоку даних безпечного каналу	Вимкнено
93.	Член домену: максимальний термін дії	Не визначено

	пароля облікових записів комп'ютера	
94.	Член домену: відключити зміну пароля облікових записів комп'ютера	Вимкнено
95.	Член домену: вимагати стійкого сеансового ключа (Windows 2000 або вище)	Вимкнено

ДОДАТОК Ґ

Таблиця з рекомендованими параметрами системних служб

№	Назва параметру	Значення параметру
1.	Branch Cache	Не визначено
2.	DHCP-клієнт	Заборонено
3.	DNS-клієнт	Заборонено
4.	Plug-and-Play	Автоматичний
5.	Автоналаштування WWAN	Заборонено
6.	Агент захисту мережевого доступу	Заборонено
7.	Агент політики IPsec	Заборонено
8.	Архівація Windows	Вручну
9.	Брандмауер Захисника Windows	Автоматичний
10.	Браузер комп'ютерів	Заборонено
11.	Веб-клієнт	Вручну
12.	Віртуальний диск	Заборонено
13.	Допоміжна служба IP	Заборонено
14.	Вторинний вхід до системи	Вручну
15.	Дефрагментація диску	Вручну
16.	Диспетчер Автоматичних підключень для віддаленого доступу	Заборонено
17.	Диспетчер друку	Автоматичний
18.	Диспетчер підключень для віддаленого доступу	Заборонено
19.	Диспетчер сеансів Диспетчер вікон робочого столу	Автоматичний
20.	Диспетчер посвідчення мережевих учасників	Заборонено

№	Назва параметру	Значення параметру
21.	Диспетчер облікових даних	Вручну
22.	Диспетчер облікових записів безпеки	Автоматичний
23.	Доступ до HID-пристроїв	Вручну
24.	Журнал подій Windows	Автоматичний
25.	Журнали та оповіщення продуктивності	Вручну

Продовження таблиці з рекомендованими параметрами системних служб

№	Назва параметру	Значення параметру
26.	Захист програмного забезпечення	Автоматичний
27.	Захисник Windows	Автоматичний
28.	Захищене сховище	Автоматичний
29.	Інформація про сумісність програм	Вручну
30.	Клієнт групової політики	Автоматичний
31.	Клієнт відстеження зв'язків, що змінилися	Автоматичний
32.	Координатор розподілених транзакцій	Автоматичний
33.	Пастка SNMP	Заборонено
34.	Локатор віддаленого виклику процедур (RPC)	Вручну
35.	Маршрутизація та віддалений доступ	Заборонено
36.	Модулі ключів IPsec для обміну ключами в Інтернеті та протоколу IP з автентичністю	Заборонено
37.	Модуль запуску процесів DCOM-серверу	Автоматичний
38.	Модуль підтримки NetBIOS через TCP/IP	Заборонено
39.	Налаштування сервера віддалених робочих столів	Заборонено
40.	Негайне підключення Windows - реєстратор налаштування	Вручну
41.	Виявлення SSDP	Заборонено
42.	Виявлення інтерактивних служб	Вручну
43.	Загальний доступ до Інтернету (ICS)	Заборонено

44.	Визначення оболонок	Автоматичний
45.	Основні служби довіреного платформного модуля	Вручну
46.	Перенаправник портів користувача режиму служби віддалених робочих столів	Заборонено
47.	Перелічник IP-шин PnP-X	Заборонено
48.	Питання	Автоматичний
49.	Планувальник завдань	Автоматичний
50.	Планувальник класів мультимедіа	Вручну

Продовження таблиці з рекомендованими параметрами системних служб

№	Назва параметру	Значення параметру
51.	Постачальник домашньої групи	Вручну
52.	Програмний постачальник тіньового копіювання (Microsoft)	Автоматичний
53.	Публікація ресурсів можливостей	Вручну
54.	Робоча станція	Заборонено
55.	Поширення сертифіката	Заборонено
56.	Розширюваний протокол перевірки довжини (EAP)	Вручну
57.	Складальник подій Windows	Заборонено
58.	Відомості про програму	Вручну
59.	сервер	Заборонено
60.	Сервер упорядкування потоків	Вручну
61.	Мережевий вхід до системи	Заборонено
62.	Мережеві підключення	Заборонено
63.	Система розвитку COM+	Автоматичний
64.	Системний додаток COM+	Вручну
65.	Служба SSTP	Заборонено
66.	Служба автоматичного виявлення веб-проксі роботи WinHTTP	Заборонено
67.	Служба автоналаштування WLAN	Заборонено
68.	Служба базової фільтрації	Вручну

69.	Служба введення планшетного ПК	Вручну
70.	Служба часу Windows	Автоматичний
71.	Служба завантаження зображень Windows (WIA)	Автоматичний
72.	Служба ініціатора Майкрософт iSCSI	Заборонено
73.	Служба інтерфейсу збереження мережі	Заборонено
74.	Служба кешу шрифтів Windows	Автоматичний
75.	Служба медіаприставки Media Center	Вручну

Продовження таблиці з рекомендованими параметрами системних служб

№	Назва параметру	Значення параметру
76.	Служба модуля архівації на рівні блоків	Автоматичний
77.	Служба загальних мережних ресурсів медіапрогравача Windows	Заборонено
78.	Служба перечислювача переносних пристроїв	Вручну
79.	Служба планувальника Windows Media Center	Вручну
80.	Служба підтримки Bluetooth	Заборонено
81.	Служба політики діагностики	Автоматичний
82.	Служба помічника із сумісності програм	Автоматичний
83.	Служба профілів користувачів	Автоматичний
84.	Служба публікації імен комп'ютерів PNRP	Заборонено
85.	Служба реєстрації помилок Windows	Вручну
86.	Служба ресивера Windows Media Center	Вручну
87.	Служба відомостей про підключені мережі	Заборонено
88.	Служба списку мереж	Заборонено
89.	Служба технологій активації Windows	Вручну
90.	Служба сповіщення SPP	Вручну
91.	Служба сповіщення про системні події	Автоматичний
92.	Служба дистанційного керування Windows	Заборонено
93.	Служба сховища	Вручну

94.	Служба шифрування дисків BitLocker	Вручну
95.	Служба шлюзу рівня програми	Заборонено
96.	Служби криптографії	Автоматичний
97.	Служби віддалених робочих столів	Заборонено
98.	Смарт-картка	Вручну
99.	Зіставник кінцевих точок RPC	Автоматичний
100.	Засіб побудови кінцевих точок Windows Audio	Вручну
101.	Телефонія	Заборонено

Продовження таблиці з рекомендованими параметрами системних служб

№	Назва параметру	Значення параметру
102.	Теми	Вручну
103.	Тіньове копіювання тому	Вручну
104.	Видалений виклик процедур (RPC)	Автоматичний
105.	Віддалений реєстр	Автоматичний
106.	Посвідчення програми	Автоматичний
107.	Вузол системи діагностики	Вручну
108.	Вузол служби діагностики	Вручну
109.	Вузол універсальних PNP-пристроїв	Автоматичний
110.	Управління програмами	Автоматичний
111.	Управління сертифікатами та ключем працездатності	Вручну
112.	Інсталятор ActiveX (AxInstSV)	Вручну
113.	Інсталятор Windows	Вручну
114.	Інсталятор модулів Windows	Вручну
115.	Факс	Вручну
116.	Фонова інтелектуальна служба передачі (BITS)	Заборонено
117.	Центр забезпечення безпеки	Автоматичний
118.	Центр оновлення Windows	Вручну
119.	Шифрована файлова система (EFS)	Вручну

ДОДАТОК Д

Таблиця з рекомендованими параметрів файлової системи.

Папка або файл	Група користувачів	Рекомендований дозвіл	Застосовуються до	Метод успадкування
C:\Users\	Адміністратори	Повний доступ	Для цієї папки, її підпапок та файлів	Поширення
	Система	Повний доступ	Для цієї папки, її під-папок та файлів	
	Користувачі	Повний доступ	Для цієї папки, її підпапок та файлів	
C:\ProgramData\Microsoft\	Адміністратори	Повний доступ	Для цієї папки, її підпапок та файлів	Заміна
	Система	Повний доступ	Для цієї папки, її підпапок та файлів	
	Користувачі	Повний доступ	Для цієї папки, її підпапок та файлів	
%SystemDrive%\	Адміністратори	Повний доступ	Для цієї папки, її підпапок та файлів	Поширення
	Ті, що пройшли перевірку	Траверс папок/виконання файлів, вміст папки/читання даних, читання атрибутів, читання додаткових атрибутів, створення файлів/запис даних, створення папок/дозапис даних, запис атрибутів, запис додаткових атрибутів	Тільки для папок та файлів	

Продовження таблиці з рекомендованими параметрами файлової системи

Папка або файл	Група користувачів	Рекомендований дозвіл	Застосовуються до	Метод успадкування
	Система	Повний доступ	Для цієї папки, її підпапок та файлів	
	Користувачі	Читання та виконання	Для цієї папки, її підпапок та файлів	
%SystemDrive%\Windows\Speech\Engines\TTS	Адміністратори	Читання та виконання	Для цієї папки, її підпапок та фалів	
	Система	Читання та виконання	Для цієї папки, її підпапок та фалів	
	Користувачі	Читання та виконання	Для цієї папки, її підпапок та фалів	
	TrustInstaller	Повний доступ	Для цієї папки, її підпапок та фалів	
%PROGRAMDATA%\Microsoft\Windows\DRM	Усі	Траверс папок/виконання файлів, зміст папки/читання даних, читання атрибутів, читання додаткових атрибутів, створення файлів/запис даних, створення папок/дозапис даннях, запис атрибутів, запис додаткових атрибутів, видалення папок та файлів, читання дозволів, зміна дозволів, зміна власника	Тільки для цієї папки	

Продовження таблиці з рекомендованими параметрами файлової системи

Папка або файл	**Група користувачів**	**Рекомендований дозвіл**	**Застосовуються до**	**Метод успадкування**
	Система	Повний доступ	Тільки для цієї папки	
	Гість	Все Заборонено	Для цієї папки, її підпапок та файлів	
	Гості	Все Заборонено	Для цієї папки, її підпапок та файлів	
%PROGRAM DATA%\Microsoft\Windows\DRM\Cache	Усі	Траверс папок/виконання файлів, вміст папки/читання даних, читання атрибутів, читання додаткових атрибутів, створення файлів/запис даних, створення папок/дозапис даннях, запис атрибутів, запис додаткових атрибутів, видалення папок та файлів	Тільки для цієї папки	
		Повний доступ	Тільки для підпапок та файлів	
	Система	Повний доступ	Тільки для цієї папки	
	Гість	Все Заборонено	Для цієї папки, її підпапок та файлів	
	Гості	Все Заборонено	Для цієї папки, її підпапок та файлів	

Продовження таблиці з рекомендованими параметрами файлової системи

Папка або файл	Група користувачів	Рекомендований дозвіл	Застосовуються до	Метод успадкування
C:\windows\ installer	Адміністратори	Повний доступ	Для цієї папки, її підпапок та файлів	
	Усі	Читання та виконання	Для цієї папки, її підпапок та файлів	
	Система	Повний доступ	Для цієї папки, її підпапок та файлів	
C:\windows\system32\appmgmt	Адміністратори	Повний доступ	Для цієї папки, її підпапок та файлів	
	Усі	Повний доступ	Тільки для цієї папки	
%Systemroot%\config\ntuser.dat	Адміністратори	Повний доступ	Для цього файлу	
	Система	Повний доступ	Для цього файлу	
%Systemroot%\ config\sam	Адміністратори	Повний доступ	Для цього файлу	
	Система	Повний доступ	Для цього файлу	
%Systemroot%\config\security	Адміністратори	Повний доступ	Для цього файлу	
	Система	Повний доступ	Для цього файлу	
%Systemroot%\ config\software	Адміністратори	Повний доступ	Для цього файлу	
	Система	Повний доступ	Для цього файлу	
%Systemroot%\config\system	Адміністратори	Повний доступ	Для цього файлу	
	Система	Повний доступ	Для цього файлу	

ДОДАТОК Е

Таблиця з рекомендованими параметрами реєстру ОС

№	Назва параметру	Шлях	Значення	Формат	Значення
1.	Рівень захисту маршрутизації IP-джерела	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\	DisableIPSourceRouting	DWORD (32 біти) REG_DWORD	0
2.	Дозволити автоматичне виявлення неробочих мережних шлюзів	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\	DeadGWDetectDefault	DWORD (32 біти) REG_DWORD	0
3.	Дозволити переадресацію ICMP для перевизначення створених маршрутів OSPF	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\	EnableICMPRedirect	DWORD (32 біти) REG_DWORD	0
4.	Вимкнути автозапуск для всіх дисків	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\	NoDriveTypeAutoRun	DWORD (32 біти) REG_DWORD	FF
5.	Дозволити комп'ютеру не створювати імена файлів у форматі 8.3	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\	NtfsDisable8dot3NameCreation	DWORD (32 біти) REG_DWORD	1

ДОДАТОК Є

Текст скрипту

```
$UserPassword = ConvertTo-SecureString "Pa$$word!!" -AsPlainText -Force
New-LocalUser "User1" -Password $UserPassword -FullName "User1"
Set-LocalUser -Name User1 -Password $UserPassword –Verbose
Add-LocalGroupMember -Group 'Пользователи' -Member ('User1') –Verbose
$UserPassword = ConvertTo-SecureString "Pa$$word!!" -AsPlainText -Force
New-LocalUser "User2" -Password $UserPassword -FullName "User2"
Set-LocalUser -Name User2 -Password $UserPassword –Verbose
Add-LocalGroupMember -Group 'Пользователи' -Member ('User2') –Verbose
$UserPassword = ConvertTo-SecureString "Pa$$word!!" -AsPlainText -Force
New-LocalUser "User3" -Password $UserPassword -FullName "User3"
Set-LocalUser -Name User3 -Password $UserPassword –Verbose
Add-LocalGroupMember -Group 'Пользователи' -Member ('User3') –Verbose
[adsi]$user = "WinNT://./User1,user"
$user.SetPassword("Qwerty777")
$user.SetInfo()
[adsi]$user = "WinNT://./User2,user"
$user.SetPassword("Qwerty777")
$user.SetInfo()
[adsi]$user = "WinNT://./User3,user"
$user.SetPassword("Qwerty777")
$user.SetInfo()
New-Item -Path 'D:\User1' -ItemType Directory
New-Item -Path 'D:\User2' -ItemType Directory
New-Item -Path 'D:\User3' -ItemType Directory
$path = 'd:\User1'
$acl = Get-ACL -Path $path
$acl.SetAccessRuleProtection($True, $True)
Set-Acl -Path $path -AclObject $acl
$path = 'd:\User2'
$acl = Get-ACL -Path $path
$acl.SetAccessRuleProtection($True, $True)
Set-Acl -Path $path -AclObject $acl
$path = 'd:\User3'
$acl = Get-ACL -Path $path
$acl.SetAccessRuleProtection($True, $True)
Set-Acl -Path $path -AclObject $acl
Remove-NTFSAccess -Path d:\User1 -Account 'BUILTIN\Пользователи' -AccessRights
ReadAndExecute -PassThru
Remove-NTFSAccess -Path d:\User2 -Account 'BUILTIN\Пользователи' -AccessRights
ReadAndExecute -PassThru
Remove-NTFSAccess -Path d:\User3 -Account 'BUILTIN\Пользователи' -AccessRights
ReadAndExecute -PassThru
Add-NTFSAccess -Path D:\User1 -Account 'User1' -AccessRights 'Fullcontrol' -PassThru
Add-NTFSAccess -Path D:\User2 -Account 'User2' -AccessRights 'Fullcontrol' -PassThru
Add-NTFSAccess -Path D:\User3 -Account 'User3' -AccessRights 'Fullcontrol' -
PassThruNew-ItemProperty -Path HKLM:System\CurrentControlSet\Services\Tcpip\Parameters
-Name "DisableIPSourceRouting" -Value ”0” -PropertyType "Dword"
```

```
New-ItemProperty -Path HKLM:System\CurrentControlSet\Services\Tcpip\Parameters -Name "DeadGWDetectDefault" -Value ”0” -PropertyType "Dword"
New-ItemProperty -Path HKLM:System\CurrentControlSet\Services\Tcpip\Parameters -Name "EnableICMPRedirect" -Value ”0” -PropertyType "Dword"
New-ItemProperty -Path HKLM:SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer -Name "NoDriveTypeAutoRun" -Value ”255” -PropertyType "Dword"
Set-ItemProperty -Path HKLM:\System\CurrentControlSet\Control\FileSystem -Name NtfsDisable8dot3NameCreation -Value 1
```