

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії

Кафедра комп'ютерних інформаційних технологій

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

Савченко А.С.

“ ” 2020 р.

**ДИПЛОМНА РОБОТА**  
**(ПОЯСНЮВАЛЬНА ЗАПИСКА)**

*ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ*  
**“МАГІСТРА”**

**ЗА СПЕЦІАЛІЗАЦІЄЮ “ІНФОРМАЦІЙНІ УПРАВЛЯЮЧІ СИСТЕМИ ТА  
ТЕХНОЛОГІЇ (ЗА ГАЛУЗЯМИ)”**

**Тема:** “Система інформаційної безпеки підприємства від кіберзагроз”

**Виконавець:** Харьков Олександр Сергійович

**Керівник:** к.т.н., доцент Куклінський Максим Володимирович

**Нормоконтролер:** Райчев І.Е.

**Київ 2020**

# НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії

Кафедра Комп'ютерних інформаційних технологій

Галузь знань, спеціальність, спеціалізація: 12 “Інформаційні технології”, 122 “Комп'ютерні науки”, “Інформаційні управляючі системи та технології (за галузями)”

ЗАТВЕРДЖУЮ  
Завідувач кафедри

\_\_\_\_\_ Савченко А.С.  
“ ” \_\_\_\_\_ 2020 р.

## ЗАВДАННЯ

на виконання дипломної роботи студента

Харькова Олександра Сергійовича

- 1. Тема роботи:** “Система інформаційної безпеки підприємства від кіберзагроз”.  
Затверджена наказом ректора від “ 2 ” жовтня 2020 року за № 1891 ст.
- 2. Термін виконання роботи:** з 5 жовтня 2020р. до 31 грудня 2020р.
- 3. Вихідні данні до роботи:** дослідження інформаційної безпеки підприємства, види та системи захисту інформації. Види витоку інформації. Несанкціоноване заволодіння інформацією. Сучасні методи для забезпечення захисту інформації. Сервери на базі Windows Server. Доменні служби Active Directory.
- 4. Зміст пояснювальної записки:** 1) Розроблено технологію комплексного забезпечення захисту інформації. 2) Створено концепцію доменних політик 3) Запроваджено технічне забезпечення. 4) Визначено основні способи доменного захисту. 5) Розгорнуто технологію доменних служб Active Directory, за допомогою яких реалізовується управління обліковими записами, комп'ютерами, політиками та правилами.
- 5. Перелік обов'язкового ілюстративного матеріалу:** теоритичні та практичні матеріали, рисунки, реферат та слайди презентації доповіді у PowerPoint.

## 6. Календарний план-графік

<i>№ з/п</i>	<i>Завдання</i>	<i>Термін виконання</i>	<i>Підпис керівника</i>
1.	Розгляд загроз інформаційної безпеки	5.10.20 – 10.10.20	
2	Розгляд методів захисту та запобігання витоку інформації.	11.10.20 – 15.10.20	
3	Пошук існуючих систем захисту інформації.	16.10.20 – 20.10.20	
4	Розгляд та дослідження систем захисту інформації на предмет її витоку.	21.10.20 – 25.10.20	
5	Побудова плану вирішення проблеми витоку інформації.	26.10.20 – 31.10.20	
6	Розробка концепції та роботи системи.	1.11.20 – 09.11.20	
7	Установка Windows Server, доменних служб Active Directory та їх налагодження.	10.11.20 – 25.11.20	
8	Структурування інформації та написання розділів.	26.11.20 – 5.12.20	
9	Створення доповіді та слайдів.	6.12.20 – 14.12.20	
10.	Оформлення та друк пояснювальної записки дипломної роботи.	15.12.20 – 20.12.20	

7. Дата видачі завдання \_\_\_\_\_

Керівник дипломної роботи \_\_\_\_\_ Райчев І.Е. .

*Завдання* *прийняв* *до* *виконання*

(підпис випускника)

(ПІБ)

## РЕФЕРАТ

Пояснювальна записка до дипломної роботи на тему "Система інформаційної безпеки підприємства від кіберзагроз". Містить 96 сторінок, 50 рисунків та 12 наукових джерел. Дипломна робота складається з вступу, трьох розділів та двох додатків А і Б.

**Об'єкт дослідження:** система інформаційної безпеки на підприємстві.

**Мета роботи:** дослідити сучасні технології систем інформаційного захисту від несанкціонованого зовнішнього втручання. Побудувати систему для забезпечення інформаційного захисту підприємства.

**Методи дослідження:** розробка системи інформаційної безпеки для забезпечення захисту інформації на підприємстві, запровадження правил та політик для захисту інформації, запровадження безпеки працівників та доступу до ресурсів.

**Результати магістерської роботи:** На базі віртуальної машини Hyper-V, встановив та налаштував Windows Server 2016 з ролями Active Directory, а також з суміжними ролями і установив компоненти для шифрування диску BitLocker. Налаштував політику паролів для доменних облікових записів. У кінцевому результаті вийшла система захисту облікових записів, корпоративної техніки та обмеження доступу до ресурсів, яка може керуватися адміністраторами.

**КЛЮЧОВІ СЛОВА:** ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, БЕЗПЕКА ДАНИХ, СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКА, КІБЕР АТАКА, КІБЕЗЗАХИСТ, ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, ДОМЕН, ОБЛІКОВИЙ ЗАПИС, WINDOWS SERVER.

## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ.**

ЗІ – захист інформації

ІБ – інформаційна безпека

КА – кібератака

КЗ – кіберзахист

ІТ – інформаційні технології

НСД – не санкціонований доступ

ОС – операційна система

ТЗІ – технічний захист інформації

КК – ключ-карта

IS - IT Security

WS – Windows Server

# ЗМІСТ

<b>ВСТУП.....</b>	<b>8</b>
<b>РОЗДІЛ 1. ЗАГРОЗА ІНФОРМАЦІЇ ТА ЇЇ ЗАХИСТ.....</b>	<b>10</b>
1.1 Загрози інформації.....	10
1.1.1 Загроза інформації в інтернеті.....	10
1.1.2 Відомості про кібератаку та її види.....	11
1.2 Захист інформації.....	22
1.2.1 Основні поняття захисту інформації.....	22
1.2.2 Кібербезпека та її види.....	23
1.3 Засоби захисту інформації.....	29
<b>РОЗДІЛ 2. СТРУКТУРА ТА ВИДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ.....</b>	<b>37</b>
2.1 Інформаційна безпека на підприємстві.....	37
2.1.1 Система захисту інформації, її функції та методи.....	37
2.1.2. Запровадження норм ІБ організації.....	39
2.2. Управління вразливістю.....	41
2.2.1. Етапи виявлення вразливостей.....	41
2.2.2. Процес аналізу вразливостей.....	42

2.2.3.	Етапи	усунення
вразливостей.....	43	
2.2.4.		Моніторинг
подій.....	45	
3.3	Реалізація	та вимоги до безпеки
даних.....	46	
3.3.1	Безпека даних.....	46
3.3.2	Вимоги.....	48
3.3.3	Вимоги до інфраструктури. ....	49
3.3.4	Вимоги щодо управління доступом.....	49
3.4	Принцип та поряд створення системи кібербезпеки.....	50
<b>РОЗДІЛ 3. НАЛАГОДЖЕННЯ РОБОТИ WINDOWS SERVER ТА</b>		
<b>ДОМЕННОЇ СЛУЖБИ ACTIVE DIRECTORY.....</b>		
3.1	Домен, доменні облікові записи та керування ними.....	56
3.1.1	Політика домену.....	56
3.1.2.	Вимоги до пароля.....	57
3.1.3.	Вимоги до техніки.....	62
3.2	Інсталювання та налаштування Windows Server.....	65
3.3	Розгортання	Active
Directory.....	71	
3.4.	Реалізація безпеки підприємства за допомогою доменних правил, політик, облікових записів в Active	
Directory.....	78	
3.4.1	Налаштування	політики
паролів.....	78	

3.4.2 Створення підрозділів, облікового запису та додання груп до нього.....	79
3.4.3. Створення та додання комп'ютера до домену.....	83
<b>ВИСНОВКИ.....</b>	<b>87</b>
<b>СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ.....</b>	<b>88</b>
<b>Додаток А.....</b>	<b>89</b>
<b>Додаток Б.....</b>	<b>93</b>

## ВСТУП

На сьогоднішній день інформаційні технології (ІТ) мають дуже швидкий рівень росту і більшість людей не замислюються над тим, яку цінність несе в собі інформація. Тому вона є однією з основних цілей кіберзлочинців. За допомогою інформації, яку було отримано у разі нападу, злочинці можуть заволодіти вашими логінами, паролями, документами, коштами та інше.

Кожного дня, люди використовують різні види техніки (комп'ютери, ноутбуки, планшети, телефони, тощо), які мають доступ до інтернет середовища та інтенсивно переглядають різні види інформації, тим самим вже надаючи певні дані про себе. Адже, веб-сайти збирають конфіденційну інформацію так тонко, що ми, навіть, не знаємо, що саме їм відомо. Переходячи за посиланням до будь-якого інтернет ресурсу, ми даємо згоду на обробку наших даних та даних нашого комп'ютера або іншої техніки. Реєструючись на сайті користувач надає про себе ще більше інформації. Зі сторони ресурсу на якому проходить реєстрація, це вид безпеки самого ресурсу та інформації на ньому. Проте, все ж слід бути уважним переходячи за посиланням, заповнюючи форми з даними про себе та звернути увагу на те, як в подальшому ці дані можуть оброблятися.

Інформаційна безпека стосується захисту життєво важливих інтересів людини. Неправдива, неповна, невчасна інформація може нанести шкоду.

Перш за все, необхідно знати та дотримуватися основних правил користування інтернетом. Це допоможе уникнути не бажаних проблем з технікою, різних шляхів витоку інформації. Тому необхідно дотримуватись таких правил користування інтернетом, а саме:

- 1) Використовувати надійний пароль. Комбінувати букви, цифри та інші символи.
- 2) Нікому не повідомляти свої дані для входу.
- 3) Перевіряти достовірність та надійність джерела.

- 4) Не викладайти особисту, конфіденційну інформацію про себе, своїх рідних, друзів і знайомих в Інтернеті.
- 5) Не поширювати в Інтернеті контент незаконного або непристойного змісту.
- 6) Не переходити за посиланнями, які відправленні від незнайомих та мають підозрілу назву.

Дотримуючись цих правил, перебування в інтернеті вже буде більш надійне та значно зменшує можливість загрози інформації та техніки, що вже є кібербезпекою.

Кібербезпека важлива, оскільки урядові, військові, корпоративні, фінансові та медичні організації збирають, обробляють та зберігають безпрецедентні обсяги даних на комп'ютерах та інших пристроях. Значна частина цих даних може бути конфіденційною інформацією, будь то інтелектуальна власність, фінансові дані, особиста інформація або інші типи даних, для яких несанкціонований доступ або викриття можуть мати негативні наслідки. Організації передають конфіденційні дані через мережі та на інші пристрої в процесі ведення бізнесу, а кібербезпека описує дисципліну, присвячену захисту цієї інформації та систем, що використовуються для її обробки або зберігання. Зі зростанням обсягу та витонченості кібератак, компаніям та організаціям, особливо тим, яким доручено захищати інформацію, що стосується національної безпеки, охорони здоров'я чи фінансової документації, потрібно вжити заходів для захисту своєї конфіденційної інформації про бізнес та персонал. Вже в березні 2013 року найвищі представники розвідки країни застерегли, що кібератаки та цифрове шпигунство є основною загрозою національній безпеці, затемнюючи навіть тероризм.

## РОЗДІЛ 1. ЗАГРОЗА ІНФОРМАЦІЇ ТА ЇЇ ЗАХИСТ

### 1.1. Загрози інформації

#### 1.1.1. Загроза інформації в інтернеті

На сьогоднішній день, майже кожна людина використовує інтернет для пошуку інформації про щось або когось. Безпека даних є важливим аспектом повсякденного життя. Тому необхідно знати якого роду атак може підвергнутись користувач та техніка, яку він використовує. Слід зазначити, що будь-яка техніка має широкий спектр можливостей про що звичайні користувачі, мало що знають. Це також може стати причиною витоку або захоплення інформації. Тому, для кращого розуміння методів захисту комп'ютерної системи слід спочатку ознайомитися з тим, що таке кібератаки та які вони бувають.

Відповідно до властивостей інформації, виділяють такі загрози:

- загрози цілісності:
  - знищення;
  - модифікація;
- загрози доступності:
  - блокування;
  - знищення;
- загрози конфіденційності:
  - несанкціонований доступ (НСД);
  - витік;
  - розголошення.

Кафедра КІТ (47)				НАУ 20 27 44 000 ПЗ			
Виконав	Харьков О.С.			ЗАГРОЗА ІНФОРМАЦІЇ ТА ЇЇ ЗАХИСТ.	Літера	Аркуш	Аркушів
Керівник	Куклінський М.В.					10	27
Консульт					УС-211М 12211		
Н.контр.	Райчев І.Е.						

### 1.1.2. Відомості про кібератаку та її види

Хакерська атака або кібератака — це спроба реалізації загрози, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами або на виведення системи з ладу. Під атакою на інформаційну систему розуміють послідовність дій, які приводять до реалізації загроз інформаційним ресурсам, шляхом використання вразливостей цієї інформаційної системи.

Такі небезпеки зазвичай можна віднести до однієї з наступних категорій:

1. Чорний хід (Backdoor).
2. Dos-атака.
3. Атаки безпосереднього доступу.
4. Троянські програми.
5. Мережеві черв'яки.
6. Вірус.
7. Шпигунські програми.
8. Спам.
9. Перехоплення каналу зв'язку (Man-in-the-Middle).
10. Фішинг.

Це основні типи кібератак, які на даний момент дуже поширені у світі. Проте, слід детальніше розглянути, що вони собою представляють.

1. Чорний хід, або бекдор у комп'ютерній системі, криптосистемі чи алгоритмі — це метод обходу звичайного процесу аутентифікації, забезпечення віддаленого доступу до комп'ютера, одержання доступу до незашифрованої інформації тощо. Бекдори можуть відбуватися у формі встановлення програми або змін у роботі існуючої програми чи фізичного пристрою.

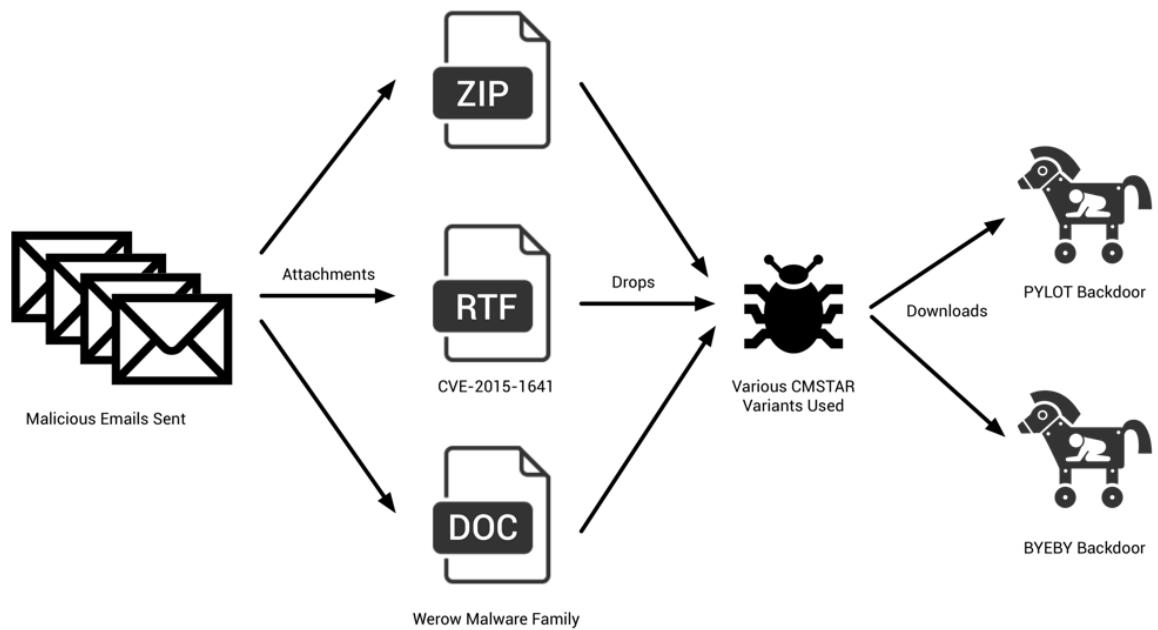


Рис.1.1. Схематичний приклад бекдору

2. На відміну від інших атак, DoS-атаки застосовуються не для одержання несанкціонованого доступу чи керування системою, а для того, щоб унеможливити роботу останньої. В результаті атаки акаунт окремої жертви може виявитися заблокованим унаслідок умисного багаторазового введення невірного пароля, або ж унаслідок перевантаження мережі буде заблоковано усіх її користувачів. На практиці цьому виду атак дуже складно перешкодити, оскільки для цього необхідно проаналізувати поведінку цілих мереж, а не лише поведінку невеличкої частини коду.

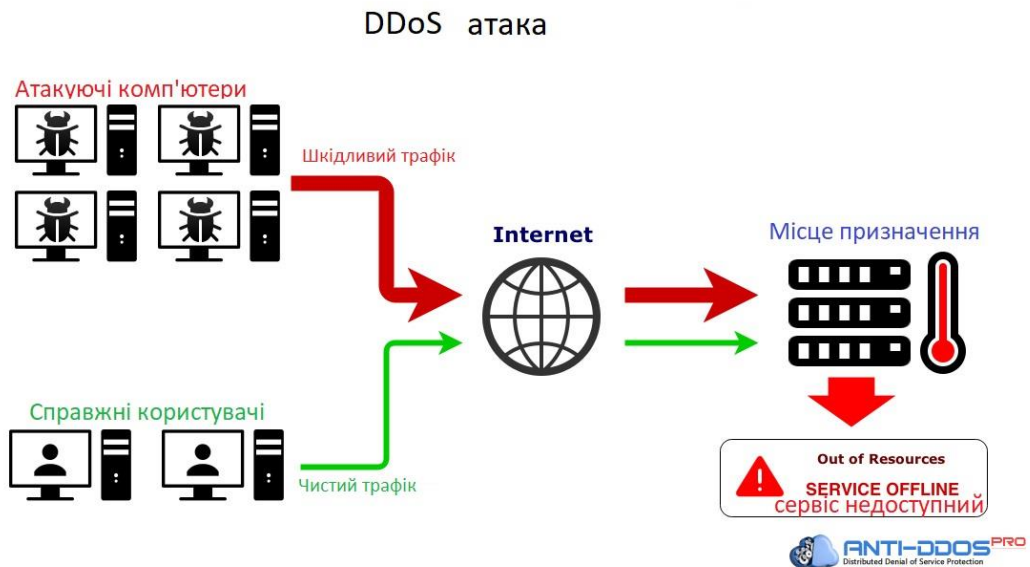


Рис.1.2. Схематичний приклад Dos-атаки

3. Атаки безпосереднього доступу – це вид доступу, коли користувач, який одержав несанкціонований доступ до комп'ютера, може встановлювати на ньому різні типи програмного (у тому числі модифікації операційних систем, віруси, програмні кілогтери) та апаратного (апаратні кілогтери, пристрої для прослуховування) забезпечення, внаслідок чого безпека системи опиниться під загрозою. Кілоггер – програма або пристрій, що реєструє кожне натискання клавіш на клавіатурі. Такий порушник може також легко скачати великі об'єми даних на зовнішні носії. Ще одним видом атак безпосереднього доступу є завантаження операційної системи з зовнішнього носія із наступним зчитуванням даних з жорсткого диску. Цей різновид атак є зазвичай єдиним методом атакування комп'ютерів, що не підключені до інтернету.



Рис.1.3. Схематичний приклад атаки безпосереднього доступу

4. Троянські програми або трояни – це різновид шкідливих програм, які завдають шкоди системі, маскуючись під якісь корисні додатки. Троянські програми можуть застосовувати в якості прикриття знайомі користувачеві додатки, з якими він працював і раніше, до появи в комп'ютері «троянського коня». При іншому підході в повній відповідності з древньою легендою троянська програма приймає вид нового додатку, який намагається зацікавити користувача - жертву якимись своїми нібито корисними функціями.



Рис.1.4. Приклад троянської програми на комп'ютері

5. Мережеві черв'яки – це програми, здатні до самостійного поширення своїх копій серед вузлів в межах локальної мережі, а також з глобальних зв'язків, переміщаючись від одного комп'ютера до іншого без будь-якої участі в цьому процесі користувачів мережі. Оскільки більшість мережевих черв'яків передаються у вигляді файлів, основним механізмом їх поширення є мережні служби, засновані на файловому обміні. Так, черв'як може розсилати свої копії по мережі у вигляді вкладень в повідомлення електронної пошти або шляхом розміщення посилань на заражений файл на якому-небудь веб-сайті. Однак існують і інші різновиди черв'яків, які для своєї експансії використовують складніші прийоми, наприклад, пов'язані з помилками («дірками») у програмному забезпеченні.

Головна мета і результат діяльності хробака полягає в тому, щоб передати свою копію на максимально можливе число комп'ютерів. При цьому для пошуку комп'ютерів - нових потенційних жертв - черв'яки задіють вбудовані в них кошти. Типова програма-черв'як не видаляти і не спотворює користувацькі та системні файли, які не перехоплює електронну пошту користувачів, не псує вміст баз даних, а завдає шкоди атакували комп'ютер шляхом споживання їх ресурсів. Якщо черв'як володіє можливістю повторного зараження, то число його копій зростає лавиноподібно, і шкідливі програми все більш і більш завантажують процесор, захоплюючи нові області пам'яті, відбираючи пропускну здатність мережевих з'єднань, поки, нарешті, програми легальних користувачів не втратять можливість виконуватися.

При створенні типового мережного хробака хакер, насамперед, визначає перелік мережевих вразливостей, які він збирається використовувати для проведення атак засобами створюваного хробака. Такими уразливими можуть бути як відомі, але не виправлені на деяких комп'ютерах помилки в програмному забезпеченні, так і поки невідомі нікому помилки, які виявив сам хакер. Чим ширше перелік вразливостей і чим більше вони поширені, тим більше вузлів може бути уражено даними хробаком.

Хробак складається з двох основних функціональних компонентів: атакуючого блоку і блоку пошуку цілей.

- Атакуючий блок складається з декількох модулів (векторів атаки), кожен з яких розрахований на поразку конкретного типу вразливості. Цей блок відкриває «вхідні двері» атакується хоста і передає через неї свою копію.
- Блок пошуку цілей (локатор) збирає інформацію про вузли мережі, а потім на підставі цієї інформації визначає, які з досліджених вузлів володіють тими уразливими, для яких хакер має засоби атаки.

Ці два функціональних блоку є обов'язковими і присутні в реалізації будь-якої програми-хробака. Деякі хробаки навантажені їх творцями та іншими допоміжними функціями, про які ми скажемо пізніше.

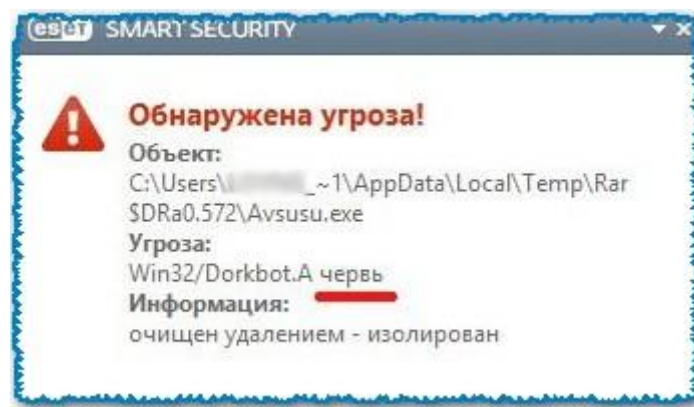


Рис.1.5. Приклад програми-хробака на комп'ютері

6. Вірус – це шкідливий програмний фрагмент, який може впроваджуватися в інші файли. Прагнення зловмисника зробити код вірусу якомога коротшим часто обмежує логіку роботи вірусу дуже простими рішеннями, які іноді призводять до дуже руйнівних наслідків. Так, наприклад, один з реально

існуючих вірусів, що складається всього з 15 байтів, записував свою копію поверх інших файлів в початок кожного сектора диска, в результаті система дуже швидко терпіла крах. Деяким розрадою в такому і подібних йому випадках є те, чого одночасно з крахом комп'ютера припиняє своє існування і вірус.

Вірус може впроваджувати свої фрагменти в різні типи файлів, у тому числі у файли виконуваних програм. При цьому можливі самі різні варіанти: заміщення коду, коли розмір інфікованого файлу не змінюється, вставка вірусного коду цілком на початок або кінець вихідної програми, заміна фрагментів програмного коду фрагментами вірусу з перестановкою заміщених фрагментів і без перестановки і т. д. Більш того, код вірусу може бути зашифрований, щоб утруднити його виявлення антивірусними програмами.

На відміну від черв'яків, віруси (так само як і троянські програми) не містять в собі вбудованого механізму активного поширення по мережі, вони здатні розмножуватися своїми силами тільки в межах одного комп'ютера. Як правило, передача копії вірусу на інший комп'ютер відбувається за участю користувача. Наприклад, користувач може записати свій файл, заражений вірусом, на мережевий файловий сервер, звідки той може бути скопійований усіма користувачами, що мають доступ до даного сервера. Користувач може також передати іншому користувачеві знімний носій із зараженим файлом або послати такий файл по електронній пошті. Тобто саме користувач є головною ланкою в ланцюжку розповсюдження вірусу за межі свого комп'ютера. Тяжкість наслідків вірусного зараження залежить від того, які шкідливі дії були запрограмовані у вірусі зловмисником. Це можуть бути дрібні, але дратівливі незручності (уповільнення роботи комп'ютера, зменшення розмірів доступної пам'яті, трата робочого часу на переустановлення додатків) або серйозні порушення безпеки, такі як витік конфіденційних даних, руйнування системного програмного забезпечення, часткова або повна втрата працездатності комп'ютерної мережі.



Рис.1.6. Приклад віруса на комп'ютері

7. Шпигунські програми – це такий тип шкідливих програм, які таємно встановлюються зловмисниками на комп'ютери нічого не підозрюють користувачів, щоб відстежувати і фіксувати всі їхні дії. Здебільшого це роблять віддалено. У число таких дій може входити введення імені та пароля під час логічного входу в систему, відвідування тих чи інших веб-сайтів, обмін інформацією з зовнішніми і внутрішніми користувачами мережі та ін., Та ін. Зібрана інформація пересилається зловмисникові, який застосовує її в злочинних цілях.



Рис.1.7. Приклад шпигунської програми на комп'ютері

8. Спам – це атака, виконана шляхом зловживання можливостями електронної пошти. Враховуючи ту важливу роль, яку відіграє електронна пошта в роботі сучасних підприємств і організацій, можна зрозуміти, чому спам, дезорганізують роботу цієї служби, став розглядатися в останні роки як одна із суттєвих загроз безпеці.

Спам забирає час і ресурси на перегляд і видалення непотрібних повідомлень, при цьому помилково можуть бути видалені листи з критично важливою інформацією, особливо велика ймовірність цього при автоматичної фільтрації листів. Стороння пошта, яка нерідко становить 70% одержуваних повідомлень, не тільки знижує ефективність роботи підприємства, а й часто служить засобом впровадження шкідливих програм. Крім того, спам часто є елементом різних шахрайських схем, жертвами яких можуть стати як окремі співробітники, так і підприємство в цілому.



Рис.1.8(1) та Рис.1.8(2). Приклади спаму

9. Перехоплення каналу зв'язку – вид атаки, коли зломисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї інформації, що передається. При отриманні доступу на такому рівні зломисник може модифікувати інформацію потрібним йому чином, щоб досягти своєї цілі. Мета такої атаки – незаконне отримання, крадіжка або фальсифікування переданої

інформації, або ж отримання доступу до ресурсів мережі. Такі атаки вкрай складно відстежити, оскільки зазвичай зломисник знаходиться всередині організації.

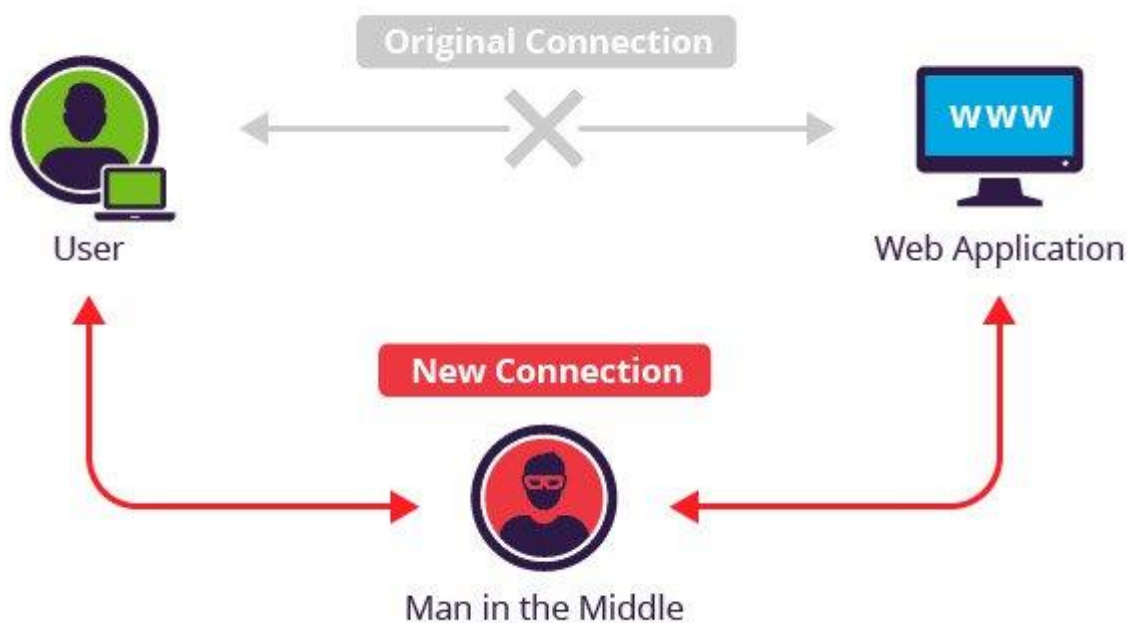


Рис.1.9. Приклад перехоплення каналу зв'язку

10. Фішинг – це спосіб виловлювання інформації різними методами. Мета фішингу полягає у отриманні доступу до конфіденційної інформації користувача (логінів, паролів, даних платіжних карток, тощо).

Фішингові повідомлення, зазвичай, приходять на електронну пошту і спонукають до негайних дій, не залишаючи часу на роздуми. Шахрайські повідомлення найчастіше надходять від імені відомих брендів, знайомих, друзів чи банків та впливають на емоційне сприйняття інформації. Вони можуть:

- викликати тривогу за стан своїх банківських рахунків;
- обіцяти грошові вигоди з докладанням мінімальних зусиль (лотереї, повідомлення про можливий неочікуваний спадок тощо);
- пропонувати фінансові угоди з неймовірно вигідними умовами;

- закликати до пожертв після новин про стихійні лиха чи ще щось або ж звертатися до вашого милосердя, пропонуючи допомогти хворим дітям.

Фішинг може використовувати не лише розсилку листів на електронні адреси, але й онлайн-оголошення, результати пошукових систем, імітацію «впливаючих» вікон із системними повідомленнями, смс-повідомлення розповсюдження інформації у соціальних мережах.

Не натискайте на подібні оголошення. Перш ніж робити якісь дії, перевірте інформацію. Задля простої і швидкої перевірки – рідним чи друзям можна зателефонувати, благодійні фонди чи банки мають офіційні контакти, через які можна уточнити будь-яку інформацію, а якщо листи від незнайомих вам осіб чи джерел – просто ігнорувати такі листи.



Рис.1.10. Приклад фішингу

Отже, існує чимало видів ЗІ та ще більше способів їх реалізації. Проте, для кожного виду ЗІ існує якийсь спосіб захисту.

## 1.2. Захист інформації

### 1.2.1. Основні поняття захисту інформації

Захист інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

Захист інформації ведеться для підтримки таких властивостей інформації як: цілісність, конфіденційність, доступність. Ці критерії мають свої аспекти захисту інформації:

- Конфіденційність – захист від несанкціонованого ознайомлення з інформацією.
- Цілісність – захист інформації від несанкціонованої модифікації.
- Доступність – захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію.

Кожен вид захисту інформації забезпечує окремі аспекти ІБ:

- Технічний – забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, маршрутизатори, фаєрволи, смарт-карти, токени тощо):
  - попередження витоку по технічним каналам;
  - попередження блокування ;
- Інженерний – попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація).

- Криптографічний – попереджує доступ за допомогою математичних перетворень повідомлення :
  - попередження несанкціонованої модифікації ;
  - попередження НС розголошення.
- Організаційний – попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів.

Захист інформації від її витоку технічними каналами зв'язку забезпечується такими засобами та заходами:

- Використанням екранованого кабелю та прокладка проводів та кабелів в екранованих конструкціях.
- Встановленням на лініях зв'язку високочастотних фільтрів;
- Побудовою екранованих приміщень («капсул»);
- Використанням екранованого обладнання;
- Встановленням активних систем зашумлення;
- Створенням контрольованої зони.

### **1.2.2. Кібербезпека та її види**

Кібербезпека - це практика захисту комп'ютерів, серверів, мобільних пристроїв, електронних систем, мереж та даних від зловмисних атак. Це також відомо як безпека інформаційних технологій або електронна інформаційна безпека. Інформаційна безпека (ІБ) – це безпека інформації, зазвичай організації чи компанії, у тому числі в ІТ системах. Кібербезпека є частиною ІБ будь-якої організації.

Безпека мережі – це заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів.

Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкційований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. Мережева безпека містить у собі дозвіл на доступ до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ID і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і програм у рамках своїх повноважень.

Мережева безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами. Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу. Мережева безпека бере участь в організаціях, підприємствах та інших типів закладів. Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.

Принципи забезпечення інформаційної безпеки містять: законність, баланс інтересів особи, суспільства і держави; комплексність; системність; інтеграція з міжнародними системами безпеки; економічна ефективність.

Неможливо створити систему, захист якої не можна буде зламати, основним принципом може бути створення такого механізму захисту, вартість взламу якого буде дорожчою за інформацію, яку можна отримати. Тому необхідним є впровадження програмних засобів безпеки, які вмонтовані до складу програмного забезпечення системи і є потрібними для виконання функцій захисту. За словами експерта з кібербезпеки Дмитра Ганжелю: "Усунення наслідків кібератак часто обходиться в кілька разів дорожче, аніж профілактика боротьби з ними." В сучасних умовах, не гарантуючи належний захист

інформації, не можливо забезпечити стабільний економічний розвиток, як окремого підприємства, так і держави.

Дивлячись на кількість можливих атак, починаєш усвідомлювати, що є дуже багато способів заволодіння сторонньою інформацією і як важко її захистити. Однак, є методи для виявлення атак на систему.

Атаки на інформаційні ресурси системи та її послуги, можна виявити або знизити ризики їх реалізації, знаючи характерні ознаки несанкціонованих дій (НСД), а саме [3] присутність повтору певних подій у системі:

- неправильні або невідповідні встановленим процесам поточні ситуації та команди;
- використання вразливостей;
- невідповідні параметри мережного трафіка;
- непередбачені атрибути;
- не пояснені проблеми;
- додаткові знання про порушення.

Стандартні засоби захисту інформаційних ресурсів системи (міжмережні екрани, сервери аутентифікації, системи розмежування доступу й т.п.) використовують у своїй роботі одну або дві ознаки, у той час як спеціалізовані системи виявлення атак, впроваджують для ідентифікації несанкціонованих дій практично весь зазначений перелік.

Також, кібератаки можна виявити по етапам, таких процесів:

Перший етап – це збір інформації про атакуючу систему та її параметри. Він включає такі дії як, визначення мережної топології, типу й версії операційної системи вузла, що атакує, а також належність доступних мережних й інших сервісів і т.п. Ці дії реалізуються різними методами.

Другий етап – вивчення оточення. На цьому етапі порушник досліджує мережну інфраструктуру з урахуванням подальшої реалізації передбаченої загрози.

Третій етап – ідентифікація топології мережі. Можна назвати два методи визначення топології мережі (network topology detection), використовуваних злоумисниками: "зміна TTL" ("TTL modulation") і "запис маршруту" ("record route").

Четвертий етап – ідентифікація вузлів. Ідентифікація вузла (host detection), як правило, здійснюється шляхом посилки за допомогою утиліти ping команди ECHO\_REQUEST протоколу ICMP. Відповідне повідомлення ECHO\_REPLY говорить про те, що вузол доступний.

П'ятий етап – ідентифікація сервісів або сканування портів. Ідентифікація сервісів (service detection), як правило, здійснюється шляхом виявлення відкритих портів (port scanning). Такі порти дуже часто пов'язані із сервісом системи, заснованим на протоколах TCP або UDP (див. Додаток А).

Шостий етап – ідентифікація операційної системи. Основний механізм вилученого визначення ОС (OS detection) - аналіз відповідей на запити, що враховують різні реалізації TCP/IP-стека в різних операційних системах.[2,3,4].

Сьомий етап – визначення вразливостей вузла. На цьому кроці злоумисник за допомогою різних автоматизованих засобів або вручну визначає уразливості, які можуть бути використані для реалізації атаки. Прикладом таких автоматизованих засобів можуть бути використані Shadow Security Scanner, nmap, Retina програми і т.д.

Восьмий етап – реалізація атаки. Із цього моменту починається спроба доступу до атакуючого вузлу. При цьому доступ може бути як безпосередній,

тобто проникнення на вузол, так й опосередкований, наприклад, при реалізації атаки типу "відмова в обслуговуванні".

Дев'ятий етап – завершення атаки. Етапом завершення атаки є приховування несанкціонованих дій з боку зловмисника. Реалізується дана дія, шляхом видалення відповідних записів з журналів реєстрації й інших дій, що повертають атаковану систему у початковий стан.

Підсистема ідентифікації атак є найважливішим компонентом у будь-якій системі виявлення НСД. Ефективність роботи всієї інформаційної системи безпосередньо залежить від цих процесів та у загальному випадку використовує три широко відомих методи для розпізнавання атак [4].

- Сигнатурний метод, заснований на використанні шаблонів сигнатур (pattern-based signatures), що характеризують атаку або іншу підозрілу діяльність. Дані сигнатури містять деякі ключові слова або вирази, виявлення яких і свідчить про атаку.
- Сигнатурний метод, заснований на контролі частоти подій або перевищенні граничної величини. Дані сигнатури описують ситуації, коли протягом деякого інтервалу часу відбуваються події, число яких перевищує задані заздалегідь показники.
- Виявлення аномалій. Даний сигнатур метод дозволяє виявляти події, що відрізняються від попередньо заданих характеристик стандартної роботи інформаційної системи.

Щодо захисту комп'ютеру, існує багато шляхів захисту, серед яких є методи, що ґрунтуються на використанні безпечних операційних систем та апаратного забезпечення, здатного захистити комп'ютерну систему.

Згідно зі слів експертів з кібербезпеки можна виділити такі методи захисту:

- безпечна побудова серверної частини
- здійснювати регулярне оновлення всіх елементів інфраструктури
- робити тестування навантаження

- проводити аналіз коду використовуваних бібліотек
- проводити аналіз коду програми
- ідентифікувати вразливості шляхом сканування
- проводити регулярний аудит інформаційної безпеки

Хоча під час проектування комп'ютерної системи необхідно взяти до уваги чимало характеристик, безпека є серед них однією з найважливіших. За даними опитування, проведеного корпорацією Symantec у 2010 році, 94 % організацій, що взяли участь в опитуванні, планували вжити заходів з підвищення безпечності їхніх комп'ютерних систем, а 42 % зазначили, що вважають неналежний рівень кібербезпеки за основний ризик.

Незважаючи на те, що більшість організацій вдосконалюють системи інформаційного захисту, чимало кіберзлочинців знаходять шляхи їхнього обходу і продовжують свою діяльність. Нині спостерігається зростання числа майже усіх типів кібератак. В опитуванні 2009 року щодо комп'ютерних злочинів і кібербезпеки, проведеному Інститутом комп'ютерної безпеки, респонденти відзначили суттєве зростання числа атак шляхом застосування зловмисних програмних засобів, DoS-атак, викрадання паролів та дефейсу сайтів.

У зв'язку з тим, що інтернет-технології проникають у всіх сфери життя людини, а подекуди й інтегруються в тіло людини, питання кібербезпеки користувача набуває особливої ваги. При сучасному рівні розвитку технологій та їхній інтегрованості в життя людини це не лише питання доступу до інформації. Технології стають все ближче до тіла, до мозку і очей, до м'язів людини. Наприклад, у 2016 в Одесі на конференції Black Sea Summit вперше в Україні людині вживили чип у руку, якою він міг оплачувати рахунки, як банківською картою. Також в останні роки набуває популярності імплантація чипів, які б замінювали ключі, карти, ідентифікаційні дані. Так, наприклад, в 2019 році проект «xNT» почав розсилку покупцям чипів для імплантації в руку. Відповідно, все більше зростає загроза, що кібератаки можуть торкнутися

фізичного стану людини. Тому кібербезпека — це також і безпека життя людини. За даними фахівців компанії InDevLab – більш ніж 90% взломів відбувається саме завдяки соціальній інженерії. Це відбувається через те що хакери намагаються залякати людину чи створити такі обставини за яких у людини є обмежений час на роздуми і потрібно здійснити якусь дію, наприклад перерахувати кошти на зазначений рахунок.

Базові правила кібербезпеки користувача:

1. Створення складного пароля, що складатиметься із довільного набору символів, букв та цифр.
2. Регулярне оновлення паролів (раз у півроку).
3. Не переходити за шкідливими або підозрілими посиланнями. Причина полягає в тому, що багато інтернет ресурсів містять комп'ютерні черв'яки або інші віруси. Особливу увагу варто звертати на Торрент-файли.
4. Найбезпечніше використовувати ліцензоване програмне забезпечення.
5. Не публікувати інформацію, що може мати компрометуючий характер.
6. Підтримка «чистоти переписок».

### **1.3. Засоби захисту інформації**

Засоби захисту інформації умовно можна поділити на 3 рівні:

- 1) Мережевий рівень. В комунікаційних системах використовуються такі засоби мережевого захисту інформації:
  - Міжмережеві екрани – для блокування атак з зовнішнього середовища. Вони керують проходженням мережевого трафіку відповідно до правил захисту. Як правило, міжмережеві екрани встановлюються на вході

мережі і розділяють внутрішні (приватні) та зовнішні (загального доступу) мережі.

- Системи виявлення втручань – для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні». Використовуючи спеціальні механізми, системи виявлення вторгнень здатні попереджувати шкідливі дії, що дозволяє значно знизити час простою внаслідок атаки і витрати на підтримку працездатності мережі.
- Засоби створення віртуальних приватних мереж – для організації захищених каналів передачі даних через незахищене середовище. Віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування.
- Засоби аналізу захищеності – для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації. Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

2) Програмний рівень. Для захисту інформації на рівні прикладного та системного ПЗ нами використовуються:

- Системи розмежування доступу до інформації.
- Системи ідентифікації та автентифікації. Способи автентифікації здійснюються паролем або

біометрикою (голосом, відбитком пальця, обличчям тощо), (див. Додаток А).

- Системи аудиту та моніторингу.
- Системи антивірусного захисту.

3) Апаратний рівень. Для захисту інформації на рівні апаратного забезпечення використовуються:

- Апаратні ключі.
- Системи сигналізації.
- Засоби блокування пристроїв та інтерфейс вводу-виводу інформації.

1) Мережева безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією. При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або 'ключ', кредитну картку або мобільний телефон, при трьохфакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі. Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS).

Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційність.

Забезпечити захищеність мережевих служб можливо за допомогою:

- Брандмауерів. Централізовані брандмауери та брандмауери окремих комп'ютерів можуть запобігати проникненню зловмисного мережного трафіку до мережі, яка підтримує діяльність компанії.
- Антивірусних засобів. Більш захищена мережа може виявляти загрози, що створюють віруси, хробаки та інше зловмисне програмне забезпечення, і боротися з ним попереджувальними методами, перш ніж вони зможуть заподіяти шкоду.
- Знаряддя, які відстежують стан мережі, грають важливу роль під час визначення мережних загроз.
- Захищений віддалений доступ і обмін даними. Безпечний доступ для всіх типів клієнтів із використанням різноманітних механізмів доступу грає важливу роль для забезпечення доступу користувачів до потрібних даних, незалежно від їх місцезнаходження та використовуваних пристроїв.

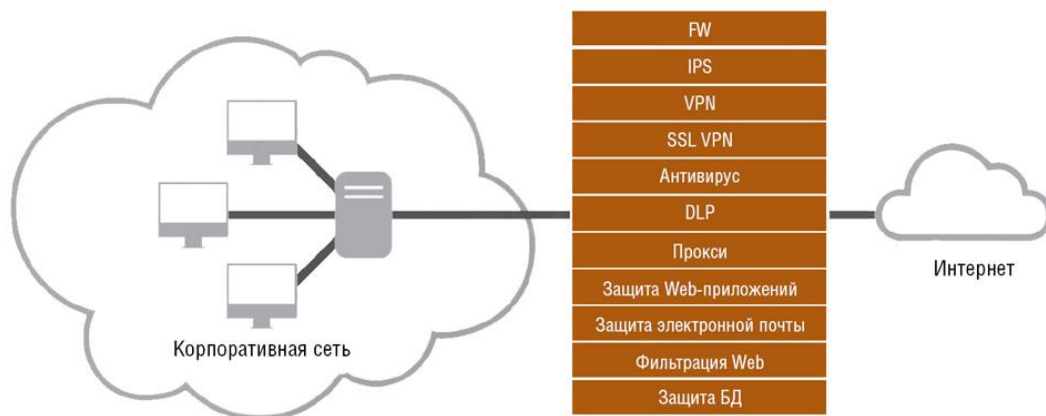


Рис.1.11. Необхідне забезпечення для захисту мережі

Спочатку firewall-и поділяються на 2 типи: host-based і network. Host-based встановлюється безпосередньо на клієнтську машину (поверх існуючої ОС) і

захищає виключно одну цю машину. Це може бути корисно в домашніх умовах (особливо, якщо у вас всього один комп'ютер і він безпосередньо підключений до модему) або в мережевому оточенні, як додатковий засіб безпеки.

Network firewall захищає всю мережу і зазвичай служить шлюзом для цієї мережі. Мережа може складатися як з одного комп'ютера, так і з багатьох тисяч. Тип firewall-а вибирається залежно від мережевого середовища та потреб.

2) Програмні засоби захисту інформації – системні та прикладні програми, призначені для захисту інформації, що передається по телекомунікаційним каналам, зберігається в базах даних і на інформаційних носіях.

Найчастіше програмні засоби захисту інформації застосовують для виконання таких процесів як ідентифікація й автентифікація користувачів, розмежування доступу користувачів до інформаційної мережі, парольний захист і перевірка повноважень шифрування інформації, а також її захист від несанкціонованих змін, зчитування, копіювання.

Найбільшу увагу розробники й користувачі сьогодні приділяють програмним засобам захисту від несанкціонованого доступу до інформаційних ресурсів і особливо до мережі Інтернет. Організаційні, технологічні й апаратні методи захисту, як правило, не можуть бути здійснені без програмної складової. При цьому слід мати на увазі, що вартість здійснення багатьох програмних системних рішень із захисту інформації суттєво перевищує за затратами апаратні, технологічні й організаційні рішення. Іншими недоліками програмних засобів захисту інформації є використання ресурсів системи, що призводить до зниження її ефективності, принципова можливість обходу такого захисту або його злочинної зміни в процесі експлуатації.

Найпоширенішими прикладами програмних засобів захисту інформації є такі:

- система контролю і управління доступом;
- антивірусні програми;

- шифрувальне програмне забезпечення;
- мережевий екран;
- система виявлення вторгнень;
- керування записами;
- пісочниця;
- система управління інформаційною безпекою
- SIEM.

Програмні засоби захисту повинні забезпечувати:



Рис.1.12. Забезпечення захисту на програмному рівні.

3) На апаратному рівні захисту ТЗІ від НДС застосовуються звичайні заходи безпеки, такі як ключ-карта, сигналізація та засоби блокування пристроїв. За допомогою карти-ключа, власним має можливість проходити до кімнат, які

мають спеціальний замок, звичайно, якщо у цієї КК відкритий доступ входу до бажаної кімнати. Сигналізація та прилади пожежної безпеки повинні бути встановлені по всьому приміщенню, як заходи безпеки. Щодо засобів блокування пристроїв, можна сказати, що вони відрізняються один від одного в залежності потреби блокування та типу пристрою. Наприклад, серверна шафа є засобом кріплення та блокування пристроїв.

Отже, можна сказати, що захист кінцевого користувача або безпека кінцевих точок є вирішальним аспектом кібербезпеки. Зрештою, часто людина (кінцевий користувач) випадково завантажує шкідливе програмне забезпечення чи іншу форму кіберзагрози на свій робочий стіл, ноутбук чи мобільний пристрій.

Отже, як заходи кібербезпеки захищають кінцевих користувачів та системи? По-перше, кібербезпека покладається на криптографічні протоколи для шифрування електронних листів, файлів та інших важливих даних. Це не тільки захищає інформацію, що передається, але й захищає від втрати або крадіжки.

Крім того, програмне забезпечення для захисту кінцевих користувачів сканує комп'ютери на наявність шкідливих кодів, розміщує цей код на карантині, а потім видаляє його з машини. Програми безпеки можуть навіть виявляти та видаляти зловмисний код, прихований у первинному завантажувальному записі, і призначені для шифрування або стирання даних з жорсткого диска комп'ютера.

Електронні протоколи безпеки також зосереджені на виявленні зловмисного програмного забезпечення в режимі реального часу. Багато використовують евристичний та поведінковий аналіз для моніторингу поведінки програми та її коду для захисту від вірусів або троянських програм, які змінюють свою форму при кожному виконанні (поліморфні та метаморфічні шкідливі програми). Програми безпеки можуть обмежувати потенційно шкідливі програми

віртуальним міхуром, відокремленим від мережі користувача, щоб проаналізувати їх поведінку та дізнатися, як краще виявити нові зараження.

Програми безпеки продовжують розвивати нові засоби захисту, оскільки фахівці з кібербезпеки визначають нові загрози та нові способи боротьби з ними. Щоб максимально використати програмне забезпечення для захисту кінцевих користувачів, працівників потрібно навчити, як ними користуватися. Найважливіше те, що його постійно працює та часто оновлюється гарантує захист користувачів від останніх кіберзагроз.

Network firewall поділяються на 2 види: PC-based (засновані на звичайному комп'ютері) і ASIC-accelerated.

ASIC – application-specific integrated circuit. Маю на увазі машини, в яких основний функціонал firewall-а відбувається на апаратному рівні. Як правило, це дуже дорогі системи, вартість яких часто доходить до декількох десятків і навіть сотень тисяч доларів. Використовуються зазвичай в ISP-подібних організаціях, яким потрібна дуже висока пропускна здатність. Всі інші firewall-и є PC-based. Не попадайтеся на вудки продавців і маркетологів: всі інші firewall-и є PC-based.

## РОЗДІЛ 2. СТРУКТУРА ТА ВИДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

### 2.1. Інформаційна безпека на підприємстві

#### 2.1.1. Система захисту інформації, її функції та методи

В Україні забезпечення ІБ здійснюється шляхом захисту інформації – у випадку, коли необхідність захисту інформації визначена законодавством в галузі ЗІ. Для реалізації захисту інформації створюється комплексна система захисту інформації (КСЗІ). КСЗІ — взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Інформаційна безпека організації – цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток. Часто здійснюється службою інформаційної безпеки.

Або, у випадку, коли суб'єкт інформаційної безпеки має наміри розробити і реалізувати політику інформаційної безпеки і може реалізовувати їх без порушення вимог законодавства.

- міжнародними стандартами ISO: ISO/IEC 17799:2005, ISO/IEC 27001:2013 та ін. – для підтримки рішень на основі ITIL та COBIT і виконання вимог. Тоді на підприємстві створюється система управління інформаційною безпекою (СУІБ), яка повинна відповідати усім вимогам міжнародних стандартів в галузі ІБ.
- власними розробками.

Кафедра КІТ (47)				НАУ 20 27 44 000 ПЗ			
Виконав	Харьков О.С.			СТРУКТУРА ТА ВИДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ.	Літера	Аркуш	Аркушів
Керівник	Куклінський М.В.					37	19
Консульт							
Н.контр.	Райчев І.Е.				УС-211М		1228

Функції, які забезпечують ІБ підприємств поділяється на:

- розробка методів аналізу загроз, оцінки рівня інформаційної безпеки підприємства і систем її забезпечення;
- організація і здійснення діяльності із захисту інформації;
- експлуатація технічних засобів захисту інформації;
- аудит і контроль функціонування системи інформаційної безпеки підприємства.

Також, існують основні методи забезпечення інформаційної безпеки підприємств, такі як:

- Резервне копіювання.
- Політика прав доступу( обмеження кола людей, які мають права доступу до важливих даних підприємства).
- Двофакторна аутентифікація.

На підприємстві функцію забезпечення ІБ може виконувати як окремий відділ Служби безпеки підприємства, так і окрема Служба (Служба захисту інформації).

Для контролю за КСЗІ в обов'язковому порядку створюється Служба захисту інформації в інформаційно-телекомунікаційній системі (сама назва «Служба» не є обов'язковою).

Функції з контролю за СУІБ покладаються на певний відділ підприємства, зокрема на операційні центри безпеки (див. Додаток А).

### 2.1.2. Запровадження норм ІБ організації

На підприємстві орган управління безпекою It Security, запроваджує певні правила, вимоги та способи захисту інформації, працівників, інших користувачів та компанії від зовнішніх та внутрішніх небезпек.

Відділ кібербезпеки запроваджую різні види правил та вимог, а саме:

- Процеси з управління та видачі доступів.
- Управління користувачами.
- IS управління інцидентами.
- Безпека мережі.
- Безпека продукту.
- Безпечна розробка.
- Шифрування даних.

Спершу слід дослідити вразливі місця в компанії. Вразливість - технічний або логічний недолік в системі, використовуючи який, можна порушити порядок роботи або отримати неавторизований доступ до системи або її окремих компонентів.

Виявлення вразливості - процес пошуку і документування вразливостей в системах. Наприклад, у компанії може використовуватися корпоративний інфраструктурний сканер "Nessus" і Web-сканер "Burp Suite".

Nessus – программа для автоматического поиска известных изъянов в защите информационных систем. Она способна обнаружить наиболее часто встречающиеся виды уязвимостей, например:

- Наличие уязвимых версий служб или доменов.
- Ошибки в конфигурации (например, отсутствие необходимости авторизации на SMTP-сервере).
- Наличие паролей по умолчанию, пустых, или слабых паролей.

Программа имеет клиент-серверную архитектуру, что сильно расширяет возможности сканирования. Согласно проведенному порталом securitylab.ru опросу, nessus используют 17 % респондентов.

Burp Suite - це платформа, в якій можна проводити аудит за безпекою веб-додатків. Він містить безліч інструментів для складання карт усіх веб-додатків, пошуку файлів та папок, модифікацій запрошень, фазингу, підбору паролів та багато іншого. Також існує у нього магазин різноманітних доповнень магазину VApp, що містить додаткові розширення, розширення функціональних додатків. Хоча ще додати про появу в останньому випуску мобільного довідника для проведення досліджень з питань безпеки мобільних додатків - MobileAssistant.

Якщо брати статистику за репортажем bug-bounty - практично на всіх скриншотах можна використовувати саме цей інструмент. На рівному з OWASP ZAP це найпопулярніший набір утиліт для тестування веб-сторінок.

Усунення уразливості - процес внесення змін в конфігурацію системи (в т.ч. операційну систему, конфігураційні файли, супутнє програмне забезпечення, правила мережевої взаємодії і т.д.), який покликаний до того, щоб усунути виявлену уразливість або мінімізувати можливі наслідки її експлуатації .

Основна функція сервера - роль, яка була визначена для сервера при його створенні.

Ролі задіяних в процесі співробітників:

Адміністратор ІТ безпеки - співробітник групи інформаційної безпеки, який відповідає за регулярне сканування, аналіз отриманих результатів, постановку задачі на усунення виявлених проблем і перевірку їх виконання.

Технічний адміністратор - технічний фахівець, який супроводжує систему, сервер або сервіс. Відповідає за усунення виявлених вразливостей.

Бізнес власник системи - відповідальний співробітник з боку бізнесу, в рамках якого працює система, сервер або сервіс. Бере участь в ухваленні

рішення щодо усунення або прийняття ризиків, пов'язаних з виявленою вразливістю.

Співробітник технічної підтримки - співробітник L1, який займається моніторингом роботи систем і оповіщенням в разі виникнення проблем. Відповідає за своєчасне інформування відповідальних співробітників в разі виявлення проблем при скануванні серверів.

Технічний адміністратор інформує адміністратора ІТ безпеки в разі змін в архітектурі системи (введення нових або виведення старих серверів з експлуатації, додавання нових основних функцій сервера, оновлення версії ОС, веб-сервісу, бази даних і т. Д.), шляхом додавання інформації в asset inventory.

## **2.2. Управління вразливістю**

### **2.2.1. Етапи виявлення вразливостей**

В даний момент контроль / реакція на нові вразливості реалізований через канал зв'язку (наприклад, месенджер):

1. Адміністратор ІТ безпеки разом з технічним адміністратором і за необхідності з бізнес власником системи, визначають Скоуп сканованих систем, час для проведення процедур виявлення вразливостей і т.д.
2. Адміністратор ІТ безпеки, на підставі домовленостей (п. 1) готує технічні налаштування ПО для проведення процедури виявлення вразливостей.
3. Адміністратор ІТ безпеки проводить процедуру сканування, попередньо поінформувавши всіх задіяних в процесі співробітників (Технічних адміністраторів, співробітників технічної підтримки, бізнес власника системи), за один робочий день і перед початком сканування.

4. Співробітник технічної підтримки в разі виявлення аномалій (Критична навантаження на сервіси, скарги клієнтів, недоступність мережевих інтерфейсів і додатків і т.д.) в сканованих системах, зобов'язаний повідомити технічного адміністратора і адміністратора ІТ безпеки про спостережуваних проблемах. Адміністратор ІТ безпеки вживає заходів щодо припинення або зниження інтенсивності проведених робіт.
5. За результатами проведеного сканування, ІТ безпеки готує звіт про виявлені вразливості, коротке резюме про критичні недоліки та можливі методи виправлення проблем.
6. На підставі проведеного сканування та аналізу результатів, ІТ безпеки створює завдання щодо усунення виявлених вразливостей в тікетінговій системі. Дане завдання призначається на технічного адміністратора. Залежно від ступеня ризику реалізації виявленої уразливості, ІТ безпеки встановлює пріоритет завдання і терміни її виконання (напр. Інформація в мережі інтернет про націлених атаках на таку вразливість з можливістю її швидкої експлуатації при мінімальному наборі навичок та інструментів - матиме максимальний пріоритет і терміновість ).

### **2.2.2. Процес аналізу вразливостей**

Кожна виявлена уразливість аналізується адміністратором ІТ безпеки на предмет її критичності і можливого негативного впливу на сервіси компанії. Вразливості діляться на 3 групи за ступенем критичності:

- 1) Критичний (Critical) – вразливість, яка може зробити прямий негативний вплив на сервіс компанії, яка не потребує особливих навичок з боку атакуючого. Технічні інструкції, ПО, код експлуатації для такої уразливості доступні у відкритих джерелах.

- 2) Середній (Medium) – вразливість, яка не може напряму впливати на сервіси компанії, може вимагати глибокого рівня знань у внутрішніх процесах та архітектури роботи окремо-взятого сервера. Експлуатація зазначеної уразливості може вимагати наявності певного рівня доступу на сервері. Загальнодоступної інформації про методи і умови експлуатації – недоступні.
- 3) Незначний (Low) – сервера, які не виконують ніяких критичних для бізнесу операцій, що не мають прямої і непрямой (через інші сервера) мережевий доступності до серверів, які виконують критичні функції для бізнесу компанії.

Підлягають усуненню наступні уразливості:

- External уразливості рівня "Medium".
- External уразливості рівня "Critical".

У разі неможливості усунення вразливості в певні терміни (з об'єктивних причин) виробляються додаткові заходи безпеки, наприклад (визначається в кожному окремому випадку):

- Обмеження мережевий доступності уразливого додатки або сервера.
- Розробка процедури моніторингу додаткових тригерів на сервері.
- Збільшення рівня журналювання подій, їх кореляція і періодичний аналіз на предмет шкідливої активності.

### **2.2.3. Етапи усунення вразливостей**

Технічний адміністратор робить наступні дії для усунення вразливостей:

1. Аналізує можливі методи усунення вразливості.
2. Вибирає оптимальний час (при необхідності, узгоджує з бізнес-власником) для проведення робіт по усуненню вразливостей з

урахуванням наступних параметрів: наявність у уразливого сервера або програми додаткової (дублюючої, вторинної і т.д.) ноди, часу простою сервера або сервісу, часових проміжків мінімальної клієнтської активності, суміжними роботами.

3. Проводить процедуру усунення вразливості згідно виставленої завдання в тікетінгговій системі.
4. У разі виникнення критичних проблем, які призводять до неможливості усунення вразливості, технічний адміністратор повинен провести документування зазначеної ситуації (напр. Зберегти лог проведення роботи, скріншоти помилок з покроковим описом виконуваних дій) в тому завданні, яка була виставлена адміністратором ІТ безпеки. При цьому, завдання не закривається до з'ясування причини виникнення проблеми.
5. Після успішного проведення робіт по усуненню вразливості, технічний адміністратор повинен упевнитися в коректній роботі всіх функцій сервера, на якому проводилися роботи (напр. Всі необхідні сервіси успішно запуснені і працюють, є мережева доступність, продуктивність сервера на аналогічному рівні як і до проведення робіт по усуненню вразливостей).
6. Уразливість вважається закритою, після підтвердження з боку адміністратора ІТ безпеки.

Після закриття завдання щодо усунення вразливості, адміністратор ІТ безпеки може ініціювати повторне сканування, з метою перевірки, що окреслені питання були усунені.

Процес виявлення та усунення вразливостей є циклічним. Сканування на виявлення вразливостей проводиться 1 раз на місяць для External (зовнішніх) і 1 раз в квартал для Internal scope (внутрішніх).

#### **2.2.4. Моніторинг подій**

1) Журнали повинні містити таку інформацію:

- Позначка часу початку події.
- Користувач-джерело
- IP-адреса джерела та / або ім'я хосту
- Вихідна програма / послуга
- Цільовий IP та / або ім'я хосту
- Цільовий об'єкт / послуга
- Тип дії
- Опис дії
- Статус (успіх / невдача)
- Причина відмови
- Мітка часу закінчення події

2) Наступні події слід реєструвати.

#### **2.1. Аутентифікація та авторизація**

- Успішні або невдалі спроби входу (включаючи спроби входу в систему для вимкнених, неіснуючих, призупинених облікових записів).
- Зміни користувачів (створення / модифікація / видалення).
- Зміни ролей, груп, дозволів (створення / зміна / видалення).
- Додавання, видалення користувачів, зміни доступів користувачів.
- Зміна та скидання пароля (успішно або невдало).
- Зміни політики щодо паролів.

#### **2.2. Доступ до ресурсів**

- Створювання, змінювання та видалення ресурс (вузли, групи ресурсів, модулі, криптографічні ключі, таблиці тощо) на всіх рівнях.
- Ресурси, системи та додатки припиняють роботу, зупиняють роботу, перезапускають.
- Зміни ACL мережі. (див. Додаток А).
- Усі привілейовані дії користувача (ОС, БД, програми, інтерфейси управління).
- Доступ користувача до важливих даних (ОС, БД, програма).
- Зв'язок внутрішніх служб із зовнішніми системами.

### 2.3. Цілісність журналів

- Увімкнення, вимкнення журналу.
- Змінюються правила реєстрації.
- Доступ до журналів.
- Видалення, модифікація журналів.

## 3.3. Реалізація та вимоги до безпеки даних

### 3.3.1. Безпека даних

Наступні типи даних є Критичними з додатковими вимогами щодо забезпечення їх безпеки:

- 1) Клієнтські персональні дані, ПІБ і підтверджуючі документи.
- 2) Платіжні дані (дані про транзакції, сума, дата, PAN, due date etc.).
- 3) Авторизовані дані, як призначені для користувача, так і сервісні (паролі, ключі, отр, etc).
- 4) Секретні питання і відповіді на них.

- 5) Secret passphrase і алгоритм генерації OTP для входу в кабінет гравця.

Наступні типи дані є даними з обмеженим доступом:

- Фінансова звітність і статистика.
- конфігураційні дані.
- Вихідний код (Source code).

Збереження даних

- Зберігання Критичних даних допускається тільки в зашифрованому або маскуватися вигляді.
- Повинні бути створені окремі ролі, які дозволяють працювати з Критичними даними / Даними з обмеженим доступом. Ролі доступу повинні створюватися відповідно до Access management requirements (for internal users).
- Непродуктивні середовища (STAGE, DEV, etc) не повинні містити Критичні дані / Дані з обмеженим доступом з продуктивною Платформи.
- Критичні дані / Дані з обмеженим доступом в непродуктивних середовищах повинні бути де-персоніфіковані. Допускається використовувати або випадковим чином створених даних або маскованих (для аналітичних задач).
- Вимоги до зберігання клієнтських авторизаційних даних.

Переміщення інформації має здійснюватися з використанням шифрованих каналів (TLS)

Резервне копіювання даних:

- Бекапірованіє критичних даних повинне здійснюватися на контрольовані компанією ресурси

- Доступ до збережених бекапів повинен бути обмежений списком відповідальних за них співробітників.
- Повинні логуватися всі дії з бекапу відповідно до вимог безпеки.

### **3.3.2. Вимоги**

До вимог безпеки даних відносять:

- Будь-яке значення змінних, яке задається (прописується) клієнтом - повинні відправлятися за допомогою POST HTTP запитів (аутентифікація, зміна пароля, установка ставки і т.д.)
- Будь-які передані значення від клієнта - повинні екрануватися, затвердити на стороні сервера. При помилках валідації змінних, запитувана клієнтом операція повинна перериватися.
- Клієнтські сесії у внутрішніх системах повинні відповідати рекомендаціям - Session Management Requirements.
- У source code, який обробляється до контексті клієнтського ПЗ (браузер, мобільний додаток і т.д.), не повинні міститися:
  - Коментарі.
  - Посилання на UAT, Stage і інші environments (див. Додаток А).
  - Логіни, паролі, приватні ключі і інші секрети.
  - Внутрішні IP адреси, імена хостів і т.д.

### **3.3.3. Вимоги до інфраструктури**

Безпеку інфраструктури поділяють на:

1. Безпека ОС і сервісів:

- Використовуємо ПО (ОС, бази даних, утиліти, веб-сервер та т. Д.)  
Повинні бути оновлені до останньої версії розробленого розробника.  
Усі використовувані версії ПО повинні бути підтриманими з боку розробників
- Утиліти, засоби та бібліотеки, які не використовуються (в ОС, веб-сервері, додатку-сервері тощо), повинні бути видалені
- ОС та основні компоненти (веб-сервер, бази даних та т. Д.) Повинні бути сконфігуровані відповідно до вимог ІТ безпеки.

2. Захист систем авторизації

- Доступ до інтерфейсу користувача повинен здійснюватися через WAF
- Для захисту від брутфорса та блокування користувачів на вхідному інтерфейсі, потрібно працювати зі скриптами модуля

3. Сервіси та інтеграція

- Сервісні навчальні записи повинні створюватися лише персоналом DevOps відповідно до парольних вимог - Вимоги до пароля
- Сервісні записи використовують окремий API і дають відмінні вимоги до управління сесіями
- Обмін даними всередині платформ та зовнішніх систем повинен проходити по шифрованому каналу (TLS)

**3.3.4. Вимоги щодо управління доступом**

Серед вимог доступу до внутрішніх ресурсів компанії виділяють:

- Внутрішні системи повинні бути доступні тільки всередині локальної офісної мережі або через VPN.
- Доступ у внутрішні системи повинен надаватися через UCS (див. Додаток А).

- Доступ у внутрішні системи повинен надаватися після аутентифікації (Введення логіна пароля, за сертифікатом і т.д.),
- Події аутентифікації, зміни або відновлення пароля, зміна прав доступу повинні Залогуватися згідно вимог - Event monitoring
- Взаємодія користувача з UI повинно здійснюватися з використанням шифрованих каналів - TLS (1.1 or higher)
- Система повинна мати можливість блокувати облікові записи користувачів при перевищенні лімітів по неуспішним логінів
- Доступ до функціонала нового продукту, повинен надаватися на основі рольової моделі доступів. Ролі повинні бути унікальні як на рівні окремих модулів та й на рівні всього продукту, і створені відповідно до Role Management Requirements.

### **3.4. Принцип та поряд створення системи кібербезпеки**

Наступні кроки описують інтерактивний процес, який можна використовувати для створення програм КБ для критичної інфраструктури. Він описує процес, який можна використовувати для розробки нової програми з КБ або вдосконалення існуючої. Усі або частини цього процесу слід повторити, коли це потрібно або дочасно. Крім того, слід повторити щоразу, коли ви вказуєте на досягнення програм, коли ви змінюєте ваші загрози, зниження ризику та ризик, або коли ви отримуєте ваш цільовий профіль та рівень життя.

#### **Крок 1. Визначте сферу діяльності програми кібербезпеки**

Враховуйте свою корпоративну місію, цілі та організаційні пріоритети.

- Виберіть процес або бізнес-підрозділ, який повинен мати програму з кібербезпеки.
- Визначте системи та активи, які підтримують ваш процес або бізнес-одиницю.

- Уточнити сферу застосування систем та активів, що використовуються цим процесом або бізнесом.
- Визначте системи та активи, пов'язані з вашими основними системами та активами.

## **Крок 2. Визначте свої загрози та вразливості**

- Визначте нормативні вимоги, які стосуються вашого процесу або бізнес-підрозділу.
- Визначте загальний підхід вашої організації до ризику та вашу толерантність до ризику.
- Визначте загрози та вразливості, які стосуються вашого процесу або бізнес-підрозділу.

## **Крок 3. Визначте поточний профіль та поточний рівень**

- Використовуйте ядро основи, щоб визначити поточний профіль вашої організації.
- Перегляньте практики управління ризиками, що складають рівні впровадження.
- Використовуйте ці рівні реалізації для визначення поточного рівня вашої організації.

## **Крок 4. Оцініть, як потенційні, так і нові ризики**

Розгляньте свій процес управління ризиками та ваші попередні дії з оцінки ризику.

- Використовуйте попередні методи управління ризиками для керівництва оцінками ризиків у вашій організації.
- Проаналізуйте операційне середовище вашої організації та оцініть свої ризики кібербезпеки.
- Виявити та описати потенційні та нові події, загрози та ризики кібербезпеки.
- Оцініть ймовірність того, що події дійсно відбудуться, та вплив, який вони можуть мати.
- Використовуйте внутрішні та зовнішні джерела для кращого розуміння ймовірностей та наслідків.

## **Крок 5. Створіть свій цільовий профіль та свій цільовий рівень**

- Використовуйте ядро основи, щоб встановити цільовий профіль вашої організації.
- Використовуйте дані внутрішніх та зовнішніх зацікавлених сторін для вдосконалення Вашого цільового профілю.
- Використовуйте вклад клієнтів, постачальників, партнерів та інших зовнішніх зацікавлених сторін.
- Використовуйте дані персоналу, менеджерів, підрядників та інших внутрішніх зацікавлених сторін.
- Перегляньте практики управління ризиками, що складають рівні впровадження.
- Використовуйте ці рівні реалізації для розробки цільового рівня вашої організації.
- Використовуйте дані внутрішніх та зовнішніх зацікавлених сторін для уточнення цільового рівня.

## **Крок 6. Визначте прогалини у вашій програмі кібербезпеки**

- Визначте прогалини в рамках порівняння поточного та цільового профілів.
- Розмістіть пріоритетні прогалини, враховуючи ризики, витрати та вигоди.
- Визначте прогалини у впровадженні, порівнюючи поточний та цільовий рівні.
- Розмістіть пріоритети в прогалинах у здійсненні, враховуючи ризики, витрати та вигоди.

## **Крок 7. Виконайте план створення програми кібербезпеки**

Розгляньте найважливіші прогалини у кібербезпеці вашої організації.

- Враховуйте прогалини у структурі, що мають пріоритет у вашій організації.
- Враховуйте першочергові прогалини у впровадженні вашої організації.
- Створіть план дій для подолання високопріоритетних прогалин у кібербезпеці.
- Враховуйте свою місію, цілі, ризики, витрати та переваги.
- Визначте кроки для усунення високопріоритетних прогалин у кібербезпеці.
- Визначте кроки для усунення прогалин у високопріоритетних рамках.
- Визначте кроки для усунення прорізів у впровадженні пріоритетів.
- Виконайте свій план дій, щоб усунути пріоритетні прогалини в кібербезпеці.

- Вжити заходів для розробки програми кібербезпеки вашої організації.
- Вжити заходів для усунення прогалин, що мають високий пріоритет.
- Вжити заходів для досягнення вищого рівня впровадження кібербезпеки.
- Вживайте заходів для усунення ваших пріоритетних прогалин у реалізації.

На мою думку найвразливішою стороною підприємства є її користувачі. Оскільки, кожен працівник не може бути інформаційно обізнаний у сфері захисту інформації. Тому, спершу слід відсторонити працівників від доступу конфіденційної інформації, яка їм не потрібна для роботи та надавати доступ лише до тої інформації та ресурсів, які необхідні для роботи працівника. Тобто, побудувати ієрархію доступів для працівників залежно від їх позиції та посади. У разі, якщо виникне необхідність у використанні ресурсів, які недоступні користувачу, це питання слід обговорити з відділом безпеки (IT Security). Вони при необхідності можуть видати необхідний доступ на деякий час або на постійній основі.

Тож, як захисти компанію від навмисного або випадкового витоку інформації від своїх же працівників? Адже, не можливо бути впевненим на всі сто відсотків, у порядності та чесності інших людей.

На даний час, більшість компаній використовую доменні служби Active Directory (AD), які реалізують на базі Windows Server. За допомогою AD, можливо контролювати доменні облікові записи працівників, обмежувати та надавати їх доступи. Також, через AD можна керувати комп'ютерами, які були

додані до домену. Розгортати політики і правила для забезпечення безпеки користувачів та інформації компанії.

Отже, слід дізнатись, що таке домен, доменні служби, Active Directory (AD), доступи, політики та як саме працюючи з ними можна забезпечити захист інформації.

## РОЗДІЛ 3. НАЛАГОДЖЕННЯ РОБОТИ WINDOWS SERVER ТА ДОМЕННОЇ СЛУЖБИ ACTIVE DIRECTORY

### 3.1. Домен, доменні облікові записи та керування ними

#### 3.1.1. Політика домену

Доме́нне ім'я або Доме́н — це частина простору ієрархічних імен мережі Інтернет, що обслуговується групою серверів системи домeнних імен (DNS-серверів) та централізовано адмініструється.

Доменне ім'я може складатися тільки з обмеженого набору ASCII символів, дозволяючи набрати адресу домену незалежно від мови користувача. ICANN затвердив засновану на Punycode систему IDNA, перетворюючи будь-який рядок в кодуванні Unicode в допустимий DNS набір символів.

Облікові записи користувачів використовуються людьми та службами, щоб їх можна було автентифікувати та отримати доступ до ресурсів. Кожен обліковий запис користувача містить інформацію про особу або службу, яка їх використовує, та забезпечує засіб надання дозволів, застосування сценаріїв, призначення профілів та контроль того, які дії користувач може виконувати та до чого він може отримати доступ. Через обліковий запис створюється набір облікових даних, що захищає від несанкціонованого доступу.

У Windows Server (див. Додаток А) можна створити два різні типи облікових записів користувачів: локальні та доменні. Локальні облікові записи користувачів використовуються для контролю доступу до комп'ютера, на якому ви працюєте. Вони створюються на Windows Server за допомогою оснастки «Локальні користувачі та групи» або вузол «Користувачі» під вузлом «Локальні користувачі та групи» в утиліті «Управління комп'ютером».

Кафедра КІТ (47)				НАУ 20 27 44 000 ПЗ			
Виконав	Харьков О.С.			НАЛАГОДЖЕННЯ РОБОТИ WINDOWS SERVER ТА ДОМЕННОЇ СЛУЖБИ ACTIVE DIRECTORY.	Літера	Аркуш	Аркушів
Керівник	Куклінський М.В.					56	33
Консульт					УС-211М 12257		
Н.контр.	Райчев І.Е.						

Після створення інформація про обліковий запис зберігається в локальній базі даних, яка називається - Менеджер облікових записів безпеки (SAM). Інформація про обліковий запис стосується лише локального комп'ютера і не копіюється на інші машини в межах домену. Коли користувач входить в систему на комп'ютері, Windows Server аутентифікує користувача за допомогою цієї інформації, або дозволяє, або забороняє доступ до машини.

Облікові записи домену створюються в Active Directory і значно відрізняються від локальних облікових записів користувачів. Замість того, щоб зберігати інформацію на локальній машині, інформація про обліковий запис зберігається в каталозі та реплікується в інші DC. Як ми вже обговорювали раніше в цьому розділі, коли користувач входить до DC, інформація про обліковий запис використовується для побудови маркера доступу. Цей маркер доступу використовується протягом усього часу, протягом якого користувач входить в мережу, і визначає, до чого користувачеві дозволений доступ в мережі, та дії, які він може виконати.

Отже важливо розуміти різницю між цими обліковими записами. Локальні облікові записи зберігаються на комп'ютерах і стосуються лише безпеки цих машин. Облікові записи доменів зберігаються в AD і налаштування безпеки для цього облікового запису можуть застосовуватися до доступу до ресурсів та служб у мережі.

### **3.1.2. Вимоги до пароля**

Також, необхідно запровадити вимоги для пароля користувачів та бажано, щоб паролі від різних облікових записів були різні. Проте, доступ до внутрішніх ресурсів компанії можна зробити за допомогою доменних груп, які зможуть отримати доступ на підключення при доменній авторизації. Основні вимоги щодо пароля обов'язкові для всіх систем, які використовуються в компанії працівниками та службами. Усі винятки з цих вимог повинні бути узгоджені з IT Security. До вимог стосовно пароллю відносять:

Вимоги до довжини та складності пароля:

- Пароль повинен відповідати принаймні 3 із наступних 4 правил складності:
  - Принаймні 1 прописний символ (A-Z).
  - Принаймні 1 маленький символ (a-z).
  - Принаймні 1 цифра (0-9).
  - Принаймні 1 спеціальний символ ("пробіл" - це також спеціальний символ).
  
- Мінімальна та максимальна довжина пароля повинна бути:
  - Щонайменше 12 символів.
  - Не більше 128 символів.
  
- Наступні комбінації НЕ повинні використовуватися в паролі:
  - 3 і більше послідовно повторюваних символів (наприклад: 111, ааа тощо).
  - суміжні символи на клавіатурі (наприклад: qwerty, 1234567 тощо).
  - загальнодоступні дані про користувача (наприклад: логін, дата народження, прізвище, назва компанії, номер телефону тощо).
  - прості словникові світи (наприклад: пароль, паримат) .
  
- Вимоги до зміни пароля
  - Для особистих акаунтів паролі потрібно міняти принаймні раз на 90 днів.

- Новий пароль не повинен відповідати попереднім 10 паролем.
  - Система повинна змусити користувача змінити пароль, який надається за замовчуванням після першого успішного входу.
  - Для службових рахунків пароль потрібно якомога швидше змінити, якщо працівник використовував їх, вийшов з компанії або перевів на іншу функцію.
  - Якщо пароль скомпрометований, його потрібно якомога швидше змінити.
  - Паролі повинні бути змінені при першому вході в систему (для пароля, встановленого адміністратором під час створення нового облікового запису в системі).
- Паролі з використанням вимог
    - НЕ використовуйте однаковий пароль для робочих облікових записів та для особистих облікових записів (наприклад: для приватних поштових акаунтів, акаунтів у соціальних мережах тощо).
    - НЕ використовуйте один і той же пароль для різних служб, щоб запобігти ситуації, коли одна служба була порушена, але ми повинні змінити паролі для багатьох служб.
    - НЕ діліться своїми паролем для особистих облікових записів ні з ким, включаючи колег, адміністраторів та персонал технічної підтримки.
    - НЕ вказуйте паролі до внутрішніх корпоративних ресурсів.
    - НЕ використовуйте однаковий пароль для особистих та службових облікових записів.
    - Паролі з облікових записів слід надсилати окремо від логіна та іншої інформації про систему.

- Додаткові вимоги до продукту
  - Для всіх ресурсів (де це технічно можливо), що містять конфіденційну інформацію \* повинна використовуватися багатофакторна автентифікація.
  - Введення пароля на екрані користувача слід закрити.
  - Операції скидання та зміни пароля вимагають того ж рівня контролю, що і створення облікового запису та автентифікація.
  - Якщо ви використовуєте скидання на основі електронної пошти, надсилайте електронні листи лише за попередньо зареєстрованою адресою з тимчасовим посиланням.
  - Тимчасові посилання повинні мати короткий час закінчення (не більше 20 хвилин).
  - Повідомте користувачів про скидання пароля.
  - Відповіді на помилки автентифікації не повинні вказувати, яка частина даних автентифікації була неправильною. Наприклад, замість "Недійсне ім'я користувача" або "Недійсний пароль", просто використовуйте "Недійсне ім'я користувача та / або пароль" для обох. Відповіді на помилки повинні бути справді однаковими як у дисплеї, так і у вихідному коді.
  - Повторно автентифікуйте користувачів перед виконанням критичних операцій.
  - Не дозволяти користувачеві використовувати наступні спеціальні символи: [ $\<$   $\>$  \ '& "].
  
- Вимоги до зберігання паролів:

- Ніколи не зберігайте паролі в простому тексті. Зберігайте лише криптографічно надійні односторонні солені хеші паролів.
- Виберіть один із наступних алгоритмів: Argon2, PBKDF2 (Використовуйте HMAC-SHA-2 як хеш ядра всередині), bcrypt або scrypt.
- Створіть унікальну сіль для кожного збереженого облікового запису (щоб гарантувати, що однакові паролі мають різні хеші).
- Нова випадкова сіль повинна створюватися кожного разу, коли користувач створює обліковий запис або змінює свій пароль. Ніколи не використовуйте сіль повторно.
- Використовуйте мінімум 32 байти солі. Хорошим емпіричним правилом є використання солі такого ж розміру, що і висновок хеш-функції.
- Сіль повинна генеруватися криптографічно захищеним генератором псевдовипадкових чисел (CSPRNG).
- Зберігайте хеші паролів та унікальну сіль окремо від інших даних користувачів на окремій схемі в БД.
- Не розкривайте вміст DB / таблиці, використовуючи імена, такі як хеш, пароль тощо.
- Обмежте доступ до таблиці / файлу, який зберігає хеші паролів на основі необхідності знати.
- База даних не повинна давати підказок щодо довжини паролів.
- Хешування паролів має бути впроваджено в надійній системі (на стороні сервера).
- Аутентифікаційні дані для доступу до зовнішніх служб програми повинні бути зашифровані та збережені в

захищеному місці в надійній системі. Вихідний код HE є надійним місцем.

- Моніторинг

Наступні події слід реєструвати:

- Успішні чи невдалі спроби входу (включаючи спроби входу в систему для вимкнених, неіснуючих, призупинених облікових записів).
- Остання зміна пароля.
- Дата закінчення терміну дії пароля.
- Зміни політики щодо паролів.
- Зміна та скидання пароля (успішно чи невдало).

### **3.1.3. Вимоги до техніки**

Важливо розуміти, що не тільки облікові та паролі мають свої вимоги. Стосовно техніки також є вимоги, які допоможуть забезпечити захист інформації на підприємстві.

Базові вимоги до корпоративної техніки компанії:

1. Використання персональних комп'ютерів у робочих цілях заборонено (робота дозволена лише на комп'ютерах, що випускаються корпорацією та відповідають вимогам безпеки).
2. Всіма системами Windows для працівників слід керувати за допомогою Active Directory (AD).
3. Системи Windows, які використовуються працівниками, повинні використовувати 64-розрядну версію Windows 10 Enterprise Edition. Застарілих версій Windows бути не повинно.

4. В операційній системі на робочій станції повинні бути встановлені всі перевірені, затверджені оновлення та виправлення безпеки. Зображення ОС повинно бути чітким (без попереднього встановленого програмного забезпечення для зображень ОС). Використання збірок з торрентів \ Інтернету або будь-яких інших джерел - ЗАБОРОНЕНО.
5. Імена хостів повинні підтримуватися відповідно до політики компанії.
6. Підрозділ, група, департамент, присвоєння сайту повинні бути поточними (постійно відображати поточний стан).
7. Усі системи повинні підтримуватися до прийнятого рівня обслуговування (оновлення програмного забезпечення повинно бути автоматизовано, щоб забезпечити, щоб операційна система використовувала останню стабільну версію та найновіші оновлення безпеки, що надаються постачальником програмного забезпечення. ОС повинна мати поточну (випускную) версію, автоматизувати виправлення, де це можливо , Виправлення безпеки повинні бути встановлені, мати план відкоту.
8. Усі системи повинні мати FullDiskEncryption, Спільні паролі повинні бути задокументовані та підтримуватися на випадок особистого проживання компанії зі спільними знаннями паролів (Bitlocker для Windows FileVault для mac Veracrypt для Linux.
9. Антивірусне програмне забезпечення (AV) із сучасними базами даних повинно використовуватися на всіх робочих станціях, має бути ввімкнений самозахист AV. Оновлення AV повинно бути регулярним. (На корпоративних комп'ютерах CrowdStrike потрібно контролювати для останньої версії, стану політики, стану окремих токенів видалення.).
10. Програмне забезпечення повинно проходити перевірку на наявність зловмисності перед установкою на хостах співробітників

(перед установкою на будь-яку корпоративну систему перевірте всі програми на наявність зловмисних дій).

11. Облікові записи користувачів корпоративних робочих станцій повинні бути персоналізованими (на робочих станціях заборонено використовувати спільні облікові записи, виключення для ВМ, тестові машини повинні бути задокументовані).
12. Тільки облікові записи, відповідальні за адміністрування системи, повинні мати права адміністратора в системі. (Виключення повинні бути задокументовані).
13. Адміністративні облікові записи не можна використовувати з програмами, що мають доступ до Інтернету, такими як веб-браузери, або з потенційними Інтернет-джерелами, такими як електронна пошта. (Заборонити використання адміністративного облікового запису для програм, що мають доступ до Інтернету, таких як веб-браузери, або з потенційними джерелами Інтернету, наприклад електронною поштою, за винятком випадків, коли це необхідно для адміністрування місцевих служб. Політика повинна визначати конкретні винятки для адміністрування місцевих служб. включати інструменти на основі HTTP (S), які використовуються для адміністрування локальної системи, служб або підключених пристроїв.
14. Прошивка системи до операції повинна мати прошивку Уніфікованого розширюваного інтерфейсу мікропрограми (UEFI) і бути налаштована на роботу в режимі UEFI, а не у застарілому BIOS для машин Windows.
15. BIOS повинен бути захищений паролем (заблокувати доступ до налаштувань BIOS паролем адміністратора, паролем утиліти мікропрограми у випадку тас, робоча станція повинна бути налаштована на основне завантаження з жорсткого диска).

16. BIOS або Firmware необхідно оновити перед передачею хосту співробітнику (завжди мати робочу резервну копію попередньої версії).
17. Налаштування BIOS. Увімкнути безпечне завантаження.
18. В одній і тій самій системі заборонено використовувати альтернативні операційні системи. (Переконайтеся, що система має одну операційну систему, використання інших операційних систем може дозволити обійти безпеку.).

Вимоги до етапів 1 та 2 можуть бути змінені з випуском найкращих практик постачальників та рекомендацій CIS. Усі інші етапи необхідно реалізовувати та перевіряти для кожної машини, яку видають працівнику. Тож, слід переходити з теорії до практики, а саме до використання Windows Server.

### **3.2. Інсталювання та налаштування Windows Server**

Найпростіший спосіб інсталяції Windows Server - це чиста інсталяція, коли ви встановлюєте на порожній сервер або перезаписуєте наявну операційну систему. Оскільки сам сервер це досить дорога річ, яка використовується у компаніях для налагодження мереж, то для своєї роботи я використаю вбудовану віртуальну машину Windows – Hyper-V. Спершу на ВМ слід встановити WS, для інсталяції я обрав WS 2016 (див. Додаток А).

Після інсталяції ОС WS 2016 у діалоговому вікні «Диспетчер серверів», необхідно налаштувати та додати ролі та компоненти.

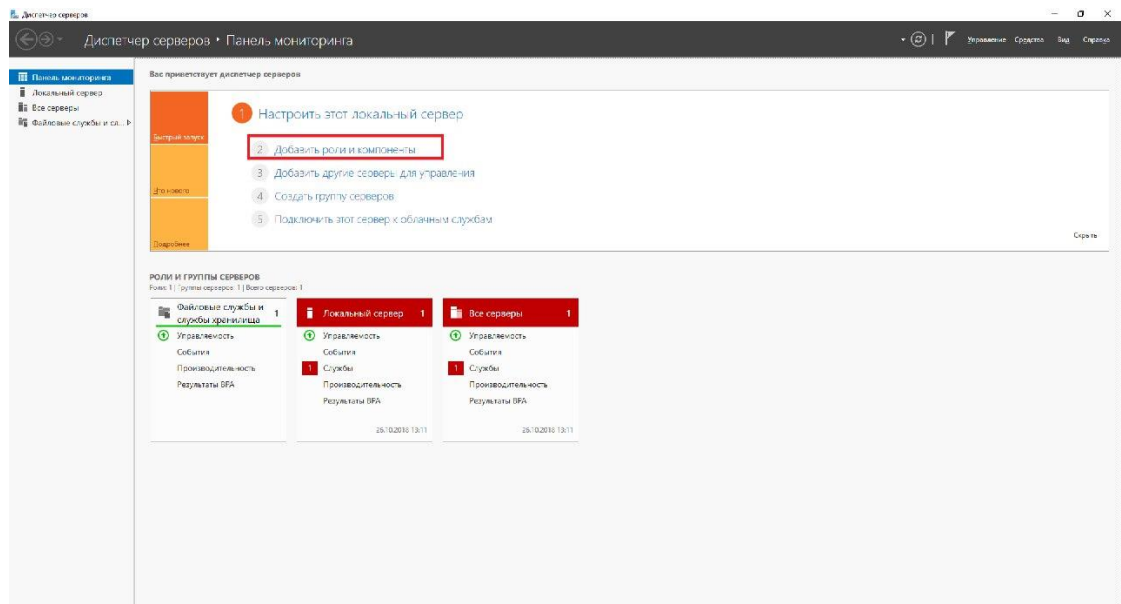


Рис. 3.1. Диспетчер серверів

Після вибору «Добавить роли и компоненты» появится страница приветствия, на которой можно нажать "Далее".

На наступному кроці ОС уточнить, що треба зробити - додати ролі і компоненти або встановити служби віддаленого доступу. Виберемо установку ролей і компонентів.

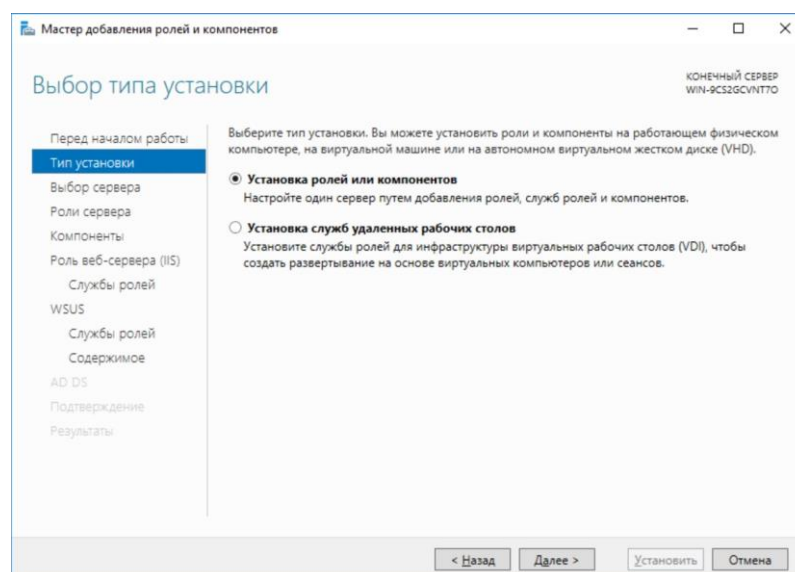


Рис. 3.2. Вибір типу інсталяції

У наступному вікні треба вибрати на які сервера встановлювати ролі і компоненти. У вас може бути кілька серверів і вони можуть бути об'єднані в пул для централізованого управління з однієї консолі. Також роль може бути встановлена на віртуальний жорсткий диск. Оскільки це новий сервер, вибираємо сервер з пулу серверів і натиснемо далі.

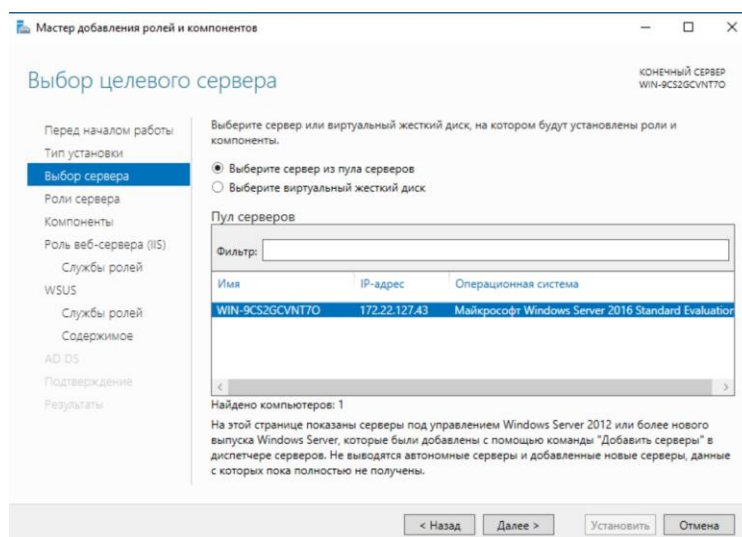


Рис. 3.3. Вибір цільового серверу

Далі, зі списку служб, необхідно вибрати "Доменні служби Active Directory".

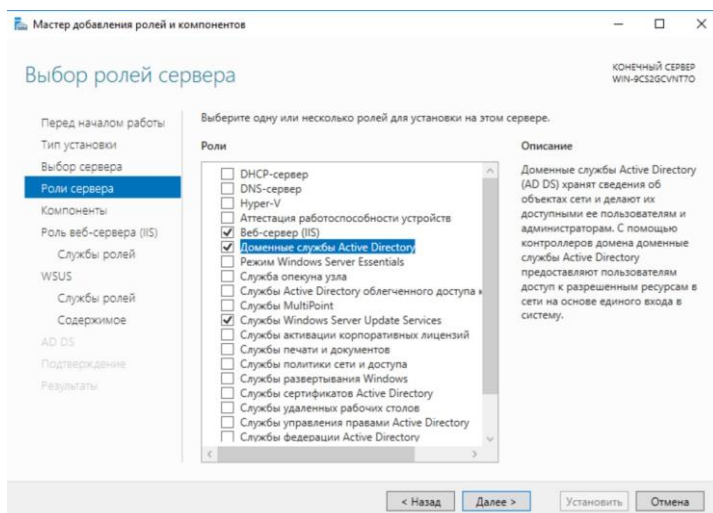


Рис. 3.4. Додавання ролей

Система також попросить встановити додаткові компоненти для вибраних служб. Погодимося, натиснувши кнопку "Додати компоненти" та переходимо до вибору компонентів. Серед яких вибираємо «Шифрование диска BitLocker». За допомогою цього компоненту можна побачити ключ шифрування BitLocker на комп'ютері, який приєднаний до домену.

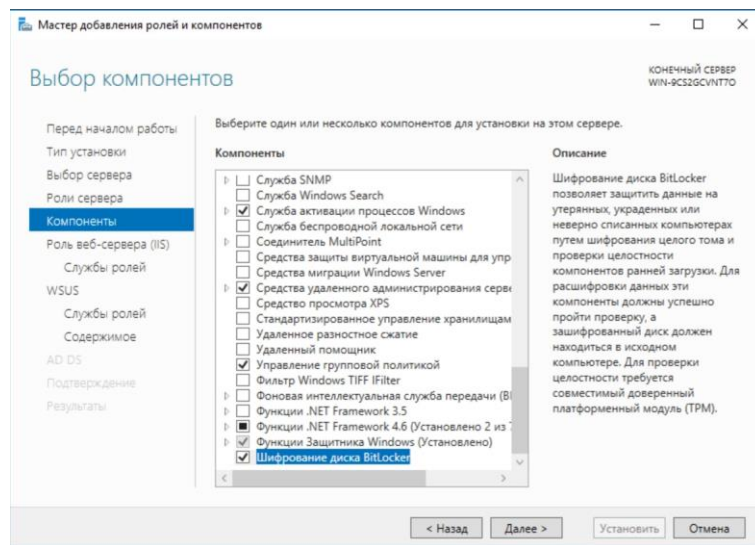


Рис. 3.5. Додавання компонентів

У вікні «Роль веб-сервера» та вікні «WSUS» при необхідності вибираємо ролі та переходимо до вибору розташування.

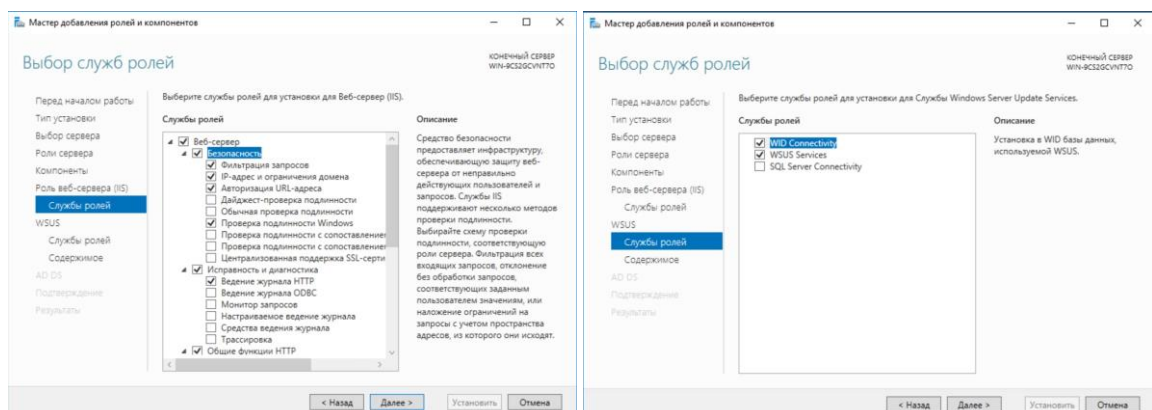


Рис. 3.6(1) та Рис. 3.6(2). Вибір компонентів служби ролей

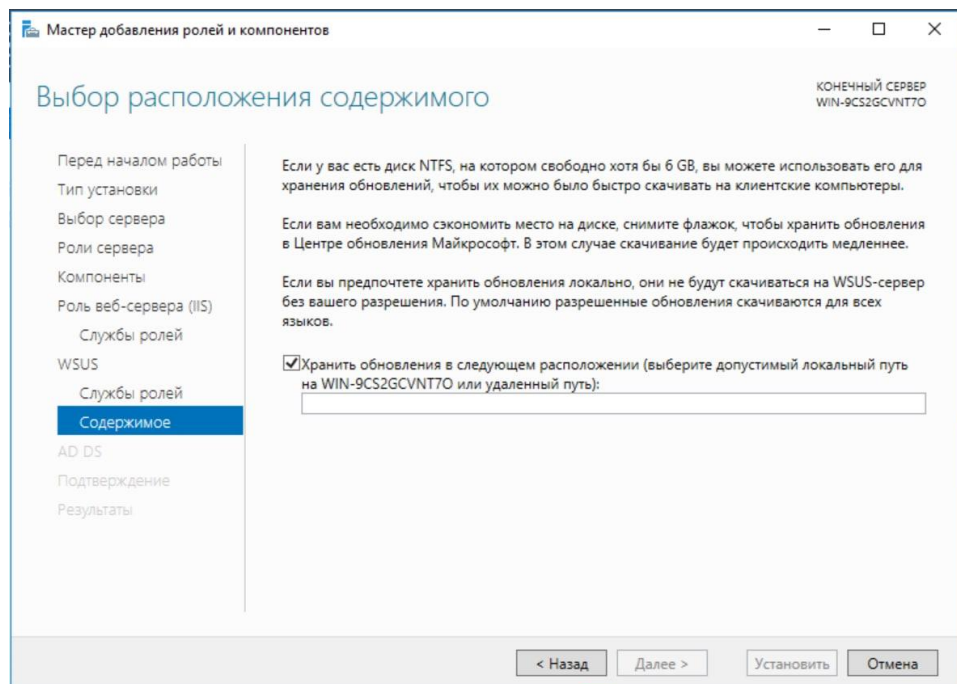


Рис. 3.6(3). Вибір сховища оновлень

Після вибору зберігання оновлень на локальній машині(у мене вона віртуальна), переходимо до наступного пункту.

У наступному вікні буде сторінка загальної інформації про те що таке AD.

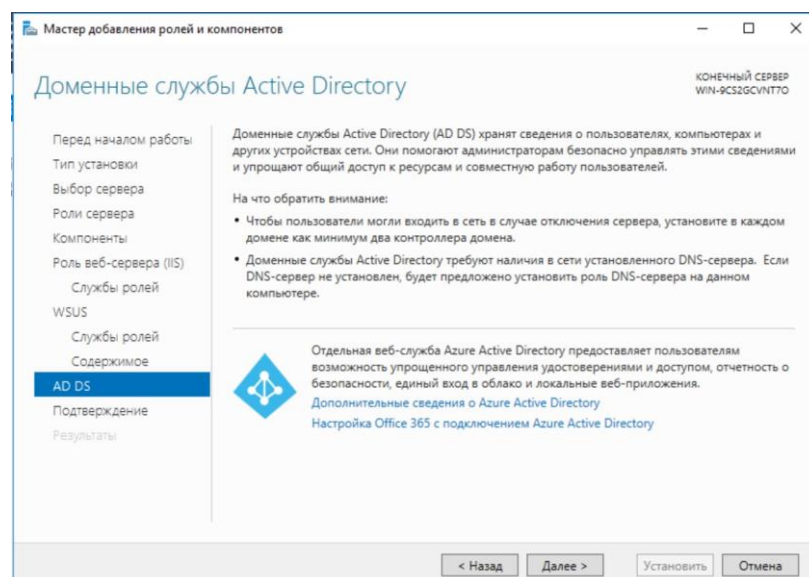


Рис. 3.7. Відомості про AD

Далі підтверджуємо інсталяцію компонентів та вибираємо автоматичний перезапуск серверу при необхідності.

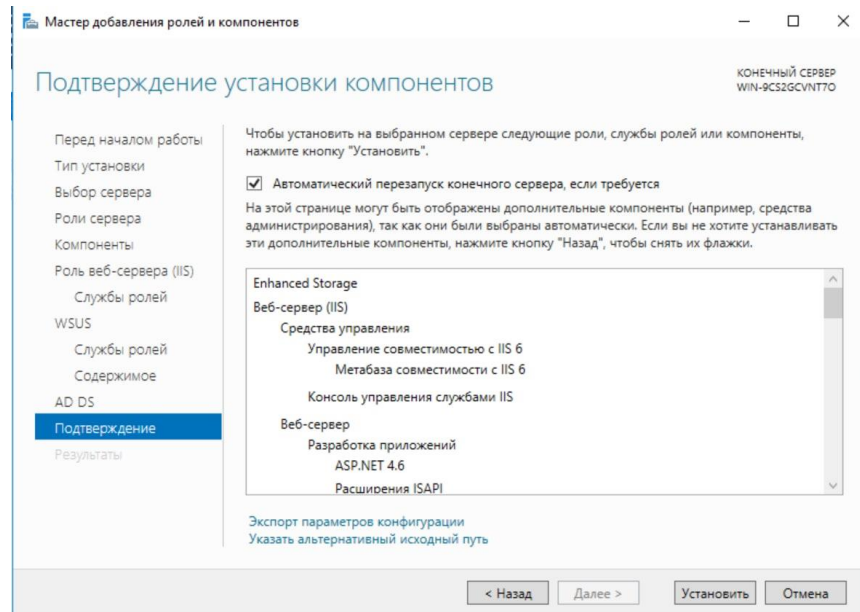


Рис. 3.8. Підтвердження інсталяції компонентів

Натискаємо кнопку «Установить» та чекаємо поки пройде інсталяція.

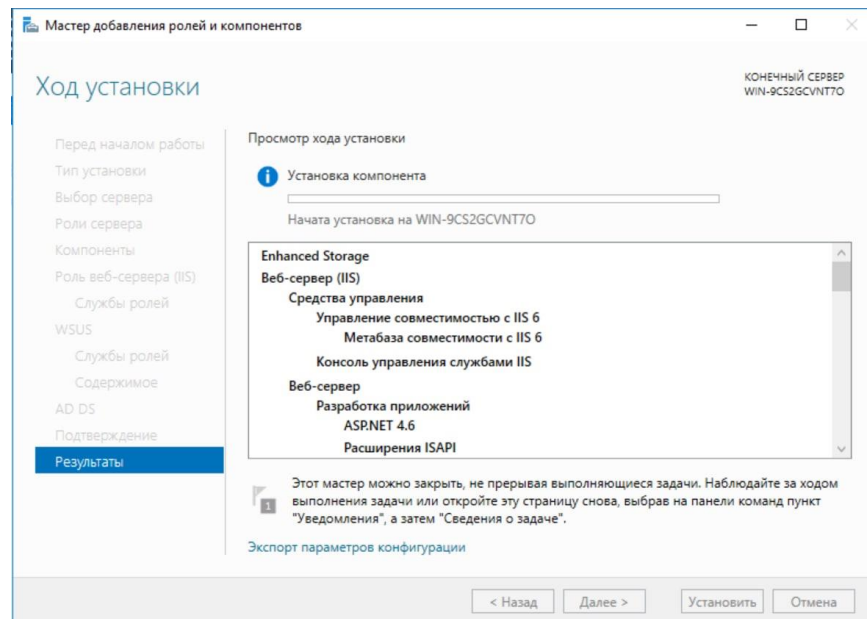


Рис. 3.9. Установка ролей та компонентів

Після установки відкриється вікно «Диспетчер серверов» з встановленими ролями та компонентами.

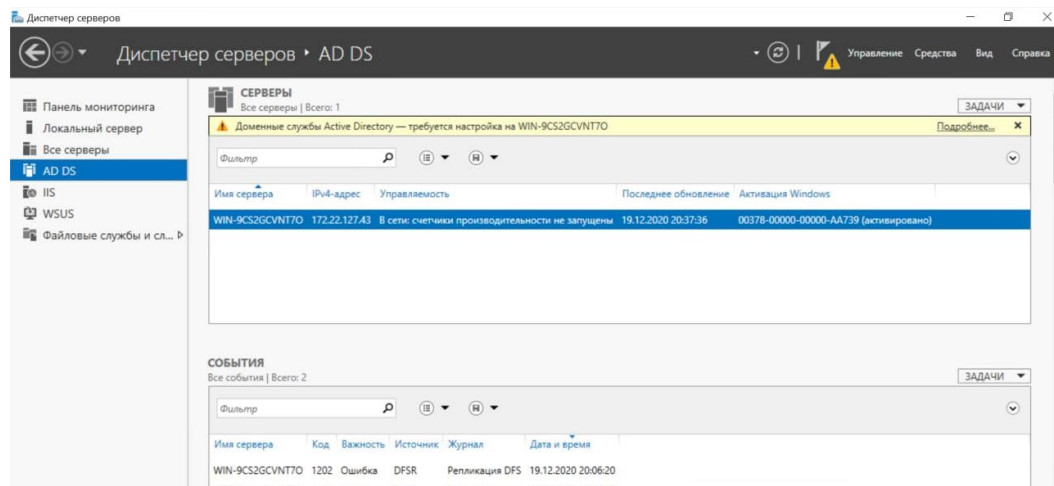


Рис. 3.10. Диспетчер серверів після встановлення ролей і компонентів

### 3.3. Розгортання Active Directory

Active Directory (AD) є основою інфраструктури домену на базі Windows Server, що забезпечує канал для впровадження та підтримки безпеки. Безпечна

AD забезпечить захист усіх елементів на підприємстві. Бо, ігнорування безпеки AD може поставити під загрозу всю вашу інфраструктуру.

Переваги від впровадження Active Directory:

1. Оптимізація витрат на впровадження, зниження витрат на технічну підтримку.
2. Надійність і захищеність системи.
3. Підвищення ефективності роботи, як кожного окремого співробітника, так і всієї компанії в цілому.
4. Утримання і лояльність клієнтів шляхом впровадження додаткових сервісів.

Однак захист AD не є тривіальним завданням. Багато підсистем безпеки Windows інтегровані з нею, і багато з них можуть бути використані для її захисту. База даних облікових записів, протокол аутентифікації Kerberos, політика паролів, визначення прав користувачів та системних засобів управління, присвоєння дозволів на об'єкти - всі вони містяться та керуються з AD. Необхідно, також врахувати розподіл його елементів і характер людей, які з ним взаємодіють. AD - це не якась сутність, яка може бути локалізована на одній машині, вона охоплюють де-яку кількість комп'ютерів та мереж. Має широку область для атаки і багато вразливостей, які повинні бути оцінені або усунені. Існує буквально сотні кроків, які слід враховувати при розробці, впровадженні та підтримці безпеки AD.

Після закінчення установки, можна приступати до розгортання AD. Для цього повернемося в диспетчер сервера і перейдемо на вкладку AD DS (Active Directory Domain Service - Доменні Служби Active Directory). На ній нас відразу попередять, що потрібно налаштування служб AD.

Натиснемо на кнопку "Подробнее" на жовтому тлі, яке показане на Рис 3.1.10. і виберемо "Підвищити роль цього сервера", яке приведено нижче на Рис 3.2.1.

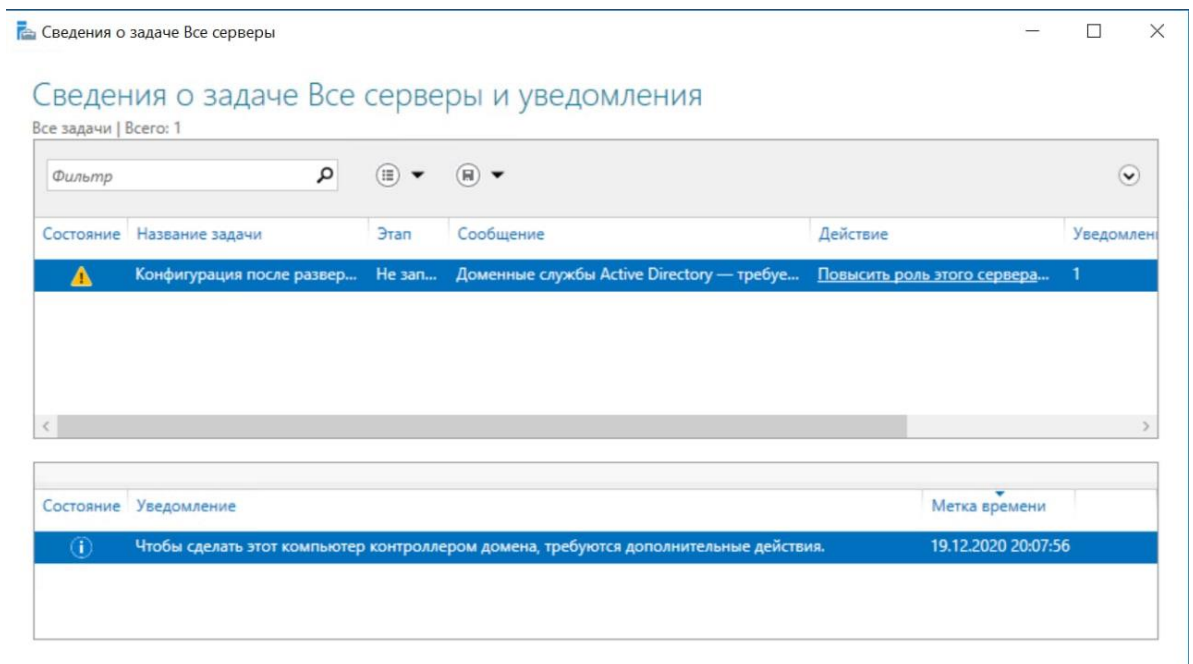


Рис 3.11. Вікно відомостей

Після чого, запуситься майстер настройки AD. На першому кроці необхідно визначити чи існує у нас інфраструктура AD або будемо створювати її з нуля.

Доменом називається основна адміністративна одиниця в мережевій інфраструктурі підприємства, в яку входять всі мережеві об'єкти, такі як користувачі, комп'ютери, принтери, загальні ресурси і т.д. Кілька доменів, пов'язаних між собою, називається лісом. Св'язані між собою домени називаються відносинами довіри або ієрархією.

Я створюю новий ліс, так як роблю нову інфраструктуру. Також, необхідно задати ім'я домену.

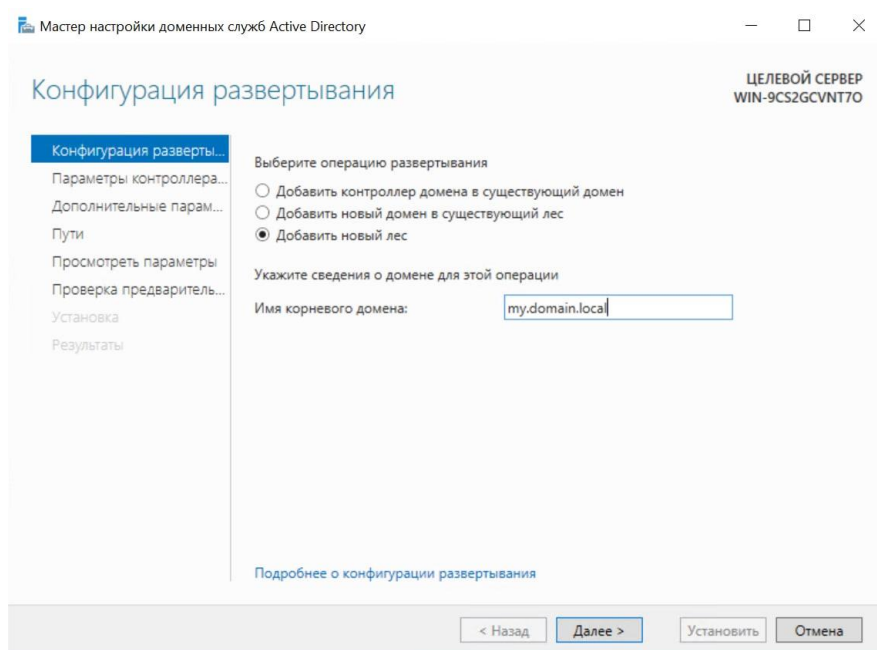


Рис 3.12. Створення лісу та вибір ім'я для домену

Наступним кроком необхідно вибрати режим роботи домену і лісу. Чим вище рівень, тим більше можливостей підтримується, але й новіша клієнтська ОС повинна використовуватися на комп'ютерах. Також, рекомендується вказати, що даний сервер буде сервером DNS. Треба, обов'язково ввести пароль для служби відновлення AD та зверніть увагу, що це не пароль адміністратора домена.

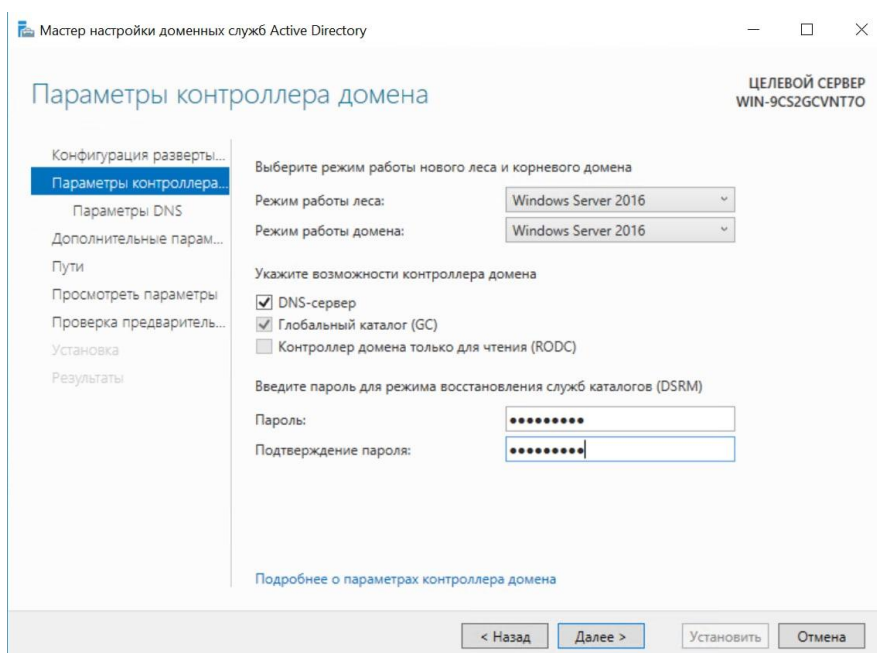


Рис 3.13. Вибір контролеру домена, як DNS-сервера та становлення пароля для відновлення AD

Якщо пароль буде занадто простий, отримаємо наступну помилку:

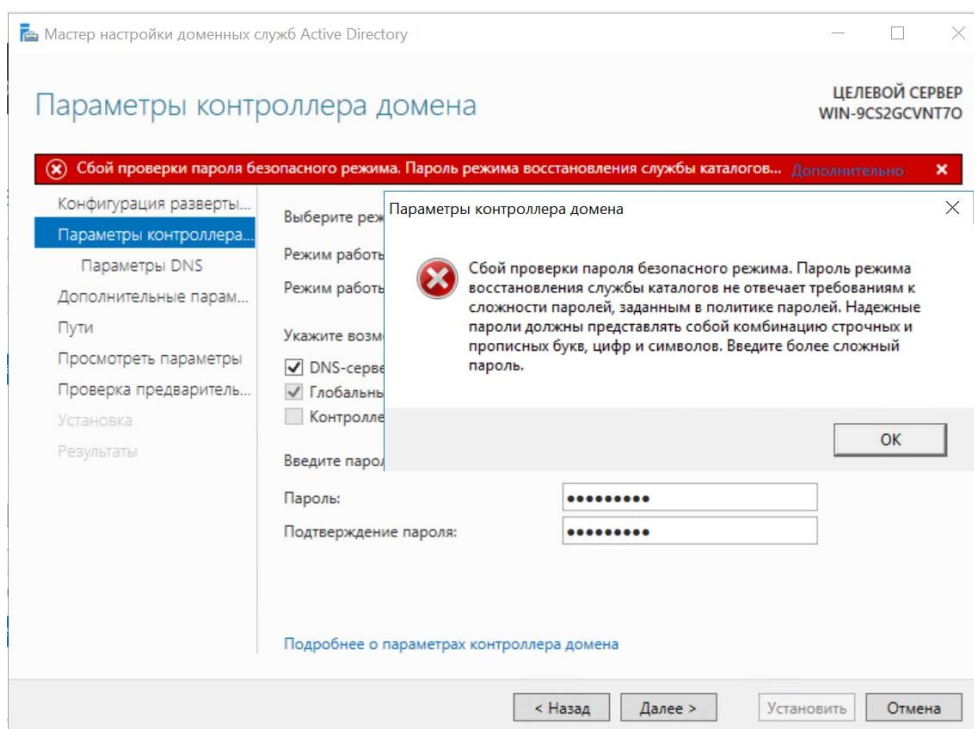


Рис 3.14. Помилка заданого паролю

Після введення надійного паролю, переходимо до наступного етапу настройки DNS.

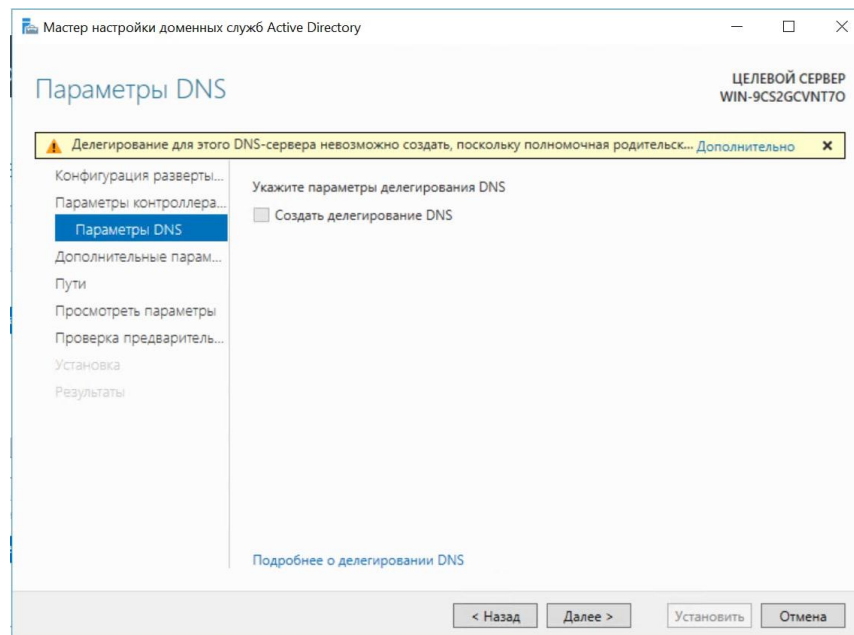


Рис 3.15. Этап настройки DNS

Наступні кроки, як «Пути», «Просмотреть параметры» та «Проверка предварительных требований» не потребують дій.

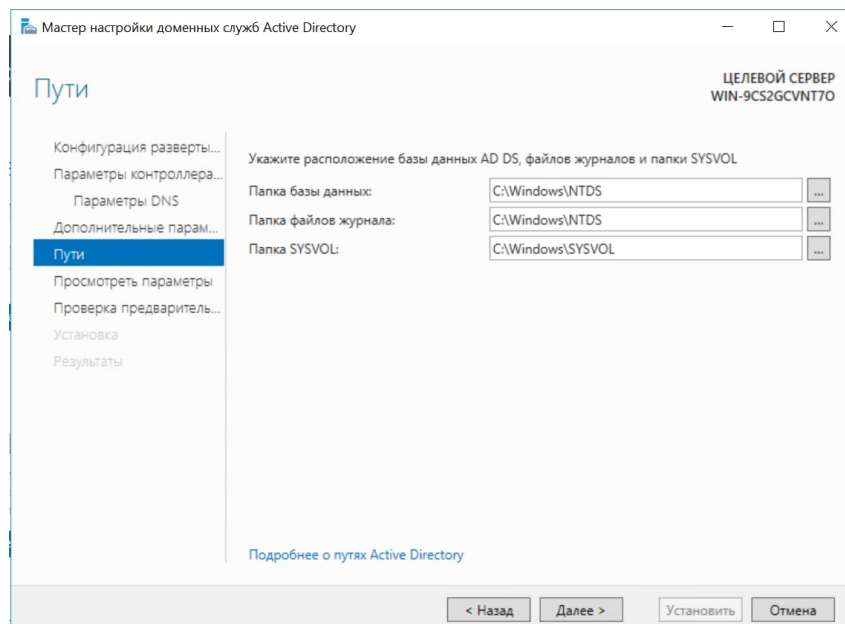


Рис. 3.16. Налаштування шляху

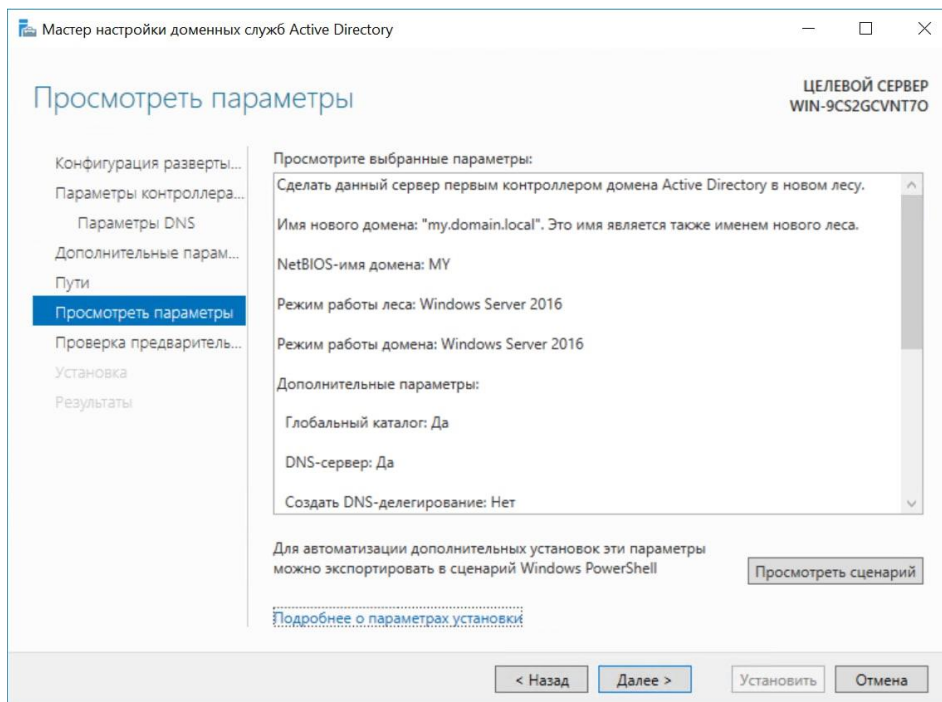


Рис. 3.17. Перегляд параметрів

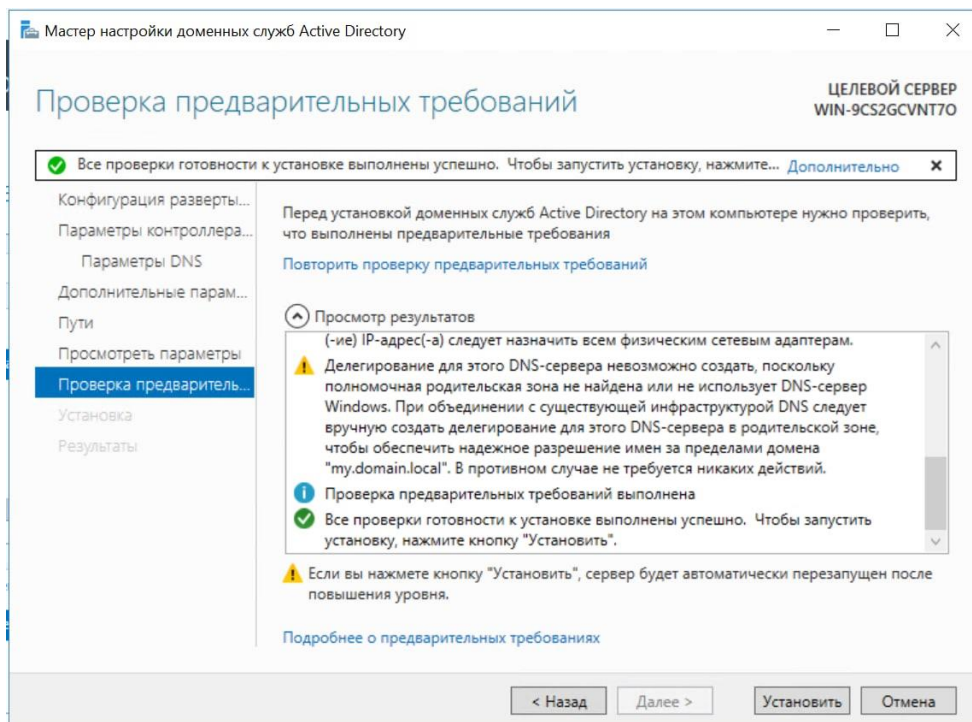


Рис. 3.18. Перевірка вимог

На цьому етапі слід натиснути кнопку «Установить», після чого почнеться інсталяція доменних служб AD та вибраних параметрів. По закінченню установки система автоматично перезавантажиться.

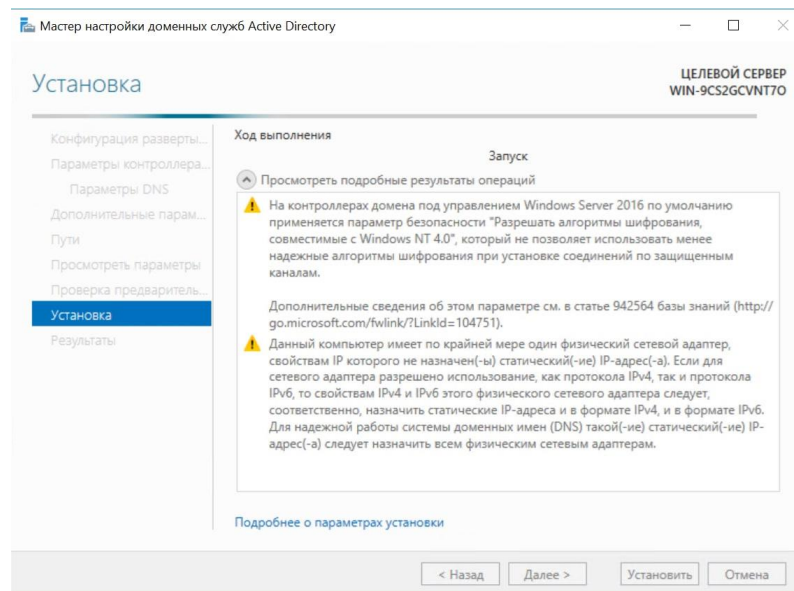


Рис. 3.19. Процес інсталяції AD

Після перезавантаження серверу у вікні диспетчера серверів можна буде відкрити вікно адміністрування Active Directory.

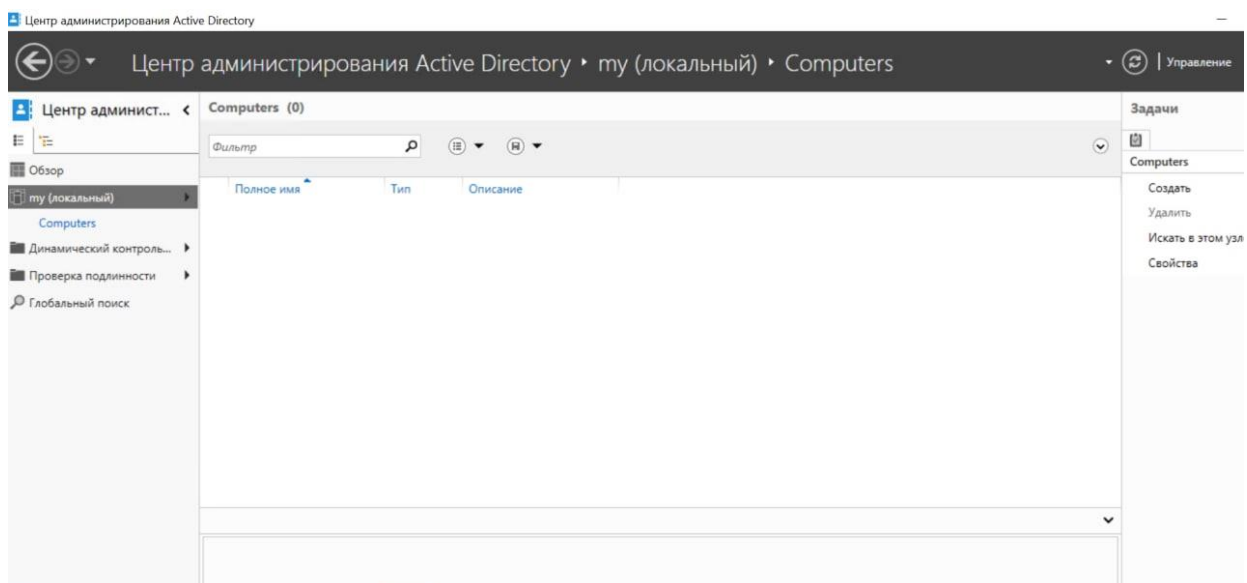


Рис. 3.20. Вікно адміністрування Active Directory

З цього вікна можна створювати та налаштовувати доменні правила, політики, облікові записи, комп'ютери, групи та інше. Тож, перейдемо до створення.

### 3.4. Реалізація безпеки підприємства за допомогою доменних правил, політик, облікових записів в Active Directory

#### 3.4.1. Налаштування політики паролів

Для забезпечення високого рівня безпеки облікових записів в домені Active Directory адміністратор повинен налаштувати і впровадити політику паролів, що забезпечує достатню складність, довжину пароля і частоту зміни пароля користувачів і сервісних облікових записів. Тим самим можна ускладнити зловмисникові можливість підбору або перехоплення паролів користувачів.

За замовчуванням в домені AD настройка єдиних вимог до паролів користувачів здійснюється за допомогою групових політик. Політика паролів облікових записів домену налаштовується в політиці Default Domain Policy. Для налаштування політики паролів та інших політик, треба відкрити консоль управління доменними GPO (Group Policy Management console - gpmmc.msc).

У відкритому вікні домену, треба знайти політику Default Domain Policy, натиснути по ній ПКМ і вибрати Edit. У відкритих полях для редагування я встановив необхідні параметри паролів.

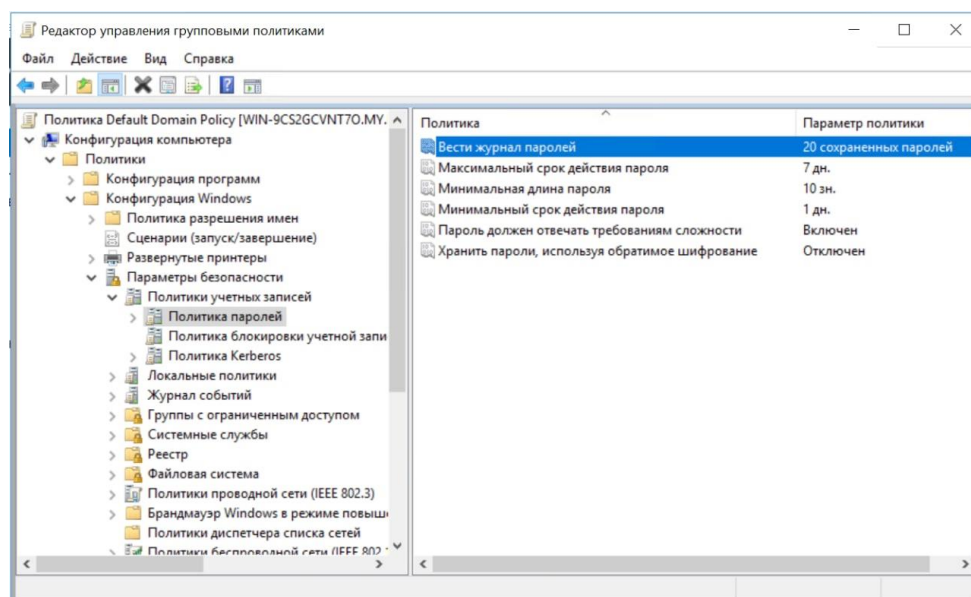


Рис. 3.21. Налаштування доменних параметрів паролю

Перевірити поточні налаштування політики паролів AD можна на будь-якому комп'ютері домену, для цього треба скористатись командою gpresult.

В домені може бути тільки одна подібна політика паролів, яка застосовується на корінь домену (тобто, звичайно, нюанси, але про них нижче). Якщо застосувати політику паролів на OU, її налаштування будуть ігноровані. За керування доменної пральний політики відповідає контролер домену, власник FSMO ролі PDC Emulator. Політика застосовується до комп'ютерів домену, а не користувачам. Для редагування налаштувань Default Domain Policy необхідні права адміністратора домена.

Параметри групової політики управління паролями діють на всіх користувачів і комп'ютери домену. Якщо потрібно створити окремі політики паролів для різних груп користувачів, вам потрібно використовувати функціонал роздільних політик паролів Fine-Grained Password Policies, які з'явилися у версії AD Windows Server 2008. Гранульовані політики паролів дозволяють, наприклад, вказати підвищену довжину або складність паролів для облікових записів адміністраторів, або навпаки спростити (відключити) пароль для якихось облікових записів, що в свою чергу є недопустимим для компанії.

#### **3.4.2. Створення підрозділів, облікового запису та додання груп до нього**

Для початку я створю новий підрозділ Company, який буде містити в собі ще 2 підрозділи – Company Computer та Company Users. З назв цих підрозділів зрозуміло, що один для зберігання доменних комп'ютерів, а другий для зберігання облікових записів користувачів.

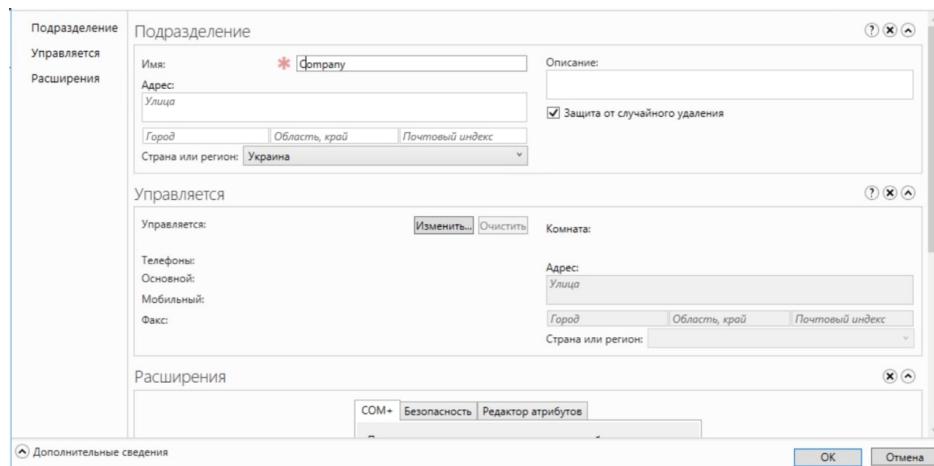


Рис.3.22. Створення підрозділу

Та створюємо в підрозділі Company ще 2 підрозділи.

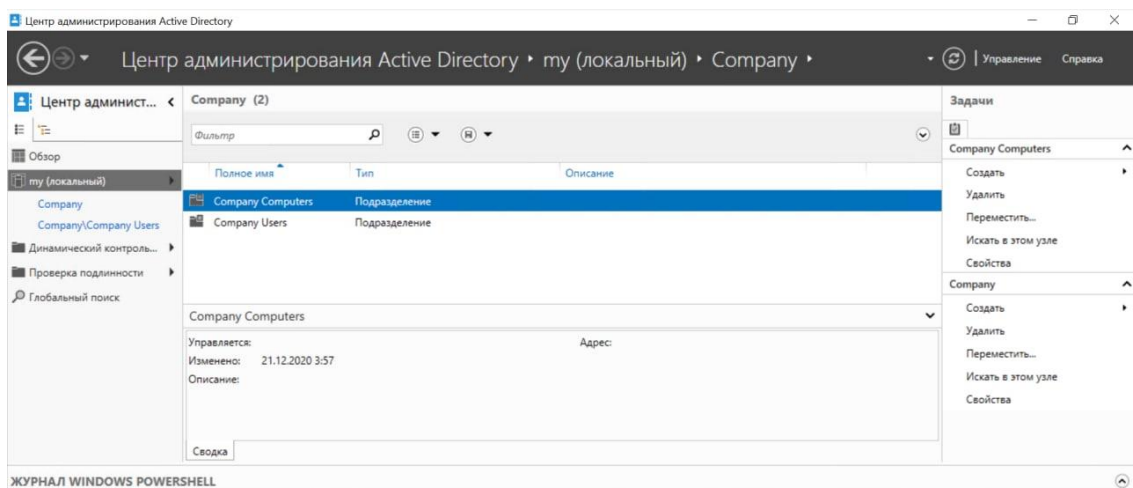


Рис.3.23. Ієрархія підрозділів

Для створення нових облікових записів і адміністраторів необхідно відкрити оснащення Active Directory Users and Computers, для цього, треба зайти у Диспетчер серверів і перейти до розділ AD DS. У контекстному меню сервера, вибрати відповідну оснастку. Проте, обліковий запис можна створити і з Центру адміністрації AD.

**Олександр Kharkov** ЗАДАЧИ РАЗДЕЛЫ

**Учетная запись**

Имя: Oleksandr  
 Отчество: Kharkov  
 Фамилия: Kharkov  
 Полное имя: Oleksandr Kharkov  
 Вход пользователя (UPN): oleksandr.kharkov @ my.domain.local  
 Вход пользователя (Sam...): my oleksandr.kharkov

Срок действия учетной з: ☒ Никогда ☐ Конец

Параметры пароля:  
☐ Требовать смены пароля при следующем входе в систему  
☒ Другие параметры пароля  
☐ Для интерактивного входа требуется смарт-карта или Micros...  
☒ Срок действия пароля не ограничен  
☐ Запретить смену пароля пользователем

Параметры шифрования:  
 Другие параметры:

☐ Защита от случайного удаления

Время входа в систему... Вход в...

**Организация**

Отображаемое имя: Oleksandr Kharkov  
 Комната:  
 Эл. почта:  
 Веб-страница:  
 Телефоны:

Должность:  
 Отдел:  
 Организация:  
 Менеджер: Изменить... Очистить  
 Подчиненные: Добавить...

Дополнительные сведения

OK Отмена

Рис.3.24. Створення облікового запису

Одразу додам до свого доменного облікового запису права адміністратора домену та інші права адміністратора.

Найдено несколько имен

Имени "админ" соответствует несколько объектов. Выберите один из них из списка или введите другое имя.

Совпадающие имена:

Имя	Описание	В папке
Администраторы домена	Назначенные администрато...	my.domain.local/Users
Администраторы основного уровня	Члены этой группы могут вы...	my.domain.local/Users
Администраторы основного уровня пред...	Члены этой группы могут вы...	my.domain.local/Users
Администраторы предприятия	Назначенные администрато...	my.domain.local/Users
Администраторы схемы	Назначенные администрато...	my.domain.local/Users

OK Отмена

Рис.3.25. Додавання груп до облікового запису

Тепер працівник, зможе підключитись доменним обліковим записом до корпоративної техніки, а адміністратор домену може керувати, змінювати, блокувати та розблоковувати облікові записи працівників.

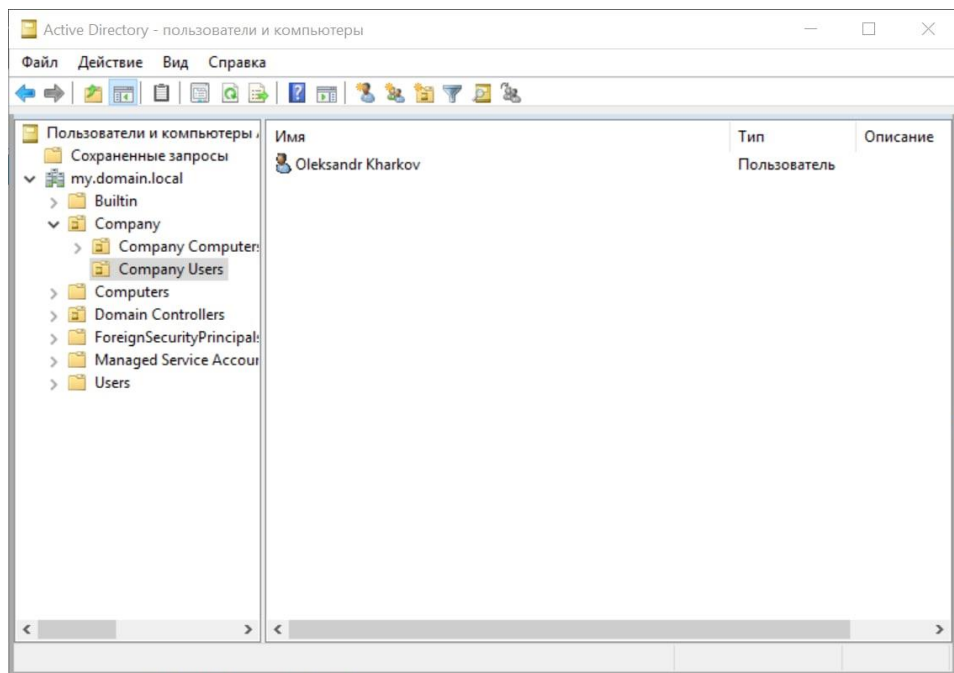


Рис.3.26. Облікового запису в оснасті Active Directory Users and Computers

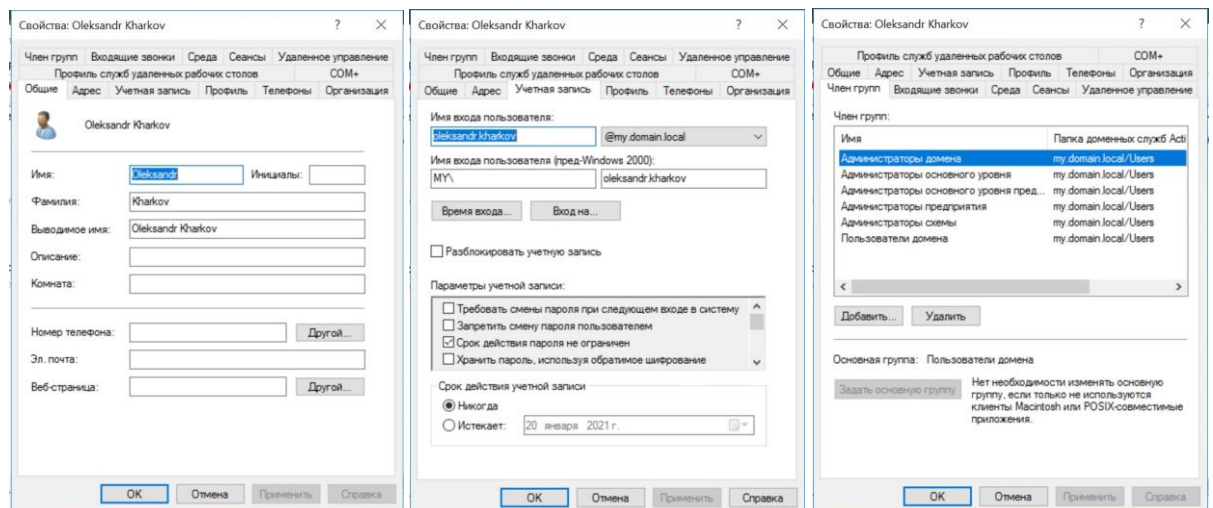


Рис.3.27(1,2,3). Параметры облікового запису.

### 3.4.3. Створення та додання комп'ютера до домену

Для початку створю комп'ютер у підрозілі Company Computers.

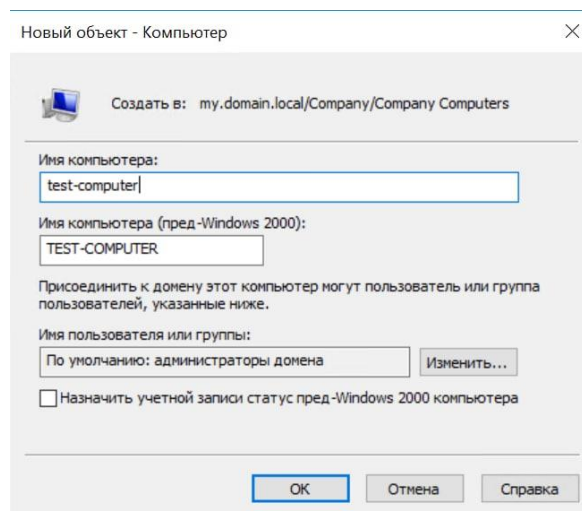


Рис.3.28. Створення комп'ютеру в домені

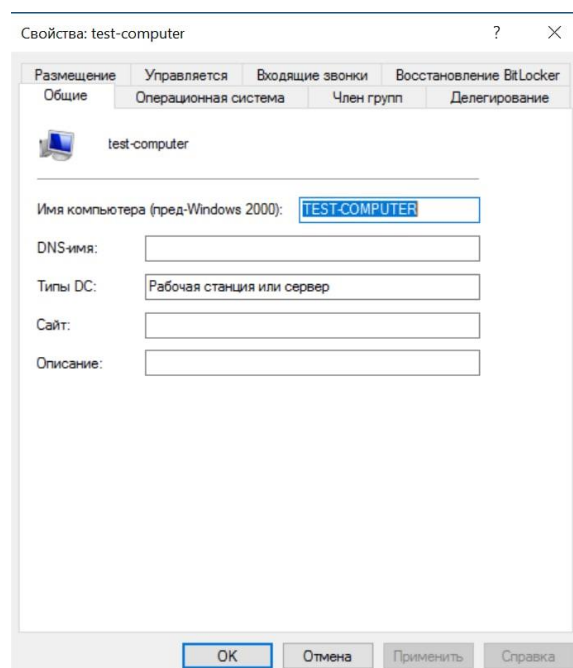


Рис.3.29. Параметры комп'ютера

Зараз розглянемо приклад того, як ввести комп'ютер в домен. Насамперед, необхідно налаштувати з'єднання з мережею. Відкриваємо центр управління мережами та ввести дані, такі як IP-адреса, маска підмережі, шлюз і DNS-сервер. Тепер перейдемо безпосередньо до додавання комп'ютера в домен.

Для додання комп'ютера в домен необхідно зайти в параметри комп'ютера, зайти до параметрів системи та змінити їх.

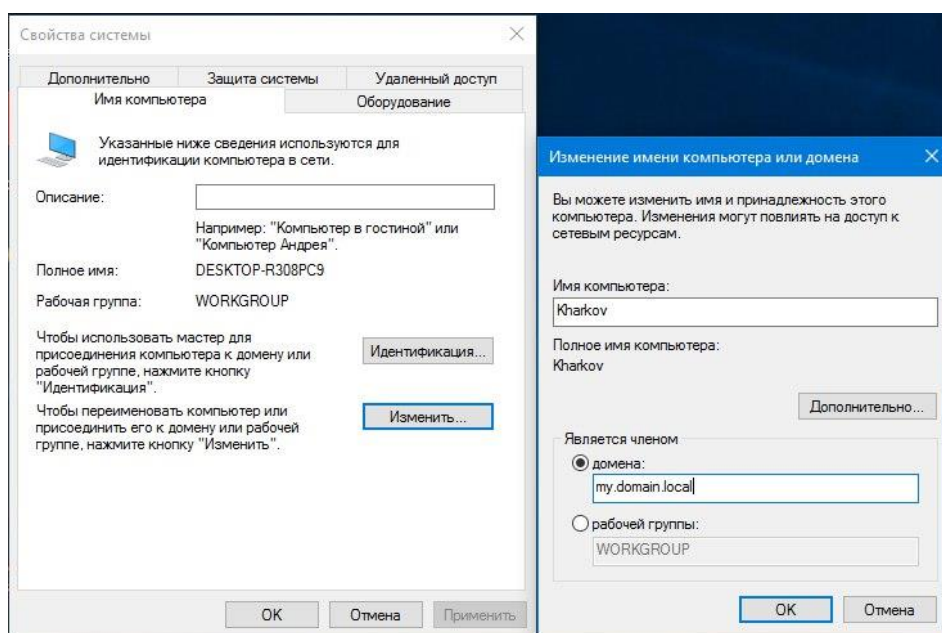


Рис.3.30. Додавання комп'ютера до домену

Після натиснення на кнопку «ОК», буде запропоновано ввести ім'я користувача і пароля, який має право на приєднання комп'ютерів до домену, тобто, адміністратора домену. Після цього машину потрібно перезавантажити. По закінченню перезавантаження комп'ютер буде в домені з встановленим ім'ям(хостом).

Комп'ютер, який було заведено в домен створюється в підрозділі Computers за замовчуванням.

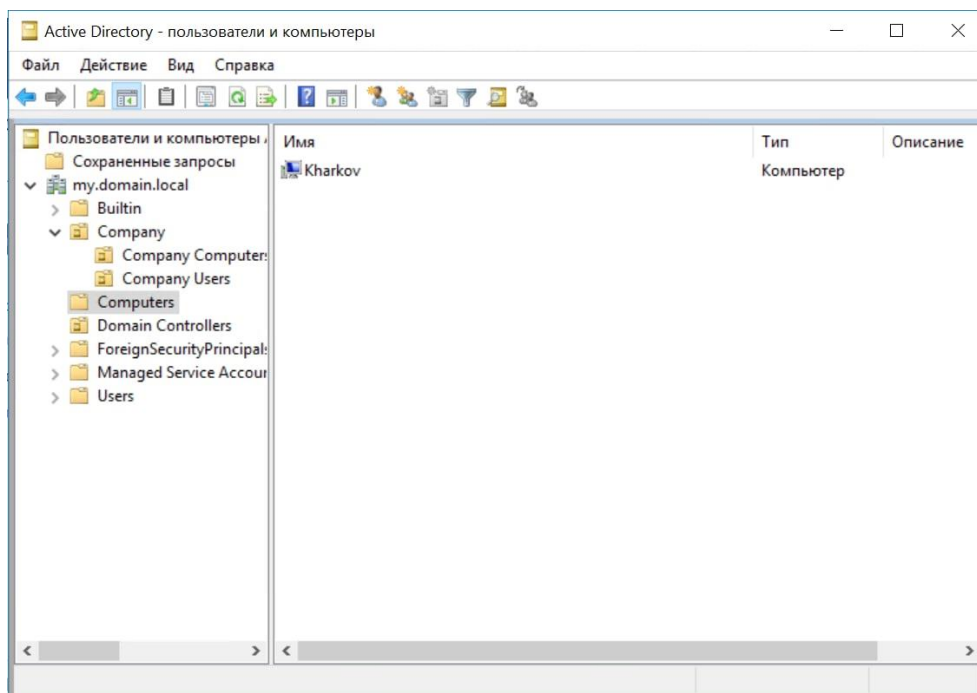


Рис.3.31. Комп'ютер, який завели в домен

Після заведення комп'ютера в домен на нього можна зайти лише з корпоративної мережі та лише за допомогою доменного облікового запису.

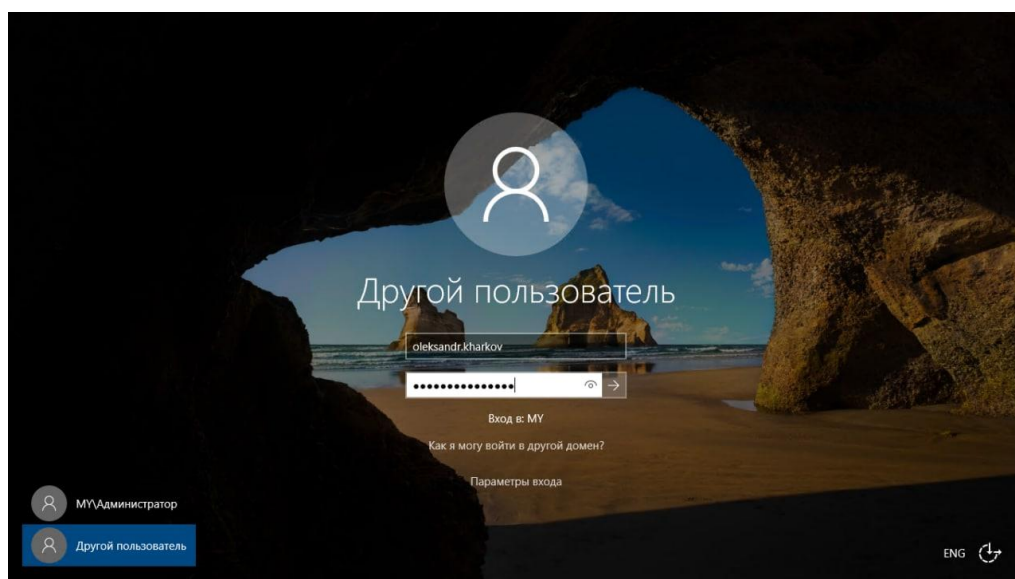


Рис.3.32. Вхід на корпоративній машині доменним обліковим записом

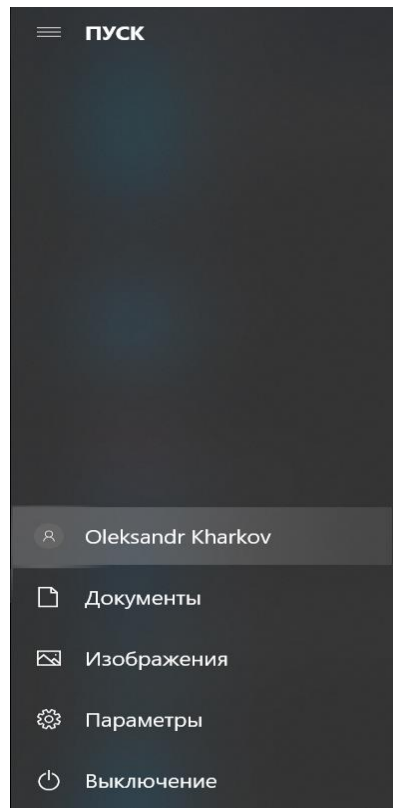


Рис.3.33. Підтвердження входу до корпоративного облікового запису

Оскільки, було встановлено служби Active Directory на базі Windows Server 2016 та налагоджено домен, облікові записи, політики та доступи для працівників. Запроваджено, правила входу до облікових записів, забезпечення безпеки техніки та можливість видавати доступ до русерсів. Тому, завдання з реалізації забезпечення інформаційної безпеки на підприємстві можна вважати виконаним.

## ВИСНОВКИ

Для забезпечення високого рівня безпеки на підприємстві, у першому розділі було розглянуто види інформаційних загроз та види атак, які можуть бути реалізовані зловмисниками для заволодіння інформацією або доступом. Далі розглядалися види та способи захисту інформації, як для звичайних користувачів мережі Інтернет, так і для працівників підприємства та ресурсів компанії.

Вже в третьому розділі я підійшов до реалізації системи захисту інформації підприємства. Установивши та налаштувавши Windows Server на віртуальній машині, розгорнув доменні служби Active Directory. В середині якої, вже з правами адміністратора налаштовував і створював облікові записи працівників компанії, корпоративну техніку, методи шифрування, політики та доступи, що забезпечує достатню захищеність для зовнішніх та внутрішніх ресурсів і т.п. Що значно ускладнює зловмисникам можливість здійснення атаки та заволодіння корпоративними даними або даними самих працівників.

Також, кожного дня слід робити бекапи домену для забезпечення резервних копій у разі виникнення проблем із сервером або атаки на нього.

## СПИСОК БІБЛЮГРАФІЧНИХ ПОСИЛАНЬ

1. *Лукацкий А.* Обнаружение атак. — СПб.: БХВ-Петербург, 2001. — 624 с.
2. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие. — М.: Горячая линия – Телеком, 2004. — 280 с.
3. *Соколов А.В., Шаньгин В.Ф.* Защита информации в распределенных корпоративных сетях и системах. — М.: ДМК Пресс, 2002. — 656 с.
4. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. — СПб.: «Наука и техника», 2004. — 384 с.
5. Інформаційна безпека людини як споживача телекомунікаційних послуг: Монографія / І.В. Арістова, Д. В. Сулацький ; НДІ інформатики і права НАПрН України. — К. : Право України; Х. : Право, 2013. — 184 с.
6. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. — К.: Кондор, 2004. — 384 с.
7. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf>
8. <http://hosteddocs.ittoolbox.com/Quest072904.pdf>
9. <https://www.praxiom.com/iso-27001.htm>
10. <https://www.praxiom.com/nist-cybersecurity-program.htm>
11. <https://1cloud.ru/help/windows/active-directory-domain-services-ustanovka-i-nastrojka-windows-server>
12. <https://myfirstcomp.ru/network/kak-vvesti-kompyuter-v-domen-na-primere-kompyutera-pod-upravleniem-windows-7/>

## Додаток А

### Визначення

**1. TCP (Transmission Control Protocol)** — разом із протоколом IP є стрижневим протоколом Інтернету, який дав назву моделі TCP/IP. Протокол призначений для управління передачею даних у комп'ютерних мережах, працює на транспортному рівні моделі OSI. На відміну від іншого поширеного протоколу транспортного рівня UDP, TCP забезпечує надійне доправлення даних від хоста-відправника до хоста-отримувача, для цього встановлюється логічний зв'язок між хостами. Таким чином TCP належить до класу протоколів зі встановленим з'єднанням.

**2. UDP (User Datagram Protocol)** — один із протоколів в стеку TCP/IP. Від протоколу TCP він відрізняється тим, що працює без встановлення з'єднання. UDP — це один з найпростіших протоколів транспортного рівня моделі OSI, котрий виконує обмін повідомленнями без підтвердження та гарантії доставки. При використанні протоколу UDP відповідальність за обробку помилок і повторну передачу даних покладена на протокол рівнем вище. Але попри всі недоліки, протокол UDP є ефективним для серверів, що надсилають невеликі відповіді великій кількості клієнтів.

**3. Автентифікація** — процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора. З позицій інформаційної безпеки автентифікація є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації і передують авторизації.

**4. Система управління інформаційною безпекою (СУІБ)** — частина загальної системи управління, яка ґрунтується на підході, що враховує ризики інформаційної безпеки як бізнес-ризик, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Для процесів СУІБ застосована модель ПВПД (плануй-виконуй-перевірй-дій):

- Plan (планування) - фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;
- Do (дія) - етап реалізації та впровадження відповідних заходів;
- Check (перевірка) - фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами;
- Act (поліпшення) - виконання превентивних і коригуючих дій

**5. ACL (access control list)** — це строго говорячий механізм для вибору з усієї потокової трафіки якої-то частини, за заданими критеріями. Наприклад, за допомогою маршрутизатора проходить безліч пакетів, і ось такий ACL вибирається з безлічі лише тих пакетів, які вводяться з підсети 192.168.1.0/24:

```
access-list 1 permit 192.168.1.0
```

Що далі робити з цим трафіком - пока невідомо. Наприклад, трафік, який потрапляє під ACL, може замовчуватися в VPN-тоннелі або підвергати трансляцію адрес (NAT). У курсі CCNA розглядається два способи використання ACL: основна - це фільтрація трафіка, вдруге - використання ACL при налаштуванні NAT. Важливо наступне: не має значення, де і для яких цілей ми можемо використовувати ACL, правила написання ACL від цього не змінюються. Крім того, якщо ми лише створили ACL, то він не вказує на те, що не впливає. ACL - це просто кілька неробочих строків у конфігурації, тому ми не можемо застосовувати їх, наприклад, на інтерфейсі, для фільтрації трафіку.

ACL-і бувають два види: стандартні та розширені. Стандартні можливості дозволяють відфільтровувати трафік лише за одним критерієм: адреса відправника, в CCNA розглядається конкретно лише ір адреса відправника.

**6. User Acceptance Testing (UAT)** — це приймальне тестування, яке проводиться кінцевими користувачами системи для прийняття рішення по впровадженню.

**7. WAF (Web application firewall, файрвол веб-додатків)** - сукупність моніторів і фільтрів, призначених для виявлення і блокування мережових атак на веб-додаток. WAF відносяться до прикладного рівня моделі OSI.

Веб-додаток може бути захищене силами розробників самого додатка без використання WAF. Це вимагає додаткових витрат при розробці. Наприклад, зміст відділу інформаційної безпеки. WAF увібрали в себе можливість захисту від усіх відомих інформаційних атак, що дозволяє делегувати йому функцію захисту. Це дозволяє розробникам зосередитись на реалізації бізнес-логіки додатка, не замислюючись про безпеку.

**8. UCS (Universal Character Set, Универсальный набор символов)** — стандарт кодировки символів, определённый ISO/IEC 10646, UCS-2, UCS-4.

**9. Microsoft Servers** (раніше називалася *Windows Server System*) — бренд, який охоплює серверні продукти Microsoft. Він включає в себе редакції Windows Server самої операційної системи Microsoft Windows, а також продукти, орієнтовані на більш широкий бізнес-ринок. На відміну від продуктів Microsoft Dynamics або Microsoft Office, більшість продуктів, які продаються під цим брендом, самі по собі не призначені для надання послуг.

До складу програмного забезпечення та технології Microsoft Servers входять:

- Операційні системи.
- Пропозиції операційної системи.
- Продуктивність.
- Безпека.

**10.** Hyper-V більш відомий як технологія віртуалізації серверів; проте, починаючи з Windows 8, він також доступний в клієнтської операційної системи. У Windows 10 ми значно поліпшили роботу, зробивши Hyper-V відмінним рішенням для розробників та ІТ-спеціалістів.

Microsoft Hyper-V, кодова назва Viridian, - це нативний (тип 1) гіпервизор, який, на відміну від VMware Workstation, VirtualBox та інших гіпервизорів типу 2, працює безпосередньо на обладнанні.

## Додаток Б

### Інсталювання Windows Server

Після запуску віртуальної машини на базі Hyper-V, необхідно встановити на неї операційну серверну систему. Для своєї ВМ я обрав Windows Server 2016. Перейдемо до етапів інсталяції.

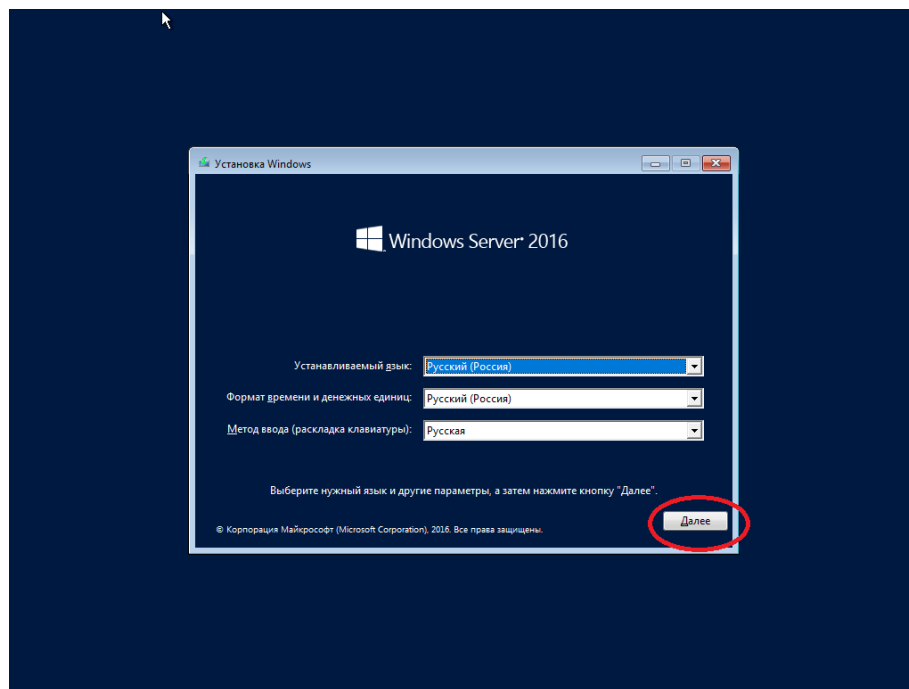


Рис. 4.1. Перший етап. Вибір мови та параметрів.

На наступному етапі у Вас запитатимуть ключ активації для Windows Server 2016, ми його введемо пізніше, вже в самій системі. А при установці вибираємо "У мене немає ключа продукту".

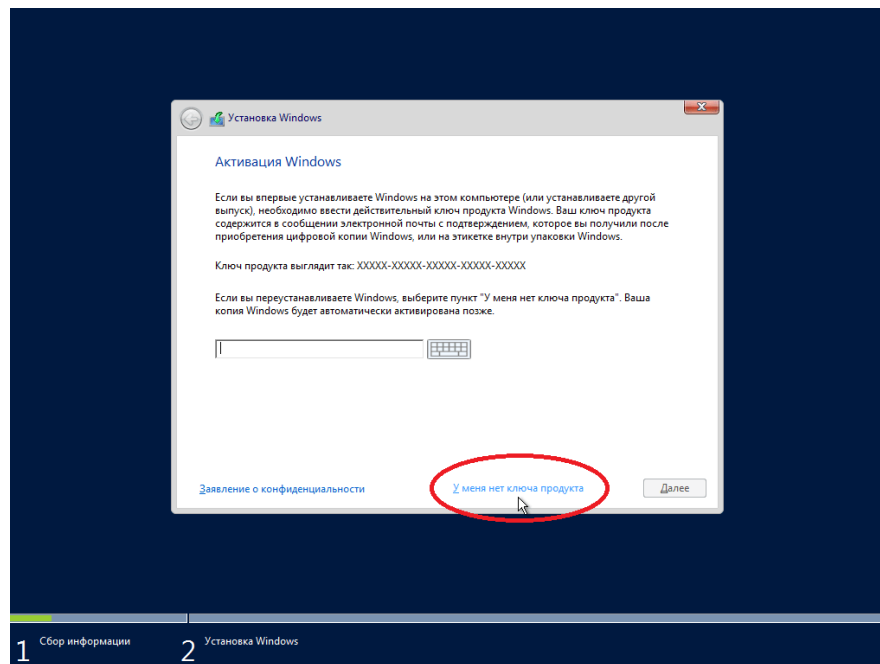


Рис. 4.2. Другой этап. Ключ продукту.

Далі попросять вибрати, яку саме версію дистрибутиву буде встановлено Standard або Datacenter. Я обрав для встановлення Standard, з можливістю робочого столу, інакше система встановиться без графічної оболонки і управління Windows Server буде доступна тільки з консолі.

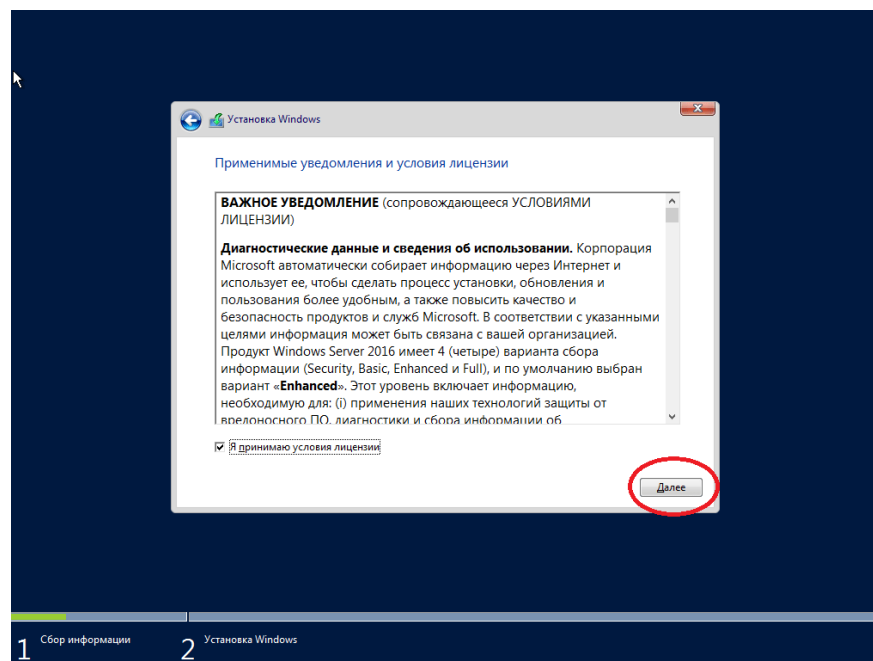


Рис. 4.3. Третій етап. Прийняття вимог ліцензії.

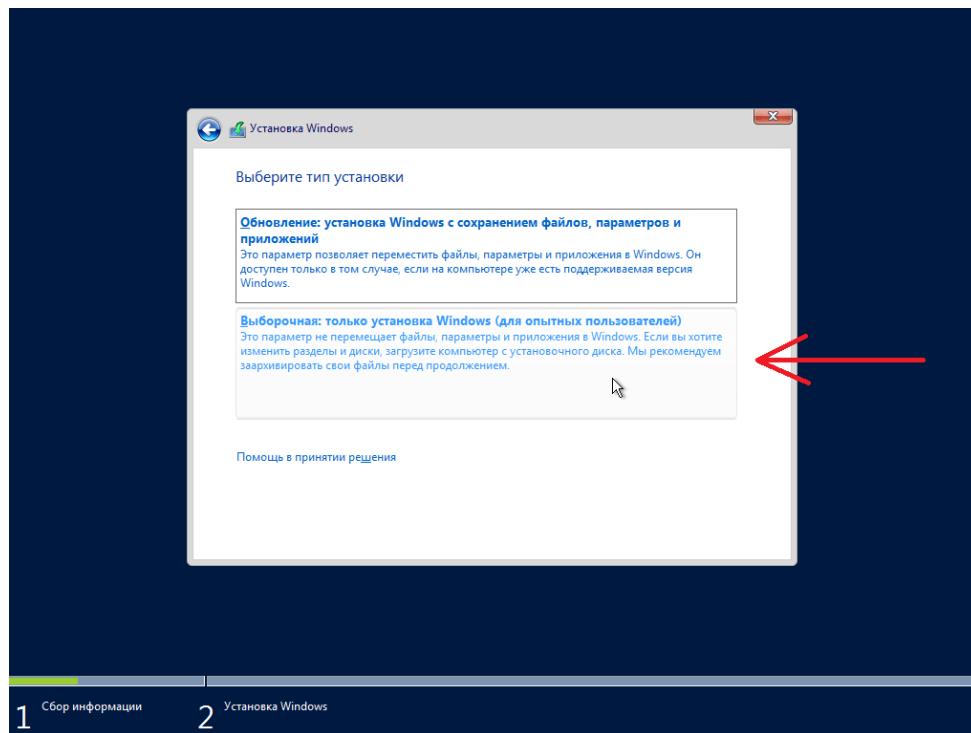


Рис. 4.4. Четвертый этап. Вибір способу встановлення.

Далі потрібно обрати диск, на який буде встановлена система.

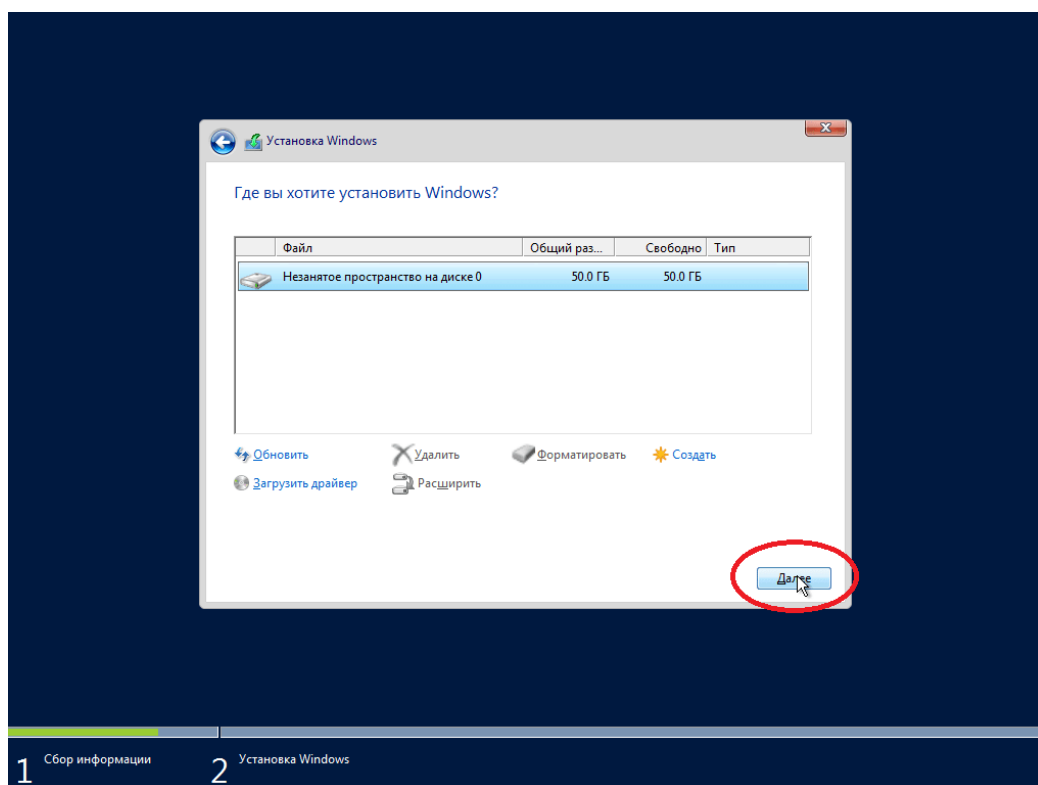


Рис. 4.5. П'ятий етап. Вибір диску для встановлення системи.

Після чого почнеться інсталяція Windows Server 2016.

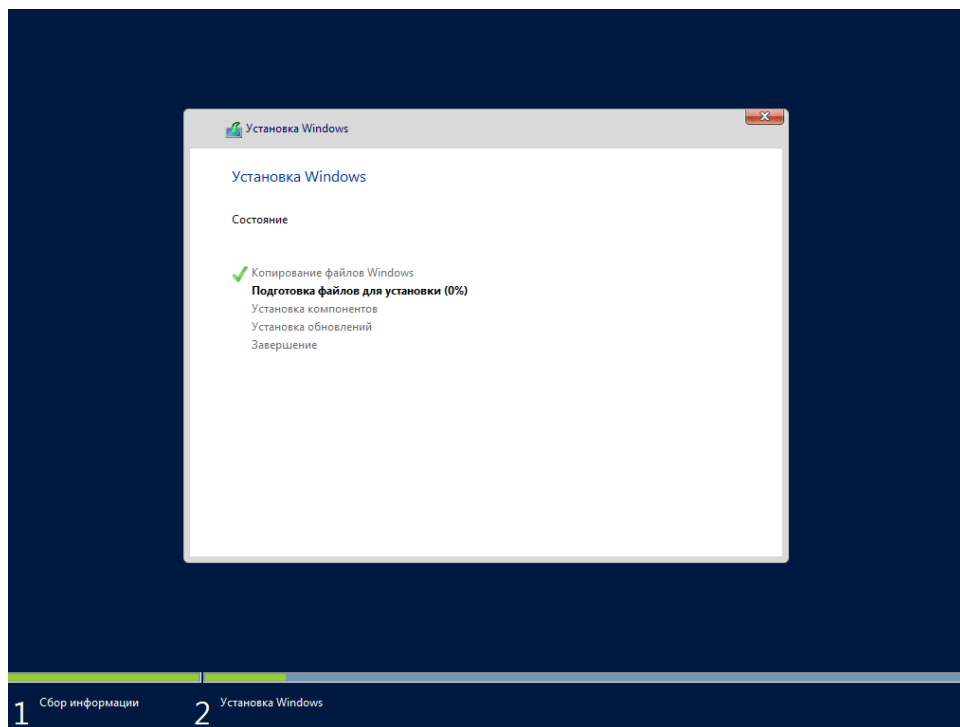


Рис. 4.6. Шостий етап. Інсталяція системи.

Після інсталяції, система запропонує встановити пароль Адміністратора. Це необхідно для забезпечення безпеки серверу.

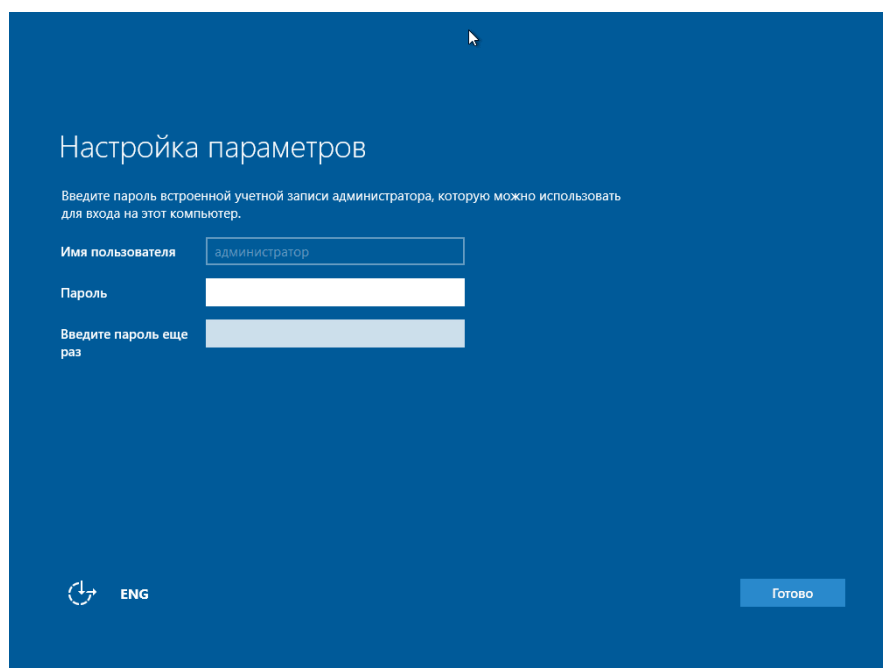


Рис. 4.7. Сьомий етап. Встановлення пароля адміністратора.

На фінальному етапі інсталяції запуститься ОС Windows Server 2016. Після входу в систему відкриється діалогове вікно «Диспетчер серверів».

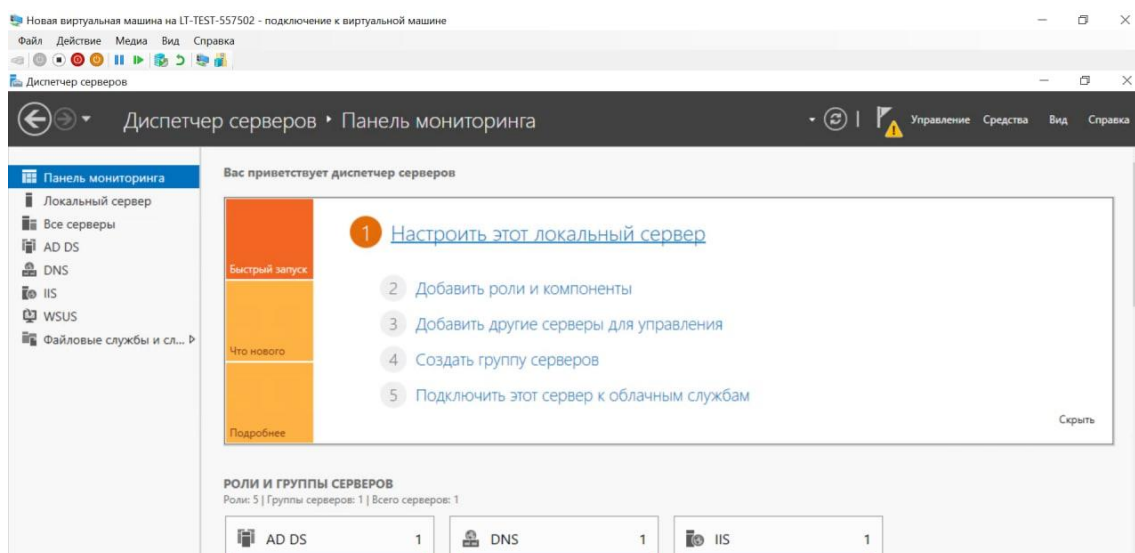


Рис. 4.8. Восьмий етап. Запуск ОС.