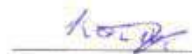


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект впровадження та управління систе-
мою Patch Management у інфраструктурі Microsoft»

Виконав: студент 4-го курсу групи КІ-21-1
спеціальності 123 «Комп'ютерна інженерія»

 Костюк І. О.

Керівник: Доцент кафедри КІ та КБ, к.т.н., доцент

 Россінський Ю.М.

Рецензент: Доцент кафедри КІ та КБ, к.пед.н., доцент

 Головня О.С.

Житомир – 2025

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	30.03.2025	
2	Збір та аналіз науково-технічної інформації	10.04.2025	
3	Огляд та порівняльний аналіз інструментів	20.04.2025	
4	Розгортання інфраструктури у VirtualBox	30.04.2025	
5	Проектування архітектури домену та середовища Patch Management	10.05.2025	
6	Базове налаштування WSUS	12.05.2025	
7	Конфігурування HTTPS-з'єднання	15.05.2025	
8	Проведення тестування системи	20.05.2025	
9	Моніторинг продуктивності	23.05.2025	
10	Написання пояснювальної записки	26.05.2025	
11	Захист	21.06.2025	

Студент  Костюк І. О.

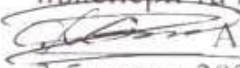
Керівник  Россінський Ю.М.

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Костюк Ігор Олександрович

Тема роботи: «Проект впровадження та управління системою Patch Management у інфраструктурі Microsoft»

затверджена Наказом університету від 3 березня 2025 р. № 79/с

Термін здачі студентом закінченої роботи 9 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Предмет дослідження: централізоване управління оновленнями на базі WSUS.

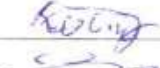
Об'єкт дослідження: доменна інфраструктура з Windows-пристроями.

Обладнання та програмне забезпечення:

1. Ноутбук із SSD-накопичувачем (1 ТБ).
2. Гіпервізор Oracle VirtualBox.
3. Операційні системи Windows Server 2019/2022, Windows 10/11.
4. Windows Server Update Services (WSUS).
5. Microsoft SQL Server 2019.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Фальковський І. Г.	25.04.2025	25.04.2025 
2	Фальковський І. Г.	10.05.2025	10.05.2025 
3	Фальковський І. Г.	19.05.2025	19.05.2025 
4	Фальковський І. Г.	21.05.2025	21.05.2025 

Студент  Костюк І. О.

Керівник  Россінський Ю.М.

АНОТАЦІЯ

Кваліфікаційна робота присвячена впровадженню централізованої системи Patch Management на основі Windows Server Update Services (WSUS) у доменній інфраструктурі kostiuk.net. Метою є створення стабільного середовища для автоматизованого оновлення клієнтів і серверів із підтримкою моніторингу та безпечного з'єднання.

Пояснювальна записка до кваліфікаційної роботи складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Текстова частина викладена на 185 сторінках. У роботі наведено 178 рисунків, 7 таблиць. Список використаних джерел містить 22 найменування та займає 3 сторінки.

У першому розділі проаналізовано сучасні підходи до управління оновленнями, порівняно інструменти WSUS, SCCM та Intune.

У другому розділі описано процес проєктування інфраструктури. Реалізовано структуру домену kostiuk.net із WSUS сервером, реплікою, контролером домену і клієнтськими машинами. Налаштовано групові політики (GPO), захищене HTTPS-з'єднання та реплікацію між серверами.

У третьому розділі розглянуто адміністрування WSUS, схвалення оновлень, моніторинг клієнтів і часткову автоматизацію через PowerShell і SQL.

У четвертому розділі наведено результати поетапного тестування продуктивності, перевірки GPO та аналізу ефективності. Запропоновано рекомендації щодо автоматизації, розширення ресурсів і впровадження зовнішнього моніторингу.

Ключові слова: PATCH MANAGEMENT, WSUS, ACTIVE DIRECTORY, WINDOWS SERVER, HTTPS, SQL, POWERSHELL.

					ДУ «Житомирська політехніка». 25.123.07.000 - ПЗ			
Вис.	Арк.	№ докум.	Підпис	Дата	Проект впровадження та управління системою Patch Management у інфраструктурі Microsoft	Літ.	Арк.	Аркушів
Розроб.		Костиук Т.О.		10.06				
Сервісник		Григор'єв В.М.		10.06			4	185
Реценз.		Григор'єв В.М.		10.06		ФІКТ, Гр. КІ-21-1		
— контр.		Григор'єв В.М.		10.06				
Затверд.		Сфмженик Д.І.		10.06				

ANNOTATION

The bachelor's qualification thesis is dedicated to the implementation of a centralized Patch Management system based on Windows Server Update Services (WSUS) within the domain infrastructure of *kostiuk.net*. The objective is to build a stable environment for automated updates of clients and servers, with integrated monitoring and secure communication.

The explanatory note consists of an introduction, four chapters, conclusions, a list of references, and appendices. The textual part spans 185 pages. The work includes 178 figures and 7 tables. The list of references contains 22 sources across 3 pages.

Chapter One analyzes modern approaches to update management and compares tools such as WSUS, SCCM, and Intune.

Chapter Two describes the infrastructure design process. The domain structure of *kostiuk.net* was implemented with a WSUS server, its replica, a domain controller, and client machines. Group Policies (GPO), secure HTTPS connections, and server replication were configured.

Chapter Three focuses on WSUS administration, update approval, client monitoring, and partial automation via PowerShell and SQL.

Chapter Four presents the results of step-by-step performance testing, GPO verification, and efficiency analysis. It also offers recommendations on automation, resource expansion, and the integration of external monitoring tools.

Keywords: PATCH MANAGEMENT, WSUS, ACTIVE DIRECTORY, WINDOWS SERVER, HTTPS, SQL, POWERSHELL.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	10
РОЗДІЛ 1 ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ СИСТЕМИ УПРАВЛІННЯ ООНОВЛЕННЯМИ	12
1.1 Аналіз концепції управління оновленнями в тестовій корпоративній інфраструктурі	12
1.2 Методи та технології Patch Management.....	14
1.3 Огляд інструментів управління оновленнями (WSUS, SCCM, Intune, сторонні сервіси).....	17
1.4 Порівняльний аналіз інструментів та обґрунтування вибору WSUS.....	22
1.4.1 Порівняння засобів централізованого управління оновленнями	22
1.4.2 Таблиця порівняння WSUS, SCCM, Intune, сторонніх рішень	24
1.4.3 Аргументи на користь WSUS у межах даної роботи.....	26
1.4.4 Обмеження WSUS і способи їх часткового вирішення	27
1.5 Ризики відсутності оновлень (вразливості, загрози).....	29
1.5.1 Вразливості та їхній вплив на системи.....	29
1.5.2 Загрози та сценарії атак	31
1.5.3 Організаційні, фінансові та репутаційні наслідки	32
1.5.4 Роль централізованого оновлення у зниженні ризиків	34
1.6 Обґрунтування вибору платформи віртуалізації (Oracle VirtualBox)	35
1.7 Ідея автоматизації за допомогою PowerShell	41
Висновки до Розділу 1	44
РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА ВПРОВАДЖЕННЯ СИСТЕМИ PATCH MANAGEMENT	46
2.1 Архітектурна модель тестового корпоративного середовища Patch Management	46
2.2. Вибір платформи віртуалізації та розгортання середовища.....	51
2.2.1 Створення віртуальної мережі	51
2.2.2 Створення та налаштування віртуальних машин	55
2.3. Налаштування контролера домену та служби Active Directory.....	62

2.3.1 Розгортання служби Active Directory	62
2.3.2 Організація структури домену	65
2.3.3 Приєднання віртуальних машин до домену	67
2.3.4 Налаштування ролей DHCP і DNS-серверів	69
2.3.5 Налаштування базових групових політик (GPO).....	73
2.4. Встановлення та початкові налаштування WSUS.....	76
2.4.1 Встановлення Microsoft SQL Server на сервер WSUS-PRIM-2019	76
2.4.2 Інсталяція ролі WSUS та підключення до SQL Server	79
2.4.3 Початкове налаштування WSUS.....	82
2.4.4 Налаштування GPO для WSUS	85
2.5 Налаштування TLS/SSL та HTTPS-з'єднання для WSUS.....	89
2.6 Налаштування резервного WSUS у режимі реплікації	93
Висновки до Розділу 2	97
РОЗДІЛ 3 АДМІНІСТРУВАННЯ, МОНІТОРИНГ І АНАЛІЗ СИСТЕМИ PATCH MANAGEMENT	99
3.1 Структурування груп клієнтів на WSUS-сервері	99
3.2 Схвалення оновлень та організація розгортання.....	102
3.3 Контроль стану оновлень (звіти WSUS + SQL-запити)	104
3.4 Моніторинг через PowerShell-скрипти	109
3.5 Моніторинг продуктивності WSUS-серверів за допомогою Perfmon.....	113
Висновки до розділу 3	116
РОЗДІЛ 4 ТЕСТУВАННЯ, ОЦІНКА ПРОДУКТИВНОСТІ ТА АНАЛІЗ ЕФЕКТИВНОСТІ СИСТЕМИ	118
4.1 Перевірка застосування базових групових політик (GPO)	118
4.2 Тестування працездатності оновлень у ключових етапах	124
4.2.1 Перевірка оновлень після початкового налаштування WSUS	124
4.2.2 Перевірка після налаштування HTTPS-з'єднання для WSUS.....	127
4.2.3 Тестування після підключення резервного WSUS-сервера	132
4.3 Оцінка ефективності продуктивності після впровадження	137
4.3.1 Показники продуктивності до запуску оновлень.....	137

4.3.2 Навантаження під час розгортання оновлень	140
4.4 Проблеми та обмеження під час реалізації.....	148
4.4.1 Початкова проблема з WID (Windows Internal Database)	148
4.4.2 Обмеження дискового простору та відмова від автоматизації	150
4.4.3 Обмеження WSUS API при роботі з PowerShell	152
4.5 Рекомендації щодо подальшої оптимізації.....	154
4.5.1 Автоматизація звітності в системі WSUS	154
4.5.2 Розширення ресурсів та реалізація повної автоматизації.....	156
4.5.3 Використання зовнішнього моніторингу (Zabbix, Grafana)	158
Висновок до Розділу 4	160
ВИСНОВКИ	162
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	164
ДОДАТКИ	167
Додаток А*	168
Додаток Б*	175
Додаток В*	179

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

- **AD** – Active Directory
- **API** – Application Programming Interface
- **BYOD** – Bring Your Own Device
- **CAL** – Client Access License
- **CSV** – Comma-Separated Values
- **CPU** – Central Processing Unit
- **DHCP** – Dynamic Host Configuration Protocol
- **GPO** – Group Policy Object
- **HTTPS** – HyperText Transfer Protocol Secure
- **IIS** – Internet Information Services
- **MAM** – Mobile Application Management
- **MDM** – Mobile Device Management
- **MECM** – Microsoft Endpoint Configuration Manager
- **OU** – Organizational Unit
- **OS** – Operating System
- **ПЗ** – Програмне Забезпечення (Program Software)
- **RAM** – Random Access Memory
- **SCCM** – System Center Configuration Manage
- **SLA** – Service Level Agreement
- **SNMP** – Simple Network Management Protocol
- **SQL** – Structured Query Language
- **TLS** – Transport Layer Security
- **WID** – Windows Internal Database
- **WSUS** – Windows Server Update Services

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Сучасні інформаційні системи функціонують у надзвичайно динамічному середовищі, де критично важливою складовою забезпечення їхньої стабільності та захищеності є своєчасне встановлення оновлень. У контексті кібербезпеки відсутність ефективної системи управління оновленнями (Patch Management) створює прямі загрози — від вразливостей до успішних атак з боку злоумисників. Враховуючи зростання кількості кіберінцидентів та ускладнення інфраструктури, зростає потреба в централізованих, автоматизованих рішеннях для підтримки актуального стану клієнтських і серверних систем.

Актуальність теми полягає в необхідності створення ефективної моделі централізованого управління оновленнями для середовища Windows, що забезпечує не лише безпеку, але й оперативність реагування на критичні оновлення. Вибір Microsoft WSUS (Windows Server Update Services) як базового інструмента обґрунтований його інтеграцією в екосистему Microsoft, широкими можливостями налаштувань, підтримкою PowerShell-автоматизації та здатністю масштабування для різних типів середовищ.

Мета роботи — проєктування, впровадження та тестування централізованої системи управління оновленнями на основі WSUS з інтегрованими механізмами моніторингу, автоматизації та захисту з'єднання.

Для досягнення мети були поставлені такі завдання:

- дослідити концепцію Patch Management та існуючі рішення;
- обґрунтувати вибір платформи WSUS;
- побудувати лабораторне середовище з головним і резервним WSUS-серверами;
- налаштувати групові політики для керування оновленнями клієнтів;
- реалізувати часткову автоматизацію процесів через PowerShell;
- забезпечити безпечну взаємодію клієнтів з WSUS через HTTPS;
- впровадити механізми контролю, моніторингу та аудиту;
- провести тестування працездатності та ефективності розробленої системи.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Об’єкт дослідження — процес централізованого управління оновленнями в корпоративному середовищі Microsoft.

Предмет дослідження — методи побудови, налаштування, автоматизації та моніторингу системи Patch Management з використанням WSUS та супутніх засобів.

Методи дослідження: аналіз відкритих джерел, порівняльний аналіз систем, моделювання інформаційної інфраструктури, скриптування PowerShell, застосування SQL-запитів до бази SUSDB, тестування та збір продуктивності через системні утиліти Windows.

Практичне значення роботи полягає у можливості використання описаної інфраструктури та сценаріїв у реальних корпоративних мережах для забезпечення захищеності клієнтських і серверних ОС. Запропоноване рішення є масштабованим, частково автоматизованим і адаптованим до потреб адміністратора без додаткових витрат на стороннє програмне забезпечення.

Структура роботи. Дипломна робота складається зі вступу, трьох основних розділів, висновків, списку використаних джерел із 20 найменувань, додатків, що включають скрипти, схеми та SQL-запити. Повний обсяг роботи становить 70 сторінок, з них 60 сторінок основного тексту.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ СИСТЕМИ УПРАВЛІННЯ ООНОВЛЕННЯМИ

1.1 Аналіз концепції управління оновленнями в тестовій корпоративній інфраструктурі

Управління оновленнями (Patch Management) є ключовим інженерним процесом у забезпеченні стабільності, продуктивності та функціональності корпоративних інформаційних систем. Цей процес передбачає систематичне виявлення, оцінювання, тестування, встановлення та моніторинг оновлень (патчів) для операційних систем, програмного забезпечення, драйверів і компонентів інфраструктури. Метою Patch Management є підтримка актуального стану інформаційних систем, виправлення функціональних помилок, оптимізація роботи пристроїв і забезпечення їхньої сумісності з сучасними вимогами корпоративного середовища.

У контексті комп'ютерної інженерії Patch Management розглядається як комплексне інженерне завдання, що поєднує проектування мережевої інфраструктури, автоматизацію процесів і моніторинг систем для забезпечення їх ефективної роботи. У корпоративному середовищі, де інфраструктура включає численні сервери, робочі станції та мережеве обладнання, управління оновленнями відіграє важливу роль у підтримці безперебійної роботи систем. Несвоєчасне оновлення може призвести до зниження продуктивності, несумісності програмного забезпечення, збоїв у роботі додатків або навіть зупинки бізнес-процесів. Patch Management сприяє підвищенню безпеки систем, оскільки несвоєчасне застосування патчів може призвести до серйозних кіберзагроз, таких як зараження шкідливим програмним забезпеченням (наприклад, вірусами-вимагачами типу WannaCry чи NotPetya), компрометація даних, порушення цілісності систем або зупинка бізнес-процесів. За даними звіту Verizon Data Breach Investigations Report (2024), близько 50% кібератак у 2023 році були пов'язані з експлуатацією вразливостей, для яких існували патчі, але вони не були застосовані.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Концепція Patch Management охоплює повний життєвий цикл управління оновленнями, який включає такі ключові етапи:

- **Інвентаризація активів:** Ідентифікація всіх пристроїв і програмного забезпечення в корпоративній мережі, що потребують оновлень.
- **Виявлення патчів:** Моніторинг доступних оновлень від постачальників програмного забезпечення, таких як Microsoft, Adobe чи Oracle.
- **Оцінювання та пріоритизація:** Визначення критичності патчів, зокрема для вразливостей типу zero-day, та оцінка їх впливу на продуктивність системи.
- **Тестування:** Перевірка оновлень у контрольованому тестовому середовищі для запобігання збоям у продуктивних системах.
- **Розгортання:** Встановлення патчів на цільові пристрої з урахуванням політик і графіків оновлення.
- **Моніторинг і аудит:** Контроль стану оновлень на пристроях, аналіз їх успішності та формування звітів для аудиту.

З інженерної точки зору, ефективне управління оновленнями вимагає централізованої моделі, яка забезпечує уніфіковане керування процесами, зниження навантаження на мережеві ресурси та автоматизацію рутинних завдань. Централізація дозволяє інженерам керувати оновленнями через єдиний інтерфейс, оптимізувати розподіл патчів між групами пристроїв (наприклад, сервери, робочі станції) і забезпечувати відповідність технічним стандартам. Такий підхід сприяє економії ресурсів, підвищенню продуктивності мережі та спрощенню адміністрування складних інфраструктур.

Серед найпопулярніших рішень для управління оновленнями в корпоративних інфраструктурах можна виділити:

- **Windows Server Update Services (WSUS):** Інструмент Microsoft для централізованого управління оновленнями в локальних мережах, який підтримує інтеграцію з Active Directory і автоматизацію через групові політики.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

- **System Center Configuration Manager (SCCM):** Платформа Microsoft для комплексного управління IT-інфраструктурою, включаючи розгортання оновлень і моніторинг систем.
- **Microsoft Intune:** Хмарне рішення для управління оновленнями та пристроями, що підходить для гібридних і мобільних інфраструктур.
- **ManageEngine Patch Manager Plus:** Сторонній інструмент для автоматизованого управління патчами на різних платформах, включаючи Windows і Linux.
- **SolarWinds Patch Manager:** Рішення для автоматизації оновлень із функціями моніторингу та звітності.

Ці інструменти дозволяють інженерам адаптувати процес Patch Management до потреб конкретної інфраструктури, враховуючи її масштаб, типи пристроїв і вимоги до продуктивності. У контексті комп'ютерної інженерії Patch Management є не лише технічним процесом, а й частиною стратегії оптимізації IT-інфраструктури, що забезпечує стабільність, сумісність і ефективність корпоративних систем, а також сприяє їх захисту від потенційних загроз.

1.2 Методи та технології Patch Management

Управління оновленнями (Patch Management) становить важливий інженерний процес у комп'ютерній інженерії, спрямований на забезпечення актуальності, стабільності та продуктивності корпоративних інформаційних систем. Цей процес охоплює виявлення, оцінювання, тестування, розгортання та моніторинг оновлень для операційних систем, програмного забезпечення та драйверів, що дозволяє оптимізувати роботу складних мереж і підтримувати їхню сумісність із сучасними вимогами. У корпоративному середовищі, де інфраструктура включає численні пристрої, такі як сервери та робочі станції, Patch Management спрощує адміністрування, зменшує ймовірність збоїв і сприяє економії ресурсів.

Управління оновленнями реалізується через різні методи, які визначаються рівнем автоматизації, масштабами інфраструктури та технічними можливостями

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

організації. Ручне управління є найпростішим підходом, при якому адміністратор самостійно виконує всі етапи: від пошуку оновлень на офіційних джерелах, таких як Microsoft Update Catalog, до їх встановлення через графічний інтерфейс Windows Update або командний рядок. Цей метод не потребує складної інфраструктури, але є трудомістким і малоефективним для великих мереж, оскільки підвищує ризик пропущення важливих патчів і ускладнює контроль версій програмного забезпечення. Ручне управління доцільне лише в невеликих організаціях із кількома пристроями (до 5–10) або для специфічного програмного забезпечення, яке не підтримує автоматизацію.

Плюси та мінуси ручного управління:

– **Плюси:**

- Простота реалізації, не вимагає додаткових інструментів.
- Повний контроль адміністратора над кожним етапом.

– **Мінуси:**

- Висока трудомісткість і витрати часу.
- Відсутність централізованого обліку оновлень.
- Ризик пропущення критичних патчів.

Автоматизоване управління оновленнями використовує вбудовані механізми операційних систем, такі як служба Windows Update, для виконання процесів із мінімальним втручанням адміністратора. У цьому підході оновлення автоматично завантажуються та встановлюються відповідно до заданих параметрів, наприклад, графіка перевірки чи типу патчів, які налаштовуються через локальні політики безпеки (Local Group Policy). Автоматизація зменшує навантаження на персонал і забезпечує швидше реагування на нові оновлення, що є перевагою для організацій із середньою кількістю пристроїв. Проте цей метод не дозволяє точно контролювати типи оновлень, такі як драйвери чи телеметричні пакети, і ускладнює аудит результатів, що обмежує його застосування в складних інфраструктурах.

Плюси та мінуси автоматизованого управління:

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

– **Плюси:**

- Зменшення рутинної роботи адміністраторів.
- Швидке реагування на нові оновлення.

– **Мінуси:**

- Обмежений контроль над типами оновлень.
- Складність формування звітів і аудиту.
- Ризик збоїв через несумісність патчів.

Для великих корпоративних мереж оптимальним є централізоване управління оновленнями, яке передбачає використання спеціалізованого сервера або платформи для координації всіх етапів Patch Management. У такому підході оновлення завантажуються на центральний репозиторій, звідки розподіляються на клієнтські пристрої відповідно до заданих політик. Централізоване управління економить мережеві ресурси, забезпечує уніфікований контроль і спрощує адміністрування, дозволяючи створювати групи пристроїв, наприклад, для серверів і робочих станцій. Інтеграція з доменною інфраструктурою, такою як Active Directory, дає змогу автоматизувати розгортання через групові політики, що підвищує масштабованість і ефективність системи.

Плюси та мінуси централізованого управління:

– **Плюси:**

- Економія мережевих ресурсів і спрощення адміністрування.
- Гнучкість у налаштуванні політик для груп пристроїв.
- Можливість моніторингу та звітності.

– **Мінуси:**

- Потреба в додатковій інфраструктурі (сервери, бази даних).
- Складність початкового налаштування.

Реалізація Patch Management спирається на низку технологій, які підтримують інженерне проєктування корпоративних інфраструктур. Локальні сервери управління оновленнями, такі як Windows Server Update Services (WSUS), забез-

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

печують централізоване зберігання патчів і їх розподіл у локальній мережі, дозволяючи адміністраторам завантажувати оновлення з офіційних джерел і налаштовувати політики розгортання. Хмарні платформи, наприклад, Microsoft Intune, пропонують управління оновленнями через вебінтерфейс, що зручно для віддалених і мобільних пристроїв у гібридних інфраструктурах, хоча залежить від якості інтернет-з'єднання. Автоматизація є ключовою технологією, де PowerShell використовується для створення скриптів, які спрощують схвалення оновлень і моніторинг стану клієнтів, а SQL-запити до баз даних, таких як SUSDB, дають змогу аналізувати детальну інформацію про патчі. Інструменти моніторингу, такі як Performance Monitor (Perfmon), дозволяють оцінювати вплив оновлень на продуктивність системи. Технології віртуалізації, наприклад, Hyper-V або VMware, забезпечують створення тестових середовищ для перевірки патчів, що мінімізує ризик збоїв. Для захисту передачі даних застосовується шифрування TLS/HTTPS, яке забезпечує безпечний обмін між сервером і клієнтами.

У корпоративних інфраструктурах для Patch Management використовуються різні рішення, які адаптуються до потреб організації. Наприклад, Windows Server Update Services (WSUS) підтримує локальне управління оновленнями, System Center Configuration Manager (SCCM) пропонує комплексне адміністрування, а Microsoft Intune орієнтований на хмарне управління. Сторонні інструменти надають розширені функції автоматизації та звітності, що полегшують управління в різномірних мережах. У контексті комп'ютерної інженерії ці методи та технології дозволяють створювати ефективні інфраструктури, що забезпечують стабільність, продуктивність і оптимальне адміністрування корпоративних систем.

1.3 Огляд інструментів управління оновленнями (WSUS, SCCM, Intune, сторонні сервіси)

Управління оновленнями (Patch Management) є ключовим інженерним процесом у комп'ютерній інженерії, спрямованим на забезпечення стабільності,

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

продуктивності та актуальності корпоративних інформаційних систем. Цей процес вимагає спеціалізованих інструментів, які автоматизують розгортання патчів, оптимізують мережеві ресурси та спрощують адміністрування складних інфраструктур. Вибір інструменту залежить від розміру організації, типу інфраструктури, рівня автоматизації та вимог до масштабованості. У корпоративному середовищі широко використовуються продукти Microsoft, такі як Windows Server Update Services (WSUS), System Center Configuration Manager (SCCM) і Microsoft Intune, а також сторонні сервіси, які пропонують додаткові функції для управління оновленнями.

Windows Server Update Services (WSUS) є базовим інструментом Microsoft для централізованого управління оновленнями в локальних мережах. WSUS інтегрується як роль у Windows Server і дозволяє завантажувати оновлення з Microsoft Update на центральний сервер, звідки вони розподіляються на клієнтські пристрої, що зменшує навантаження на мережу. Інструмент підтримує інтеграцію з Active Directory для групування пристроїв через групові політики (GPO) і забезпечує захист передачі даних через TLS/HTTPS. Основні можливості WSUS включають:

- Фільтрацію оновлень за категоріями (безпекові, функціональні, драйвери) та продуктами (Windows 10, Windows Server 2022).
- Схвалення оновлень вручну або через PowerShell-скрипти.
- Моніторинг стану клієнтів через консоль або SQL-запити до бази SUSDB.
- Формування базових звітів про встановлення патчів.

WSUS є безкоштовним і не вимагає додаткових ліцензій, але його функціональність обмежена підтримкою лише продуктів Microsoft і відсутністю автоматичного схвалення оновлень. У 2024 році Microsoft оголосила про припинення розвитку WSUS у Windows Server 2025, рекомендуючи хмарні альтернативи, такі як Intune або Azure Update Manager.

System Center Configuration Manager (SCCM), відомий також як Microsoft Endpoint Configuration Manager (MECM), є комплексною платформою для управління IT-інфраструктурою, яка виходить за межі Patch Management. SCCM

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

працює за клієнт-серверною моделлю, вимагаючи встановлення агентів на клієнтських пристроях, і може інтегруватися з WSUS для доставки оновлень. Інструмент підтримує автоматизацію розгортання патчів, інсталяцію програмного забезпечення, інвентаризацію та моніторинг інфраструктури. SCCM дозволяє налаштовувати розклади оновлень, проводити попереднє тестування патчів і створювати детальні звіти для відповідності вимогам SLA. Основні можливості SCCM включають:

- Управління оновленнями для продуктів Microsoft і деяких сторонніх програм.
- Інвентаризацію апаратного та програмного забезпечення.
- Налаштування політик безпеки з інтеграцією Microsoft Defender.
- Автоматизацію розгортання через групові політики та розклади.

SCCM є комерційним продуктом, що потребує ліцензування та кваліфікованого персоналу для налаштування, але його потужність робить його ідеальним для великих організацій зі складною інфраструктурою.

Microsoft Intune, частина платформи Microsoft Endpoint Manager, є хмарним рішенням для управління кінцевими пристроями, яке охоплює Patch Management, керування мобільними пристроями (MDM) і застосунками (MAM). Intune орієнтований на гібридні та віддалені інфраструктури, що робить його придатним для організацій із політикою Bring Your Own Device (BYOD). Інструмент інтегрується з Azure Active Directory і Microsoft 365, забезпечуючи централізоване управління через вебінтерфейс. Основні можливості Intune включають:

- Управління оновленнями для Windows, macOS, iOS і Android.
- Налаштування профілів політик для групового розгортання патчів.
- Моніторинг стану пристроїв у реальному часі.
- Хмарну архітектуру без потреби в локальних серверах.

Intune забезпечує високу масштабованість і простоту використання, але має обмеження в кастомізації, що робить його оптимальним для організацій, орієнтованих на хмарні екосистеми.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

ManageEngine Patch Manager Plus є універсальним інструментом для управління оновленнями, який підтримує Windows, macOS, Linux і понад 850 сторонніх додатків, таких як Adobe, Java та WinRAR. Цей сервіс пропонує автоматизоване розгортання патчів через вебінтерфейс, що спрощує адміністрування в різномірних середовищах. ManageEngine дозволяє створювати тестові групи для оцінки патчів перед розгортанням і забезпечує детальну звітність для моніторингу відповідності. Основні можливості ManageEngine Patch Manager Plus включають:

- Автоматизацію виявлення, тестування та розгортання патчів.
- Підтримку широкого спектра операційних систем і стороннього ПЗ.
- Інтеграцію з Active Directory для групового управління.
- Генерацію детальних звітів про стан оновлень.

ManageEngine є платним рішенням із гнучкими моделями ліцензування (підписка або постійна ліцензія), що робить його привабливим для середніх і великих організацій.

PDQ Deploy є інструментом для автоматизації розгортання програмного забезпечення та патчів у Windows-середовищах, відомим своєю простотою та швидкістю налаштування. Сервіс підтримує бібліотеку з понад 250 попередньо підготовлених пакетів для популярних додатків, таких як Google Chrome, Zoom і Adobe Reader, що спрощує оновлення стороннього ПЗ. PDQ Deploy дозволяє створювати власні пакети та налаштовувати розклади розгортання. Основні можливості PDQ Deploy включають:

- Автоматизацію розгортання патчів і програм через централізовану консоль.
- Підтримку попередньо протестованих пакетів для стороннього ПЗ.
- Реальний час відстеження розгортання та звіти про результати.
- Інтеграцію з Active Directory та PDQ Inventory для інвентаризації.

PDQ Deploy є платним, із ліцензуванням на основі кількості адміністраторів, і підходить для малих і середніх організацій, які потребують простого рішення.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

SolarWinds Patch Manager є інструментом для автоматизації Patch Management, який розширює можливості WSUS і SCCM, додаючи підтримку стороннього ПЗ, зокрема Adobe, Java та Google Chrome. Сервіс пропонує централізовану консоль для управління оновленнями Windows-серверів і робочих станцій, а також детальну аналітику для відстеження відповідності. SolarWinds підтримує автоматизацію через розклади та попередньо протестовані патчі. Основні можливості SolarWinds Patch Manager включають:

- Розгортання патчів для Microsoft і стороннього ПЗ.
- Інтеграцію з WSUS і SCCM для розширення їхньої функціональності.
- Генерацію детальних звітів про стан оновлень.
- Автоматизацію розгортання через налаштовані розклади.

SolarWinds є платним інструментом із вартістю від \$2,274 на рік залежно від кількості вузлів, що робить його придатним для організацій, які потребують розширеної автоматизації.

Ivanti Patch, відомий також як Ivanti Patch for Endpoint Manager, є рішенням для управління оновленнями в складних інфраструктурах, підтримуючи Windows, macOS, Linux і численні стороннього ПЗ. Інструмент автоматизує виявлення даних, пріоритизацію та розгортання патчів, що дозволяє оптимізувати процеси в великих мережах. Ivanti інтегрується з SCCM і Intune, пропонуючи єдину консоль для управління та детальну звітність. Основні можливості Ivanti Patch включають:

- Автоматизацію пріоритизації патчів на основі оцінок.
- Підтримку широкого спектра ОС і сторонніх додатків.
- Інтеграцію з SCCM і Intune для гнучкого управління.
- Генерацію звітів для аналізу відповідності вимогам.

Ivanti є платним рішенням із вартістю залежною від кількості кінцевих точок, що робить його популярним серед великих організацій із розгалуженою інфраструктурою.

У контексті комп'ютерної інженерії інструменти Patch Management, такі як WSUS, SCCM, Intune, ManageEngine Patch Manager Plus, PDQ Deploy, SolarWinds

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Patch Manager і Ivanti Patch, дозволяють створювати ефективні системи для автоматизації оновлення, оптимізації ресурсів і забезпечення стабільності корпоративних мереж. Їхня базова функціональність забезпечує гнучкість у проектуванні інфраструктури відповідно до потреб організації.

1.4 Порівняльний аналіз інструментів і обґрунтування вибору WSUS

1.4.1 Порівняння засобів централізованого управління оновленнями

Централізоване управління оновленнями (Patch Management) є критично важливим інженерним процесом у комп'ютерній інженерії, спрямованим на забезпечення стабільності, продуктивності та актуальності корпоративних інформаційних систем. Для порівняльного аналізу інструментів, таких як Windows Server Update Services (WSUS), System Center Configuration Manager (SCCM), Microsoft Intune, ManageEngine Patch Manager Plus, PDQ Deploy, SolarWinds Patch Manager і Ivanti Patch, використано критерії: функціональність, рівень автоматизації, підтримка платформ, інтеграція з іншими системами, складність впровадження, масштабованість, звітність і ліцензування/вартість. Ці критерії дозволяють оцінити інструменти з точки зору їхньої здатності оптимізувати інфраструктуру та автоматизувати процеси.

Функціональність. WSUS забезпечує базові можливості управління оновленнями продуктів Microsoft, таких як Windows, Office і Server. Адміністратори можуть фільтрувати оновлення за типами (безпекові, функціональні, драйвери), створювати групи пристроїв через Active Directory і групові політики (GPO), а також схвалювати оновлення вручну або за допомогою PowerShell. SCCM пропонує комплексний функціонал, включаючи Patch Management, інсталяцію ПЗ, інвентаризацію, налаштування політик безпеки та інтеграцію з Microsoft Defender. Intune фокусується на хмарному управлінні кінцевими пристроями, підтримуючи оновлення та керування мобільними пристроями (MDM) і застосунками (MAM). ManageEngine Patch Manager Plus підтримує оновлення для Windows, macOS, Linux і понад 850 сторонніх додатків, таких як Adobe і Java.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

PDQ Deploy автоматизує розгортання патчів і ПЗ у Windows-середовищах, використовуючи бібліотеку з 250+ готових пакетів. SolarWinds Patch Manager розширює можливості WSUS і SCCM, додаючи підтримку стороннього ПЗ. Ivanti Patch автоматизує управління оновленнями в складних інфраструктурах, підтримуючи численні додатки.

Рівень автоматизації. WSUS має низький рівень автоматизації: схвалення оновлень виконується вручну або через PowerShell, а розгортання залежить від GPO. SCCM забезпечує високу автоматизацію з розкладами, тестовими групами та автоматичним розгортанням. Intune автоматизує процеси через хмарні профілі політик, але залежить від інтернет-з'єднання. ManageEngine автоматизує виявлення, тестування та розгортання патчів із налаштуванням розкладів. PDQ Deploy підтримує автоматичне розгортання за розкладами та відправку звітів. SolarWinds автоматизує розгортання через попередньо протестовані патчі та інтеграцію з WSUS/SCCM. Ivanti пропонує автоматизацію з пріоритизацією патчів на основі оцінок.

Підтримка платформ. WSUS обмежується Windows-середовищем, без підтримки macOS, Linux чи стороннього ПЗ. SCCM орієнтований на Windows, але частково підтримує сторонні додатки через плагіни. Intune підтримує Windows, macOS, iOS і Android. ManageEngine охоплює Windows, macOS, Linux і сторонні додатки. PDQ Deploy працює лише з Windows, але підтримує численні сторонні програми. SolarWinds підтримує Windows і стороннє ПЗ через WSUS/SCCM. Ivanti керує Windows, macOS, Linux і сторонніми додатками.

Інтеграція з іншими системами. WSUS інтегрується з Active Directory, GPO і SQL Server Express, але не підтримує сторонні системи. SCCM інтегрується з WSUS, Active Directory, Microsoft Defender і частково з Intune. Intune працює з Azure Active Directory і Microsoft 365. ManageEngine інтегрується з Active Directory і підтримує власну консоль. PDQ Deploy інтегрується з Active Directory і PDQ Inventory. SolarWinds інтегрується з WSUS і SCCM. Ivanti інтегрується з SCCM, Intune і Active Directory.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

Складність впровадження. WSUS є простим у встановленні як роль Windows Server, потребує базового налаштування GPO і SQL. SCCM вимагає складного впровадження через клієнт-серверну модель і встановлення агентів. Intune спрощує впровадження завдяки хмарній архітектурі, але потребує Azure AD. ManageEngine має простий вебінтерфейс і швидке налаштування. PDQ Deploy вирізняється мінімальною складністю завдяки інтуїтивній консолі. SolarWinds потребує інтеграції з WSUS/SCCM, що підвищує складність. Ivanti вимагає складного налаштування через інтеграцію з іншими системами.

Масштабованість. WSUS підходить для малих і середніх мереж (до 1500 пристроїв), але має проблеми з продуктивністю у великих середовищах. SCCM масштабується до десятків тисяч пристроїв, але потребує значних ресурсів. Intune є високома масштабованим завдяки хмарній інфраструктурі. ManageEngine масштабується для великих мереж із підтримкою тисяч пристроїв. PDQ Deploy більше підходить для малих та середніх організацій. SolarWinds масштабується через інтеграцію з WSUS/SCCM. Ivanti в свою чергу підтримує великі інфраструктури з тисячами вузлів.

Звітність. WSUS пропонує базові звіти через консоль або SQL-запити до SUSDB, але вони обмежені. SCCM забезпечує детальну звітність із SLA-аналітикою. Intune пропонує звіти в реальному часі, але з обмеженою кастомізацією.

Ліцензування та вартість. WSUS є безкоштовним, але потребує ліцензії Windows Server і CAL для клієнтів. SCCM є комерційним із високою вартістю ліцензування. Intune доступний за підпискою (\$6–10/користувач/місяць). ManageEngine коштує від \$245 за 50 пристроїв. PDQ Deploy — від \$500 за адміністратора. SolarWinds — від \$2,274 за 250 вузлів. Ivanti не публікує ціни, але залежить від кількості кінцевих точок.

1.4.2 Таблиця порівняння WSUS, SCCM, Intune, сторонніх рішень

Порівняльний аналіз інструментів управління оновленнями показує, що кожен інструмент адаптований до специфічних потреб організації. WSUS є еко-

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

номічним для Windows-середовищ, SCCM — комплексним для великих інфраструктур, Intune — універсальним для хмарних і гібридних мереж, а сторонні рішення (ManageEngine, PDQ Deploy, SolarWinds, Ivanti) пропонують підтримку стороннього ПЗ та гнучкість. Нижче наведено таблицю з ключовими характеристиками.

Таблиця 1.1. Порівняння WSUS з іншими рішеннями

Критерій	WSUS	SCCM	Intune	Manage Engine	PDQ Deploy	SolarWinds	Ivanti
Тип розгортання	Локальний	Локальний	Хмарний	Локальний /хмарний	Локальний	Локальний	Локальний /хмарний
Підтримка ОС	Windows	Windows, частково сторонні	Windows, macOS, iOS, Android	Windows, macOS, Linux	Windows	Windows	Windows, macOS, Linux
Підтримка стороннього ПЗ	Ні	Частково (плагіни)	Ні	Так (>850 додатків)	Так (250+ пакетів)	Так (Adobe, Java)	Так (численні додатки)
Автоматизація	Низька (PowerShell)	Висока (розклади)	Висока (хмарні політики)	Висока (автовиявлення)	Висока (розклади)	Висока через WSUS/SCCM	Висока (пріоритизація)
Інтеграція	AD, GPO, SQL	WSUS, AD, Defender, Intune	Azure AD, M365	AD, власна консоль	AD, PDQ Inventory	WSUS, SCCM	SCCM, Intune, AD
Складність впровадження	Низька	Висока	Середня	Низька	Низька	Середня	Висока
Масштабованість	Мала–середня (до 1500)	Висока (тисячі)	Висока (хмарна)	Висока (тисячі)	Мала–середня	Висока (з WSUS/SCCM)	Висока (тисячі)
Звітність	Базова (SQL)	Детальна (SLA)	Реальний час (обмежена)	Детальна (відповідність)	Базова (email)	Детальна (аналітика)	Детальна (відповідність)
Вартість	Безкоштовно (з Windows Server)	Висока (ліцензії)	\$6–10/користувач/місяць	Від \$245/50 пристроїв	Від \$500/адмін	Від \$2,274/250 вузлів	Залежить від вузлів

Примітки до таблиці:

- **ManageEngine:** Підтримує >850 додатків, гнучкі плани (підписка/постійна ліцензія).
- **PDQ Deploy:** Ліцензування за кількістю адміністраторів, не вузлів.
- **SolarWinds:** Ціна залежить від кількості вузлів, інтеграція з WSUS/SCCM.
- **Ivanti:** Ціна доступна за запитом, фокус на великих інфраструктурах.

1.4.3 Аргументи на користь WSUS у межах даної роботи

Вибір Windows Server Update Services (WSUS) як основного інструменту для управління оновленнями в межах даної роботи зумовлений низкою інженерних і організаційних переваг, які відповідають потребам корпоративної інфраструктури середнього розміру, орієнтованої на Windows-середовище. WSUS забезпечує ефективне централізоване управління оновленнями, оптимізуючи ресурси та спрощуючи адміністрування, що є ключовим для реалізації проєкту в умовах обмеженого бюджету та наявної доменної інфраструктури.

Першим аргументом на користь WSUS є його економічна ефективність. Як безкоштовна роль Windows Server, WSUS не потребує додаткових ліцензій, окрім стандартних CAL для клієнтів і сервера, що робить його привабливим для організацій із обмеженим бюджетом. У порівнянні з комерційними рішеннями, такими як SCCM чи Intune, які вимагають значних витрат на ліцензування або підписку, WSUS дозволяє досягти базового рівня централізованого управління оновленнями без додаткових фінансових вкладень. Це особливо важливо для середніх організацій, де пріоритетом є зниження витрат на ІТ-інфраструктуру.

Другим важливим фактором є простота впровадження та сумісність із наявною інфраструктурою. WSUS легко інтегрується з Active Directory, що дозволяє використовувати групові політики (GPO) для налаштування груп пристроїв, таких як сервери та робочі станції, у домені kostiuk.net. Ця інтеграція спрощує адміністрування, оскільки політики розгортання оновлень можна централізовано налаштувати без потреби в додаткових інструментах. Крім того, WSUS використовує SQL Server Express або Windows Internal Database, що мінімізує вимоги до серверних ресурсів і спрощує розгортання в порівнянні з SCCM, яке потребує складної клієнт-серверної архітектури.

Третім аргументом є оптимізація мережевих ресурсів. WSUS завантажує оновлення з Microsoft Update лише один раз на центральний сервер, звідки вони розподіляються на клієнтські пристрої в локальній мережі. Це значно зменшує навантаження на інтернет-з'єднання, що є критичним для організацій із обмеженою пропускнуою здатністю мережі. У контексті даної роботи, де інфраструктура

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

включає численні Windows-пристрої, WSUS забезпечує ефективне використання мережевих ресурсів, що сприяє стабільності системи.

Четвертим фактором є підтримка базової автоматизації через PowerShell. Хоча WSUS не пропонує вбудованих механізмів автоматичного схвалення оновлень, використання PowerShell-скриптів дозволяє автоматизувати рутинні завдання, такі як схвалення патчів, моніторинг стану клієнтів і формування звітів. Це відповідає інженерному підходу до оптимізації процесів і компенсує обмеження WSUS у порівнянні з більш автоматизованими рішеннями, такими як Intune чи ManageEngine.

Нарешті, WSUS ідеально підходить для Windows-центричних середовищ, де основними продуктами є операційні системи Windows і програмне забезпечення Microsoft, як у даній роботі. Оскільки інфраструктура домену kostiuk.net базується на Windows Server і клієнтських пристроях Windows, WSUS забезпечує повне покриття потреб у оновленнях без необхідності додаткових інструментів для стороннього ПЗ, яке в даному випадку не є пріоритетом.

Таким чином, вибір WSUS зумовлений його економічністю, простотою інтеграції з Active Directory, оптимізацією мережевих ресурсів, можливостями базової автоматизації та відповідністю Windows-центричній інфраструктурі. Ці фактори роблять WSUS оптимальним рішенням для реалізації централізованого управління оновленнями в межах даної роботи.

1.4.4 Обмеження WSUS і способи їх часткового вирішення

Хоча WSUS є ефективним інструментом для централізованого управління оновленнями, він має низку обмежень, які необхідно враховувати для усвідомленого вибору. У даній роботі ці обмеження були проаналізовані, а їхній вплив пом'якшено за допомогою інженерних підходів, що відповідають наявній інфраструктурі та можливостям організації. Нижче розглянуто основні обмеження WSUS та способи їх часткового вирішення.

Першим обмеженням є відсутність підтримки стороннього програмного забезпечення. WSUS підтримує лише оновлення продуктів Microsoft, таких як

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

Windows, Office і Server, що ускладнює управління патчами для сторонніх додатків, наприклад, Adobe, Java чи Google Chrome. Для вирішення цієї проблеми в межах може бути використано ручне управління сторонніми оновленнями через PowerShell-скрипти, які автоматизують завантаження та розгортання патчів із офіційних джерел постачальників.

Другим обмеженням є низький рівень автоматизації. WSUS не підтримує автоматичне схвалення оновлень за розкладом, що вимагає ручного втручання адміністратора або створення скриптів. Для пом'якшення цього недоліку може бути використано PowerShell-скрипти для автоматизації схвалення оновлень на основі заданих критеріїв, таких як категорія патчів чи критичність. Крім того, інтеграція з GPO дозволяє налаштувати автоматичне розгортання оновлень за розкладом, що зменшує навантаження на адміністраторів.

Третім обмеженням є обмежена звітність. WSUS пропонує базові звіти через консоль або SQL-запити до бази даних SUSDB, але вони не забезпечують детальної аналітики чи кастомізації, як у SCCM чи ManageEngine. Для вирішення цієї проблеми можна використати SQL-запити для створення кастомізованих звітів про стан клієнтів і оновлень, які експортуються для подальшого аналізу. Додатково може застосовуватись Performance Monitor (Perfmon) для моніторингу впливу оновлень на продуктивність системи, що компенсує брак вбудованої аналітики.

Четвертим обмеженням є обмежена масштабованість. WSUS ефективний для мереж із кількістю пристроїв до 1500, але у великих інфраструктурах можуть виникати проблеми з продуктивністю сервера. У даній роботі, де кількість пристроїв у домені kostiuk.net є помірною, це обмеження не є критичним. Проте для підвищення продуктивності використано розподілені WSUS-сервери, які синхронізуються з основним сервером, що забезпечує балансування навантаження в мережі.

Основні способи вирішення обмежень WSUS:

- Використання PowerShell для автоматизації схвалення та розгортання сторонніх оновлень.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

- Створення тестових віртуальних середовищ на Hyper-V для перевірки патчів.
- Розробка кастомізованих SQL-звітів для аналізу стану оновлень.
- Застосування Perfmon для моніторингу продуктивності системи.
- Розгортання додаткових WSUS-серверів для підвищення масштабованості.

Таким чином, вибір WSUS у даній роботі є усвідомленим, з урахуванням його обмежень, які частково компенсуються за допомогою інженерних рішень, таких як автоматизація через PowerShell, інтеграція з Active Directory і використання віртуалізації. Ці підходи дозволяють оптимізувати процес Patch Management, забезпечуючи стабільність і ефективність інфраструктури.

1.5 Ризики відсутності оновлень (вразливості, загрози)

Відсутність своєчасного встановлення оновлень операційних систем і програмного забезпечення спричиняє найбільші загрози у корпоративних інформаційних системах, що впливають на їхню стабільність, продуктивність і безпеку. У складних інфраструктурах, таких як доменні мережі з великою кількістю пристроїв, оновлення відіграють ключову роль у виправленні помилок, забезпеченні сумісності та усуненні вразливостей, які можуть призвести до збоїв або компрометації системи. У контексті комп'ютерної інженерії управління оновленнями є важливим інженерним завданням, спрямованим на підтримку надійності та ефективності мережі. У межах даної роботи, де використовується Windows Server Update Services (WSUS) для централізованого Patch Management у домені kostiuk.net, аналіз ризиків підкреслює необхідність своєчасного оновлення для забезпечення стабільної роботи Windows-систем.

1.5.1 Вразливості та їхній вплив на системи

Вразливість — це недолік у програмному забезпеченні, який може бути використаний для порушення конфіденційності, цілісності або доступності ін-

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

формаційної системи. Такі недоліки виникають через помилки в коді, неправильну конфігурацію або застарілу архітектуру ПЗ. Усі вразливості реєструються в загальнодоступних базах, зокрема в системі Common Vulnerabilities and Exposures (CVE), яка станом на 2023 рік містить понад 200,000 записів, із яких значна частка стосується операційних систем Windows, серверного ПЗ Microsoft і популярних додатків, таких як Adobe Acrobat чи Java. Виробники регулярно випускають оновлення безпеки для закриття вразливостей, але їхня ефективність залежить від швидкості встановлення, що є критично важливим для корпоративних мереж.

З інженерного погляду, вразливості впливають не лише на безпеку, а й на технічну стабільність і продуктивність системи. Наприклад, вразливість у протоколі SMBv1 (CVE-2017-0144), використана в атаці WannaCry, могла спричинити не лише компрометацію, а й перевантаження мережі через несанкціонований доступ до ресурсів. Аналогічно, вразливості в Microsoft Exchange Server (CVE-2021-26855, ProxyLogon) призводили до надмірного використання серверних ресурсів, що знижувало продуктивність і викликало збої. Невстановлені оновлення також можуть спричинити проблеми сумісності, коли нові програми чи апаратне забезпечення некоректно працюють із застарілим ПЗ, що є актуальним для домену kostiuk.net, де використовуються Windows Server і клієнтські системи Windows.

У корпоративних середовищах вразливості створюють системні ризики, оскільки одна незакрита вразливість на сервері чи робочій станції може стати точкою входу для атаки на всю мережу. Наприклад, вразливість у драйверах друку Windows (CVE-2021-34527, PrintNightmare) дозволяла локальну ескалацію привілеїв, що могло скомпрометувати домен Active Directory. Крім того, застарілі системи, такі як Windows XP або Windows Server 2003, які не отримують оновлень, залишаються особливо вразливими, що підкреслює необхідність модернізації інфраструктури. У даній роботі, де використовується сучасна Windows-інфраструктура, WSUS дозволяє оперативно доставляти патчі, зменшуючи ризик експлуатації вразливостей і підтримуючи стабільність системи.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

1.5.2 Загрози та сценарії атак

Відсутність оновлень створює умови для реалізації різноманітних загроз, які можуть мати руйнівний вплив на корпоративну інфраструктуру. Ці загрози варіюються від локальних збоїв до масштабних атак, що охоплюють усю мережу. Основні типи загроз, пов'язаних із невстановленими оновленнями, включають:

- **Віддалене виконання коду (Remote Code Execution, RCE):** Зловмисники використовують вразливості для запуску довільного коду без фізичного доступу. Наприклад, вразливість EternalBlue (CVE-2017-0144) у протоколі SMBv1 дозволяла віддалено виконувати код, що стало основою для атак WannaCry і NotPetya.
- **Ескалація привілеїв:** Вразливості дозволяють зловмисникам отримувати адміністративні права, обходячи обмеження безпеки. Вразливість PrintNightmare (CVE-2021-34527) у спулєрі друку Windows давала змогу локально підвищувати привілеї, що загрожувало доменним мережам.
- **Розширення атаки в мережі (Lateral Movement):** Скомпрометована система стає плацдармом для подальшого проникнення. Наприклад, після використання вразливості в Microsoft Exchange Server (ProxyLogon, CVE-2021-26855) зловмисники отримували доступ до інших вузлів через Active Directory.
- **Шифрування або викрадення даних (Ransomware):** Вразливості використовуються для доставки шкідливого ПЗ, яке шифрує дані або викрадає конфіденційну інформацію. Атака NotPetya розгортала шифрувальник через вразливість EternalBlue, паралізуючи роботу організацій.
- **Інфікування мережі через один вузол:** Одна вразлива система може заразити всю мережу, як у випадку WannaCry, де атака поширювалася автоматично через мережеві протоколи.

Історичні та сучасні атаки демонструють серйозність цих загроз. Атака **WannaCry (2017)** заразила понад 200,000 систем у 150 країнах, використовуючи вразливість EternalBlue, яку Microsoft закрила патчем MS17-010 за два місяці до атаки. Збитки оцінюються в \$4 млрд, а постраждали лікарні, банки та промислові

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

об'єкти через затримку з оновленнями. **NotPetya (2017)**, також базуючись на EternalBlue, завдала збитків у \$10 млрд, вплинувши на компанії, такі як Maersk і Merck, через відсутність патчів. **ProxyLogon (2021)** скомпрометувала тисячі серверів Microsoft Exchange через затримку з установкою патчів, випущених у березні 2021 року, що призвело до витоків даних і встановлення веб-шеллів. **PrintNightmare (2021)** загрожувала доменним мережам через вразливість у спулері друку, яку Microsoft закрила в липні 2021 року. **Log4Shell (2021, CVE-2021-44228)**, вразливість у бібліотеці Apache Log4j, дозволяла віддалене виконання коду, вплинувши на мільйони систем через повільне оновлення серверного ПЗ. **MOVEit (2023, CVE-2023-34362)**, вразливість у ПЗ для передачі файлів, призвела до витоків даних у сотнях організацій через затримку з патчами. Нарешті, інцидент **CrowdStrike Falcon Update (2024)**, викликаний дефектним оновленням драйвера, порушив роботу мільйонів Windows-систем, підкресливши важливість тестування оновлень перед розгортанням.

Ці сценарії атак ілюструють, що навіть коротка затримка з оновленням (дні чи тижні) може мати катастрофічні наслідки, особливо в Windows-центричних мережах, як у домені kostiuk.net. З інженерного погляду, ці загрози підкреслюють необхідність централізованого Patch Management для швидкого реагування та мінімізації ризиків.

1.5.3 Організаційні, фінансові та репутаційні наслідки

Відсутність оновлень створює не лише технічні, а й організаційні, фінансові та репутаційні ризики, які впливають на функціонування організації та її взаємодію з клієнтами, партнерами та регуляторами. Ці наслідки виходять за межі інженерних аспектів, але тісно пов'язані з ефективністю Patch Management, що є ключовим у даній роботі.

Фінансові витрати є одним із найсерйозніших наслідків. Відновлення після атак, таких як WannaCry чи NotPetya, обходиться значно дорожче, ніж впровадження системи оновлень. Згідно зі звітом IBM Security 2023 року, середня вартість атаки з шифрувальником становить \$4.45 млн, включаючи викуп,

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

відновлення даних і простої. Навіть без атак, збої через несумісність ПЗ чи баги можуть призводити до значних втрат. Наприклад, простій критичних систем у банківському секторі може коштувати тисячі доларів на хвилину, що актуально для організацій із доменом kostiuk.net, де використовуються Windows-сервери для бізнес-процесів.

Порушення стандартів комплаєнсу є ще одним важливим аспектом. Міжнародні стандарти безпеки, такі як ISO 27001, NIST 800-53 і GDPR, вимагають регулярного оновлення систем для захисту даних. Наприклад, стаття 32 GDPR прямо вказує на необхідність технічного захисту, включаючи патчі. Невідповідність може призвести до штрафів до 4% річного доходу або €20 млн, а також до втрати сертифікацій, що обмежує можливості співпраці з партнерами. У контексті даної роботи WSUS забезпечує звітність про оновлення, що допомагає відповідати вимогам комплаєнсу.

Репутаційні втрати суттєво впливають на довіру до організації. Витоки даних через вразливості, як у випадку з Equifax (2017, CVE-2017-5638 в Apache Struts), призвели до падіння вартості акцій на 35% і втрати клієнтів. Подібні інциденти знижують довіру партнерів і ускладнюють залучення нових контрактів. Для середніх організацій, таких як та, що використовує домен kostiuk.net, репутаційні втрати можуть обмежити конкурентоспроможність на ринку.

Порушення безперервності бізнес-процесів є ще одним наслідком. Оновлення усувають не лише вразливості, а й баги, які можуть спричинити відмови ПЗ. Наприклад, неоновлені сервери можуть зіткнутися з проблемами продуктивності, що впливає на критичні процеси, такі як обробка транзакцій чи логістика. У 2023 році 60% організацій повідомляли про збої через застаріле ПЗ (звіт Ponemon Institute), що підкреслює важливість своєчасного Patch Management.

Юридичні наслідки виникають у разі витоків даних через невстановлені патчі. Організації можуть зіткнутися з позовами від клієнтів або регуляторів, що посилює фінансове навантаження. Наприклад, після атаки на British Airways (2018) через вразливість у вебдодатку компанія отримала штраф у £20 млн за

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

порушення GDPR. У даній роботі використання WSUS мінімізує такі ризики, забезпечуючи контрольоване оновлення Windows-систем.

1.5.4 Роль централізованого оновлення у зниженні ризиків

У складних корпоративних інфраструктурах із сотнями чи тисячами пристроїв своєчасне оновлення можливе лише за наявності централізованої системи Patch Management. У даній роботі такою системою є WSUS, який реалізує інженерні принципи автоматизації, оптимізації ресурсів і підвищення стабільності мережі. WSUS відіграє ключову роль у зниженні ризиків, пов'язаних із відсутністю оновлень, завдяки своїм функціональним можливостям.

По-перше, WSUS забезпечує швидке розгортання патчів. Оновлення завантажуються з Microsoft Update на центральний сервер і розподіляються на клієнтські пристрої через локальну мережу, що скорочує час реагування на нові вразливості. Наприклад, патч MS17-010 для EternalBlue міг бути розгорнутий через WSUS за лічені години, запобігаючи атакам WannaCry. У домені kostiuk.net це дозволяє оперативно закривати вразливості на серверах і робочих станціях. По-друге, WSUS забезпечує контроль стану пристроїв. Адміністратори можуть використовувати консоль WSUS і SQL-запити до бази SUSDB для моніторингу статусу оновлень на кожному вузлі. Це дозволяє виявляти пристрої, які не отримали патчі, і вживати заходів, що є критично важливим для великих мереж. У даній роботі SQL-запити використовуються для створення кастомізованих звітів, що підвищує ефективність адміністрування.

По-третє, WSUS знижує ймовірність людських помилок. Інтеграція з Active Directory і груповими політиками (GPO) дозволяє централізовано налаштовувати політики оновлення для різних груп пристроїв, таких як сервери чи робочі станції. PowerShell-скрипти додатково автоматизують схвалення патчів, що зменшує залежність від ручного втручання. У домені kostiuk.net GPO використовуються для розгортання оновлень за розкладом, що мінімізує пропуски.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

По-четверте, WSUS підтримує тестування оновлень перед масовим розгортанням. Адміністратори можуть створювати тестові групи пристроїв, що дозволяє перевіряти патчі на сумісність і стабільність. У даній роботі віртуальні середовища на базі Hyper-V використовуються для тестування, що запобігає збоям, як у випадку з дефектним оновленням CrowdStrike 2024. Це підкреслює інженерний підхід до забезпечення надійності системи.

По-п'яте, WSUS створює доказову базу для аудиту та комплаєнсу. Базова звітність через консоль, доповнена SQL-звітами, дозволяє документувати стан оновлень, що відповідає вимогам ISO 27001 і GDPR. Додаткове використання Performance Monitor (Perfmon) для оцінки впливу патчів на продуктивність системи підвищує якість управління.

З інженерного погляду, WSUS оптимізує мережеві ресурси, оскільки оновлення завантажуються лише один раз на сервер, що зменшує навантаження на інтернет-з'єднання. Це особливо важливо для організацій із обмеженою пропускною здатністю, як у даній роботі. Крім того, інтеграція з Active Directory спрощує адміністрування, дозволяючи гнучко налаштовувати політики для різних груп пристроїв. У контексті домену kostiuk.net WSUS реалізує контрольовану модель Patch Management, що включає етапи тестування, схвалення та розгортання, забезпечуючи стабільність, продуктивність і зниження ризиків, пов'язаних із відсутністю оновлень.

1.6 Обґрунтування вибору платформи віртуалізації (Oracle VirtualBox)

Для реалізації тестового корпоративного середовища Patch Management, яке імітує типову інфраструктуру середньої організації, необхідно було обрати платформу віртуалізації, що забезпечить створення ізольованих віртуальних машин (VM), налаштування мереж та тестування сценаріїв управління оновленнями. У цьому підпункті буде детально обґрунтовано вибір гіпервізору VirtualBox шляхом аналізу теоретичних аспектів віртуалізації, порівняння з альтернативами (Microsoft Hyper-V, VMware Workstation Pro) та оцінки їхньої відповідності вимогам проекту.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

Теоретичні відомості про гіпервізори та віртуалізацію

Віртуалізація є ключовою технологією для створення тестових середовищ, оскільки дозволяє імітувати складні інфраструктури на одному фізичному хості, ізолюючи компоненти та забезпечуючи гнучкість у тестуванні. Основним інструментом віртуалізації є гіпервізор – програмне забезпечення, яке створює та управляє віртуальними машинами, дозволяючи одночасно запускати кілька операційних систем на одному апаратному забезпеченні.

Гіпервізори поділяються на два основні типи:

- **Гіпервізори типу 1 (нативні або "bare-metal"):** Працюють безпосередньо на апаратному рівні, без проміжної хост-операційної системи. Вони забезпечують високу продуктивність і ефективність завдяки прямому доступу до апаратних ресурсів. Приклади: Microsoft Hyper-V, VMware ESXi, XenServer. Такі гіпервізори зазвичай використовуються в корпоративних середовищах, де потрібна висока продуктивність і масштабування.
- **Гіпервізори типу 2 (хостові):** Працюють поверх хост-операційної системи, як звичайна програма. Вони простіші в налаштуванні, але мають нижчу продуктивність через додатковий рівень абстракції. Приклади: Oracle VirtualBox, VMware Workstation, Parallels Desktop. Цей тип гіпервізорів частіше використовується в лабораторних умовах, для розробки та тестування.

Роль гіпервізора в тестовому середовищі Patch Management полягає в наступному:

- **Ізоляція компонентів:** Кожен вузол (контролер домену, WSUS-сервери, клієнти) працює у власній віртуальній машині, що дозволяє уникнути конфліктів.
- **Гнучкість тестування:** Знімки (snapshots) дозволяють швидко відновлювати стан VM після тестування аварійних сценаріїв, наприклад відмови WSUS-сервера.
- **Моделювання мережі:** Гіпервізор забезпечує створення ізованих мереж (наприклад, NAT-мережі), що імітують корпоративну топологію.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Економія ресурсів:** Віртуалізація дозволяє розгорнути кілька серверів і клієнтів на одному фізичному хості.

Для вибору гіпервізора в рамках цього проєкту було визначено такі критерії:

- **Безкоштовність:** Оскільки проєкт є студентським, платформа має бути доступною без фінансових витрат.
- **Простота налаштування:** Гіпервізор повинен мати інтуїтивний інтерфейс для швидкого розгортання VM.
- **Підтримка гостей ОС:** Необхідна підтримка Windows Server 2022, 2019, Windows 10/11.
- **Мережеві можливості:** Можливість створення ізольованих мереж (NAT, внутрішня мережа).
- **Гнучкість у тестуванні:** Підтримка знімків для відновлення стану VM.
- **Кросплатформність:** Бажана підтримка різних хост-систем (Windows, macOS, Linux) для універсальності.

На основі цих критеріїв було розглянуто три популярні гіпервізори: Oracle VirtualBox, Microsoft Hyper-V і VMware Workstation Pro.

Порівняння гіпервізорів.

Oracle VirtualBox. Oracle VirtualBox – це гіпервізор типу 2, розроблений компанією Oracle. Він є безкоштовним і має відкритий вихідний код (ліцензія GPL), хоча деякі додаткові функції, такі як підтримка USB 3.0 або шифрування дисків, доступні через платний Extension Pack. VirtualBox підтримує широкий спектр хост-систем (Windows, macOS, Linux) і гостей ОС, включаючи Windows Server 2022, 2019, Windows 10/11, Linux, Solaris і FreeBSD. Завдяки інтуїтивному графічному інтерфейсу створення віртуальних машин і налаштування мереж (NAT, внутрішня мережа, мостовий адаптер) відбувається швидко і без складнощів. VirtualBox також підтримує знімки, що дозволяє легко повертатися до попереднього стану VM, що є критичним для тестування аварійних сценаріїв, таких як відмова сервера. Однак, як гіпервізор типу 2, VirtualBox має нижчу продуктивність порівняно з гіпервізорами типу 1 через додатковий рівень абстракції між апаратним забезпеченням і гостьовими ОС. Крім того, він менш

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

підходить для великих корпоративних середовищ через обмежені можливості масштабування та управління.

Microsoft Hyper-V. Microsoft Hyper-V – це гіпервізор типу 1, який вбудований у Windows 10/11 Pro, Enterprise та Windows Server. Також існує окрема безкоштовна версія Hyper-V Server. Hyper-V працює безпосередньо на апаратному рівні, що забезпечує високу продуктивність і ефективне використання ресурсів. Він підтримує гостьові ОС Windows, Linux і FreeBSD, а також має розширені функції, такі як реплікація VM, кластеризація, міграція VM і підтримка віртуальних комутаторів для складних мережевих конфігурацій. Hyper-V є безкоштовним у складі Windows Pro або як окремий продукт, що робить його привабливим для користувачів Windows-екосистеми. Проте Hyper-V має обмеження: він працює лише на Windows-хостах (Windows 10/11 Pro, Enterprise або Server), що виключає використання на macOS або Linux. Налаштування Hyper-V складніше для початківців, особливо якщо використовується Hyper-V Server, який не має графічного інтерфейсу і потребує управління через PowerShell або віддалені інструменти. Крім того, для використання Hyper-V на клієнтських системах потрібна Windows Pro або Enterprise, що може бути недоступним для студентів із базовими версіями Windows (наприклад, Home).

VMware Workstation Pro. VMware Workstation Pro – це гіпервізор типу 2, розроблений компанією VMware. Із травня 2024 року, після придбання VMware компанією Broadcom, Workstation Pro і Workstation Player стали безкоштовними для особистого використання, хоча для комерційного використання потрібна ліцензія. Workstation Pro підтримує Windows і Linux як хост-системи та широкий спектр гостьових ОС, включаючи Windows Server 2022, 2019, Windows 10/11. Він забезпечує високу продуктивність (кращу, ніж VirtualBox, завдяки оптимізації), розширені функції (шифрування VM, інтеграція з VMware ESXi, підтримка VLAN), а також підтримує знімки. Проте інтерфейс Workstation Pro складніший, ніж у VirtualBox, що може бути перешкодою для початківців. Крім того, Workstation Pro не підтримує macOS як хост-систему, що обмежує його універсальність порівняно з VirtualBox. Також він є більш вимогливим до апаратного

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

забезпечення, що може ускладнити використання на менш потужних машинах, які часто доступні студентам.

Для наочності наведено таблицю з основними характеристиками розглянутих гіпервізорів:

Таблиця 2.1. Порівняння гіпервізорів

Критерій	Oracle VirtualBox	Microsoft Hyper-V	VMware Workstation Pro
Тип гіпервізора	Тип 2 (над хост-ОС)	Тип 1 (безпосередньо на апаратурі)	Тип 2 (над хост-ОС)
Вартість	Безкоштовний (Extension Pack платний)	Безкоштовний (у Windows Pro/Server)	Безкоштовний (з 2024, для особистого використання)
Хост-ОС	Windows, macOS, Linux	Windows Pro/Server	Windows, Linux
Гостьові ОС	Windows, Linux, Solaris, FreeBSD	Windows, Linux, FreeBSD	Windows, Linux, FreeBSD
Простота налаштування	Висока (інтуїтивний інтерфейс)	Середня (складніше для початківців)	Середня (складніший інтерфейс)
Продуктивність	Середня (тип 2)	Висока (тип 1)	Висока (краща за VirtualBox)
Мережеві можливості	NAT, внутрішня мережа, мостовий	Розширені (VLAN, віртуальні комутатори)	Розширені (VLAN, інтеграція з ESXi)
Знімки (snapshots)	Підтримує	Підтримує	Підтримує
Корпоративні функції	Обмежені	Розширені (реплікація, кластери)	Розширені (інтеграція з ESXi)
Відповідність проєкту	Висока (простота, безкоштовність)	Середня (складність, Windows-залежність)	Середня (складність, вимоги до ресурсів)

Обґрунтування вибору. Для цього проєкту ключовими критеріями вибору гіпервізора були безкоштовність, простота налаштування, підтримка Windows-гостьових систем (Windows Server 2022, 2019, Windows 10/11), можливість створення ізольованих мереж (NAT-мережа 192.168.7.0/24) і гнучкість у тестуванні (знімки). Oracle VirtualBox повністю відповідає цим вимогам:

- **Безкоштовність:** Базова версія VirtualBox є безкоштовною, що ідеально для студентського проєкту. Extension Pack, який пропонує додаткові функції, не був потрібен для реалізації цього середовища.
- **Простота:** Інтуїтивний графічний інтерфейс дозволяє швидко створювати VM, налаштовувати мережу та управляти знімками, що значно спрощує роботу для користувачів без глибокого досвіду у віртуалізації.

- **Підтримка ОС:** VirtualBox підтримує всі необхідні гостьові ОС, включаючи Windows Server 2022 для контролера домену (DC-2022), Windows Server 2019 для WSUS-серверів (WSUS-PRIM-2019, WSUS-REPL-2019) та Windows 10/11 для клієнтів (Win-10-1-KOST, Win-11-1-KOST, Win-10-2-KOST).
- **Мережеві можливості:** Режим NAT у VirtualBox дозволяє створити ізольовану мережу (192.168.7.0/24), що забезпечує стабільний зв'язок між вузлами та ізоляцію від зовнішньої мережі, як описано в пункті 2.1.
- **Гнучкість у тестуванні:** Підтримка знімків дозволяє швидко відновлювати стан VM після тестування аварійних сценаріїв, наприклад відмови основного WSUS-сервера (WSUS-PRIM-2019).
- **Кросплатформність:** VirtualBox працює на Windows, macOS і Linux, що робить його універсальним вибором, хоча в цьому проєкті хост-система – Windows.

Microsoft Hyper-V, попри високу продуктивність як гіпервізор типу 1, був відхилений через кілька причин. По-перше, Hyper-V працює лише на Windows Pro, Enterprise або Server, що може бути обмеженням для людей, які використовують Windows Home. По-друге, налаштування Hyper-V складніше для початківців, особливо якщо використовується Hyper-V Server, який потребує управління через командний рядок. По-третє, хоча Hyper-V підтримує створення ізольованих мереж, його розширені функції (наприклад, віртуальні комутатори, VLAN) були надлишковими для цього проєкту, де потрібна проста NAT-мережа.

VMware Workstation Pro, хоча й став безкоштовним для особистого використання з 2024 року, також не був обраний. Його інтерфейс складніший, ніж у VirtualBox, що ускладнює роботу для користувачів без досвіду. Крім того, Workstation Pro більш вимогливий до апаратного забезпечення, що може бути проблемою на менш потужних машинах. Також Workstation Pro не підтримує macOS як хост-систему, що обмежує його універсальність порівняно з VirtualBox. Хоча Workstation Pro пропонує кращу продуктивність і розширені

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

функції (наприклад, інтеграція з VMware ESXi), ці можливості не були потрібні для цього проєкту, де пріоритетом є простота та швидкість розгортання.

1.7 Ідея автоматизації за допомогою PowerShell

Автоматизація процесів адміністрування є важливим інженерним завданням у комп'ютерній інженерії, що дозволяє оптимізувати ресурси, зменшити кількість рутинних операцій і підвищити ефективність управління інформаційною інфраструктурою. У контексті централізованого управління оновленнями за допомогою Windows Server Update Services (WSUS) автоматизація відіграє ключову роль у спрощенні таких завдань, як схвалення оновлень, моніторинг стану клієнтів і створення звітів. PowerShell, як потужний інструмент автоматизації для Windows-середовищ, пропонує широкі можливості для управління WSUS, що робить його перспективним рішенням для корпоративних мереж. У межах даної роботи, де WSUS використовується для Patch Management у домені kostiuk.net, ідея автоматизації за допомогою PowerShell розглядається як теоретична концепція, оскільки практична реалізація не проводилася через технічні обмеження, пов'язані з особливостями розгортання оновлень.

PowerShell є сценарною мовою та командною оболонкою, розробленою Microsoft для автоматизації адміністративних завдань у Windows-системах. Завдяки модульній архітектурі, інтеграції з .NET Framework і підтримці API WSUS, PowerShell дозволяє створювати скрипти для виконання складних операцій, які зазвичай потребують ручного втручання через консоль WSUS. У контексті Patch Management PowerShell забезпечує доступ до об'єктів WSUS, таких як оновлення, групи комп'ютерів, клієнти та база даних SUSDB, через модуль UpdateServices або COM-об'єкти (Microsoft.UpdateServices.Administration). Це дає змогу адміністраторам налаштовувати процеси управління оновленнями, адаптуючи їх до потреб організації.

Основні можливості PowerShell для автоматизації WSUS включають:

- **Автоматичне схвалення оновлень:** Скрипти можуть фільтрувати оновлення за категоріями (наприклад, безпекові, критичні), продуктами

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

(Windows, Office) і схвалювати їх для певних груп комп'ютерів, створених через Active Directory і GPO. Наприклад, можна автоматично схвалювати критичні патчі для серверів, міняючи ручне підтвердження.

- **Моніторинг стану клієнтів:** PowerShell дозволяє отримувати дані про статус оновлень на клієнтських пристроях (встановлені, очікувані, невдалі) через запити до SUSDB або API WSUS, що спрощує виявлення проблемних вузлів.
- **Генерація звітів:** Скрипти можуть створювати кастомізовані звіти про відповідність оновлень, використовуючи SQL-запити до бази SUSDB, і експортувати їх у формати CSV або HTML для аналізу.
- **Очищення застарілих оновлень:** PowerShell автоматизує видалення непотрібних або заміненіх оновлень із сервера WSUS, оптимізуючи дисковий простір і продуктивність.
- **Розгортання за розкладом:** Скрипти можуть налаштовувати розклади встановлення оновлень через GPO або WSUS API, синхронізуючи їх із піковими періодами низького навантаження мережі.
- **Тестування оновлень:** PowerShell може автоматизувати розгортання патчів на тестові групи, створені в WSUS, з подальшим аналізом результатів через Performance Monitor (Perfmon) для оцінки впливу на продуктивність.

Ці можливості дозволяють значно зменшити час, необхідний для адміністрування WSUS, і підвищити точність виконання завдань. Наприклад, скрипт для автоматичного схвалення критичних оновлень для Windows Server може виглядати так: фільтрування оновлень за класифікацією Critical і продуктом Windows Server, перевірка їхньої актуальності (не замінені іншими патчами) і схвалення для групи серверів через метод Approve() об'єкта Update. Аналогічно, скрипт для моніторингу може періодично перевіряти статус клієнтів і надсилати сповіщення адміністратору, якщо певний відсоток пристроїв не оновлено. У домені kostiuk.net такі скрипти могли б оптимізувати управління оновленнями, зменшивши залежність від ручних операцій.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Незважаючи на потенціал PowerShell, у даній роботі автоматизація не була реалізована через технічні обмеження, пов'язані з особливостями конфігурації WSUS. Зокрема, на сервер завантажувалися лише метадані оновлень, а не повні пакети, що дозволяло аналізувати доступні патчі без їхнього фізичного збереження. Однак WSUS не надає вбудованих засобів для точного сортування оновлень за специфічними критеріями, окрім продуктів (наприклад, Windows 10, Office) і класифікацій (критичні, безпекові). Це унеможливило створення скриптів, які б автоматично відбирали лише необхідні оновлення, виключаючи сотні чи тисячі непотрібних патчів. Наприклад, автоматичне схвалення всіх безпекових оновлень могло б призвести до встановлення нерелевантних драйверів або патчів для застарілих версій ПЗ, що перевантажило б сервер і мережу, а також підвищило ризик несумісності. Крім того, обмежена гнучкість API WSUS для фільтрації метаданих ускладнила розробку скриптів із достатньою точністю.

Іншими обмеженнями автоматизації є:

- **Складність розробки скриптів:** Створення надійних скриптів вимагає глибокого розуміння API WSUS і PowerShell, а також тестування для уникнення помилок, що потребує додаткового часу.
- **Ризик помилок:** Неправильно налаштовані скрипти можуть схвалити некоректні оновлення, викликаючи збої, як у випадку з дефектним оновленням CrowdStrike 2024.
- **Обмеження метаданих:** Без повних пакетів оновлень автоматизація обмежується аналізом, а не розгортанням, що знижує її практичну цінність.
- **Ресурси сервера:** Виконання складних скриптів може навантажувати WSUS-сервер, особливо в мережах із тисячами клієнтів, хоча в домені kostiuk.net це менш критично через помірну кількість пристроїв.

Теоретично, ці обмеження можна частково подолати. Наприклад, використання SQL-запитів до SUSDB могло б розширити можливості фільтрації оновлень за додатковими атрибутами, такими як дата випуску чи розмір патча. Крім того, інтеграція PowerShell із зовнішніми інструментами, такими як PDQ Deploy,

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

могла б забезпечити управління сторонніми оновленнями, які WSUS не підтримує. У даній роботі такі підходи не застосовувалися через обмеження часу та пріоритетність стабільності системи, але вони залишаються перспективними для майбутніх досліджень.

Таким чином, ідея автоматизації WSUS за допомогою PowerShell має значний потенціал для оптимізації Patch Management, пропонуючи інструменти для схвалення оновлень, моніторингу, звітності та очищення. Теоретичний аналіз підкреслює цінність PowerShell як інженерного інструменту, що може бути використаний у майбутніх проєктах для підвищення ефективності управління оновленнями в Windows-середовищах, подібних до домену kostiuk.net.

Висновки до Розділу 1

У першому розділі кваліфікаційної роботи проведено комплексний аналіз концепції управління оновленнями (Patch Management) у корпоративній інфраструктурі, з особливим акцентом на використання Microsoft Windows Server Update Services (WSUS) як основного інструмента для централізованого управління оновленнями в Windows-середовищах. Досліджено ключові аспекти Patch Management, включаючи його життєвий цикл, який охоплює інвентаризацію активів, виявлення, оцінювання, тестування, розгортання, моніторинг та аудит оновлень. Підкреслено важливість своєчасного застосування патчів для забезпечення безпеки, стабільності та продуктивності інформаційних систем, а також зменшення ризиків, пов'язаних із кіберзагрозами, такими як експлуатація вразливостей типу zero-day.

Аналіз підтвердив, що Patch Management є невід'ємною частиною інженерного процесу в комп'ютерній інженерії, який вимагає централізованого підходу для ефективного управління оновленнями в складних корпоративних мережах. Обґрунтовано вибір WSUS як оптимального рішення завдяки його інтеграції з екосистемою Microsoft, підтримці автоматизації через PowerShell, масштабованості та економічній ефективності порівняно з комерційними альтернативами.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

Теоретичне дослідження можливостей PowerShell для автоматизації WSUS продемонструвало значний потенціал для оптимізації таких процесів, як схвалення оновлень, моніторинг стану клієнтів, створення звітів, очищення застарілих патчів і розгортання за розкладом. Хоча практична реалізація автоматизації в межах роботи не проводилася через технічні обмеження, теоретичний аналіз підкреслює перспективність цього підходу для майбутніх проєктів.

Отже, перший розділ встановлює теоретичну основу для подальшого проєктування, впровадження та тестування централізованої системи управління оновленнями на базі WSUS. Результати аналізу підтверджують актуальність теми, обґрунтовують вибір інструментів і методів, а також визначають ключові напрями для практичної реалізації в наступних розділах роботи, зокрема створення лабораторного середовища, налаштування групових політик, забезпечення захищеного з'єднання через HTTPS і впровадження механізмів моніторингу та аудиту.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА ВПРОВАДЖЕННЯ СИСТЕМИ PATCH MANAGEMENT

2.1 Архітектурна модель тестового корпоративного середовища Patch Management

Для практичної реалізації централізованої системи управління оновленнями (Patch Management) на базі Microsoft Windows Server Update Services (WSUS) було спроектовано та розгорнуто тестове середовище, яке імітує типову інфраструктуру середньої за розміром організації. Метою створення такого середовища було забезпечення умов для тестування, налаштування та перевірки функціональності WSUS у реальному сценарії експлуатації, що включає клієнтські пристрої на базі Windows 10 Pro та Windows 11 Pro, розподіл групових політик (GPO), використання сертифікатів для безпечного з'єднання та моніторинг стану оновлень. Архітектурна модель розроблена з урахуванням ключових принципів корпоративних мереж: масштабованості, розподілення ролей, безпеки та модульності, що робить її гнучкою до потреб організації.

Мета та принципи проектування. Основною метою проектування тестового середовища було створення лабораторної інфраструктури, яка:

- Відтворює реальні умови корпоративної мережі з доменною структурою на базі Active Directory.
- Забезпечує централізоване управління оновленнями через WSUS із можливістю автоматизації та моніторингу.
- Дозволяє протестувати ключові аспекти Patch Management, включаючи синхронізацію оновлень, розгортання патчів, налаштування HTTPS-з'єднання та резервування.
- Підтримує гнучкість для моделювання різних сценаріїв, таких як відмова основного WSUS-сервера або масштабування мережі.

Архітектура побудована на основі таких принципів:

1. **Масштабованість:** Структура дозволяє додавати нові клієнтські пристрої, сервери або зони без значних змін у конфігурації.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

2. **Розподілення ролей:** Функції контролера домену, WSUS, бази даних SQL Server та клієнтських пристроїв розподілені між окремими вузлами для підвищення надійності та ефективності.
3. **Безпека:** Впроваджено HTTPS-з'єднання, використання сертифікатів і обмеження доступу через групові політики для захисту комунікацій між компонентами.
4. **Тестованість і модульність:** Використання віртуалізації забезпечує можливість створення резервних копій, ізоляцію компонентів і швидке відновлення системи після тестування аварійних сценаріїв.

Опис компонентів середовища. Тестове середовище складається з кількох ключових компонентів, кожен із яких виконує специфічні функції в системі Patch Management. Усі компоненти розгорнуті у віртуальній інфраструктурі на базі Oracle VirtualBox, що забезпечує гнучкість у керуванні та ізоляцію від основної системи.

1. Контролер домену (DC-SRV-2022):

- Операційна система: Windows Server 2022 Standard.
- Ролі: Контролер домену Active Directory, DNS-сервер, джерело групових політик (GPO).
- Функції: Управління доменною структурою (kostiuk.net), аутентифікація користувачів і пристроїв, розподілення політик для серверів і клієнтів, розв'язання імен у мережі.
- Виділені ресурси: 2 ядра, 4 ГБ ОЗП, 50 ГБ дискового простору.

2. Основний WSUS-сервер (WSUS-PRIM-2019):

- Операційна система: Windows Server 2019 Standard.
- Ролі: WSUS, Internet Information Services (IIS), SQL Server Standard 2019.
- Функції: Завантаження оновлень із серверів Microsoft, схвалення патчів, їх розповсюдження на клієнтські пристрої та резервний WSUS-сервер, зберігання метаданих і конфігурацій у базі даних SQL Server.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

- Виділені ресурси: 4 ядра, 9 ГБ ОЗП, 420 ГБ дискового простору.

3. Резервний WSUS-сервер (WSUS-REPL-2019):

- Операційна система: Windows Server 2019 Standard.
- Ролі: WSUS, Internet Information Services (IIS).
- База даних: Windows Internal Database (WID).
- Функції: Реплікація метаданих і схвалень із основного WSUS-сервера, резервне обслуговування клієнтів у разі недоступності основного сервера.
- Виділені ресурси: 2 ядра, 6 ГБ ОЗП, 300 ГБ дискового простору.

4. Клієнтські машини:

- Операційні системи:
- Windows 10 Pro: Win-10-1-KOST, Win-10-2-KOST.
- Windows 11 Pro: Win-11-1-KOST.
- Функції: Імітація типових робочих станцій у корпоративній мережі, отримання та встановлення оновлень від WSUS-серверів.
- Виділені ресурси: 2 ядра, 4 ГБ ОЗП, 50 ГБ дискового простору.

5. Інфраструктурна мережева модель:

- Мережа: NAT-мережа в Oracle VirtualBox із підмережею 192.168.7.0/24
- Іменування: Усі вузли використовують доменне іменування за шаблоном *.kostiuk.net (наприклад, dc-2022.kostiuk.net).
- Маршрутизація: У Oracle VirtualBox створено NAT-мережу з адресою 192.168.7.0/24, до якої підключено мережеві адаптери всіх віртуальних машин. Це забезпечує ізоляцію від зовнішньої мережі та стабільний зв'язок між вузлами.

Топологія середовища. Логічна структура мережі відображає взаємозв'язки між компонентами та їх функціональні ролі. Нижче наведено схематичне представлення топології:

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Россінський Ю.М.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

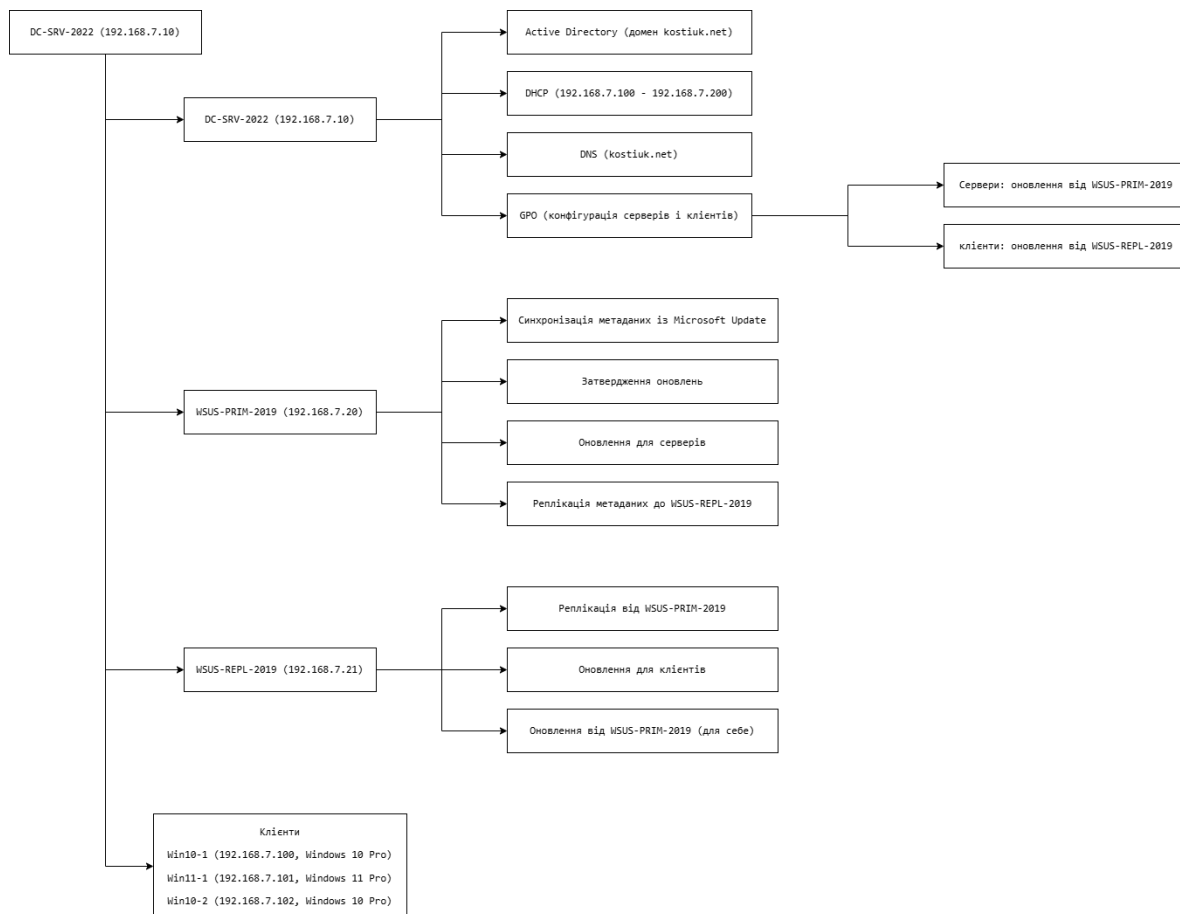


Рис. 2.1. – Архітектура інфраструктури централізованого оновлення систем

Ця топологія забезпечує чіткий розподіл ролей і дозволяє ефективно тестувати сценарії управління оновленнями, включаючи резервування та безпечну взаємодію.

Вибір платформи віртуалізації. Для розгортання тестового середовища обрано Oracle VirtualBox, безкоштовний гіпервізор із відкритим вихідним кодом, через його доступність, простоту налаштування та підтримку створення ізольованих мереж. Детальний вибір платформи віртуалізації описано в пункті 2.2.1.

Обґрунтування архітектурних рішень

1. **Використання SQL Server на основному WSUS-сервері:** SQL Server Standard 2019 обрано для WSUS-PRIM-2019 через його здатність обробляти великі обсяги даних і підтримувати масштабованість у порівнянні з Windows Internal Database (WID). Це рішення дозволяє ефективно керувати оновленнями в середовищах із десятками або сотнями клієнтів.

2. **Резервний WSUS із WID:** Для економії ресурсів резервний сервер (WSUS-REPL-2019) використовує WID, оскільки він не потребує складних операцій із базою даних, а лише реплікує метадані та схвалення.
3. **Фіксовані IP-адреси:** Використання статичних IP-адрес спрощує конфігурацію DNS і забезпечує стабільність зв'язку між компонентами.
4. **Доменно-орієнтована структура:** Active Directory обрано як основу для управління пристроями та політиками, оскільки це стандарт для корпоративних мереж, що забезпечує централізоване адміністрування та безпеку.
5. **Різноманітність клієнтських ОС:** Використання Windows 10 Pro і Windows 11 Pro дозволяє протестувати сумісність WSUS із різними версіями клієнтських систем, що відображає реальні корпоративні сценарії.

Переваги та обмеження моделі

Переваги:

- Реалістичність: Середовище імітує типову корпоративну інфраструктуру, що робить результати тестування застосовними до реальних сценаріїв.
- Гнучкість: VirtualBox дозволяє швидко змінювати конфігурацію, створювати знімки та моделювати аварійні ситуації.
- Безпека: Налаштування HTTPS і GPO забезпечує захист комунікацій і обмеження доступу.
- Масштабованість: Модель може бути розширена додатковими серверами або клієнтами.

Обмеження:

- Обмежені ресурси: Тестове середовище розгорнуто на одному фізичному хості з VirtualBox, що може обмежувати продуктивність при моделюванні великих мереж.
- Спрощена топологія: Мережа використовує одну підмережу без сегментації, що не повною мірою відображає складні корпоративні середовища.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

- Відсутність зовнішнього доступу: Середовище ізольоване, що виключає тестування сценаріїв із підключенням до зовнішніх ресурсів (наприклад, хмарних сервісів).
- Обмеження VirtualBox: У порівнянні з корпоративними гіпервізорами (наприклад, VMware ESXi), VirtualBox має меншу продуктивність і обмежену підтримку складних мережевих конфігурацій.

Розроблена архітектурна модель тестового корпоративного середовища забезпечує надійну основу для реалізації та тестування централізованої системи Patch Management на базі WSUS. Завдяки використанню Oracle VirtualBox, Active Directory, SQL Server і чіткому розподілу ролей між компонентами, середовище дозволяє відтворити реальні умови експлуатації, включаючи управління оновленнями, безпечну взаємодію та резервування. Наявність клієнтських машин із Windows 10 Pro та Windows 11 Pro забезпечує перевірку сумісності системи з різними ОС. Ця модель стала фундаментом для подальших етапів роботи, зокрема розгортання доменної структури, налаштування WSUS і групових політик, а також тестування системи, результати якого будуть представлені в розділі 4.

2.2. Вибір платформи віртуалізації та розгортання середовища

2.2.1 Створення віртуальної мережі

Для реалізації тестового середовища Patch Management, яке імітує корпоративну інфраструктуру, необхідно було створити ізольовану віртуальну мережу, що забезпечує зв'язок між усіма компонентами (контролер домену, WSUS-сервери, клієнтські машини), а також контрольований доступ до зовнішньої мережі для синхронізації оновлень. Усі компоненти середовища (DC-SRV-2022, WSUS-PRIM-2019, WSUS-REPL-2019, Win-10-1-KOST, Win-11-1-KOST, Win-10-2-KOST) підключені до мережі NAT із підмережею 192.168.7.0/24, створеної в Oracle VirtualBox. Для WSUS-серверів додатково налаштовано другий адаптер у режимі NAT для доступу до зовнішньої мережі. У цьому підпункті описано

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

вибір типу мережі, налаштування мережевих параметрів, розподіл IP-адрес, перевірку зв'язку між вузлами та синхронізацію часу.

Вибір типу мережі в Oracle VirtualBox. Oracle VirtualBox надає кілька типів віртуальних мереж, які дозволяють моделювати різні топології:

- **NAT (Network Address Translation):** Віртуальні машини отримують IP-адреси від внутрішнього DHCP-сервера VirtualBox (зазвичай у діапазоні 10.0.2.0/24) і мають доступ до зовнішньої мережі через трансляцію адрес, але не можуть спілкуватися між собою напряму.
- **NAT Network:** Розширений режим NAT, який дозволяє створити ізольовану мережу з власним адресним простором. VM у такій мережі можуть спілкуватися між собою, а також мати доступ до зовнішньої мережі через хост.
- **Внутрішня мережа (Internal Network):** VM спілкуються лише між собою, без доступу до зовнішньої мережі.
- **Мостовий адаптер (Bridged Adapter):** VM підключаються до фізичної мережі хоста, отримуючи IP-адреси з тієї ж підмережі, що й хост.
- **Хостовий адаптер (Host-Only):** VM спілкуються лише з хостом і між собою через спеціальну мережу.

Для цього проєкту як основний режим для всіх віртуальних машин обрано **NAT Network**, що забезпечує ізоляцію внутрішньої інфраструктури та зв'язок між компонентами:

- **Ізоляція:** Мережа ізольована від зовнішнього світу, що відповідає вимогам безпеки тестового середовища.
- **Зв'язок між вузлами:** Усі компоненти можуть обмінюватися даними в межах підмережі 192.168.7.0/24, що необхідно для роботи домену kostiuk.net, DNS, GPO і передачі оновлень.
- **Гнучкість:** Можливість налаштування власного адресного простору дозволяє імітувати типову корпоративну мережу.

Для WSUS-серверів (WSUS-PRIM-2019 і WSUS-REPL-2019) додатково використано другий адаптер у режимі **NAT**, щоб забезпечити доступ до зовнішньої

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

мережі, зокрема до Microsoft Update, для синхронізації оновлень. У режимі NAT зв'язок із зовнішньою мережею здійснюється через трансляцію адрес, а IP-адреси призначаються автоматично внутрішнім DHCP-сервером VirtualBox.

Режим звичайного NAT як основний не відповідав вимогам, оскільки не забезпечує прямого зв'язку між VM, що унеможливило б роботу домену та служб. Внутрішня мережа була відхилена через відсутність доступу до зовнішньої мережі, необхідного для WSUS-серверів. Мостовий і хостовий адаптери не розглядалися, оскільки вони не забезпечують ізоляції від зовнішньої мережі, що суперечить вимогам безпеки.

Створення та налаштування NAT Network. Для ізоляції внутрішньої інфраструктури в Oracle VirtualBox створено нову NAT-мережу з назвою PatchManagementNet. У розділі мережевих налаштувань VirtualBox задано адресний простір 192.168.7.0/24 із маскою підмережі 255.255.255.0. DHCP-сервер у цій мережі відключено, що дозволило повністю контролювати розподіл IP-адрес вручну. Шлюз за замовчуванням (192.168.7.1) забезпечує маршрутизацію в межах NAT Network.

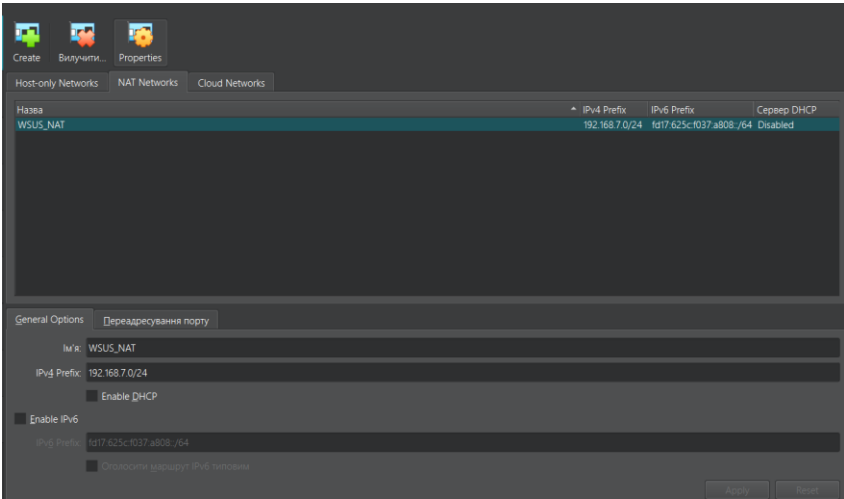


Рис. 2.2 - Налаштування NAT Network у VirtualBox.

Мережеві адаптери всіх віртуальних машин (DC-SRV-2022, WSUS-сервери, клієнти) підключені до створеної мережі PatchManagementNet. Для адаптерів обрано тип Intel PRO/1000 MT Desktop, що забезпечує стабільну роботу з Windows-гостями, та увімкнено опцію підключення кабелю, щоб адаптери були

активними. Це дозволило всім компонентам обмінюватися даними в межах підмережі 192.168.7.0/24.

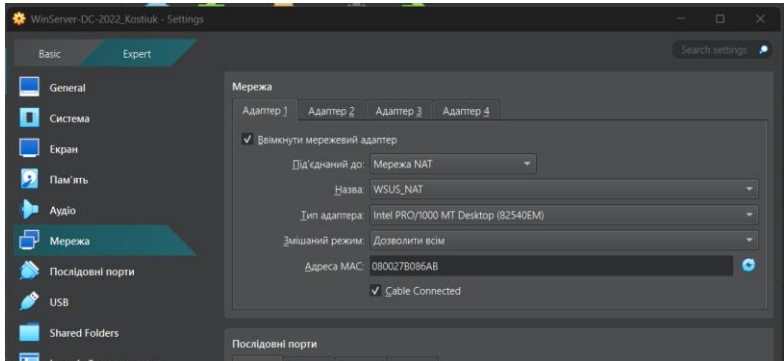


Рис. 2.3 - Налаштування мережевого адаптера для DC-SRV-2022.

Для WSUS-серверів (WSUS-PRIM-2019 і WSUS-REPL-2019) додатково налаштовано другий адаптер у режимі NAT. Цей адаптер забезпечує доступ до зовнішньої мережі через трансляцію адрес, а IP-адреси призначаються автоматично внутрішнім DHCP-сервером VirtualBox (діапазон 10.0.2.0/24). Такий підхід дозволив WSUS-серверам синхронізуватися з Microsoft Update, зберігаючи ізоляцію основної мережі.

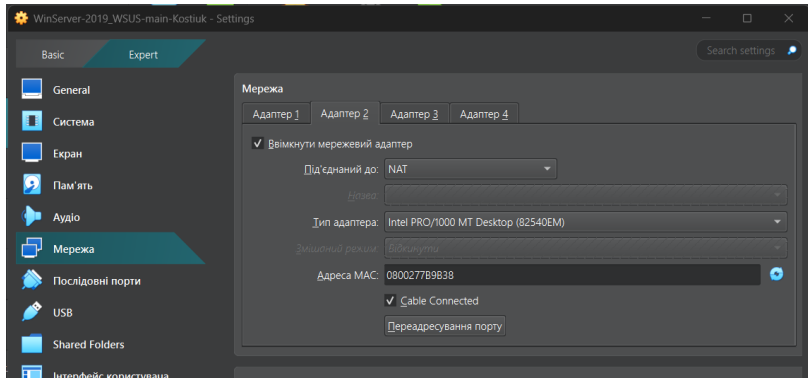


Рис. 2.4 - Налаштування другого адаптера для WSUS-PRIM-2019.

Забезпечення функціональності середовища. Налаштована мережа забезпечує виконання всіх вимог проєкту:

- **Зв'язок між вузлами:** Усі компоненти можуть обмінюватися даними в межах підмережі 192.168.7.0/24, що дозволяє DC-SRV-2022 надавати послуги Active Directory, DNS і GPO, WSUS-REPL-2019 – розподіляти оновлення клієнтам, а WSUS-PRIM-2019 – реплікувати метадані до WSUS-REPL-2019.

- **Доступ до зовнішньої мережі:** Другий адаптер WSUS-серверів у режимі NAT забезпечує контрольований доступ до Microsoft Update для синхронізації оновлень.
- **Ізоляція:** Основна мережа ізольована від зовнішнього світу, що відповідає вимогам безпеки тестового середовища.

Налаштування NAT Network із підмережею 192.168.7.0/24 і додаткового адаптера в режимі NAT для WSUS-серверів дозволило створити ізольовану віртуальну мережу, яка забезпечує зв'язок між компонентами тестового середовища Patch Management, а також контрольований доступ до зовнішньої мережі для синхронізації оновлень.

2.2.2 Створення та налаштування віртуальних машин

У цьому підпункті описано процес створення VM, їх базову конфігурацію, включаючи налаштування IP-адрес і DNS, а також початкову перевірку функціональності, що забезпечує основу для подальшого розгортання доменної структури.

Опис компонентів і їх ролі. Тестове середовище включає шість віртуальних машин із визначеними ролями. DC-SRV-2022 виконує функцію контролера домену та забезпечує послуги Active Directory і DNS. WSUS-PRIM-2019 слугує основним сервером WSUS для синхронізації оновлень із Microsoft Update, тоді як WSUS-REPL-2019 є резервним сервером для реплікації оновлень. Клієнтські машини Win-10-1-KOST, Win-10-2-KOST і Win-11-1-KOST призначені для тестування розподілу оновлень і доменних політик. Усі компоненти підключено до NAT-мережі з підмережею 192.168.7.0/24, а WSUS-сервери додатково мають другий адаптер у режимі NAT для доступу до зовнішньої мережі.

Процес створення віртуальних машин. Створення віртуальних машин у Oracle VirtualBox проводилося з урахуванням їхніх ролей та апаратних вимог. Було створено кожен VM, визначивши її ім'я та обравши відповідний тип і версію операційної системи (Microsoft Windows, наприклад, Windows Server

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

2019 для серверів і Windows 10/11 для клієнтів), після чого задано обсяг оперативної пам'яті, кількість віртуальних процесорів і розмір динамічного віртуального диска у форматі VDI. Специфікації кожної віртуальної машини наведено нижче:

- DC-SRV-2022: 50 ГБ диска, 4 ГБ оперативної пам'яті, 2 процесори.
- WSUS-PRIM-2019: 420 ГБ диска, 9 ГБ оперативної пам'яті, 5 процесорів.
- WSUS-REPL-2019: 300 ГБ диска, 6 ГБ оперативної пам'яті, 2 процесори.
- Win-10-1-KOST: 50 ГБ диска, 4 ГБ оперативної пам'яті, 1 процесор.
- Win-10-2-KOST: 50 ГБ диска, 4 ГБ оперативної пам'яті, 1 процесор.
- Win-11-1-KOST: 80 ГБ диска, 6 ГБ оперативної пам'яті, 2 процесори.

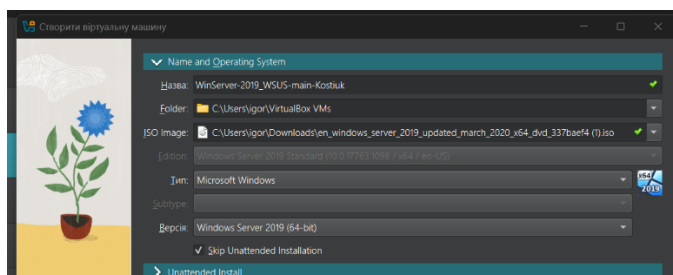


Рис. 2.5 - Вибір ISO-образа для створення нової віртуальної машини.

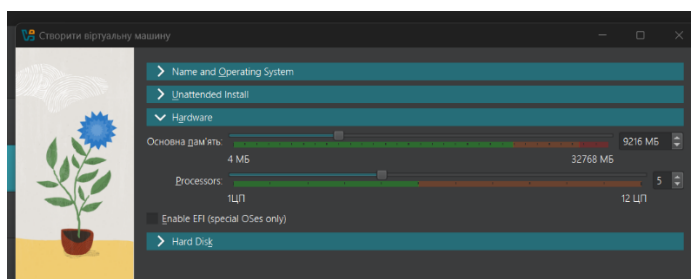


Рис. 2.6 - Вибір обсягу оперативної пам'яті, та кількості ядер процесора.

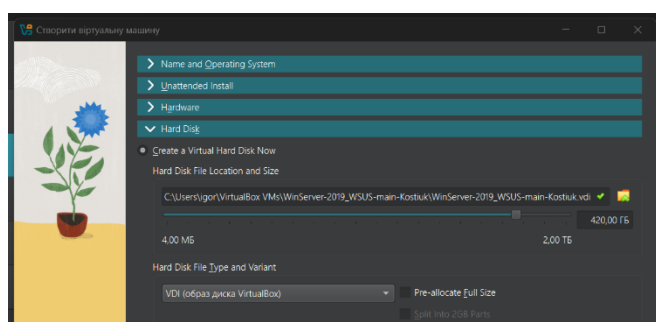


Рис. 2.7 - Встановлення обсягу дискового простору.

Для початку установки операційних систем було підключено ISO-образ через меню налаштувань VM, після чого обрано завантаження з оптичного диска

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

та запущено машину. У процесі установки було пропущено введення ключа активації, обрано відповідну редакцію (наприклад, Windows Server 2019 Standard (Desktop Experience) для WSUS-серверів) (див. рис. 2.9), погоджено ліцензійну угоду (див. рис. 2.10), після чого виконано інсталяцію з типом "Custom", що передбачав автоматичне розбиття дискових розділів (див. рис. 2.11). На завершальному етапі було встановлено пароль для адміністраторського акаунта (див. рис. 2.12), після чого машина перезавантажилася. Оновлення операційних систем на цьому етапі не застосовувалися, щоб уникнути конфліктів із подальшою конфігурацією.

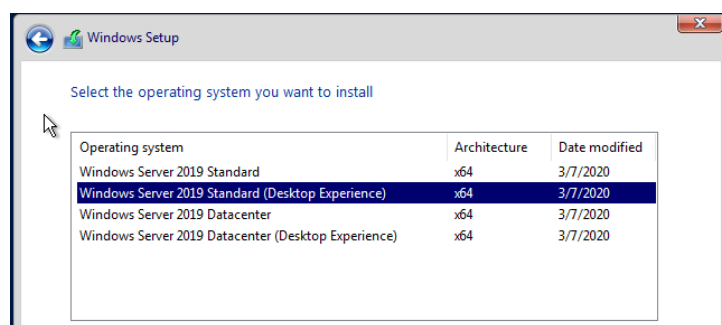


Рис. 2.8 - Вибір редакції Windows Server 2019 Standard (Desktop Experience).

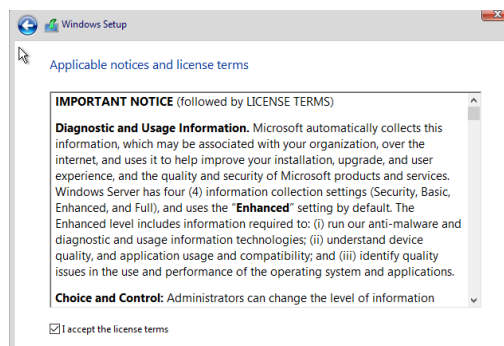


Рис. 2.9 - Погодження ліцензійної умови.

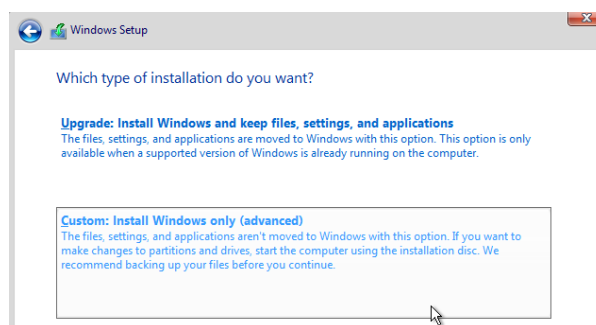


Рис. 2.10 - Вибір типу інсталяції "Custom".

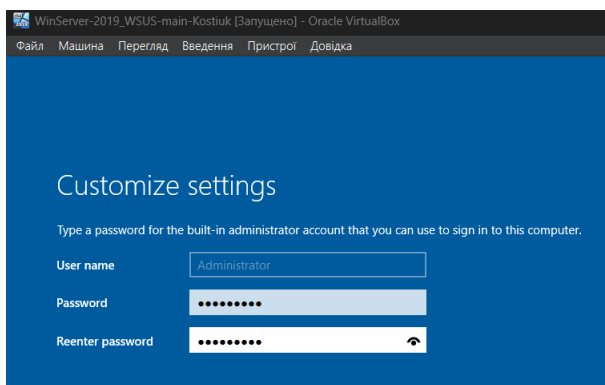


Рис. 2.11 - Встановлення паролю для адміністраторського акаунта.

Конфігурація операційних систем. Після установки ОС було проведено базову конфігурацію для забезпечення мережевої взаємодії. Спочатку змінено імена комп'ютерів через системні налаштування для відповідності доменному іменуванню:

- DC-SRV-2022.
- WSUS-PRIM-2019.
- WSUS-REPL-2019.
- Win-10-1-KOST.
- Win-10-2-KOST.
- Win-11-1-KOST.

Зміна імен завершилася перезавантаженням кожної машини, що забезпечило коректну ідентифікацію в мережі.

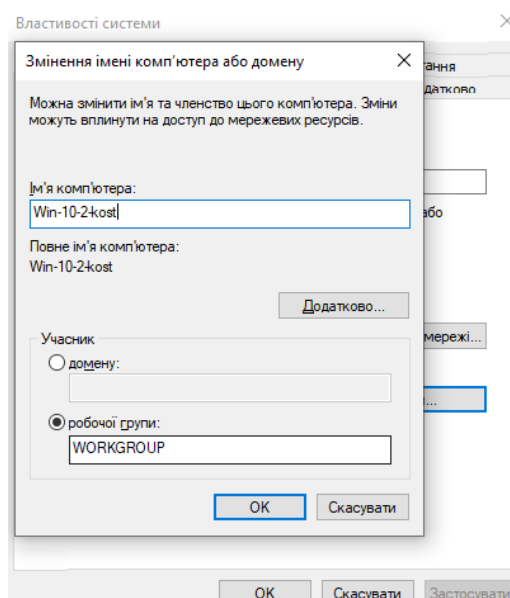


Рис. 2.12 - Зміна імені комп'ютера для WIN-10-2-KOST.

Налаштування IP-адрес. Для всіх VM у підмережі 192.168.7.0/24 було призначено статичні IP-адреси відповідно до таблиці адресації:

Таблиця 2.2. таблиця IP-адресації

Мережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс
Мережа	-	192.168.7.0	255.255.255.0	/24
Маршрутизатор R-21-7-1	Fa0/1	192.168.7.1	255.255.255.0	/24
Domain controller Windows server 2022	Fa0	193.168.7.10	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.7.1	-	-
WSUS server Windows server 2019	Fa0	192.168.7.20	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.7.1	-	-
WSUS server (replica) Windows server 2019	Fa0	192.168.7.21	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.7.1	-	-
Робоча станція Windows 10 - 1	Fa0	192.168.7.100	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.7.1	-	-
Робоча станція Windows 11	Fa0	192.168.7.101	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.7.1	-	-
Робоча станція Windows 10 - 2	Fa0	192.168.7.100	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.7.1	-	-

Налаштування проводилося через мережеві параметри Windows, де відкривалися властивості адаптера, вручну задавалися статична IP-адреса, маска підмережі 255.255.255.0, шлюз за замовчуванням 192.168.7.1 і DNS-сервер 192.168.7.10 (DC-SRV-2022), після чого зберігалися зміни. Для WSUS-серверів другий адаптер у режимі NAT залишався з автоматичним отриманням IP-адреси від DHCP VirtualBox.

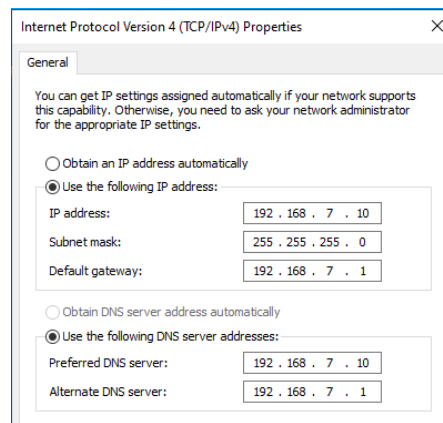


Рис. 2.13 - Призначення IP-адреси для DC-SRV-2022.

Налаштування брандмауера. Для спрощення діагностики мережі було увімкнено правило "File and Printer Sharing (Echo Request - ICMPv4-In)" у Windows Defender Firewall для всіх профілів (домен, приватний, публічний), що дозволило використовувати команду ping для перевірки зв'язку між машинами.

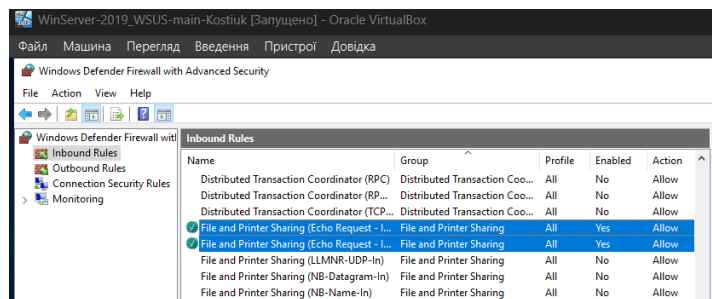


Рис. 2.14 - Налаштування брандмауера на Win-11-1-KOST.

Налаштування часових зон. Щоб забезпечити узгодженість часу для коректної роботи доменних служб, робочі станції було налаштовано на часову зону EEST (FLE Standard Time). Для цього використано PowerShell, де виконано команду для встановлення часової зони, перевірено результат і, за потреби, перезавантажено машини. Цей процес проведено для всіх віртуальних машин в мережі.

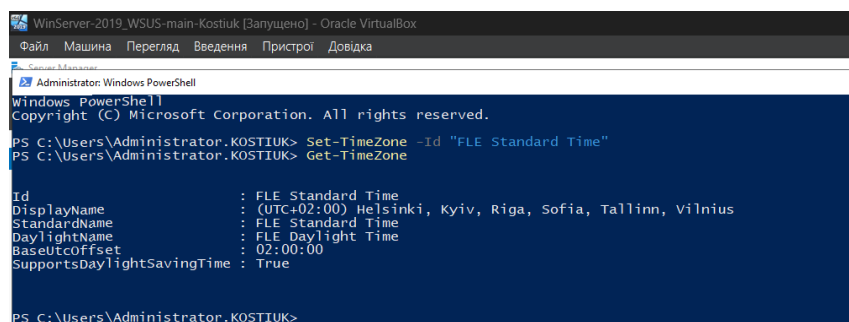


Рис. 2.15 - Налаштування часової зони на WSUS-PRIM-2019.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Перевірка функціональності. Після завершення базової конфігурації проведено перевірку функціональності розгорнутих VM:

- Команда ping від DC-SRV-2022 до клієнтів (Win-10-1-KOST, Win-11-1-KOST, Win-10-2-KOST) і до WSUS-PRIM-2019 підтвердила доступність робочих станцій (див. рис. 2.16).
- Перевірка доступу до зовнішньої мережі через другий адаптер WSUS-PRIM-2019 (режим NAT): команда ping google.com показала успішний зв'язок, що забезпечує синхронізацію з Microsoft Update (див. рис. 2.17).
- Перевірка DNS: Запит nslookup kostiuk.net із клієнтів повернув IP-адресу 192.168.7.10, що свідчить про коректну роботу DNS-сервера на DC-SRV-2022 (див. рис. 2.18).

```

C:\Users\Administrator>ping 192.168.7.20

Pinging 192.168.7.20 with 32 bytes of data:
Reply from 192.168.7.20: bytes=32 time=1ms TTL=128
Reply from 192.168.7.20: bytes=32 time=1ms TTL=128
Reply from 192.168.7.20: bytes=32 time=1ms TTL=128
Reply from 192.168.7.20: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.7.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>ping 192.168.7.21

Pinging 192.168.7.21 with 32 bytes of data:
Reply from 192.168.7.21: bytes=32 time=1ms TTL=128
Reply from 192.168.7.21: bytes=32 time=1ms TTL=128
Reply from 192.168.7.21: bytes=32 time=1ms TTL=128
Reply from 192.168.7.21: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.7.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 192.168.7.100

Pinging 192.168.7.100 with 32 bytes of data:
Reply from 192.168.7.100: bytes=32 time=1ms TTL=128
Reply from 192.168.7.100: bytes=32 time=1ms TTL=128
Reply from 192.168.7.100: bytes=32 time=1ms TTL=128
Reply from 192.168.7.100: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.7.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 192.168.7.101

Pinging 192.168.7.101 with 32 bytes of data:
Reply from 192.168.7.101: bytes=32 time=1ms TTL=128
Reply from 192.168.7.101: bytes=32 time=1ms TTL=128
Reply from 192.168.7.101: bytes=32 time=1ms TTL=128
Reply from 192.168.7.101: bytes=32 time=1ms TTL=128
  
```

Рис. 2.16 - Перевірка зв'язку між робочими станціями.

```

C:\Users\Administrator.KOSTIUK>ping google.com

Pinging google.com [172.217.16.46] with 32 bytes of data:
Reply from 172.217.16.46: bytes=32 time=34ms TTL=117
Reply from 172.217.16.46: bytes=32 time=34ms TTL=117
Reply from 172.217.16.46: bytes=32 time=33ms TTL=117
Reply from 172.217.16.46: bytes=32 time=32ms TTL=117

Ping statistics for 172.217.16.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 34ms, Average = 33ms

C:\Users\Administrator.KOSTIUK>
  
```

Рис. 2.17 - Перевірка доступу WSUS сервера до інтернету.

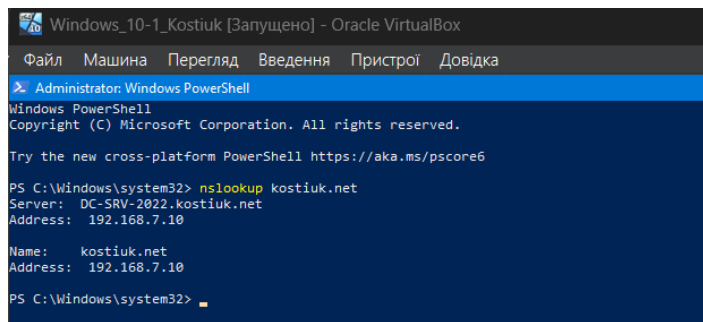


Рис. 2.18 - Перевірка працездатності DNS-сервера.

2.3. Налаштування контролера домену та служби Active Directory

2.3.1 Розгортання служби Active Directory

Одним із ключових етапів у побудові централізованої системи Patch Management є створення доменної інфраструктури, яка дозволяє централізовано керувати обліковими записами, політиками безпеки та конфігураціями клієнтів. Для цього на сервері DC-SRV-2022, що працює під керуванням Windows Server 2022, було розгорнуто службу Active Directory Domain Services (AD DS) з одночасною інтеграцією ролі DNS-сервера.

Створення нового домену та промоція сервера до контролера домену. Для підвищення сервера DC-SRV-2022 до статусу контролера домену було встановлено роль Active Directory Domain Services (AD DS) через Server Manager у Windows Server 2022 (рис. 2.19). Після завершення установки ролі з'явився Notification Flag, де обрано опцію "Promote this server to a domain controller", для ініціювання процесу підвищення сервера до контролера домену з утворенням нового лісу. В процесі налаштування було створено новий домен з ім'ям kostiuk.net (рис. 2.21), що відображає умовну корпоративну назву організації. Автоматично згенероване NetBIOS-ім'я домену — KOSTIUK (рис. 2.22).

Конфігурація включала:

- вибір опції створення нового лісу;
- встановлення пароля для **Directory Services Restore Mode (DSRM)** — аварійного відновлення каталогу. (рис. 2.23)
- вибір шляху збереження баз даних, журналів та SYSVOL (рис. 2.24);

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

Після завершення налаштувань (рис. 2.25) сервер було автоматично перезавантажено. Після перезапуску було підтверджено успішне завершення проміжної: у вікні **System** з'явилась вказівка, що пристрій є контролером домену kostiuk.net, а в оснастці **Active Directory Users and Computers** доступна структура домену.

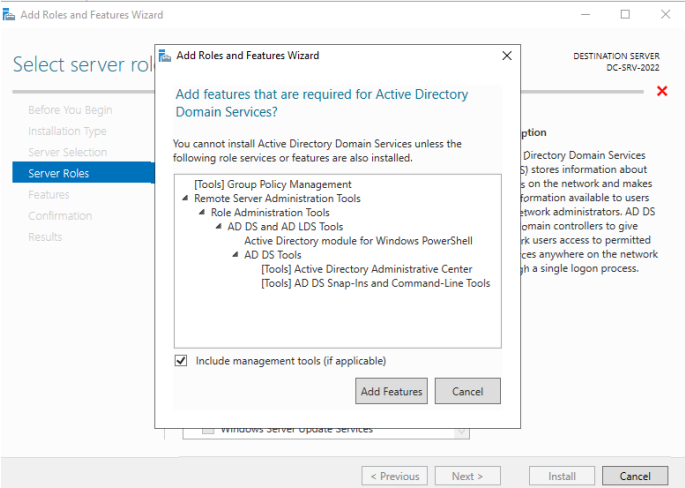


Рис. 2.19 - Вибір ролі Active Directory Domain Services (AD DS) для встановлення.

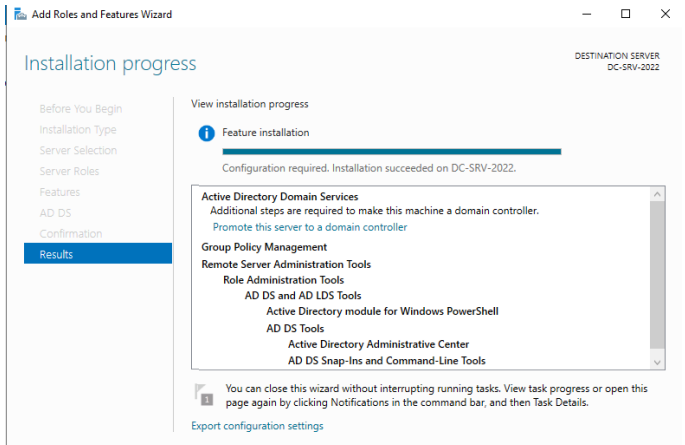


Рис. 2.20 - Успішне встановлення ролі AD DS на DC-SRV-2022.

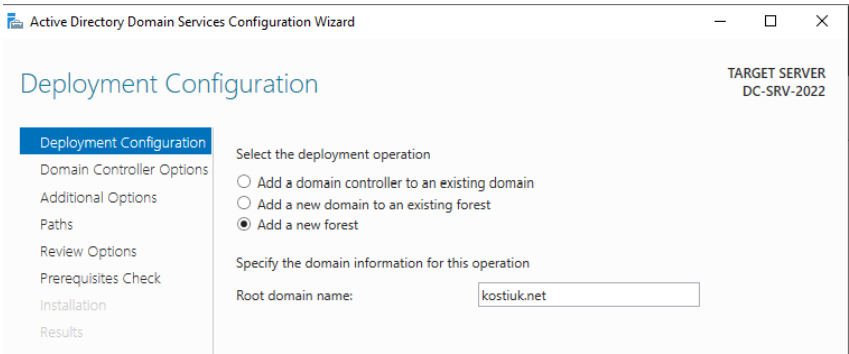


Рис. 2.21 - Введення доменного імені для створення нового лісу.

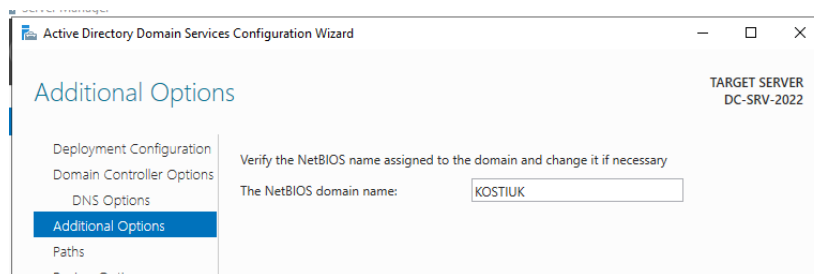


Рис. 2.22 - NetBIOS-ім'я за замовчуванням.

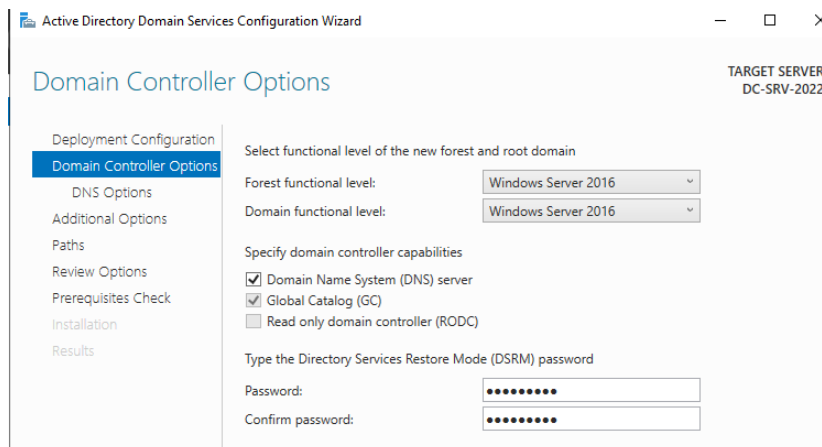


Рис. 2.23 - Введення паролю для Directory Services Restore Mode.

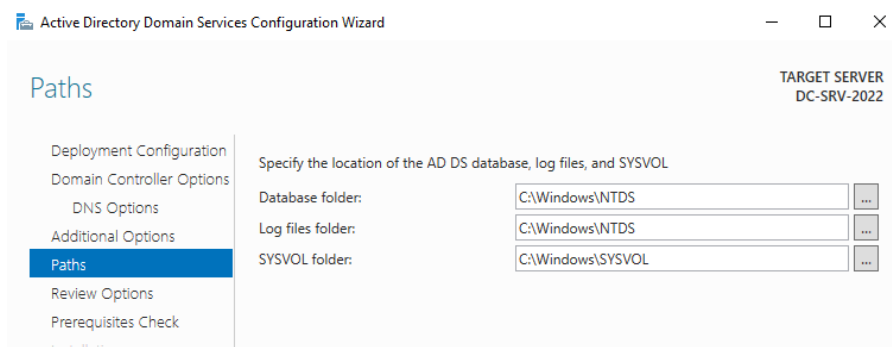


Рис. 2.24 - Вибір шляхів зберігання бази даних і логів.

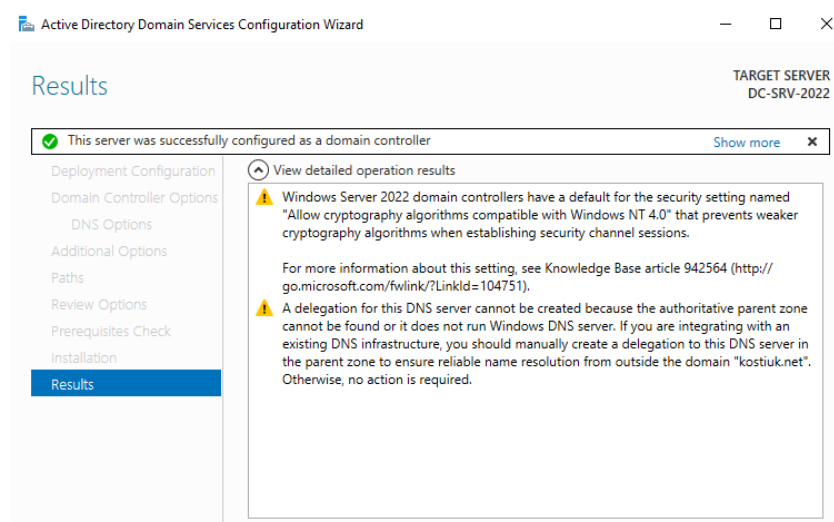


Рис. 2.25 - Успішна промоція сервера до контролера домену.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк. 64
		Росініський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Перевірка доступності служби та імен. Для підтвердження коректної роботи доменної служби було перевірено:

- доступність DNS-записів (kostiuk.net);
- відкриття оснастки **Active Directory Users and Computers** без помилок;
- наявність стандартних контейнерів (Users, Computers, Domain Controllers);
- доступність служб через мережу з інших ВМ (ping, nslookup по імені).

Таким чином, сервер DC-SRV-2022 успішно виконує роль єдиного контролера домену в інфраструктурі з назвою kostiuk.net, а також забезпечує розв'язання імен завдяки вбудованій службі DNS. Його розгортання стало основою для наступних етапів — створення організаційної структури, реалізації групових політик та підключення інших вузлів до домену.

2.3.2 Організація структури домену

Після розгортання служби Active Directory на сервері DC-SRV-2022, описаного в пункті 2.3.1, було організовано структуру домену kostiuk.net для ефективного управління об'єктами Active Directory. Створена ієрархія відображає ролі та підрозділи організації, яка імітується, і готує основу для застосування групових політик (GPO) та обмеження доступу в подальших етапах. Цей підпункт описує створення організаційних підрозділів (OU), розміщення користувачів і підготовку до групування комп'ютерів відповідно до їхніх ролей.

Створення організаційних підрозділів (OU). У консолі Active Directory Users and Computers (ADUC) на сервері DC-SRV-2022 було створено ієрархію OU, яка моделює організаційну структуру з філіями та підрозділами. На верхньому рівні домену kostiuk.net сформовано три основні підрозділи, що відповідають філіям: Branch-21-7-1, Branch-21-7-2 і Branch-21-7-3. У кожній філії створено по два підрозділи для користувачів (Dep-21-7-X-Y) та окремий OU для адміністраторів (Admins-21-7-X). Наприклад, для Branch-21-7-1 створено OU Dep-21-7-1-1, Dep-21-7-1-2 і Admins-21-7-1. Аналогічна структура застосована до Branch-21-7-2 і Branch-21-7-3, що забезпечило чітке розділення підрозділів і ролей.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

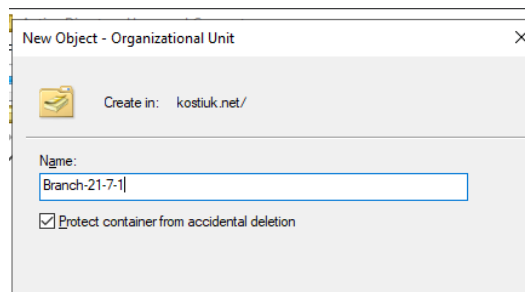


Рис. 2.26 – Приклад створення організаційної одиниці.

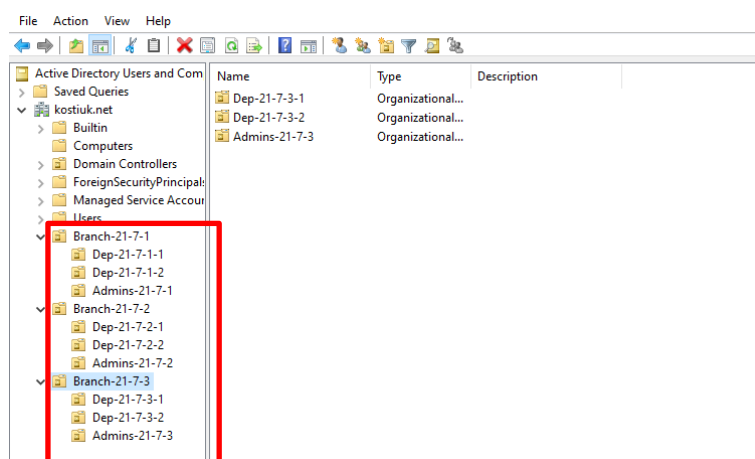


Рис. 2.27 – Фінальний результат створення структури ОУ.

Створення користувачів. Для імітації роботи організації в кожному ОУ, крім груп локальних адміністраторів, створено по три користувацькі облікові записи, що загалом становить 21 користувач. Користувачів розміщено відповідно до їхнього підрозділу чи ролі адміністратора, із зазначенням повного імені та логіну. Як приклад, у філії Branch-21-7-1 створено:

- Dep-21-7-1-1:
 - Іванов Андрій Петрович (dep11-iap);
 - Коваль Олексій Сергійович (dep11-kos);
 - Мельник Роман Іванович (dep11-mri).
- Dep-21-7-1-2:
 - Шевченко Дмитро Олегович (dep12-sdo);
 - Бондар Антон Юрійович (dep12-bay);
 - Сидоренко Артем Володимирович (dep12-sav).
- Admins-21-7-1:
 - Костюк Ігор Олександрович (b1-AdminKIO).

Повний список користувачів для всіх філій наведено в Додатку А.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

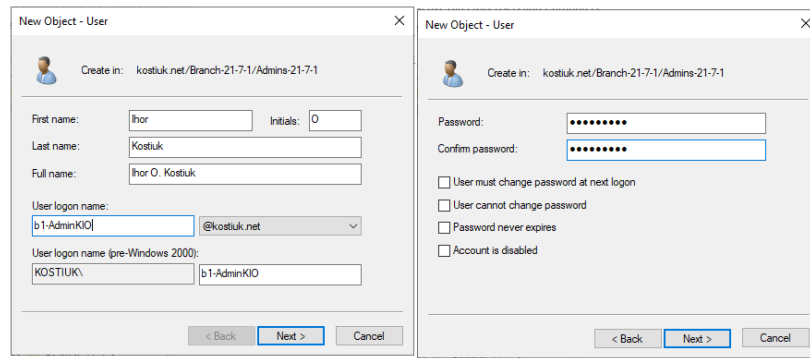


Рис. 2.28 – Приклад створення нового користувача.

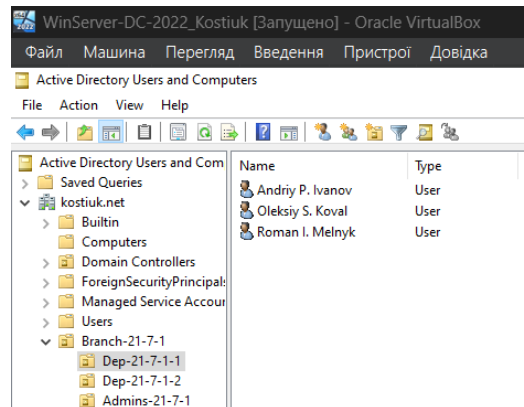


Рис. 2.29 – результат створення користувачів для OU Dep-21-7-1-1.

Групування об'єктів відповідно до ролей. Створена ієрархія OU забезпечує основу для групування об'єктів Active Directory відповідно до їхніх ролей. Користувачі розміщені в OU підрозділів і адміністраторів, що відповідає організаційній структурі.

Організація структури домену kostiuk.net із створенням ієрархії OU і розміщенням користувачів забезпечила основу для ефективного управління об'єктами Active Directory. Створена структура відповідає ролям і підрозділам організації та підготувала платформу для приєднання віртуальних машин до домену і подальшого налаштування політик.

2.3.3 Приєднання віртуальних машин до домену

Для забезпечення централізованого управління тестовими віртуальними машинами через Active Directory, було виконано приєднання WSUS-серверів (WSUS-PRIM-2019, WSUS-REPL-2019) і клієнтських машин (Win-10-1-KOST, Win-10-2-KOST, Win-11-1-KOST) до домену kostiuk.net. Цей підпункт описує

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

два методи приєднання, а також перевірку авторизації, що підготувало платформу для подальшого налаштування.

Приєднання WSUS-серверів та клієнтів до домену. Приєднання віртуальних машин до домену kostiuk.net може здійснюватись двома методами. Перший метод передбачав використання системних налаштувань Windows, де відкривалися властивості комп'ютера (System Properties → Computer Name → Change), вказувалося доменне ім'я kostiuk.net, а для автентифікації вводилися дані облікового запису адміністратора домену (kostiuk.net\Administrator) із відповідним паролем (рис. 2.30). Після успішного приєднання кожна машина перезавантажувалася для застосування змін. Другий метод використовував PowerShell, де виконувалася команда Add-Computer -DomainName kostiuk.net -Credential (Get-Credential) із введенням тих самих облікових даних адміністратора домену, після чого також проводилося перезавантаження (рис. 2.31). Цей процес застосовано до всіх віртуальних машин в мережі

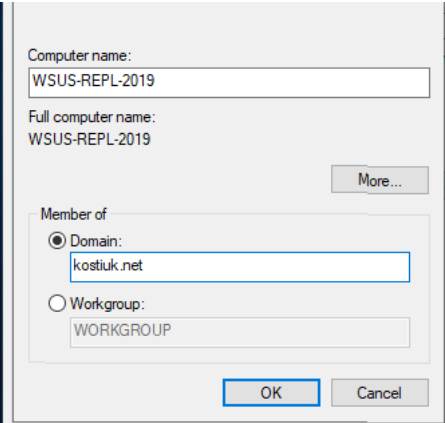


Рис. 2.30 - Приєднання VM до домену через системні налаштування.

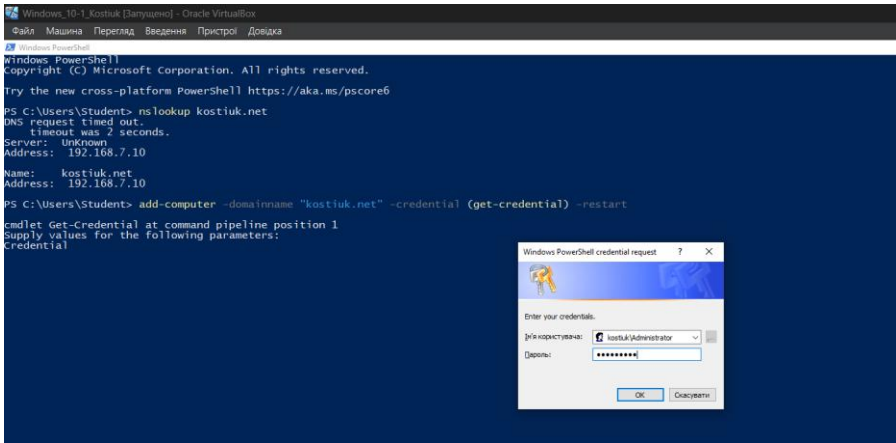


Рис. 2.31 - Приєднання VM до домену через PowerShell.

Перевірка успішної авторизації в AD. Для підтвердження коректності роботи Active Directory проведено перевірку авторизації на одній із клієнтських машин. На Win-10-1-KOST виконано із використанням облікового запису адміністратора домену (рис. 2.32), що підтвердило успішне приєднання до домену. Також для підтвердження успішного додавання всіх VM додомену, було перевірено відображення комп'ютерів у AD (рис. 2.33).

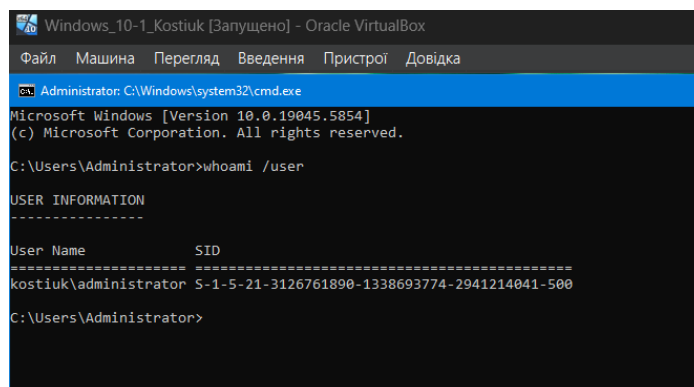


Рис. 2.32 - Підтвердження успішного входу в обліковий запис адміна домена.

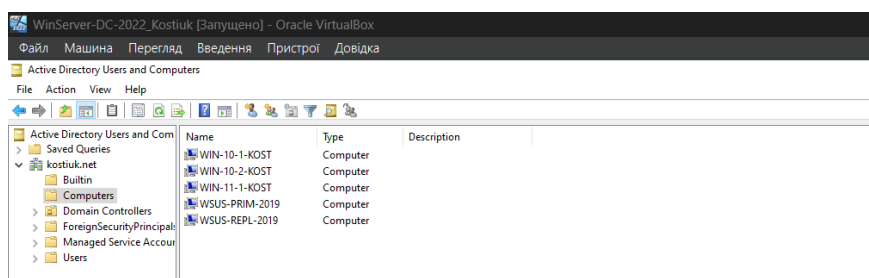


Рис. 2.33 - Відображення всіх комп'ютерів у AD.

Приєднання WSUS-серверів і клієнтських машин до домену kostiuk.net завершено з використанням системних налаштувань Windows і PowerShell, а перевірка авторизації підтвердила працездатність Active Directory. Ці дії підготували платформу для подальшого налаштування DHCP і DNS.

2.3.4 Налаштування ролей DHCP і DNS-серверів.

Для автоматизації розподілу IP-адрес клієнтським машинам і підтримки доменної інфраструктури після приєднання віртуальних машин до домену kostiuk.net, було налаштовано служби DHCP і DNS на сервері DC-SRV-2022. Цей підпункт описує встановлення ролі DHCP, створення діапазону адрес, а також

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

доповнення конфігурації DNS-сервера, що підготувало платформу для подільшого налаштування групових політик.

Встановлення ролі DHCP на DC-SRV-2022. На сервері DC-SRV-2022 через Server Manager було встановлено роль DHCP-сервера. Після завершення установки проведено базову конфігурацію, включаючи авторизацію DHCP-сервера в Active Directory для коректної роботи в домені.

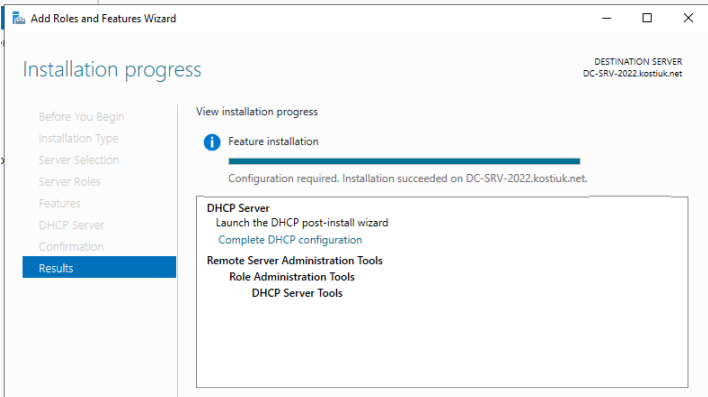


Рис. 2.34 – Успішне встановлення ролі DHCP на DC-SRV-2022.

Створення діапазону IP-адрес. У консолі DHCP Manager створено діапазон IP-адрес від 192.168.7.1 до 192.168.7.254 (рис. 2.35) для автоматичного розподілу клієнтським машинам. Налаштування включали маску підмережі 255.255.255.0 (див. рис. 2.35) і шлюз за замовчуванням 192.168.7.1 (рис. 2.37). Для уникнення конфліктів із статичними адресами серверів було виключено діапазон 192.168.7.1–192.168.7.99 (рис. 2.36), що охоплює адреси DC-SRV-2022 (192.168.7.10), WSUS-PRIM-2019 (192.168.7.21) і WSUS-REPL-2019 (192.168.7.22), а також резервую певну кількість адрес, для можливих потреб в майбутньому.

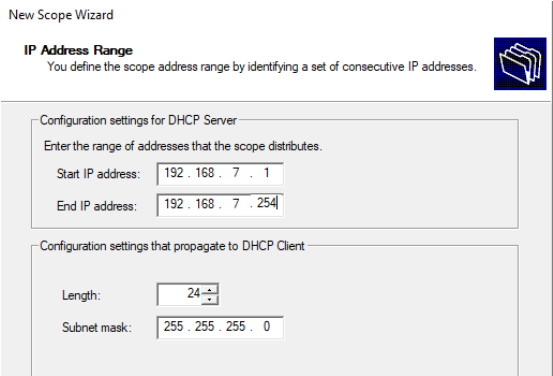


Рис. 2.35 - Створення діапазон IP-адрес для DHCP.

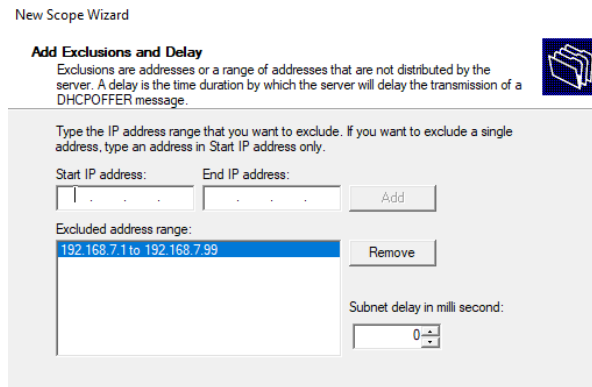


Рис. 2.36 – Виключення діапазону адрес із загального пулу.

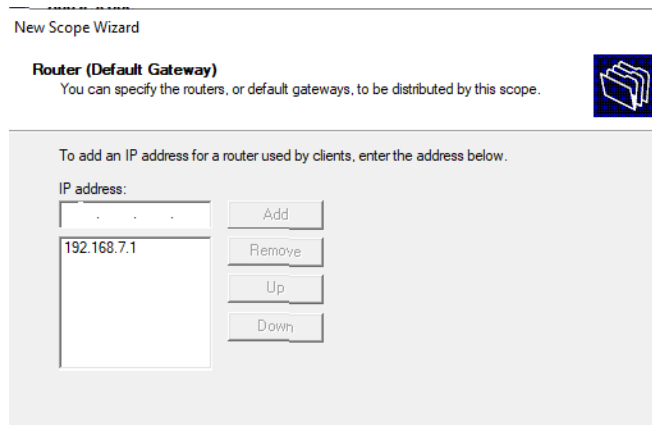


Рис. 2.37 - Налаштування шлюзу за замовчуванням.

Налаштування DNS-сервера. Для підтримки доменної інфраструктури на DC-SRV-2022 доповнено конфігурацію DNS-сервера, який було активовано під час промоції в пункті 2.3.1. У оснащенні DNS Manager перевірено відсутність зони зворотного перегляду, після чого створено зону для підмережі 192.168.7.0/24 (рис. 2.38). Далі командний рядок запущено реєстрацію DNS-записів основних ресурсів (рис. 2.39).

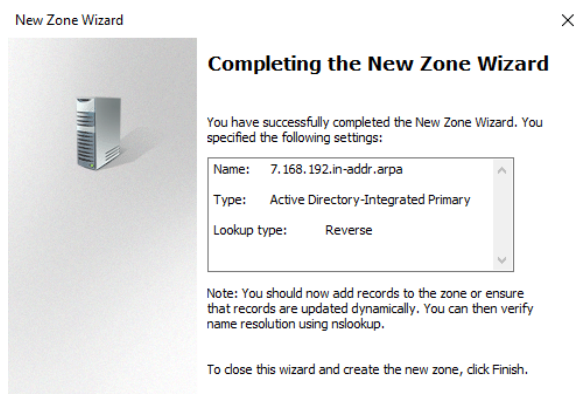


Рис. 2.38 – Створення нової зони зворотнього перегляду.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк. 71
		Росініський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		

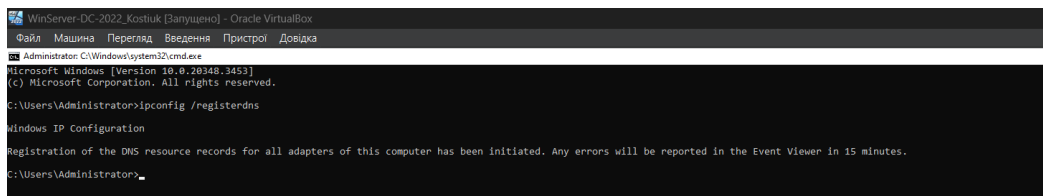


Рис. 2.39 – Виконання руєстрації DNS-записів основних ресурсів.

Перевірка функціональності. Для підтвердження коректності роботи DHCP і DNS виконано перевірку на клієнтській машині Win-10-1-KOST. Команда `ipconfig /all` підтвердила успішне отримання IP-адреси з діапазону 192.168.7.100–192.168.7.200 (рис. 2.40). Також через контролер домену було перевірено всі зарезервовані адреси (рис. 2.41). Крім того, команда `nslookup kostiuk.net` засвідчила коректність роботи DNS, повернувши IP-адресу 192.168.7.10 (рис. 2.42).

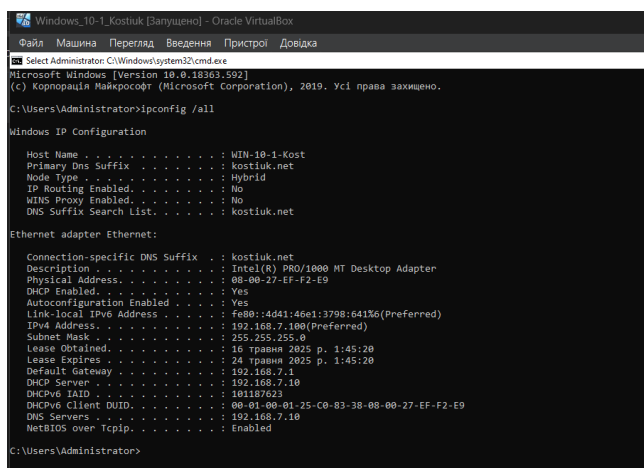


Рис. 2.40 – Перевірка динамічного отримання IP-адреси

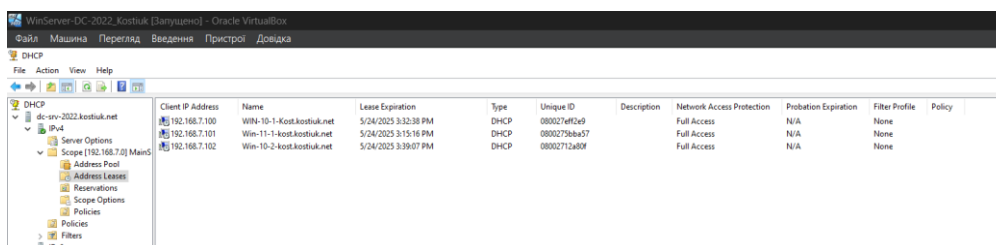


Рис. 2.41 – Перегляд списку зарезервовани IP-адрес.

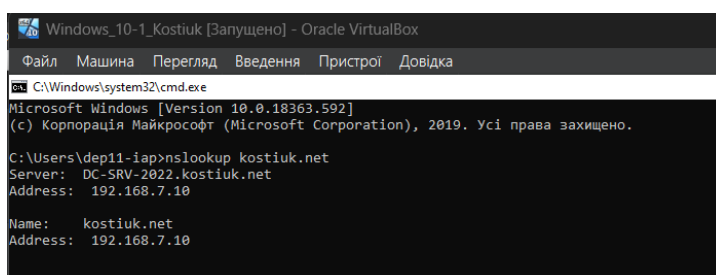


Рис. 2.42 – Виконання команди `nslookup` для перевірки налаштувань.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк. 72
		Росініський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування служб DHCP і DNS на сервері DC-SRV-2022 забезпечило автоматичний розподіл IP-адрес для клієнтських машин і підтримку доменної інфраструктури. Створений діапазон адрес і конфігурація DNS підготували платформу для подальшого налаштування групових політик.

2.3.5 Налаштування базових групових політик (GPO)

Після завершення базової мережевої конфігурації домену kostiuk.net, включаючи створення структури OU, приєднання машин та налаштування служб DHCP/DNS, наступним етапом стало впровадження групових політик (GPO). Вони дозволяють реалізувати єдині правила для безпеки, доступу та конфігурації систем на рівні організації. У цьому підпункті описано реалізацію GPO для клієнтських машин, серверів та доступу до мережевих ресурсів.

Політики для клієнтів. На сервері DC-SRV-2022 через консоль Group Policy Management створено GPO під назвою PasswordPolicy-Branch-1 для клієнтських машин у філії Branch-21-7-1. У цій політиці встановлено вимогу мінімальної довжини пароля 10 символів (рис. 2.43). Додатково до всього домену через Default Domain Policy було налаштовано ліміт спроб входу для запобігання несанкціонованого доступу та можливість розблокування облікових записів лише адміністратором (рис. 2.44), що забезпечило єдині стандарти для всіх користувачів.

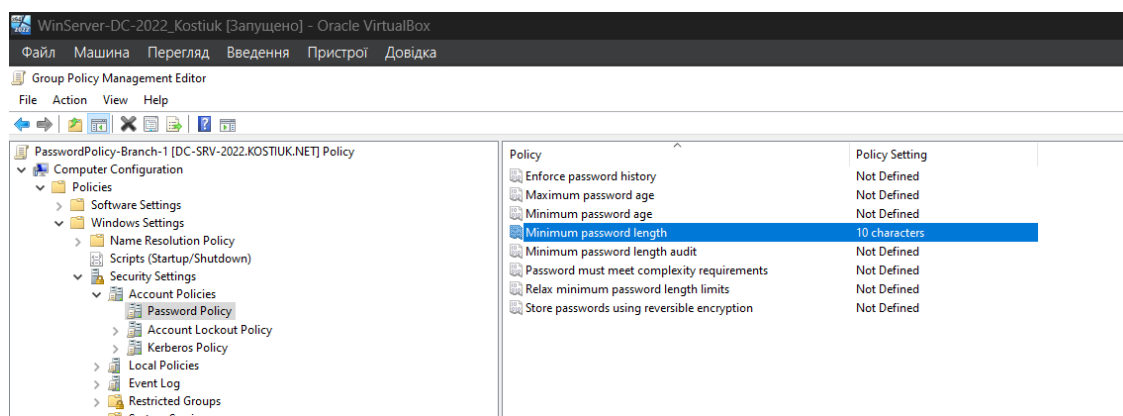


Рис. 2.43 – Встановлення вимоги мінімальної довжини пароля Branch-21-7-1.

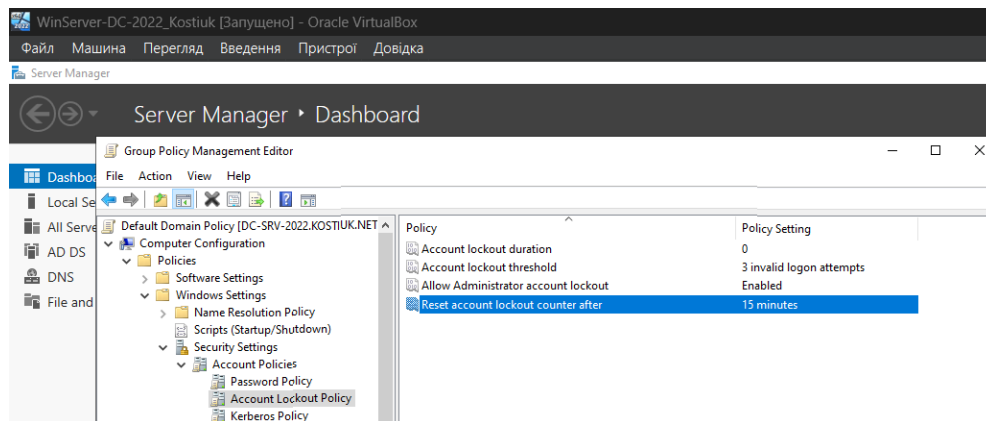


Рис. 2.44 - Налаштовання ліміту спробу входу.

Налаштування мережевих дисків. Перед налаштуванням мережевих дисків було створено групи локальних адміністраторів для OU Admins-21-7-X (наприклад, LocalAdmins-21-7-1 для Admins-21-7-1) (рис. 2.45) і налаштовано делегування для кожної філії Branch-21-7-X (рис. 2.46), що дозволило адміністраторам цих OU керувати відповідними підрозділами. Далі створено дві GPO для підключення мережевих дисків: MapDrive-Admin, яка забезпечує доступ до папок лише для локальних адміністраторів із відповідними правами, і MapDrive-ALL, яка надає доступ до іншої папки для всіх користувачів. Обидві політики налаштовано з урахуванням різного рівня прав доступу до папок.

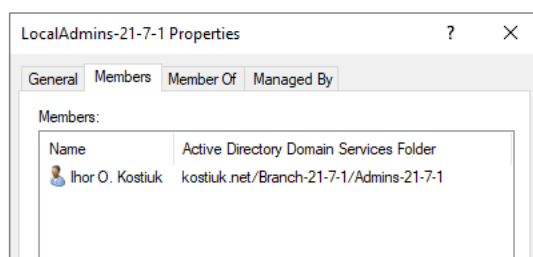


Рис. 2.45 – Перевірка наявності облікового запису в новоствореній групі.

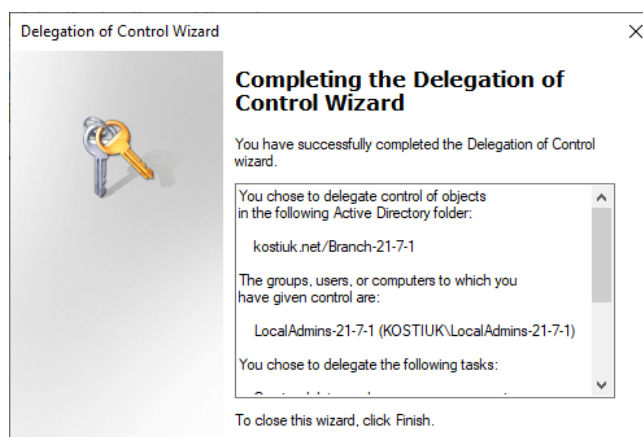


Рис. 2.46 – Налаштування делегування для філії Branch-21-7-1.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

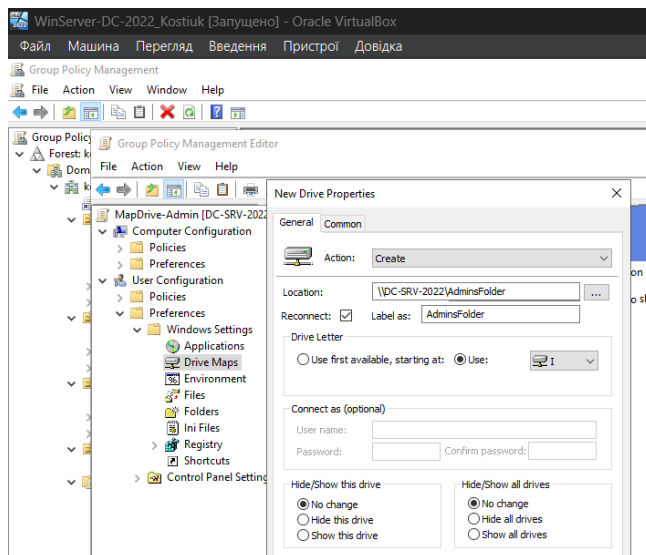


Рис. 2.47 – Налаштування мережевого диску для адміністраторів.

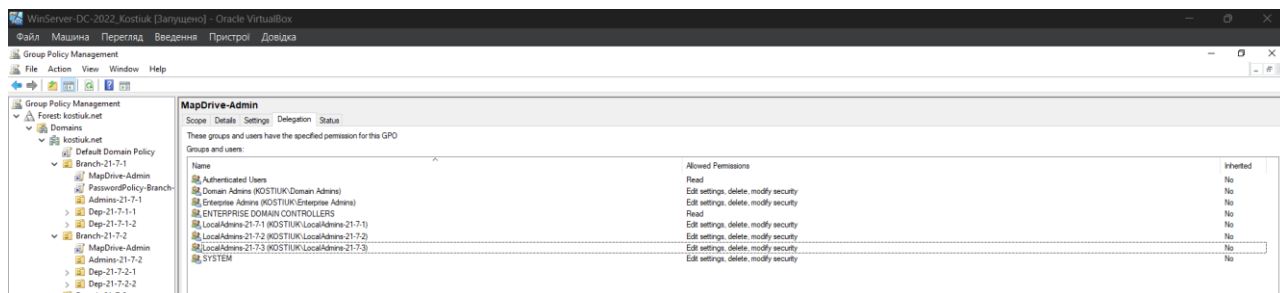


Рис. 2.48 – Налаштування прав доступу до мережевого диску.

Політики для серверів. Для серверів (DC-SRV-2022, WSUS-PRIM-2019, WSUS-REPL-2019) створено окрему GPO, яка включає базові налаштування. У цій політиці дозволено локальний вхід членам групи локальних адміністраторів на контролерах домену, зокрема на DC-SRV-2022.

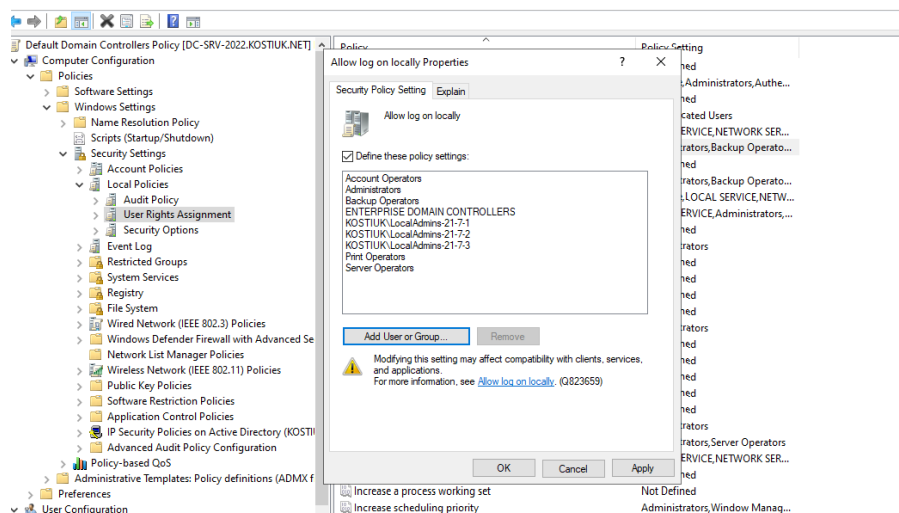


Рис. 2.49 – Дозвіл входу членам груп локальних адміністраторів.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

Прив'язка політик до відповідних OU. Політика PasswordPolicy-Branch-1 прив'язана до OU Branch-21-7-1, що забезпечило її застосування до клієнтських машин у цій філії. GPO для серверів прив'язана до створеного OU Servers, де в подальшому будуть розміщені DC-SRV-2022 та WSUS-сервери (WSUS-PRIM-2019, WSUS-REPL-2019). Політики MapDrive-Admin і MapDrive-ALL прив'язані до всіх філій (Branch-21-7-1, Branch-21-7-2, Branch-21-7-3), що забезпечило доступ до мережеских дисків для відповідних груп користувачів.

Перевірка застосування політик. Після створення та прив'язки групових політик було виконано базову перевірку їхнього застосування на клієнтській машині Win-10-1-KOST. Для цього здійснено примусове оновлення параметрів командою `groupdate /force` та перевірено локальні налаштування безпеки. Політика PasswordPolicy-Branch-1 була застосована коректно — відображено зміну вимог до пароля та обмеження кількості спроб входу.

Детальні результати перевірки ефективності GPO будуть подані в розділі 4, присвяченому тестуванню системи.

Налаштування базових групових політик у домені kostiuk.net забезпечило єдині стандарти безпеки, доступ до мережеских ресурсів і централізоване керування часом для серверів. Ці дії завершили конфігурацію доменної інфраструктури, розпочату в пункті 2.3, і підготували платформу для подальшого розгортання служб.

2.4. Встановлення та початкові налаштування WSUS

2.4.1 Встановлення Microsoft SQL Server на сервер WSUS-PRIM-2019

Для забезпечення роботи WSUS-сервера на WSUS-PRIM-2019 було необхідно розгорнути інфраструктуру бази даних. З цією метою на сервер встановлено Microsoft SQL Server 2019 Standard, який забезпечує гнучкість у зберіганні, адмініструванні та обробці великого обсягу метаданих оновлень. Цей підпункт описує процес інсталяції SQL Server і його початкову конфігурацію для подальшої інтеграції з WSUS.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

Встановлення SQL Server. На сервері WSUS-PRIM-2019 інсталяція SQL Server 2019 була виконана за допомогою офіційного дистрибутива, завантаженого з сайту Microsoft. У процесі інсталяції обрано такі компоненти:

- **Database Engine Services** – ядро серверної частини бази даних;
- **Client Tools Connectivity** – забезпечує підключення до SQL Server;
- **Client Tools Backwards Compatibility** – надає сумісність із попередніми версіями клієнтських інструментів.

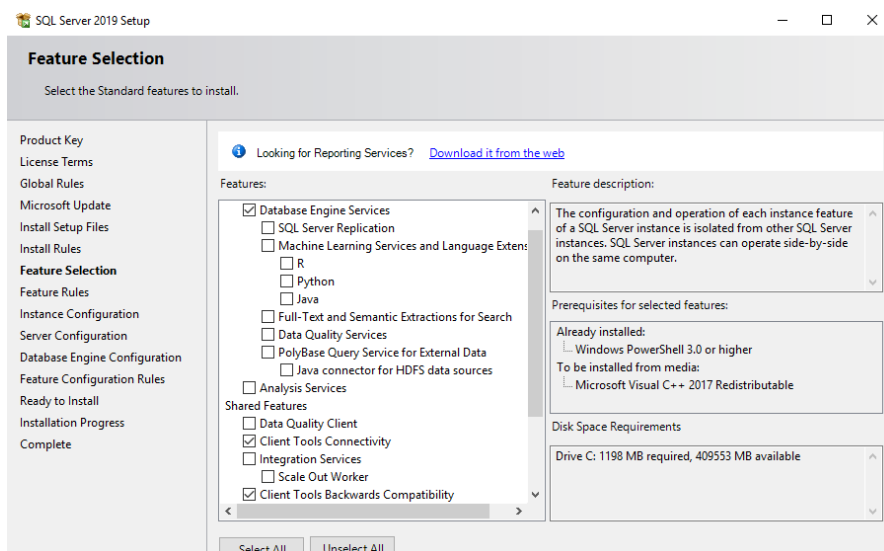


Рис. 2.50 – Вибір компонентів для встановлення.

Інсталяцію виконано для стандартного інстансу MSSQLSERVER (рис. 2.51) у режимі автентифікації Mixed Mode (рис. 2.52), який дозволяє вхід як через Windows-облікові записи, так і за допомогою логіна sa. Для облікового запису sa задано складний пароль (див. рис. 2.52). Додатково було включено доменний обліковий запис kostiuk\Administrator (див. рис. 2.52).

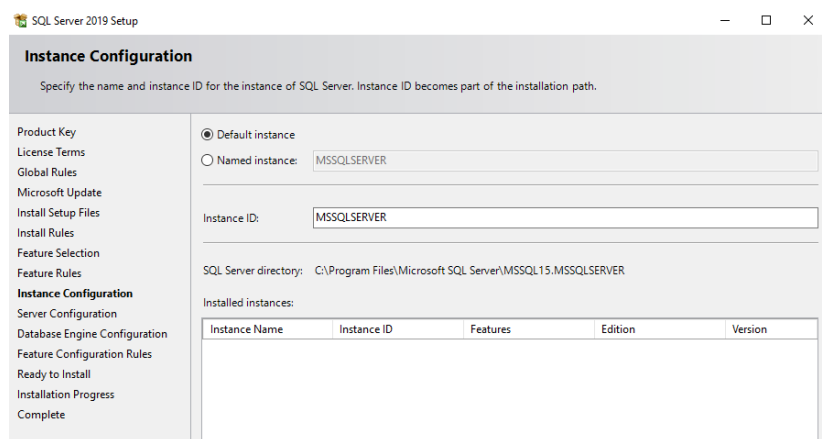


Рис. 2.51– Використання стандартного інстансу MSSQLSERVER.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		
						77

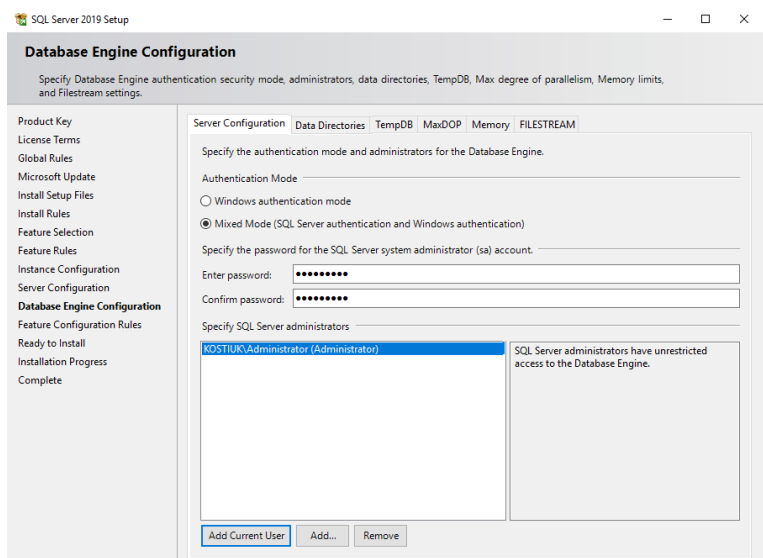


Рис. 2.52 – Встановлення паролю та додавання доменного облікового запису.

Конфігурація шляхів. Для підвищення продуктивності та ізоляції даних від системного диска було налаштовано збереження файлів бази даних на диску **I:**, який в подальшому також буде місцем зберігання оновлень. У відповідному розділі налаштувань встановлено такі каталоги:

- I:\SQLData - **Data root directory**
- I:\SQLData\MSSQL15.MSSQLSERVER\MSSQL\Data - **System database directory**
- I:\SQLData\MSSQL15.MSSQLSERVER\MSSQL\Data - **User database directory**
- I:\SQLData\MSSQL15.MSSQLSERVER\MSSQL\Data - **User database log directory**
- I:\SQLData\MSSQL15.MSSQLSERVER\MSSQL\Backup - **Backup directory**

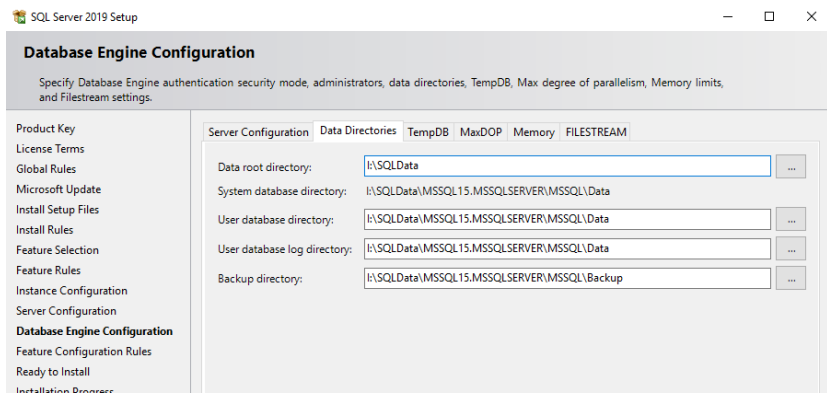


Рис. 2.53 – Вибір каталогів для подальшого зберігання файлів бази даних

Це забезпечує централізоване зберігання даних, логів і резервних копій, що відповідає вимогам до надійного управління оновленнями у корпоративному середовищі.

Встановлення SQL Server 2019 із відповідними шляхами зберігання даних, налаштуванням автентифікації та призначенням адміністраторів підготувало надійну основу для подальшої роботи WSUS. Ця конфігурація забезпечує масштабованість, централізоване керування та відповідність практикам корпоративного розгортання.

2.4.2 Інсталяція ролі WSUS та підключення до SQL Server.

Після встановлення SQL Server 2019 на сервері Групова політика (GPO) дозволяє централізовано керувати параметрами оновлень, описаного в пункті 2.4.1, було виконано розгортання ролі Windows Server Update Services (WSUS) з прив'язкою до попередньо створеної бази даних на SQL Server. Це дозволило уникнути обмежень Windows Internal Database (WID) і забезпечити масштабованість для роботи з великою кількістю клієнтських пристроїв у домені kostiuk.net. Цей підпункт описує процес установки ролі WSUS та її інтеграції з SQL Server.

Встановлення ролі WSUS. На сервері WSUS-PRIM-2019 через Server Manager було розпочато встановлення ролі WSUS (рис. 2.55), де на етапі Role Services було обрано компоненти «WSUS Services» і «SQL Server Connectivity» для інтеграції з SQL Server (рис. 2.56). Перед інсталяцією було перевірено доступність служби SQL Server, наявність адміністративного доступу доменного користувача та достатній обсяг вільного місця на диску I:. Для зберігання оновлень визначено кастомний шлях I:\WSUSUpdates (рис. 2.57), де диск I: попередньо створено як окремий том для оптимізації простору та зменшення інтернет-трафіку під час доставки оновлень клієнтам (рис. 2.54).

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

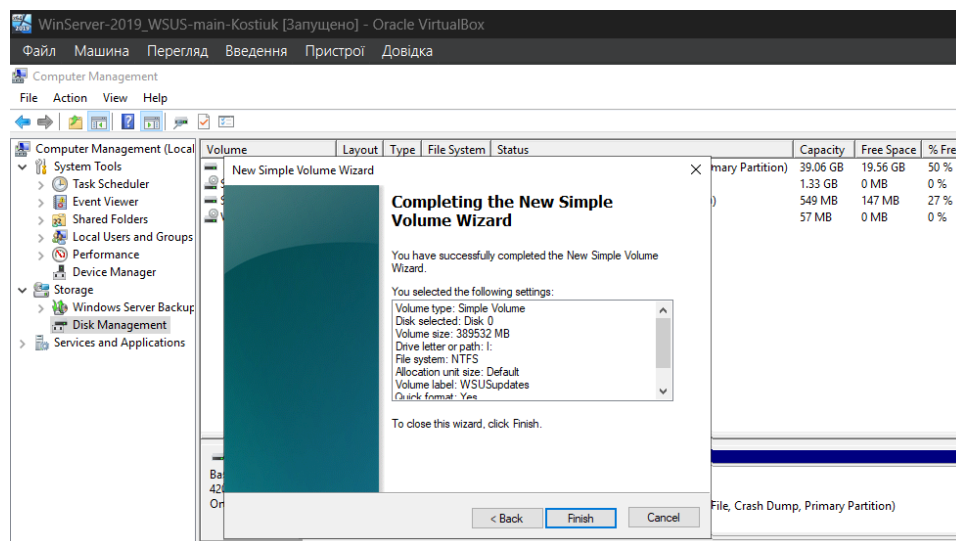


Рис. 2.54 – Створення нового тому для зберігання оновлень.

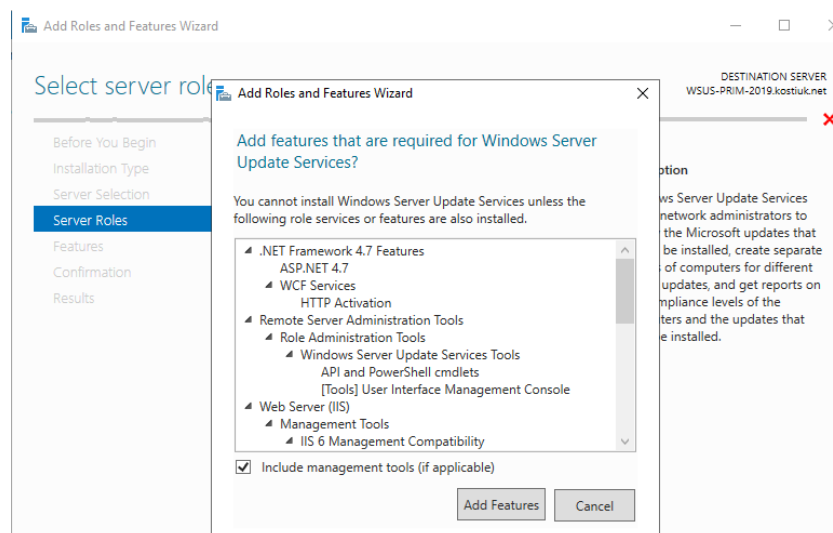


Рис. 2.55 – Вибір ролі WSUS для встановлення.

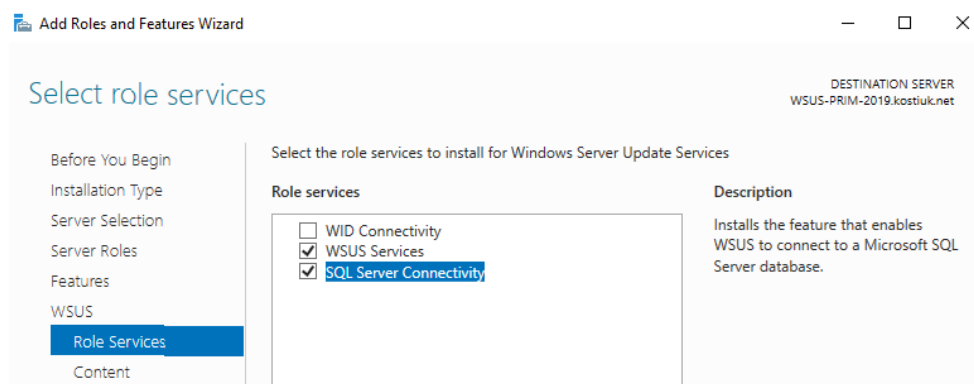


Рис. 2.56 – Вибір компонентів WSUS Services і SQL Server Connectivity.

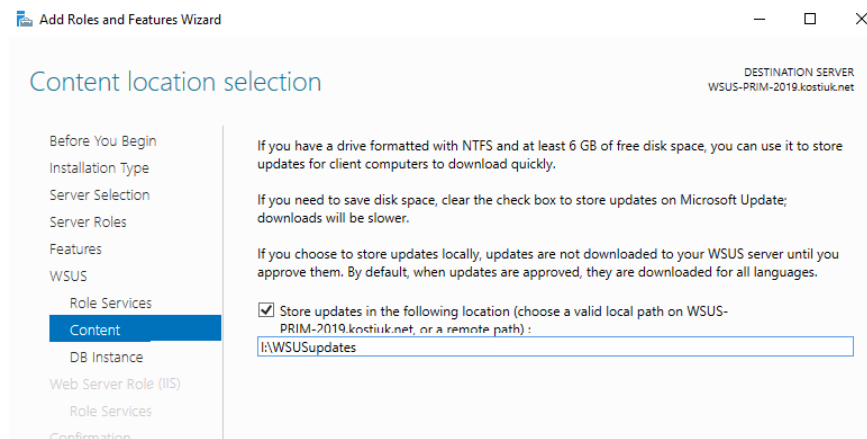


Рис. 2.57 – Введення кастомного шляху I:\WSUSUpdates для зберігання оновлень.

Прив'язка WSUS до SQL Server. У процесі установки було виконано підключення до екземпляра SQL Server на тому ж сервері (WSUS-PRIM-2019) за IP-адресою 192.168.7.20, де використано стандартний (default) інстанс MSSQLSERVER. У майстрі вказано підключення до екземпляра SQL Server за IP-адресою 192.168.7.20, після чого натиснуто "Check Connection", що підтвердило успішне з'єднання з використанням доменного облікового запису kostiuk\Administrator (рис. 2.58). У результаті інсталяції WSUS створює базу даних SUSDB у вказаному екземплярі SQL Server. У цій базі зберігаються метадані оновлень, політики схвалення, а також статуси клієнтів і звіти.

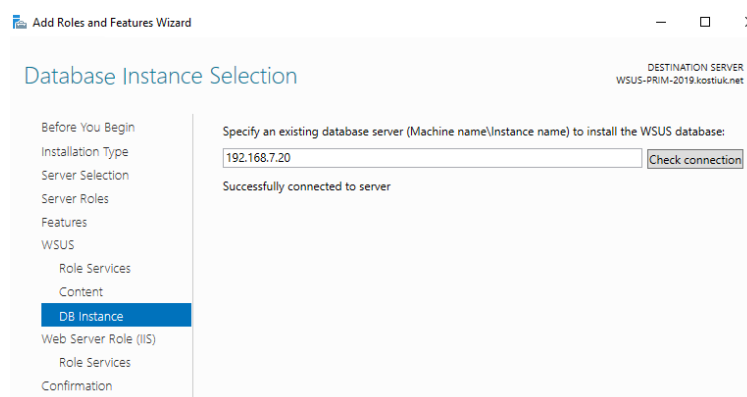


Рис. 2.58 – Підключення до екземпляра SQL Server за IP-адресою.

Перевірка доступності та готовності WSUS. Після завершення інсталяції відкрито консоль керування Windows Server Update Services, що підтвердило успішну ініціалізацію служби та коректне підключення до SQL Server (рис. 2.59).

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк. 81
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		

Перевірка бази даних SUSDB через SQL Server Management Studio додатково засвідчила її створення та готовність до використання.



Рис. 2.59 – Відкриття консолі керування Windows Server Update Services.

Інсталяція ролі WSUS на WSUS-PRIM-2019 із прив’язкою до SQL Server забезпечила необхідну інфраструктуру для управління оновленнями в домені. Ці дії стали основою для початкового налаштування WSUS у наступному пункті.

2.4.3 Початкове налаштування WSUS

Після встановлення ролі WSUS на сервері WSUS-PRIM-2019 було виконано її початкове налаштування для підготовки до розповсюдження оновлень у домені kostiuk.net. Цей підпункт описує вибір джерела оновлень, налаштування синхронізації, вибір продуктів, класифікацій і мов, а також деталі процесу синхронізації.

Вибір джерела оновлень. Для забезпечення актуальності оновлень WSUS-PRIM-2019 налаштовано на синхронізацію напряму з Microsoft Update. Використання проксі-сервера не передбачалося, що спростило процес налаштування.

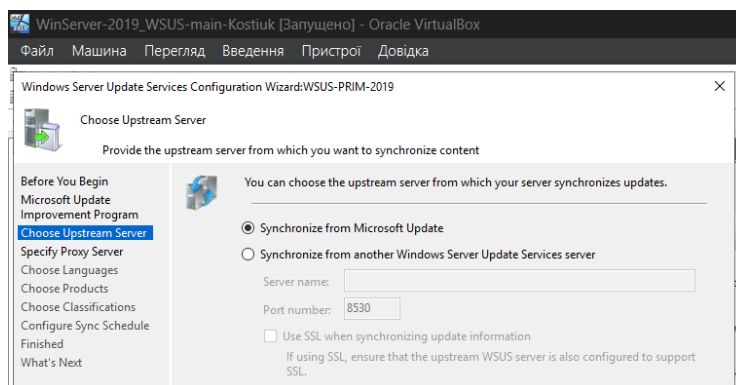


Рис. 2.60 – Налаштування синхронізації напряму з Microsoft Update.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування синхронізації. У консолі WSUS обрано ручну синхронізацію, що дозволило контролювати процес оновлення метаданих. WSUS налаштовано таким чином, що спочатку завантажуються лише метадані оновлень, а двійкові файли завантажуються лише після затвердження конкретного пакета. Етап початкової конфігурації тривав близько 15 хвилин до вибору мови, після чого розпочалася перша синхронізація.

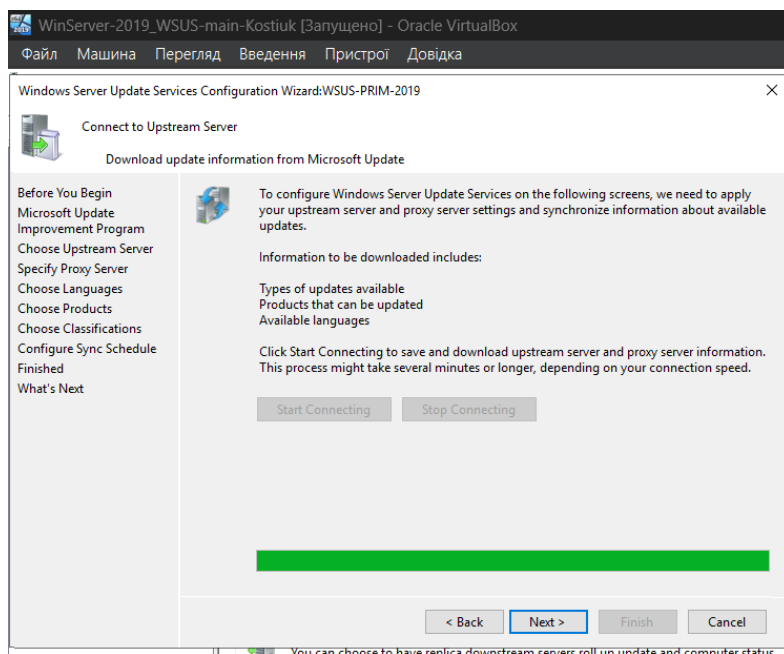


Рис. 2.61 – Проведення синхронізації.

Вибір продуктів, класифікацій і мов. У налаштуваннях WSUS визначено перелік продуктів, для яких завантажуватимуться оновлення. Спочатку обрано Windows 10, Windows 11, Windows Server 2019 і Windows Server 2019 and later, Upgrade & Servicing Drivers, після чого виконано першу синхронізацію. Згодом додано решту продуктів, у результаті чого загальна кількість оновлень перевищила 5000. Повний перелік продуктів включав:

- Windows 10
- Windows 10, version 1903 and later
- Windows 10 GDR-DU FOD
- Windows 10 Dynamic Update
- Windows 10 Feature on Demand
- Windows 11
- Windows Server 2019

- Windows Server 2019 and later, Servicing Drivers
- Windows Server 2019 and later, Upgrade & Servicing Drivers

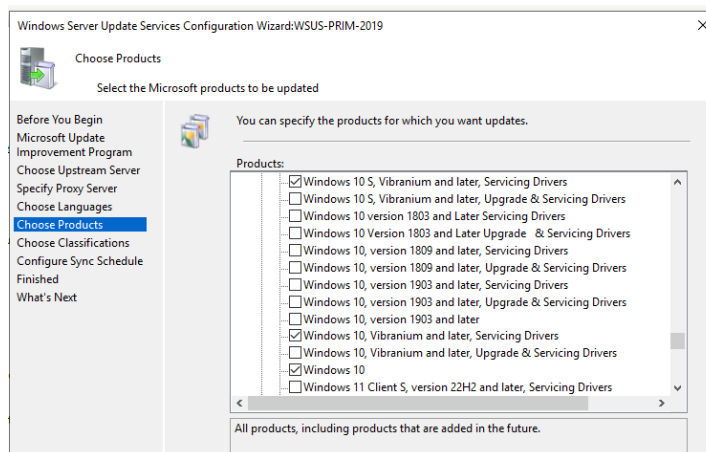


Рис. 2.62 – Приклад вибору продуктів для оновлень.

Як мову оновлень обрано лише англійську. Для класифікацій оновлень було вибрано ключові категорії, які охоплюють критичні оновлення, визначення безпеки, оновлення компонентів і переходи між версіями. Перелік включав:

- Critical Updates
- Definition Updates
- Security Updates
- Updates
- Upgrades

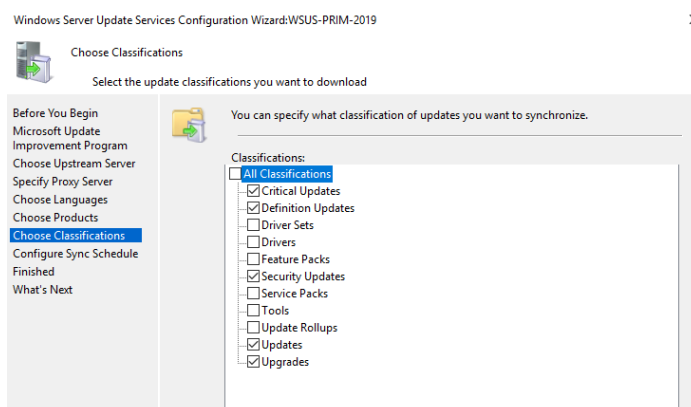
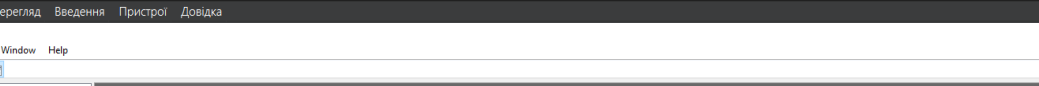


Рис. 2.63 – Приклад вибору класифікацій оновлень.

Перше з'єднання та деталі синхронізації. Після вибору початкового переліку продуктів (Windows 10, Windows 11, Windows Server 2019 і Windows Server 2019 and later, Upgrade & Servicing Drivers) одразу запущено першу синхронізацію з Microsoft Update. Цей процес тривав близько 9 годин і завершився

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				84
Змн.	Арк.	№ докум.	Підпис	Дата		



WinServer-2019_WSUS-main-Kostiuk (Запущено) - Oracle VM VirtualBox

Файл Машина Перегляд Введення Пристрої Довідка

Update Services

File Action View Window Help

Update Services

WSUS-PRIM-2019

Updates

Computers

All Computers

Downstream Servers

Synchronizations

Reports

Options

Synchronizations (15 synchronizations)

Started	Finished	Type	Result	New Updates	Revised Updates	Expired Updates
Started	Finished	Type	Result	New Updates	Revised Updates	Expired Updates
5/25/2025 9:30 AM	5/25/2025 9:30 AM	Manual	Succeeded	0	0	0
5/25/2025 9:27 AM	5/25/2025 9:29 AM	Manual	Succeeded	18	0	0
5/25/2025 8:17 AM	5/25/2025 8:17 AM	Manual	Succeeded	0	0	0
5/22/2025 4:48 PM	5/22/2025 5:44 PM	Manual	Succeeded	3,404	0	0
5/22/2025 4:27 PM	5/22/2025 4:34 PM	Manual	Succeeded	0	0	0
5/22/2025 4:21 PM	5/22/2025 4:25 PM	Manual	Succeeded	0	0	0
5/22/2025 4:10 PM	5/22/2025 4:21 PM	Manual	Succeeded	0	0	0
5/22/2025 4:07 PM	5/22/2025 4:07 PM	Manual	Succeeded	0	0	0
5/18/2025 2:59 PM	5/18/2025 5:06 PM	Manual	Succeeded	1,717	0	0
5/18/2025 2:38 PM	5/18/2025 2:38 PM	Manual	Succeeded	0	0	0
5/17/2025 11:30 PM	5/17/2025 11:29 PM	Manual	Succeeded	0	0	0

[illegible]

2.4.4 Налаштування GPO для WSUS

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росинський Ю.М.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

описує створення, налаштування та застосування GPO для серверів і робочих станцій, а також перевірку їхньої коректності.

Призначення групових політик. Для інтеграції клієнтів із WSUS-сервером створено дві окремі групові політики, враховуючи специфіку оновлення різних типів пристроїв. Сервери потребують контрольованого встановлення оновлень, щоб уникнути неочікуваних перезапусків критичних служб, таких як контролер домену чи сам WSUS. Натомість робочі станції можуть автоматично застосовувати оновлення в неробочий час для зручності користувачів.

Створення GPO для WSUS. Створення групових політик виконано через Group Policy Management на контролері домену DC-SRV-2022. Для організаційної одиниці "Servers", що включає контролер домену та WSUS-сервери, створено групову політику "WSUS_Servers_Policy" із такими параметрами:

- Specify intranet Microsoft update service location: <http://wsus.kostiuk.net:8530> (як джерело оновлень і статистичний сервер) (рис. 2.66).
- Configure Automatic Updates: режим 3 — автоматичне завантаження з повідомленням про встановлення (рис. 2.67).
- Scheduled install day/time: щоденно о 00:00 (див. рис. 2.67).
- Enable client-side targeting: група "Servers" для сортування в консолі WSUS (рис. 2.68).

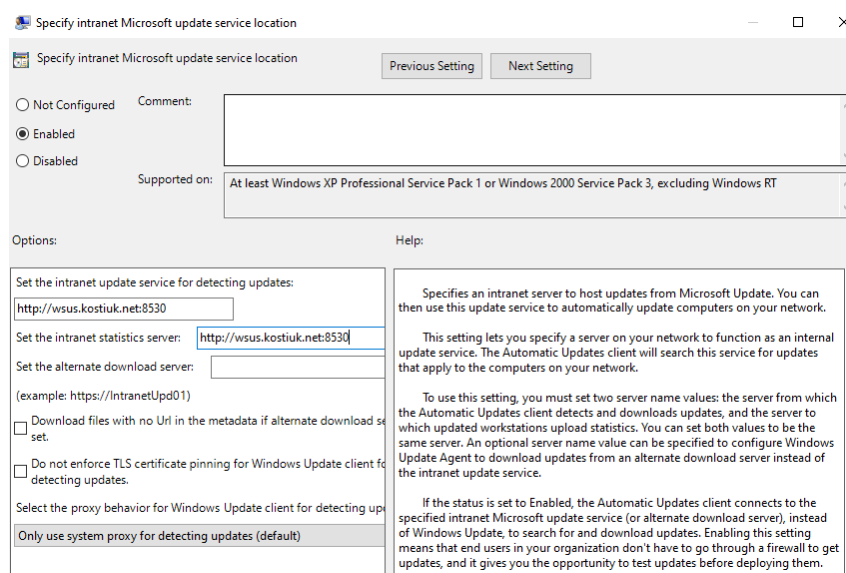


Рис. 2.66 – Введення джерела оновлень.

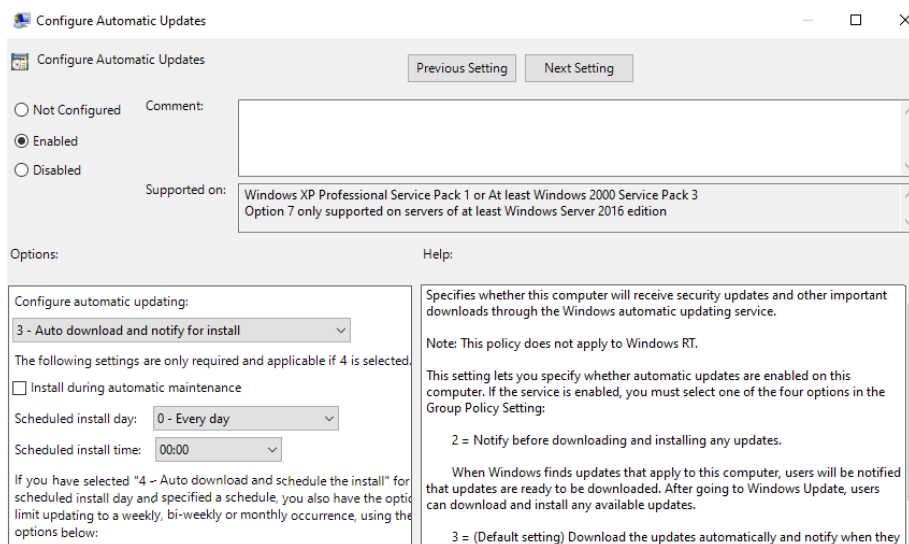


Рис. 2.67 – Вибір режиму автоматизації оновлень та планування застосування.

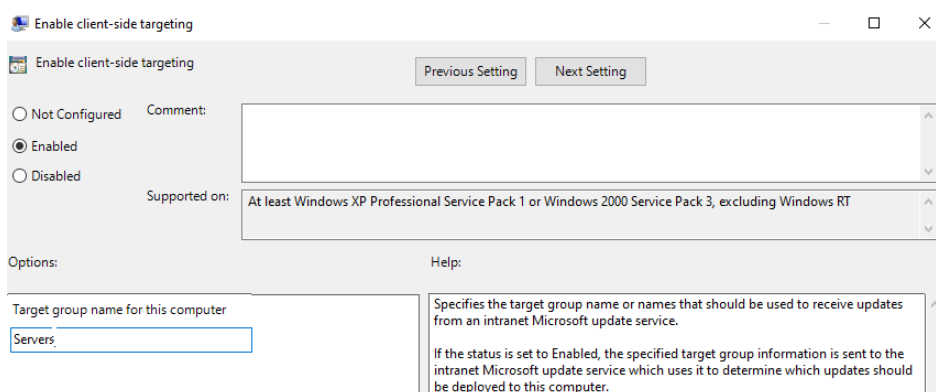


Рис. 2.68 – Вибір групи для сортування.

Для організаційної одиниці "Workstations", яка містить робочі станції, створено групову політику "WSUS_Workstations_Policy" із такими налаштуваннями:

- Specify intranet Microsoft update service location: <http://wsus.kostiuk.net:8530> (як джерело оновлень і статистичний сервер) (див. рис. 2.66).
- Configure Automatic Updates: режим 4 — автоматичне завантаження та встановлення (рис. 2.69).
- Scheduled install day/time: щоденно о 23:00 (див. рис. 2.69).
- Always automatically restart at the scheduled time: перезапуск через 15 хвилин (рис. 2.70).
- Enable client-side targeting: група "Workstations" для сортування в консолі WSUS (рис. 2.71).

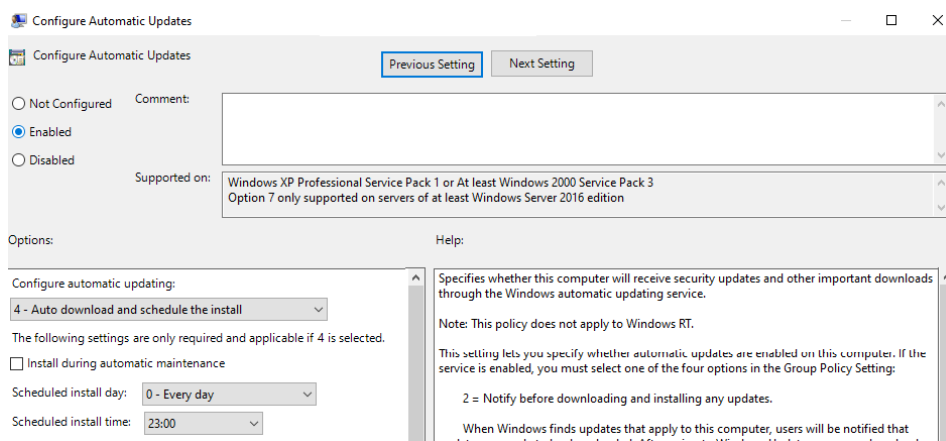


Рис. 2.69 - Вибір режиму автоматизації оновлень та планування застосування.

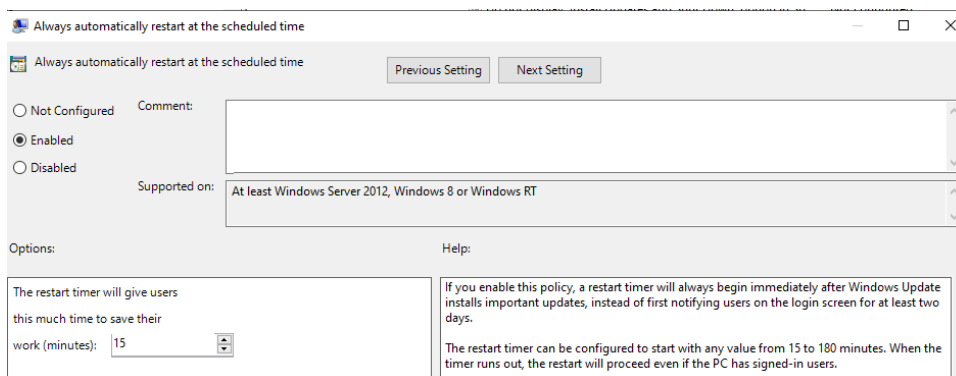


Рис. 2.70 – Встановлення примусового перезавпуску після встановлення оновлень.

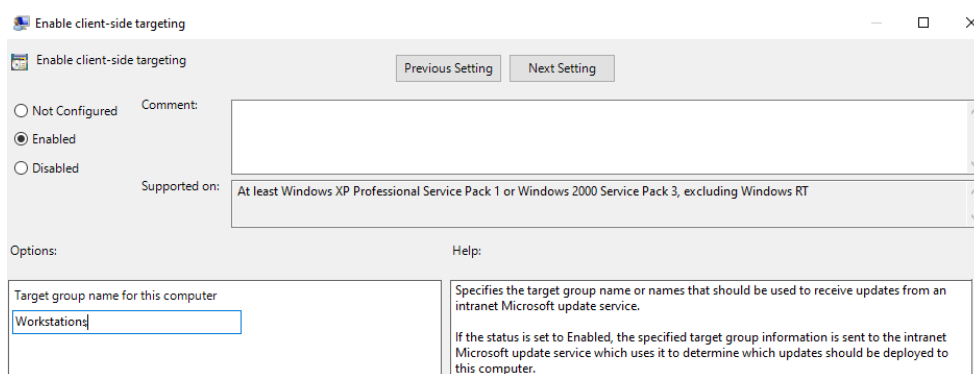


Рис. 2.71 - Вибір групи для сортування.

Ці налаштування забезпечили гнучке управління оновленнями відповідно до ролі пристроїв у домені.

Прив'язка GPO до OU. Створені групові політики прив'язано до відповідних організаційних одиниць: "WSUS_Servers_Policy" до OU "Servers", а "WSUS_Workstations_Policy" до OU "Workstations". Це забезпечило застосування налаштувань до всіх серверів і робочих станцій у домені.

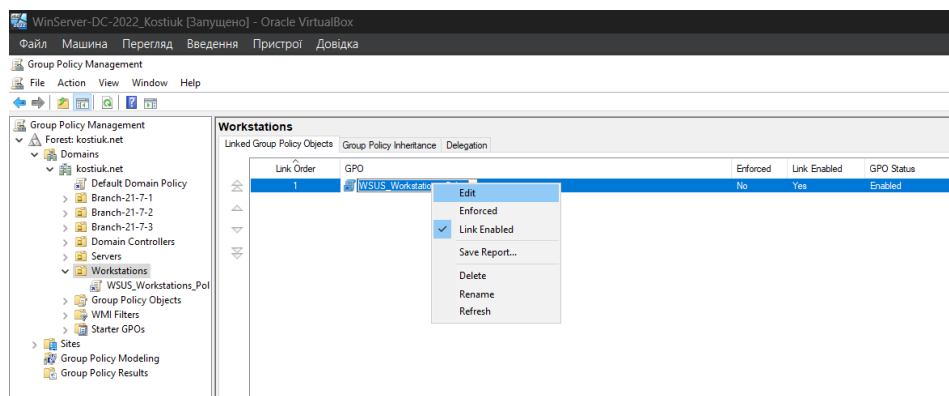


Рис. 2.72 – Перевірка прив'язки GPO до організаційної одиниці.

Перевірка застосування GPO. Для підтвердження коректності налаштувань дочекалися, поки віртуальні машини завершили перевірку оновлень і відправили звіт до WSUS-сервера. У консолі WSUS успішно відображено реєстрацію всіх клієнтів, що свідчить про правильне застосування групових політик.

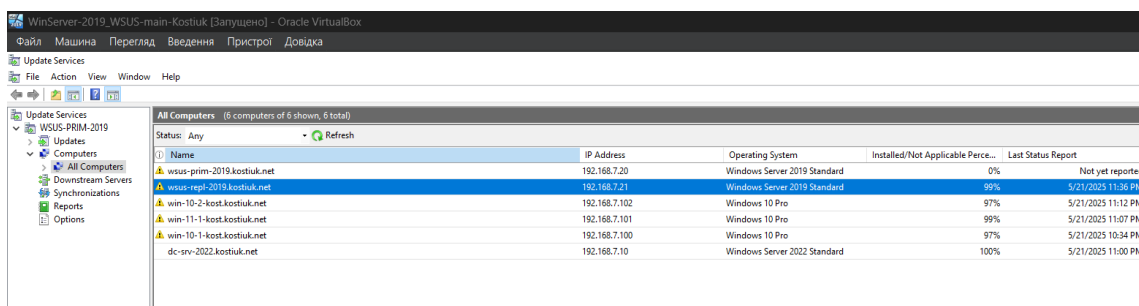


Рис. 2.73 – Перевірка відображення реєстрації всіх клієнтів в мережі.

Налаштування групових політик для WSUS на сервері WSUS-PRIM-2019 завершило підготовку інфраструктури для централізованого управління оновленнями в домені kostiuk.net. GPO "WSUS_Servers_Policy" забезпечила контрольований процес оновлення серверів, тоді як GPO "WSUS_Workstations_Policy" автоматизувала оновлення робочих станцій із мінімальним впливом на користувачів.

2.5 Налаштування TLS/SSL та HTTPS-з'єднання для WSUS

Після налаштування групових політик для WSUS, було налаштовано HTTPS-з'єднання на сервері WSUS-PRIM-2019 із використанням TLS-сертифі-

ката для забезпечення безпечного зв'язку з клієнтами у домені kostiuk.net. Перехід на HTTPS є обов'язковим у виробничих середовищах, особливо з 2022 року, відповідно до рекомендацій Microsoft, щоб гарантувати захист даних під час передачі оновлень. Цей пункт описує генерацію, експорт, імпорт сертифіката, налаштування IIS, розгортання на клієнтах, оновлення GPO та перевірку зв'язку.

Генерація TLS-сертифіката. Для шифрування зв'язку між WSUS і клієнтами на сервері WSUS-PRIM-2019 створено самопідписаний сертифікат (Self-Signed Certificate), який не вимагає використання центру сертифікації (CA). Це виконано за допомогою PowerShell-команди New-SelfSignedCertificate -DnsName "WSUS-PRIM-2019.kostiuk.net" -CertStoreLocation "cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(5), що забезпечило термін дії на 5 років. Як загальне ім'я (CN) використано "wsus.kostiuk.net", яке збігається з іменем, що використовують клієнти для підключення до WSUS-сервера.

```

WinServer-2019_WSUS-main-Kostiuk [Запущено] - Oracle VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.KOSTIUK> [System.Net.Dns]::GetHostByName(($env:computerName)).HostName
WSUS-PRIM-2019.kostiuk.net
PS C:\Users\Administrator.KOSTIUK> New-SelfSignedCertificate -DnsName "WSUS-PRIM-2019.kostiuk.net" -CertStoreLocation "cert:\LocalMachine\My" -NotAfter (Get-Date).AddYears(5)

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint                Subject
-----
418FDE9866F7F411653D699E9808083291372A0D  CN=WSUS-PRIM-2019.kostiuk.net

PS C:\Users\Administrator.KOSTIUK>
  
```

Рис. 2.74 – Створення самопідписаного сертифікату.

Експорт сертифіката. Щоб поширити сертифікат серед клієнтів, його експортовано у форматі .cer із локального сховища "My" на WSUS-PRIM-2019. Формат .cer обрано, оскільки він містить лише публічну частину сертифіката, що робить його безпечним для розгортання без ризику компрометації приватного ключа.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				90
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис. 2.75 – Експортування сертифікату у форматі .cer.

Розгортання сертифіката на клієнтах. Оскільки сертифікат було створено на WSUS-PRIM-2019, його передано через мережевий диск на контролер домену DC-SRV-2022 для подальшого розгортання. Щоб усі клієнти довіряли сертифікату для встановлення HTTPS-з'єднання, його розгорнуто через існуючі групові політики "WSUS_Servers_Policy" і "WSUS_Workstations_Policy". Сертифікат імпортовано у сховище "Trusted Root Certification Authorities" на всіх віртуальних машинах у домені через контролер домену DC-SRV-2022.

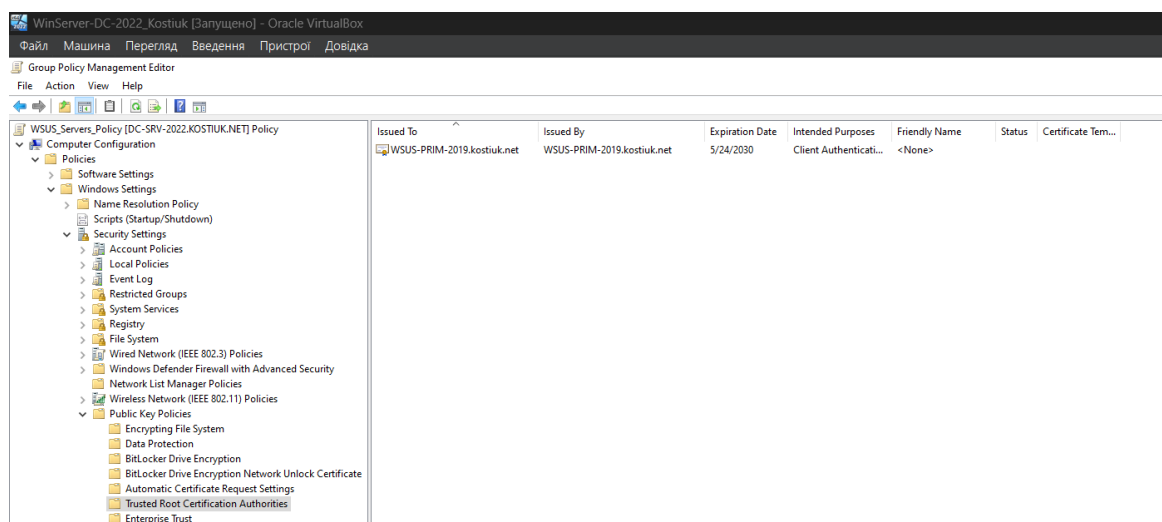


Рис. 2.76 – Імпорт сертифікату у совище "Trusted Root Certification Authorities".

Налаштування IIS. Для активації HTTPS-з'єднання на WSUS-PRIM-2019 виконано прив'язку TLS-сертифіката до порту 8531 у IIS, редагуючи сайт "WSUS Administration". Це дало змогу замінити незахищене HTTP-з'єднання на безпечний протокол із URL <https://wsus.kostiuk.net:8531>.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

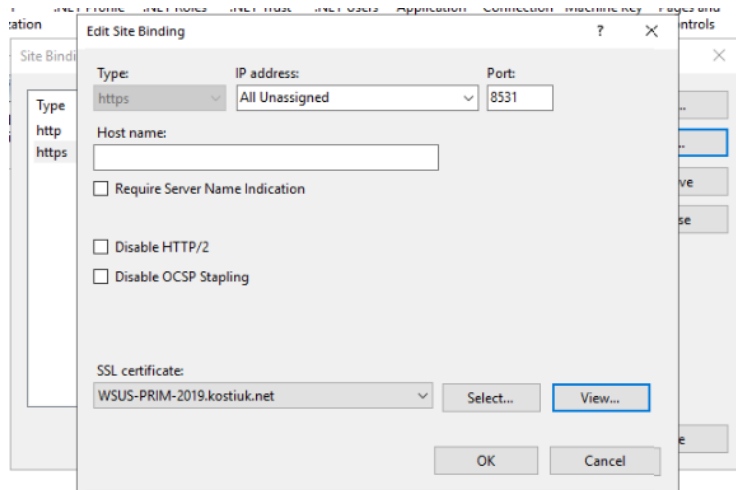


Рис. 2.77 – Прив'язка TLS-сертифіката до порту 8531 у IIS.

Оновлення GPO для вказування HTTPS-адреси. Для переключення клієнтів на безпечне з'єднання оновлено групові політики "WSUS_Servers_Policy" і "WSUS_Workstations_Policy". У параметрі "Specify intranet Microsoft update service location" змінено обидва поля (update і statistics) із `http://wsus.kostiuk.net:8530` на `https://wsus.kostiuk.net:8531`. Цей крок є обов'язковим для коректної роботи клієнтів із HTTPS-протоколом.

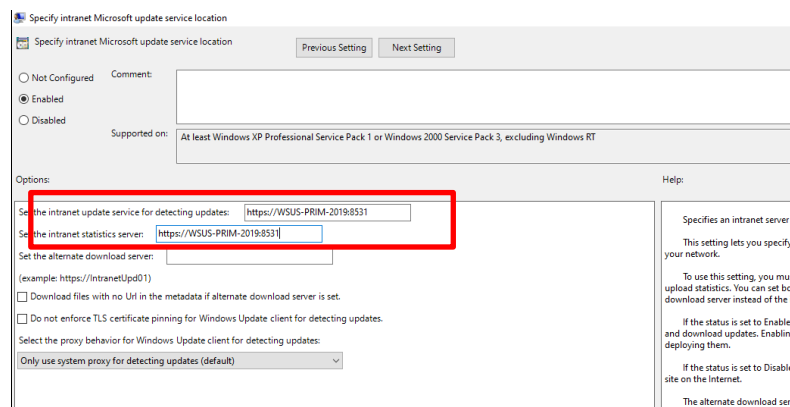


Рис. 2.78 - Переключення клієнтів на безпечне з'єднання.

Перевірка можливості зв'язку робочої станції з WSUS-сервером після оновлення політик. Для підтвердження коректності налаштувань HTTPS-з'єднання дочекалися, поки робочі станції, наприклад Win-10-1-KOST, відправили звіт до WSUS-сервера через новий URL. Перевірка статусу в консолі WSUS підтвердила успішне підключення всіх клієнтів.

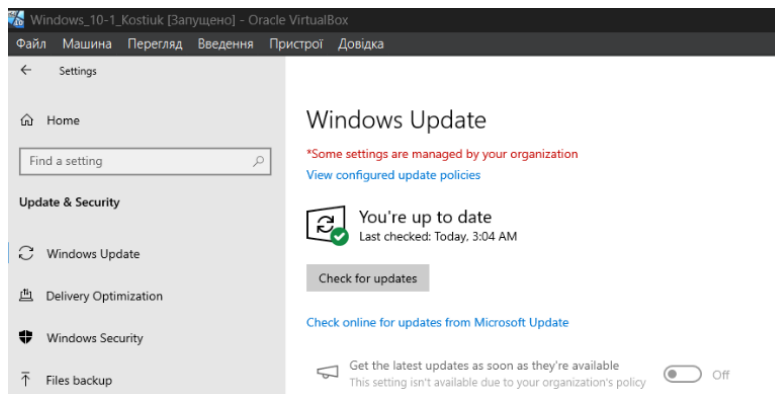


Рис. 2.79 – Проведення перевірки оновлень на робочій станції Win-10-1-KOST.

All Computers (6 computers of 6 shown, 6 total)					
Status: Any	Refresh				
Name	IP Address	Operating System	Installed/Not Applicable Perce...	Last Status Report	
win-10-1-kostiuk.kostiuk.net	192.168.7.100	Windows 10 Pro	99%	5/24/2025 3:31 AM	
wsus-repl-2019.kostiuk.net	192.168.7.21	Windows Server 2019 Standard	33%	5/22/2025 12:55 AM	
win-11-1-kostiuk.kostiuk.net	192.168.7.101	Windows 10 Pro	99%	5/23/2025 9:55 PM	
wsus-prim-2019.kostiuk.net	192.168.7.20	Windows Server 2019 Standard	99%	5/23/2025 11:28 PM	
dc-srv-2022.kostiuk.net	192.168.7.10	Windows Server 2022 Standard	100%	5/24/2025 3:10 AM	
win-10-2-kostiuk.kostiuk.net	192.168.7.102	Windows 10 Pro	100%	5/23/2025 2:40 AM	

Рис. 2.80 – Підтвердження наявності зв'язку.

Налаштування HTTPS-з'єднання для WSUS на WSUS-PRIM-2019 із використанням TLS-сертифіката забезпечили безпечний зв'язок із клієнтами, завершивши підготовку інфраструктури для централізованого управління оновленнями в домені kostiuk.net.

2.6 Налаштування резервного WSUS у режимі реплікації

Резервний WSUS-сервер (репліка) забезпечує підвищену відмовостійкість та часткове розвантаження основного сервера WSUS-PRIM-2019, налаштування якого було виконано в пункті 2.4. WSUS-REPL-2019 синхронізується з основним сервером у режимі реплікації, що дозволяє робочим станціям отримувати оновлення навіть у разі тимчасової недоступності WSUS-PRIM-2019. У цьому пункті описано встановлення ролі WSUS, налаштування реплікації, реалізацію HTTPS-з'єднання, оновлення групових політик та перевірку коректності роботи репліки.

Інсталяція WSUS із WID. Для розподілу навантаження на WSUS-REPL-2019 встановлено роль Windows Server Update Services. На відміну від основного сервера, який використовує SQL Server, репліка побудована на базі Windows Internal Database (WID), що дозволяє економити ресурси, оскільки WID не пот-

ребує окремого управління чи додаткових ліцензій (рис. 2.82). Під час встановлення обрано опцію "Replicas of an upstream server" із вказаною адресою основного сервера <https://wsus.kostiuk.net:8531> (рис. 2.83). У режимі реплікації WSUS-REPL-2019 не зберігає двійкові файли оновлень, а лише завантажує метадані, статуси схвалення та структуру групування клієнтів, отримуючи всю необхідну інформацію з головного сервера. Такий підхід дозволив оптимізувати споживання дискового простору й забезпечити коректну синхронізацію

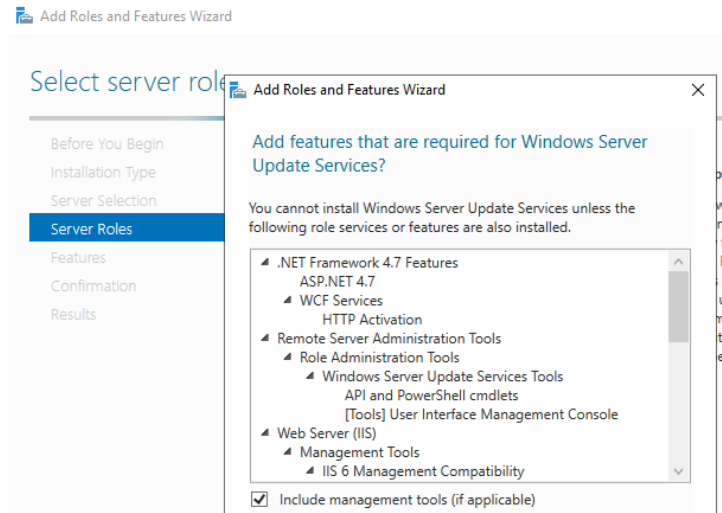


Рис. 2.81 – Вибір ролі WSUS для встановлення.

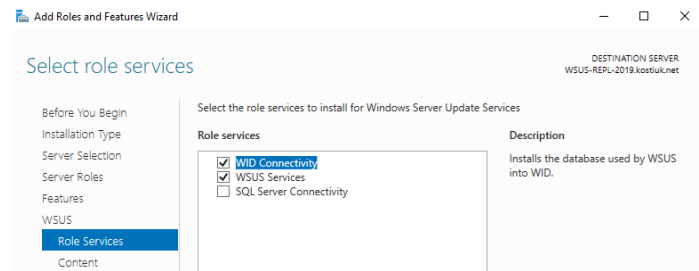


Рис. 2.82 – Вибір Windows Internal Database (WID) як основної бази даних.

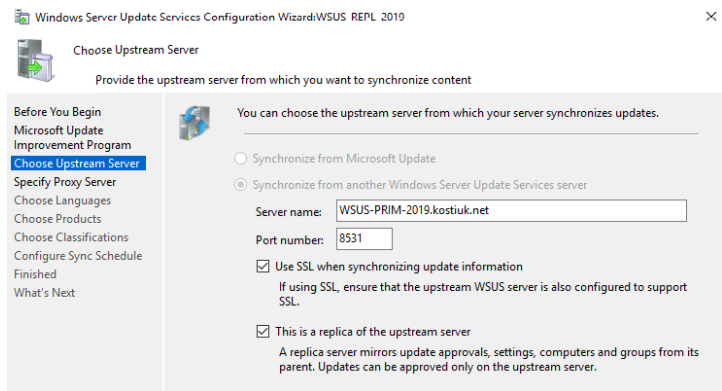


Рис. 2.83 – Налаштування реплікації основного WSUS сервера.

Реплікація. WSUS-REPL-2019 автоматично синхронізується з WSUS-PRIM-2019, отримуючи дані про оновлення, затвердження та групи клієнтів. Репліка працює в режимі **read-only**, що унеможливорює будь-яке ручне втручання в керування оновленнями на стороні резервного сервера та виключає ризик виникнення конфліктів. Це дозволяє централізувати управління патчами, одночасно маючи резервну точку доступу для клієнтів. Початкова синхронізація пройшла без помилок або затримок, після чого в консолі WSUS-REPL-2019 з'явився повний список продуктів, класифікацій і затверджених оновлень.

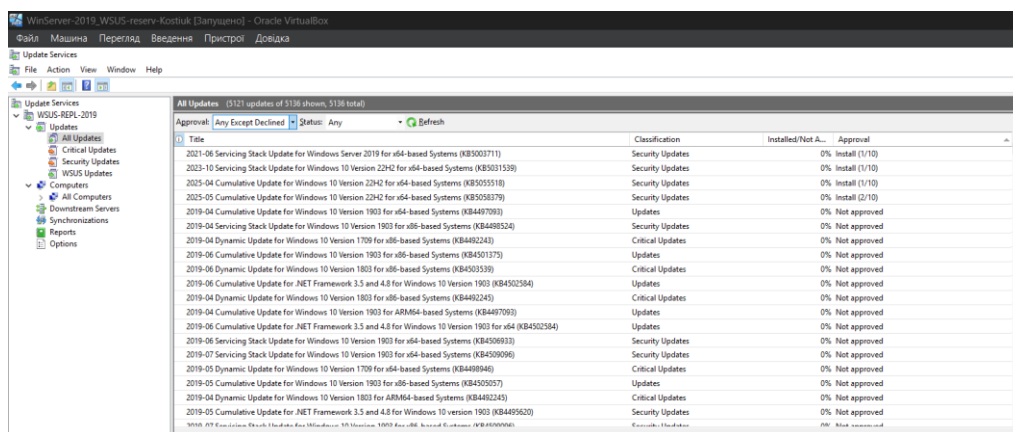


Рис. 2.84 – Перегляд синхронізованих оновлень.

Налаштування HTTPS. Щоб забезпечити захищене з'єднання через HTTPS і автентифікацію сервера на клієнтах, на WSUS-REPL-2019 було розгорнуто TLS-сертифікат, подібний до основного сервера. Сертифікат було поширено через групові політики, описані в пункті 2.5, із використанням DNS-імені wsus-repl-2019.kostiuk.net і порту 8531. У диспетчері IIS виконано прив'язку сертифіката до відповідного сайту, що забезпечило надійне шифрування та автентичність трафіку між клієнтами та WSUS-REPL-2019.

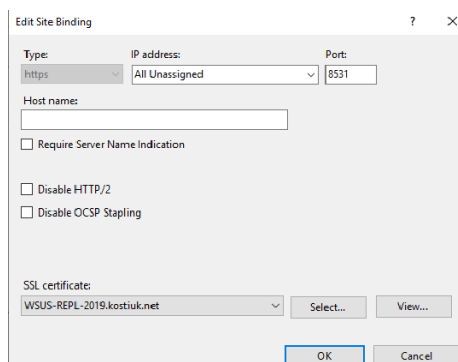


Рис. 2.85 – Налаштування HTTPS.

		Костюк І.О.			Арк.
		Росієнський Ю.М.			95
Змн.	Арк.	№ докум.	Підпис	Дата	

Оновлення GPO. Для розподілу навантаження між серверами було оновлено існуючу групову політику "WSUS_Workstations_Policy". У параметрі **Specify intranet Microsoft update service location** змінено обидва поля — для завантаження оновлень (update) та статистики (statistics) — з адреси основного сервера на адресу репліки <https://wsus-repl-2019.kostiuk.net:8531>. Клієнтські машини, розміщені в організаційній одиниці Workstations, почали надсилати запити на резервний сервер, тим самим зменшуючи навантаження на головний WSUS. Водночас сервери, які використовують політику WSUS_Servers_Policy, продовжують отримувати оновлення виключно від WSUS-PRIM-2019, що дозволяє чітко розмежувати трафік між різними категоріями пристроїв.

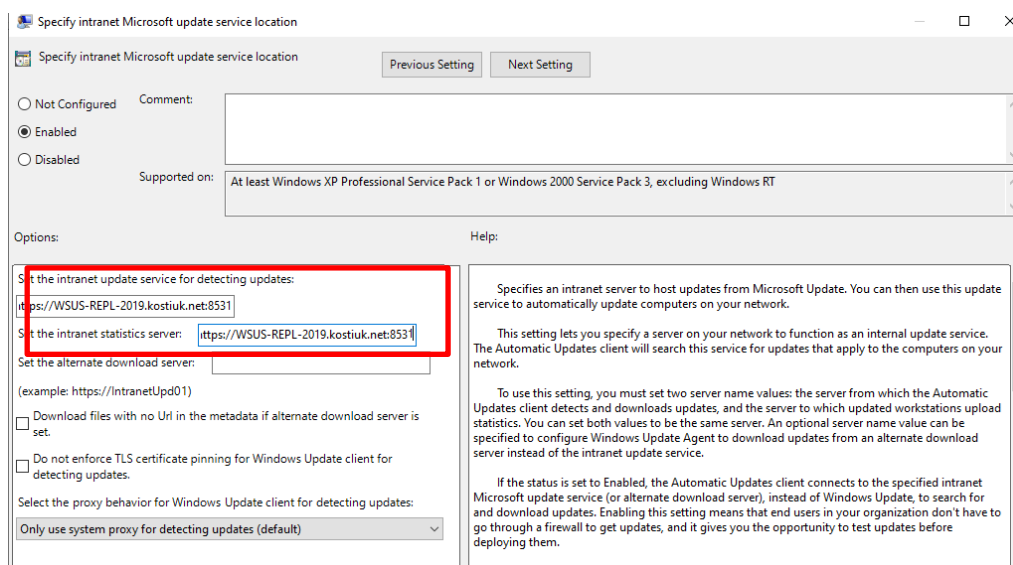


Рис. 2.86 – Оновлено існуючої групової політики "WSUS_Workstations_Policy".

Перевірка роботи. Для підтвердження коректності налаштувань дочекалися, поки клієнти з'явилися в консолі WSUS-REPL-2019 після оновлення GPOУ консолі WSUS з'явилися відповідні комп'ютери, відображались метадані, схвалення та статуси встановлення оновлень. Водночас метадані оновлень не зберігаються локально, що підтверджує правильність конфігурації реплікації. Групування клієнтів було виконано вручну в межах WSUS-REPL-2019 — цей процес описано детальніше в пункті 3.1.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				96
Змн.	Арк.	№ докум.	Підпис	Дата		

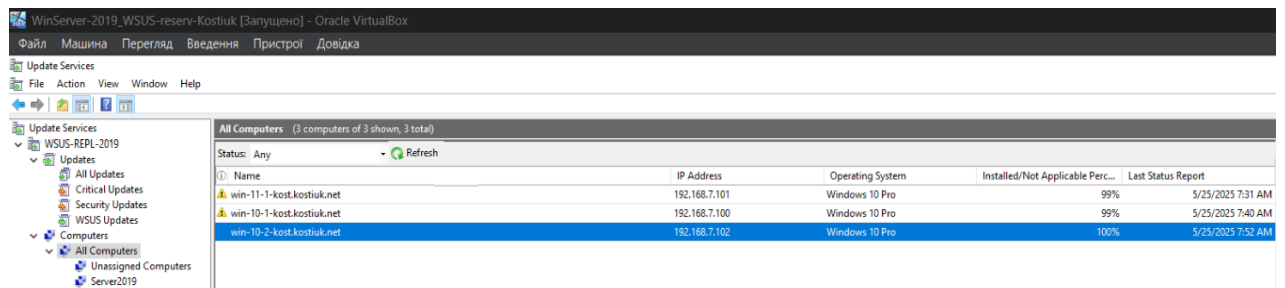


Рис. 2.87 – Відображення робочих станцій після синхронізації.

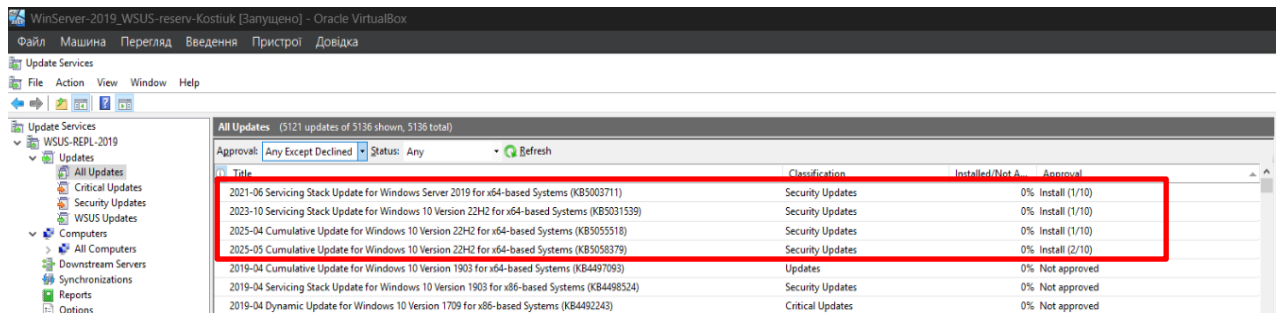


Рис. 2.88 – Відображення схвалених оновлень.

Налаштування WSUS-REPL-2019 як репліки WSUS-PRIM-2019 забезпечило високу доступність служби оновлень, централізований контроль, економію ресурсів і відмовостійкість. Впроваджена реплікаційна модель дозволила ефективно розподілити навантаження між двома вузлами WSUS та завершила побудову масштабованої інфраструктури Patch Management у домені kostiuk.net.

Висновки до Розділу 2

У розділі 2 було здійснено проєктування та впровадження системи Patch Management на базі Microsoft Windows Server Update Services (WSUS) у домені kostiuk.net, що моделює інфраструктуру типової середньої організації. У процесі реалізації використано принципи масштабованості, розподілення ролей, безпеки та модульності, що дозволило сформувати надійну тестову інфраструктуру.

Розроблена архітектурна модель, побудована на платформі Oracle VirtualBox, включала контролер домену DC-SRV-2022, основний WSUS-сервер WSUS-PRIM-2019 із базою SQL Server, резервний WSUS-сервер WSUS-REPL-2019 із Windows Internal Database, а також клієнтські машини з Windows 10 і Windows 11. Створено ізольовану NAT-мережу з підмережею 192.168.7.0/24, що

забезпечила стабільний зв'язок між компонентами. Для синхронізації оновлень із зовнішніми джерелами налаштовано контрольований доступ до Інтернету.

Налаштування доменної інфраструктури на базі Active Directory включало розгортання служби AD DS, організацію ієрархії OU, приєднання віртуальних машин до домену та конфігурацію служб DHCP і DNS. Встановлення та початкове налаштування WSUS на WSUS-PRIM-2019 із синхронізацією понад 5000 оновлень із Microsoft Update, а також створення групових політик "WSUS_Servers_Policy" і "WSUS_Workstations_Policy" забезпечили основу для централізованого управління. Впровадження HTTPS-з'єднання з використанням TLS-сертифіката на порту 8531 підвищило безпеку передачі даних. Налаштування WSUS-REPL-2019 як репліки в режимі "read-only" із перенаправленням клієнтів через оновлені GPO на URL <https://wsus-repl-2019.kostiuk.net:8531> завершило створення відмовостійкої інфраструктури.

Отже, реалізована система Patch Management забезпечила централізований контроль, безпеку та відмовостійкість у тестуванні оновлень, підготувавши платформу для подальшого аналізу ефективності та оптимізації, результати якого будуть представлені в розділі 4. Розгорнуте середовище повністю відображає архітектуру сучасної системи Patch Management і стало основою для практичного дослідження, що розглядатиметься в наступних розділах.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				98
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 АДМІНІСТРУВАННЯ, МОНІТОРИНГ І АНАЛІЗ СИСТЕМИ PATCH MANAGEMENT

3.1 Структурування груп клієнтів на WSUS-сервері

Для ефективного управління оновленнями в домені kostiuk.net було виконано структурування груп клієнтів у консолі WSUS, що дозволило логічно організувати пристрої за операційними системами, ролями та функціональним призначенням. Це спрощує адміністрування, забезпечує контрольоване тестування оновлень і знижує ризики для критичних вузлів. Цей пункт описує створення груп і призначення клієнтів, спираючись на попередні етапи розгортання WSUS.

Опис створених груп. Щоб забезпечити гнучке управління оновленнями, у консолі WSUS створено набір груп, які відображають специфіку пристроїв і сценаріїв використання. Групи поділено на три категорії: за операційними системами, для тестування та адміністративні. Нижче наведено їхній склад і призначення:

– **За операційними системами:**

- **Win10-Standard:** Включає Win-10-1-KOST і Win-10-2-KOST із Windows 10 Pro для одночасного розгортання оновлень на всі робочі станції з цією ОС.
- **Win11-Standard:** Включає Win-11-1-KOST із Windows 11 Pro, що дозволяє централізовано управляти оновленнями для цієї операційної системи.
- **Server2019:** Включає сервери WSUS-PRIM-2019 і WSUS-REPL-2019 на базі Windows Server 2019 для ізоляції серверних вузлів від клієнтів.
- **Server2022:** Включає контролер домену DC-SRV-2022 на Windows Server 2022, що забезпечує окремий контроль оновлень для критичного вузла.

– **Для тестування:**

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				99
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Win10-1:** Включає лише Win-10-1-KOST для ізолюваного тестування оновлень на окремій машині, що дозволяє уникнути впливу на інші пристрої у разі збоїв, а також застосовувати оновлення лише для цієї машини без затвердження для всієї групи.
- **Win10-2:** Включає лише Win-10-2-KOST, дозволяючи тестувати оновлення на іншій машині з Windows 10, а також виконувати вибіркове оновлення без поширення на всю групу.
- **Адміністративні групи:**
 - **WSUS-main-serv19:** Включає лише WSUS-PRIM-2019 для тестування оновлень, специфічних для основного WSUS-сервера.
 - **WSUS-reserv-serv19:** Включає лише WSUS-REPL-2019, що дозволяє ізолювано перевіряти оновлення для резервного сервера.

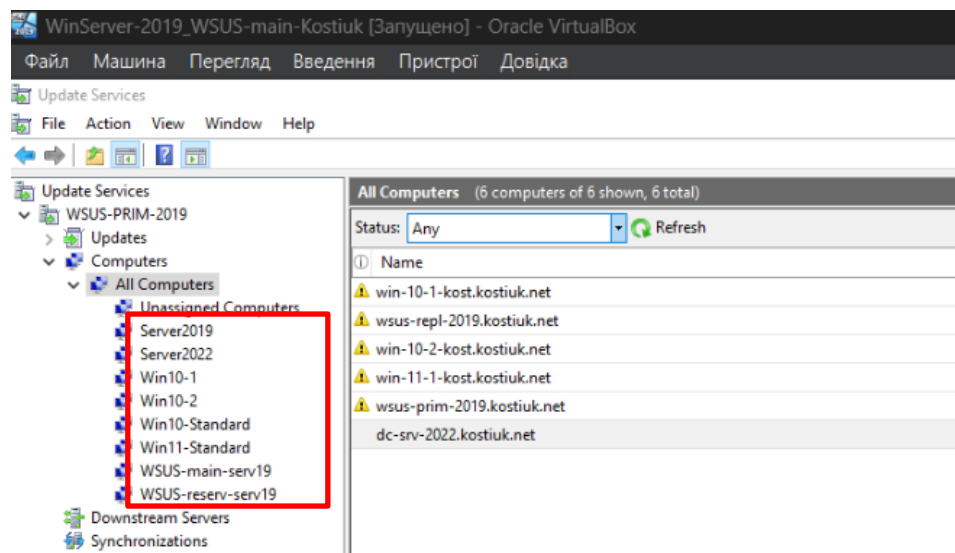


Рис. 3.1 – Структура груп клієнтів у консолі WSUS.

Такий поділ забезпечує чітку організацію клієнтів, дозволяючи управляти оновленнями залежно від їхньої ролі чи операційної системи, а також тестувати оновлення на окремих машинах перед широким розгортанням.

Принципи створення груп. Для централізованого контролю та синхронності структури групування виконано вручну на обох WSUS-серверах: WSUS-PRIM-2019 і WSUS-REPL-2019. На WSUS-PRIM-2019 створено основну структуру груп, яка автоматично синхронізувалася з WSUS-REPL-2019 завдяки режиму реплікації (див. п. 2.6). Ручне створення груп забезпечило гнучкість у

визначенні складу кожної групи та адаптацію до потреб тестування й адміністрування. Основні підстави для такого поділу:

- **Спрощення схвалення оновлень:** Групи за ОС (Win10-Standard, Win11-Standard) дозволяють схвалювати оновлення лише для конкретних систем, уникаючи непотрібних дій для інших.
- **Тестування оновлень та вибіркове оновлення:** Окремі групи Win10-1 і Win10-2 дають змогу перевіряти оновлення на одній машині, захищаючи іншу від можливих збоїв, а також застосовувати оновлення лише до окремої машини без впливу на всю групу.
- **Відокремлення серверів:** Групи Server2019, Server2022, WSUS-main-serv19 і WSUS-reserv-serv19 ізолюють сервери від клієнтів, зменшуючи ризик збоїв критичних вузлів через несумісні оновлення.

Цей підхід сприяє безпечному та ефективному управлінню оновленнями.

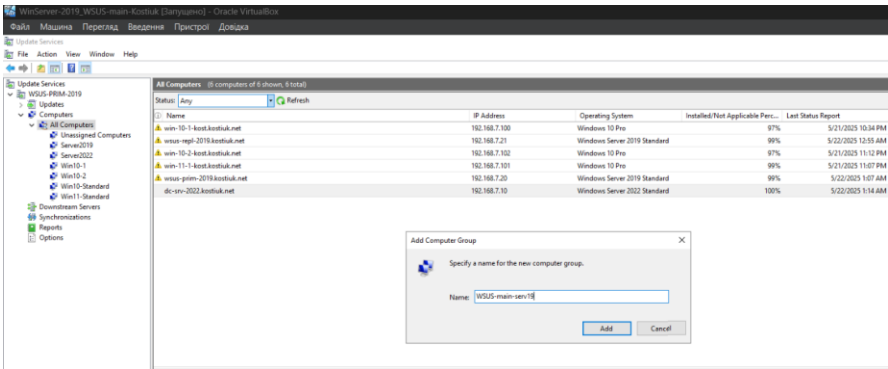


Рис. 3.2 – Приклад створення нової групи.

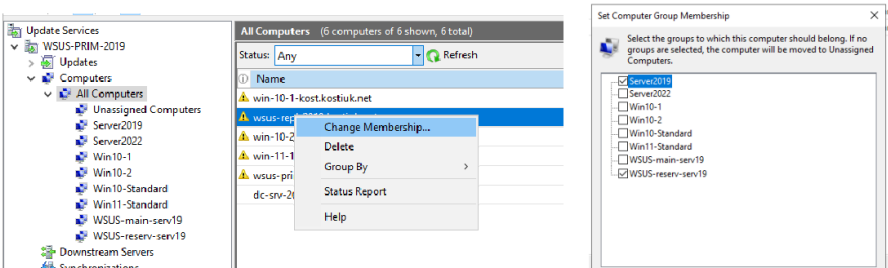


Рис. 3.3 – Приклад додавання комп'ютера до групи

Таким чином, створена структура груп у консолі WSUS дозволила класифікувати клієнтів за операційними системами, роллю в інфраструктурі та цілями тестування. Такий підхід спростив процес схвалення оновлень, унеможливив поширення неконтрольованих патчів на критичні вузли та забезпечив основу для поетапного розгортання оновлень у домені kostiuk.net.

3.2 Схвалення оновлень та організація розгортання

У процесі адміністрування системи Patch Management у домені kostiuk.net ключовим етапом стало схвалення оновлень для контрольованого розгортання. Система WSUS підтримує як ручне, так і автоматичне схвалення, але в межах проєкту було обрано повністю ручне схвалення для забезпечення повного контролю, уникнення ризиків і попереднього тестування на ізольованих групах. Цей пункт спирається на попередні етапи налаштування WSUS (п. 2.4.3) і структурування груп клієнтів (п. 3.1).

Причини ручного підходу. Рішення про ручне схвалення оновлень було зумовлене кількома факторами, які підвищують безпеку та ефективність управління оновленнями. По-перше, автоматичне схвалення було відхилено через ризик встановлення некоректних або несумісних оновлень. Як зазначено в пункті 2.4.3, під час синхронізації з Microsoft Update завантажувалися лише метадані оновлень (понад 5000, обсягом 170 МБ), а не повні двійкові файли (потенційно 890 ГБ). Оскільки WSUS не передбачає автоматичної перевірки сумісності чи актуальності оновлень, автоматичне схвалення могло б призвести до завантаження сотень або тисяч непотрібних оновлень, що перевантажило б дисковий простір серверів.

По-друге, ручне схвалення дозволило проводити попереднє тестування критичних оновлень на ізольованих групах, таких як Win10-1 або Win10-2 (див. п. 3.1), щоб уникнути збоїв на всіх клієнтах. По-третє, такий підхід дав змогу перевірити ефективність оновлень на окремих групах перед їхнім широким розгортанням, наприклад, на групі Win10-Standard. Це забезпечило контрольований і поетапний процес впровадження, знижуючи ризики для інфраструктури.

Процес схвалення. Схвалення оновлень виконувалося вручну через консоль WSUS на основному сервері WSUS-PRIM-2019, оскільки WSUS-REPL-2019, налаштований як репліка, лише синхронізував схвалені оновлення з основного сервера. Для затвердження конкретного оновлення використовувалося контекстне меню: правий клік на оновленні → "Approve...". У процесі схвалення для кожного оновлення вказувалася окрема група, наприклад, Win10-2 або Win11-

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				102
Змн.	Арк.	№ докум.	Підпис	Дата		

Standard, що дозволяло цільово розгортати оновлення лише на обраних клієнтах. Наприклад, ще до налаштування HTTPS і резервного сервера (див. п. 2.5, 2.6) було схвалено оновлення "Security Updates KB5055518" для Win10-2, щоб перевірити його вплив на одну машину перед ширшим застосуванням.

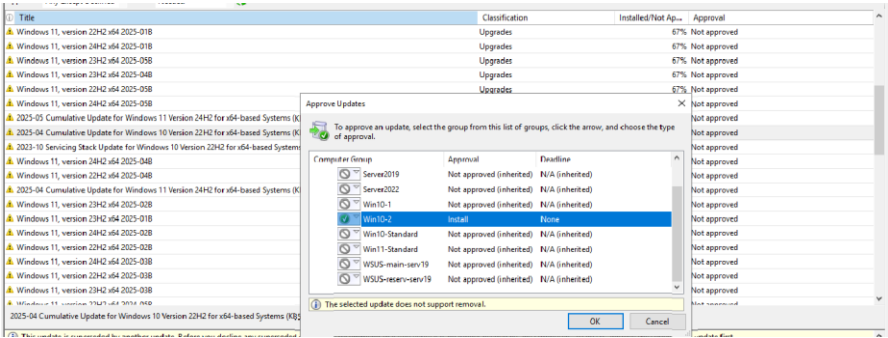


Рис. 3.4 – Вибір групи за схвалення оновлень.

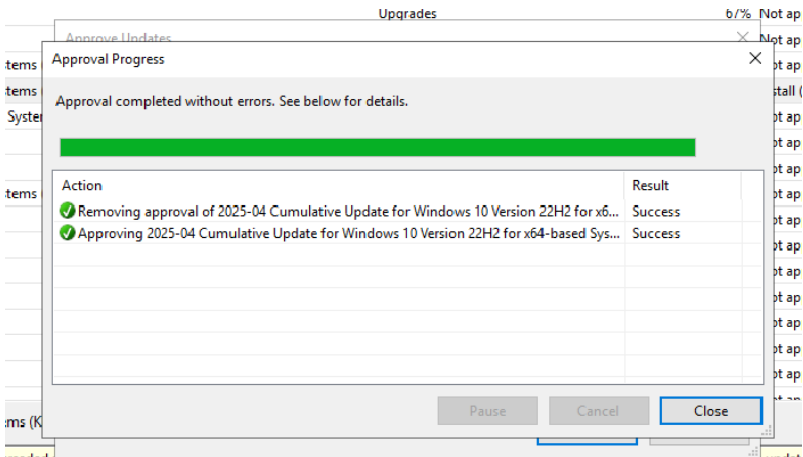


Рис. 3.5 – Підтвердження схвалення оновлень.

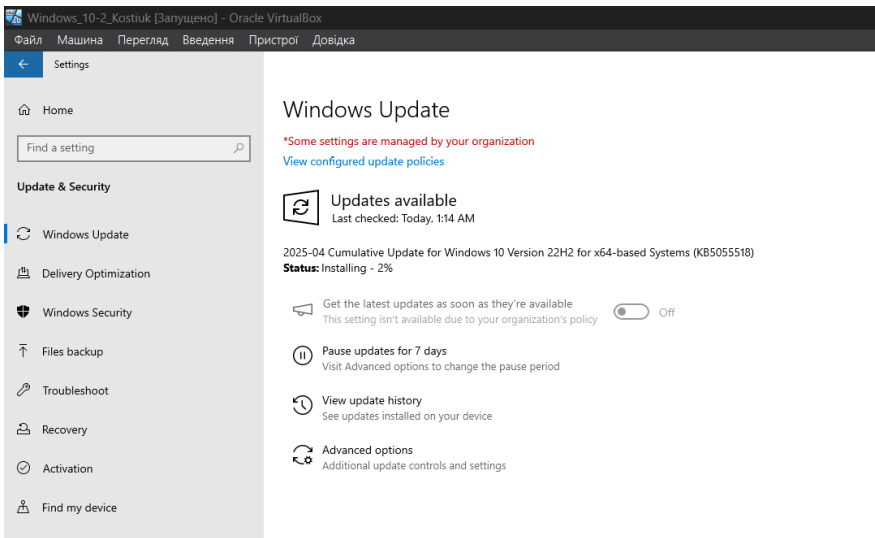


Рис. 3.6 – Встановлення оновлення на робочій станції.

Для моніторингу процесу в консолі WSUS постійно контролювалися статуси оновлень: "Approved" для затверджених і "Not Approved" для тих, що ще не

схвалені. Додатково використовувався звіт WSUS для оцінки стану схвалених оновлень, що полегшило відстеження.

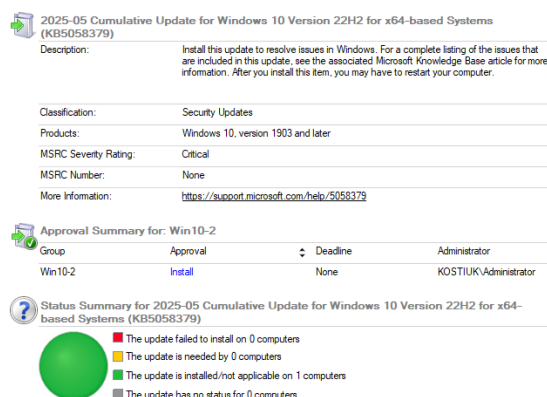


Рис. 3.7 – Створення звіту перевірки успішного встановлення оновлення.

Ручне схвалення оновлень забезпечило гнучке та безпечне розгортання в домені kostiuk.net, дозволяючи адаптувати процес до потреб кожної групи клієнтів. Наприклад, тестування оновлення на Win10-1 перед його розгортанням на групу Win10-Standard дало змогу переконатися у відсутності збоїв, перш ніж застосовувати його до всіх машин із Windows 10. Подібний підхід використовувався і для Win11-Standard та Server-груп, де критичні оновлення застосовувалися лише після тестування. Такий підхід знизив ризики помилок і створив умови для контрольованого переходу від тестування до повного впровадження оновлень.

3.3 Контроль стану оновлень (звіти WSUS + SQL-запити)

Для забезпечення стабільності системи Patch Management у домені kostiuk.net було виконано контроль стану оновлень на клієнтах через консоль WSUS і SQL-запити до бази SUSDB. Перевірка охоплювала статуси синхронізації (дати останніх звітів), схвалення оновлень ("Approved"/"Not Approved") і потрібність оновлень ("Needed"), що дало змогу оцінити готовність інфраструктури до розгортання. Цей пункт спирається на попередні етапи налаштування WSUS (див. п. 2.4), структурування груп (див. п. 3.1) і схвалення оновлень (див. п. 3.2).

Перевірка через WSUS-звіти. Для швидкого аналізу стану оновлень у консолі WSUS на WSUS-PRIM-2019 було сформовано кілька звітів, які відображали статус усіх зареєстрованих клієнтів (DC-SRV-2022, WSUS-PRIM-2019, WSUS-REPL-2019, Win-10-1-KOST, Win-10-2-KOST, Win-11-1-KOST). Звіти генерувалися через розділ "Reports" із можливістю експорту в PDF:

- **Update Status Summary:** Показував кількість оновлень у статусах "Installed", "Needed", "Not Applicable" для груп, таких як Win10-Standard, що дозволило оцінити загальний стан.

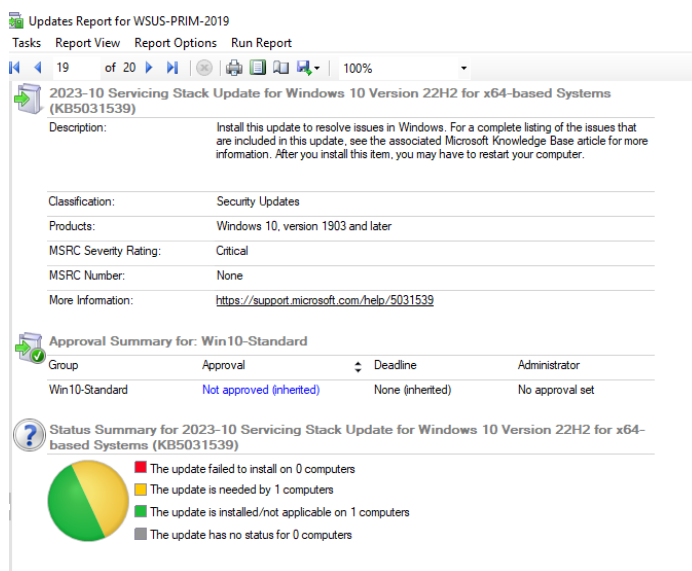


Рис. 3.8 – Звіт «Update Status Summary».

- **Computer Status Summary:** Забезпечував огляд статусу оновлень для кожного клієнта в групах, наприклад, "Servers" або "Win10-Standard", для перевірки регулярності звітів.

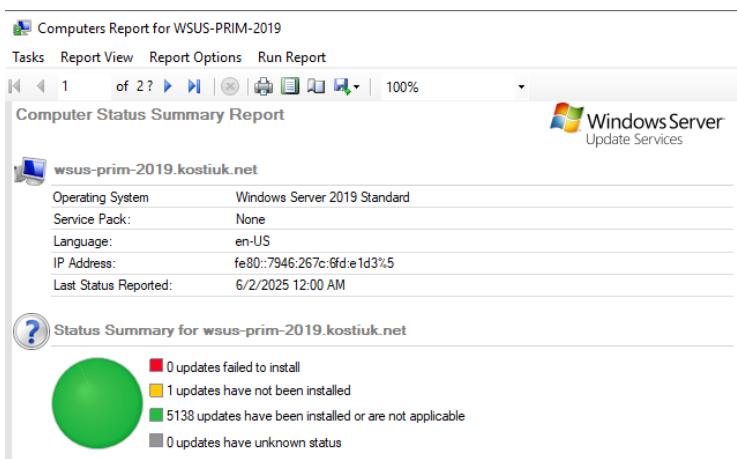


Рис. 3.9 – Звіт «Computer Status Summary»

- **Update Detailed Status:** Надавав деталі для конкретного оновлення (наприклад, KB...), показуючи його розподіл по групах, що полегшило аналіз окремих апдейтів.

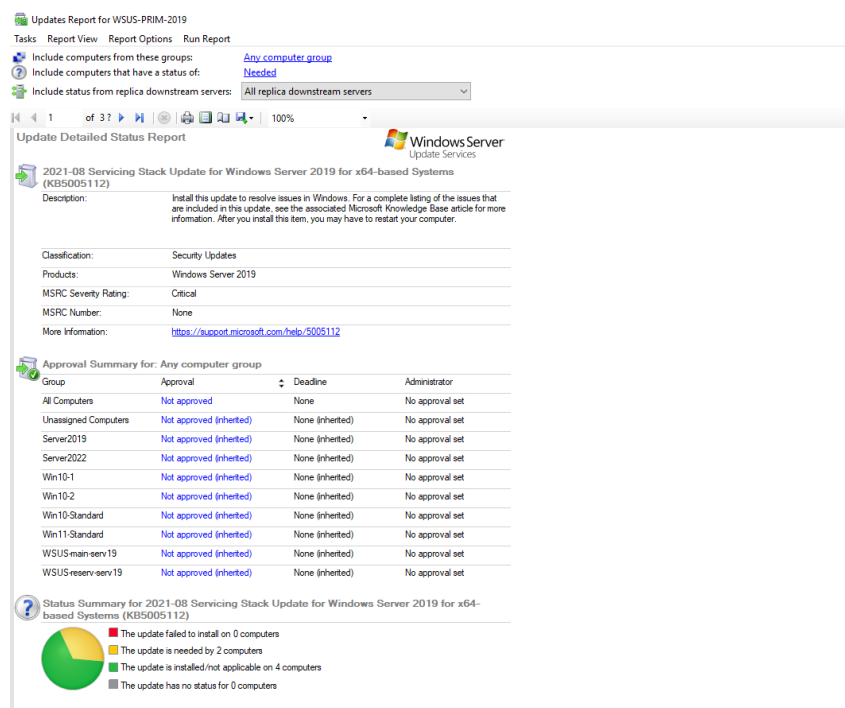


Рис. 3.10 – Звіт «Update Detailed Status»

- **Synchronization Results:** Відображав результати останньої синхронізації з Microsoft Update, підтверджуючи актуальність метаданих.

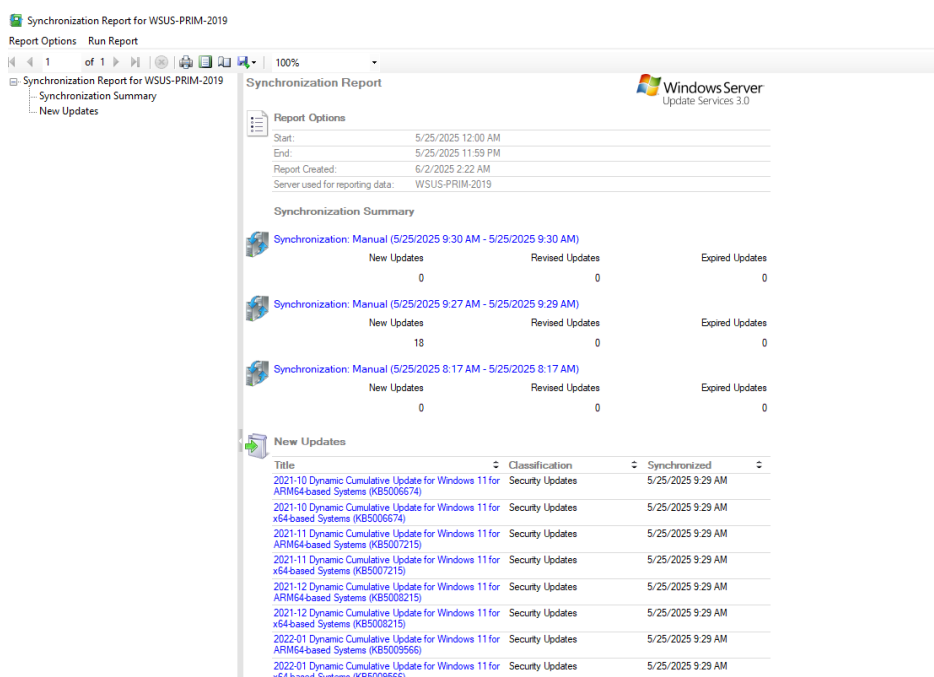


Рис. 3.11 – Звіт «Synchronization Results».

- **Update Tabular Status for Approved Updates:** Перевіряв успішність встановлення схвалених оновлень за класифікацією та групами (наприклад, Win10-Standard), що допомогло оцінити ефективність розгортання.

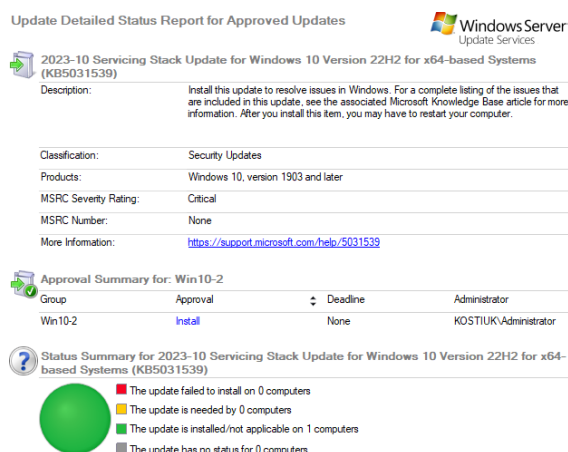


Рис. 3.12 – Звіт «Update Tabular Status for Approved Updates».

Оскільки GUI консолі WSUS має обмеження в деталізації даних (наприклад, складно отримати повний перелік потрібних оновлень), для глибшого аналізу використано SQL-запити.

Перевірка через SQL-запити до SUSDB

Для детальнішого аналізу стану оновлень виконано SQL-запити до бази SUSDB на SQL Server 2019 (WSUS-PRIM-2019, див. п. 2.4), які забезпечили гнучкість і масштабіність. Повні тексти запитів наведено в додатку Б. Нижче наведено перелік із короткими описами:

- **Список клієнтів (FullDomainName, IP, звіт):** Аналіз активності та присутності клієнтів за доменними іменами, IP-адресами та часом звіту.

Results				
	FullDomainName	IPAddress	LastReportedStatusTime	LastSyncTime
1	wsus-repl-2019.kostiuk.net	192.168.7.21	2025-05-25 19:01:30.600	2025-05-25 18:52:42.243
2	wsus-prim-2019.kostiuk.net	fe80::7946:267c:6fd:e1d3%5	2025-05-25 19:00:30.330	2025-05-25 18:48:05.800
3	dc-srv-2022.kostiuk.net	192.168.7.10	2025-05-25 18:51:31.260	2025-05-25 18:45:53.053
4	win-11-1-kost.kostiuk.net	192.168.7.101	2025-05-25 06:44:44.550	2025-05-25 06:36:02.977
5	win-10-2-kost.kostiuk.net	192.168.7.102	2025-05-25 04:52:31.407	2025-05-25 04:43:29.467
6	win-10-1-kost.kostiuk.net	192.168.7.100	2025-05-25 04:40:15.933	2025-05-25 04:34:30.570

Рис. 3.13 – Перегляд списку всіх клієнтів.

- **Затверджені оновлення та групи:** Перевірка коректності схвалень за назвами оновлень і цільовими групами, хоча дані не використовувалися в цьому аналізі.

Results Messages				
	Title	TargetID	TargetGroupID	
1	Actualizaciones críticas	7	D374F42A-98E2-4163-A0FA-3C86A401B7A7	
2	Critical Updates	6	7FC38D85-8BA9-45ED-AF3E-40ECFDDFDE73	
3	Critical Updates	6	6150123F-50FA-40D0-85C0-919525059F60	
4	Důležitá aktualizace	2	CC675BF3-76B7-4479-9776-1E580C07F589	
5	Vigtige opdateringer	3	F3682C31-B8F3-4DDC-A4B9-661C899FE314	
6	Wichtige Updates	4	8DF5C861-B892-4061-B47B-F1635340F09D	
7	Wichtige Updates	4	F5CC5F03-8708-4533-830A-F3DE070EE88C	
8	Κρίσιμες ενημερωμένες εκδόσεις	5	25669804-3627-4290-9250-3EA7BC6EA2E6	
9	Κρίσιμες ενημερωμένες εκδόσεις	5	6150123F-50FA-40D0-85C0-919525059F60	
10	التحديثات الضرورية	1	99E4F46B-6B69-46E8-8D07-E416A8858680	
11	التحديثات الضرورية	1	8DF5C861-B892-4061-B47B-F1635340F09D	

Рис. 3.14 – Перегляд коректності схвалень.

- **Зведена статистика Installed / Needed / NotApplicable:** Оцінка загального стану оновлень по кожному клієнту.

Results Messages				
	FullDomainName	Installed	Needed	NotApplicable
1	wsus-repl-2019.kostiuk.net	0	2	0
2	wsus-prim-2019.kostiuk.net	0	1	0
3	win-10-1-kost.kostiuk.net	0	1	0
4	win-11-1-kost.kostiuk.net	0	0	0
5	win-10-2-kost.kostiuk.net	0	0	0

Рис. 3.15 – Перегляд статистики стану оновлень.

- **Потрібні оновлення (status = 2):** Ідентифікація актуальних апдейтів для схвалення, із назвами оновлень і клієнтами.

Results Messages				
	Computer Name	Update Title	Status	Last Report
1	wsus-prim-2019.kostiuk.net	Windows XP Professional SP2	2	2025-05-25 19:00:30.330
2	wsus-repl-2019.kostiuk.net	Windows XP Professional SP2	2	2025-05-25 19:01:30.600

Рис. 3.16 – Перегляд актуальних оновлень.

- **Несинхронізовані машини (за останні 3 дні):** Виявлення потенційних проблем із синхронізацією.

Results Messages				
	FullDomainName	Last Sync Time	Last Reported Status Time	Days Since Last Report
1	win-10-1-kost.kostiuk.net	2025-05-25 04:34:32.823	2025-05-25 04:40:18.187	8
2	win-10-2-kost.kostiuk.net	2025-05-25 04:43:31.720	2025-05-25 04:52:33.660	8
3	win-11-1-kost.kostiuk.net	2025-05-25 20:54:28.987	2025-05-25 19:17:29.190	8

Рис. 3.17 – Перегляд машин, що не синхронізувались більше 3 днів.

Результати SQL-запитів повністю збіглися з WSUS-звітами, підтвердивши коректність роботи системи. Переваги SQL полягали в масштабності обробки даних, гнучкості аналітики та можливості експорту для звітів.

Порівняння даних із WSUS-звітів і SQL-запитів показало їхню повну відповідність, що свідчить про стабільність конфігурації WSUS і SUSDB. Це підтвердило готовність інфраструктури до розгортання оновлень у домені kostiuk.net, що буде детальніше розглянуто в наступних пунктах.

3.4 Моніторинг через PowerShell-скрипти

Для розширення можливостей моніторингу стану оновлень у домені kostiuk.net було застосовано низку PowerShell-скриптів, які взаємодіяли з WSUS через вбудоване API (Get-WsusServer, GetComputerTargets, GetUpdates). Це дало змогу автоматизувати збір даних про синхронізацію клієнтів, виявляти затримки, отримувати базову інформацію про ОС, IP-адреси та групи клієнтів, а також аналізувати потрібні чи невдалі оновлення. Однак моніторинг через PowerShell виявився обмеженим у зв'язку зі складністю обробки WSUS API та його неповною документацією.

Опис використаних скриптів. Для моніторингу розроблено кілька PowerShell-скриптів, кожен із яких виконував певну функцію. Оскільки до основного сервера WSUS-PRIM-2019 підключені всі сервери (DC-SRV-2022, WSUS-PRIM-2019, WSUS-REPL-2019), а до резервного WSUS-REPL-2019 — усі робочі станції (Win-10-1-KOST, Win-10-2-KOST, Win-11-1-KOST), результати виконання скриптів на цих серверах відрізнялися залежно від підключених клієнтів.

AllClients.ps1 Виводить список усіх клієнтів із доменними іменами, часом останньої синхронізації та звіту для оцінки їхнього стану, отримуючи дані через GetComputerTargets і відбираючи потрібні поля.

Лістинг скрипта:

```
$wsus = Get-WsusServer -Name "WSUS-PRIM-2019" -PortNumber 8530

$clients = $wsus.GetComputerTargets()

$report = $clients | Select-Object FullDomainName, LastSyncTime, LastReported-
StatusTime | Sort-Object LastSyncTime
$report | Format-Table -AutoSize
```

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				109
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Administrator: Windows PowerShell
PS C:\WSUS-Scripts> .\AllClients.ps1

FullDomainName           LastSyncTime           LastReportedStatusTime
-----
dc-srv-2022.kostiuk.net   6/1/2025 11:10:01 PM   6/1/2025 11:18:02 PM
wsus-repl-2019.kostiuk.net 6/1/2025 11:46:03 PM   6/1/2025 8:56:42 PM
wsus-prim-2019.kostiuk.net 6/2/2025 4:54:02 PM    6/2/2025 5:07:19 PM

PS C:\WSUS-Scripts>

```

Рис. 3.18 – Результат виконання скрипта «AllClients.ps1».

GetAllComputer.ps1. Доповнює список клієнтів інформацією про IP-адреси та версії ОС для базового огляду інвентаризації, витягуючи атрибути IPAddress і OSDescription із об'єктів GetComputerTargets.

Лістинг скрипта:

```

$wsus = Get-WSUSServer
$computers = $wsus.GetComputerTargets()

$computers | ForEach-Object {
    [PSCustomObject]@{
        Name = $_.FullDomainName
        LastReported = $_.LastReportedStatusTime
        OS = $_.OSDescription
        IP = $_.IPAddress
    }
} | Format-Table -AutoSize

```

```

Administrator: Windows PowerShell
PS C:\Users\Administrator.KOSTIUK> cd C:\WSUS-Scripts
PS C:\WSUS-Scripts> .\GetAllComputer.ps1

Name                               LastReported           OS                        IP
--
win-11-1-kost.kostiuk.net 5/25/2025 7:17:28 PM   Windows 10 Pro          192.168.7.101
win-10-1-kost.kostiuk.net 5/25/2025 4:40:17 AM   Windows 10 Pro          192.168.7.100
win-10-2-kost.kostiuk.net 5/25/2025 4:52:33 AM   Windows 10 Pro          192.168.7.102

PS C:\WSUS-Scripts>

```

Рис. 3.19 – Результат виконання скрипта «GetAllComputer.ps1».

LastReport.ps1. Включає інформацію про групу клієнта (RequestedTargetGroupName) для перевірки коректності групування, відбираючи відповідне поле з об'єктів GetComputerTargets разом із часом звіту.

Лістинг скрипта:

```

$wsus = Get-WSUSServer
$clients = $wsus.GetComputerTargets()

$clients | Select-Object FullDomainName, LastReportedStatusTime, LastSyncTime, RequestedTargetGroupName | Format-Table -AutoSize

```

```

Administrator: Windows PowerShell

PS C:\WSUS-Scripts> .\LastReport.ps1

FullDomainName      LastReportedStatusTime LastSyncTime      RequestedTargetGroupName
-----
win-11-1-kost.kostiuk.net 5/25/2025 7:17:28 PM 5/25/2025 8:54:28 PM Workstations
win-10-1-kost.kostiuk.net 5/25/2025 4:40:17 AM 5/25/2025 4:34:32 AM Workstations
win-10-2-kost.kostiuk.net 5/25/2025 4:52:33 AM 5/25/2025 4:43:31 AM Workstations

PS C:\WSUS-Scripts>

```

Рис. 3.20 – Результат виконання скрипта «LastReport.ps1».

NoSynch.ps1. Виявляє клієнтів, які не синхронізувалися понад 3 дні для independente підтвердження стабільності, фільтруючи об'єкти GetComputerTargets за різницею часу LastSyncTime.

Лістинг скрипта:

```

$wsus = Get-WSUSServer -Name "WSUS-REPL-2019" -PortNumber 8530

$threshold = (Get-Date).AddDays(-3)

$inactive = $wsus.GetComputerTargets() | Where-Object { $_.LastSyncTime -lt
$threshold }

$inactive | Select-Object FullDomainName, LastSyncTime | Format-Table -AutoSize

```

```

WinServer-2019_WSUS-reserv-Kostiuk [Запущено] - Oracle VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

Administrator: Windows PowerShell

PS C:\WSUS-Scripts> .\NoSynch.ps1

FullDomainName      LastSyncTime
-----
win-11-1-kost.kostiuk.net 5/25/2025 8:54:28 PM
win-10-1-kost.kostiuk.net 5/25/2025 4:34:32 AM
win-10-2-kost.kostiuk.net 5/25/2025 4:43:31 AM

PS C:\WSUS-Scripts>

```

Рис. 3.21 – Результат виконання скрипта «NoSynch.ps1».

Результати виконання цих скриптів ілюструють їхню ефективність для базового моніторингу.

Скрипт "Monitor-WSUS-Updates.ps1". Цей скрипт аналізував оновлення типу "Security Updates" і "Critical Updates" за останній рік для груп Win10-Standard і Win11-Standard, визначаючи статуси Needed, Failed, Installed. Основна логіка включала: ініціалізацію WSUS API, пошук оновлень за критеріями, аналіз статусів і виведення результатів у CSV та лог-файл із попередженнями про невідаль оновлення.

Ключові фрагменти:

```
$wsus = Get-WsusServer -Name "WSUS-REPL-2019" -PortNumber 8530 # Ініціалізація з'єднання з WSUS
$groupsToMonitor = @("Win10-Standard", "Win11-Standard") # Цільові групи для моніторингу
$results | Export-Csv -Path "C:\Reports\WSUS_Update_Status.csv" -NoTypeInformation # Виведення в CSV
```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator\KOSTIUK> cd C:\WSUS-Scripts
PS C:\WSUS-Scripts> .\Monitor-WSUS-Updates.ps1
Transcript started, output file is C:\WSUS-Scripts\MonitorUpdatesLog_20250602_222609.txt
Підключення до WSUS-сервера WSUS-REPL-2019 о 06/02/2025 22:26:09...
Обробка групи 'Win10-Standard' завершена.
Обробка групи 'Win11-Standard' завершена.
Діагностика: Загальна кількість елементів у allResults: 8
Перший елемент у allResults:
Група 'Win10-Standard' містить 2 комп'ютерів.

Знайдено 8 оновлень, які потребують уваги.
Експортуюмо результати в CSV: C:\WSUS-Scripts\MonitorUpdatesResults_20250602_222609.csv
Розмір лог-файлу: 1.296875 KB
Скрипт завершено о 06/02/2025 22:26:28.
Transcript stopped, output file is C:\WSUS-Scripts\MonitorUpdatesLog_20250602_222609.txt
PS C:\WSUS-Scripts>
```

Рис. 3.22 – Результат виконання скрипта «Monitor-WSUS-Updates.ps1».

```
WinServer-2019_WSUS-main-Kostiuk [Затушено] - Oracle VirtualBox
Файл Машина Перегляд Введення Пристрої Довідка
MonitorUpdatesLog_20250602_222609 - Notepad
File Edit Format View Help
*****
Windows PowerShell transcript start
Start time: 20250602222609
Username: KOSTIUK\Administrator
RunAs User: KOSTIUK\Administrator
Configuration Name:
Machine: WSUS-PRIM-2019 (Microsoft Windows NT 10.0.17763.0)
Host Application: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe
Process ID: 4092
PSVersion: 5.1.17763.7309
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.7309
BuildVersion: 10.0.17763.7309
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
Transcript started, output file is C:\WSUS-Scripts\MonitorUpdatesLog_20250602_222609.txt
Підключення до WSUS-сервера WSUS-REPL-2019 о 06/02/2025 22:26:09...
Обробка групи 'Win10-Standard' завершена.
Обробка групи 'Win11-Standard' завершена.
Діагностика: Загальна кількість елементів у allResults: 8
Перший елемент у allResults:
Група 'Win10-Standard' містить 2 комп'ютерів.
Знайдено 8 оновлень, які потребують уваги.
Експортуюмо результати в CSV: C:\WSUS-Scripts\MonitorUpdatesResults_20250602_222609.csv
Розмір лог-файлу: 1.296875 KB
Скрипт завершено о 06/02/2025 22:26:28.
*****
Windows PowerShell transcript end
End time: 20250602222628
*****
```

Рис. 3.23 – Перегляд створеного лог-файлу.

Повний лістинг наведено в Додатку В. Результати виконання показали дієвість скрипту.

Вивід і обмеження. PowerShell-скрипти дозволили автоматизовано контролювати синхронізацію клієнтів і статуси оновлень. Наприклад, Monitor-WSUS-Updates.ps1 виявив кілька потенційних оновлень, що дало змогу оперативно їх схвалити вручну. Проте через нестабільність WSUS API, зокрема методи на кшталт GetUpdateInstallationInfoPerComputerTarget(), які повертали

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Россінський Ю.М.				112
Змн.	Арк.	№ докум.	Підпис	Дата		

неповні результати, повноцінний аналіз був ускладнений. Це підкреслило необхідність доповнення моніторингу SQL-запитами (див. п. 3.3).

PowerShell-скрипти продемонстрували практичну цінність для автоматизованого моніторингу в домені kostiuk.net, зокрема для збору даних про клієнтів і виявлення потрібних оновлень у групах Win10-Standard і Win11-Standard. Обмеження WSUS API, такі як нестабільність результатів, було компенсовано використанням SQL-запитів (див. п. 3.3), що створило комплексну базу для управління оновленнями та подальшої оптимізації.

3.5 Моніторинг продуктивності WSUS-серверів за допомогою Perfmon

Для оцінки продуктивності WSUS-серверів у домені kostiuk.net, зокрема основного WSUS-PRIM-2019 і резервного WSUS-REPL-2019, було проведено моніторинг апаратних і сервісних ресурсів за допомогою Performance Monitor (Perfmon). Мета полягала у виявленні вузьких місць, таких як навантаження на процесор, пам'ять, диск, а також у перевірці роботи служб WSUS, IIS і SQL Server, що забезпечують функціонування системи оновлень. Це дозволило переконатися у стабільності інфраструктури під час тестового циклу.

Налаштування моніторингу. Налаштування здійснювалось однаково для обох серверів через Microsoft Management Console (MMC), щоб забезпечити послідовний аналіз продуктивності. Спочатку було запущено MMC і додано оснастку Performance Monitor для доступу до інструментів моніторингу. Потім налаштовано набір лічильників, які відстежували ключові показники системи та служб. Після завершення конфігурацію збережено до файлу WSUS_Monitor.msc для повторного використання. Такий підхід спростив доступ до моніторингу та забезпечив стандартизований збір даних.

Обрані лічильники. Для комплексного аналізу продуктивності було відібрано лічильники, згруповані за категоріями, що охоплювали роботу WSUS, IIS, SQL Server і загальні системні ресурси:

– **WSUS та IIS:**

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				113
Змн.	Арк.	№ докум.	Підпис	Дата		

- **\Process(WsusService)\% Processor Time**: Оцінює навантаження служби WSUS для виявлення надмірного використання CPU.
- **\Process(w3wp)\Working Set**: Показує споживання пам'яті процесом IIS, що важливо для веб-доступу до WSUS.
- **SQL Server**:
 - **\SQLServer:Buffer Manager\Page Life Expectancy**: Відображає ефективність кешування сторінок у пам'яті для оцінки продуктивності бази SUSDB.
 - **\SQLServer:SQL Statistics\Batch Requests/sec**: Вимірює кількість запитів до бази, що вказує на активність SQL Server.
- **Система**:
 - **\Processor\% Processor Time (_Total)**: Загальне навантаження CPU для оцінки загальної продуктивності сервера.
 - **\Memory\Available MBytes**: Показує обсяг вільної оперативної пам'яті для виявлення можливого дефіциту.
 - **\PhysicalDisk\Avg. Disk Queue Length**: Навантаження на диск (I:), де розгорнуто WSUS, для оцінки затримок у операціях введення-виведення.
 - **\Network Interface\Bytes Total/sec**: Мережевий трафік для аналізу обсягу передачі даних.

Ці лічильники дозволили охопити всі критичні компоненти системи.

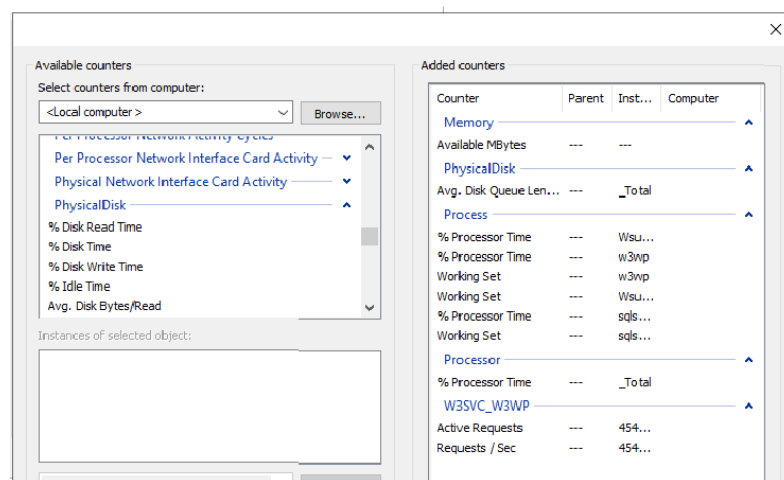


Рис. 3.24 – Налаштування лічильників у Performance Monitor

Формати збору даних. Дані збиралися двома способами: у реальному часі через Performance Monitor для миттєвого аналізу та через Data Collector Sets для періодичного запису логів. Логи зберігалися у форматі CSV у каталозі C:\PerfLogs, що забезпечило можливість їхнього подальшого перегляду в Excel для детального аналізу. Такий підхід дозволив як швидко реагувати на відхилення, так і проводити ретроспективний аналіз продуктивності.

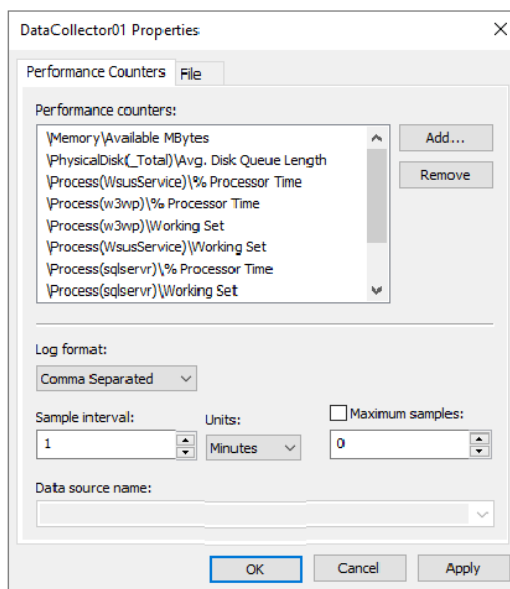


Рис. 3.25 – Налаштування Data Collector.

Приклади спостережень. На основі зібраних даних було отримано такі показники для WSUS-REPL-2019:

- Загальне навантаження CPU становило 8,1%, при цьому служби WsusService і w3wp показали 0% використання, що вказує на відсутність пікових навантажень. Процес sqlservr використовував 1,56% CPU і 2271 МБ пам'яті, що є очікуваним для бази SUSDB.
- Вільна пам'ять залишалася стабільною на рівні 4,5 ГБ, а середня довжина черги на диск (Avg. Disk Queue Length) дорівнювала 0, що свідчить про відсутність затримок у дискових операціях.

Ці результати підтвердили ефективну роботу сервера під час тестового навантаження.

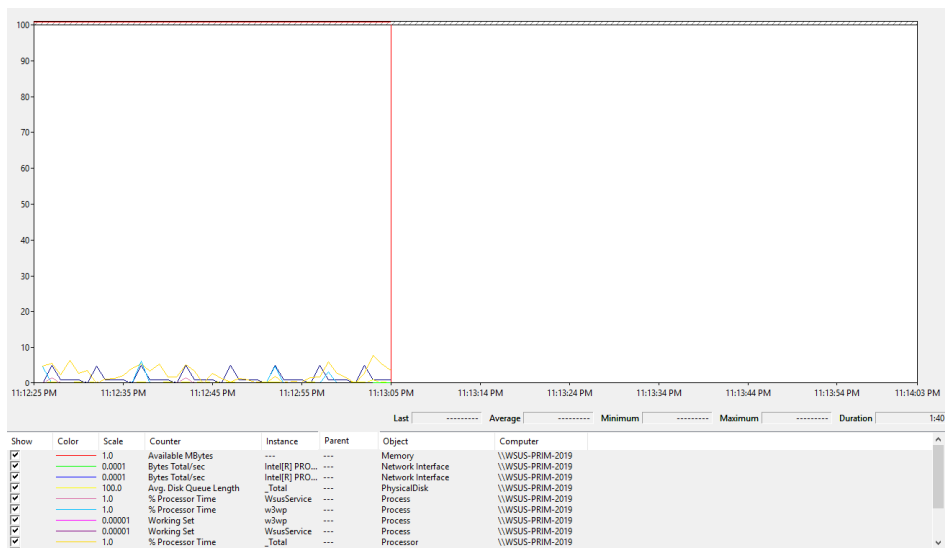


Рис. 3.26 – Моніторинг ресурсів в реальному часі.

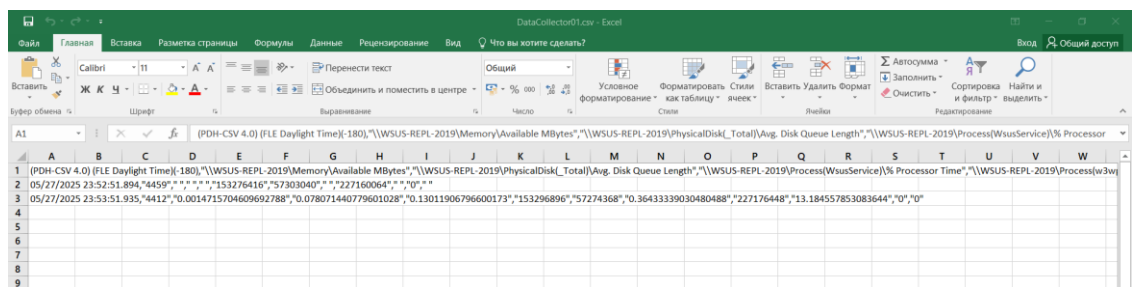


Рис. 3.27 – Перегляд автоматично створеного логу через Excel.

Моніторинг продуктивності через Perfmon на серверах WSUS-PRIM-2019 і WSUS-REPL-2019 показав стабільну роботу ключових компонентів без ознак перевантаження. Показники CPU, пам'яті та дискової активності залишалися в межах норми, що підтвердило здатність інфраструктури в домені kostiuk.net обробляти оновлення в рамках тестового навантаження. Збережені CSV-логи дозволяють проводити подальший аналіз продуктивності для порівняння з іншими циклами.

Висновки до розділу 3

У розділі 3 розглянуто процес адміністрування, моніторингу та аналізу системи Patch Management у доменному середовищі kostiuk.net, що охопив ключові етапи централізованого управління оновленнями. Структурування груп клієнтів

у WSUS забезпечило гнучкий розподіл пристроїв за ролями та ОС, ізоляцію критичних вузлів і можливість попереднього тестування оновлень на окремих клієнтах, зокрема Win10-1 і Win10-2, перед масовим розгортанням.

Ручне схвалення оновлень дозволило уникнути потенційних ризиків, пов'язаних із автоматизацією, забезпечивши поетапне впровадження, зокрема шляхом попереднього тестування оновлення KB5055518 на окремій машині перед застосуванням до групи Win10-Standard.

Моніторинг стану оновлень через звіти WSUS та SQL-запити до бази SUSDB підтвердив стабільність інфраструктури: усі клієнти були синхронізовані, а дані звітів у GUI та SQL збігалися. Застосування PowerShell-скриптів дало змогу автоматизувати збір інформації про статус клієнтів і оновлень, зокрема виявивши два актуальні оновлення для групи Win11-Standard. Водночас обмеження WSUS API вимагали паралельного використання SQL-аналітики.

Моніторинг продуктивності серверів за допомогою Performance Monitor (Perfmon) підтвердив ефективну роботу основного та резервного WSUS-серверів. Навантаження на процесор (CPU) не перевищувало 8,1%, споживання пам'яті службою sqlservr складало 2271 МБ, а середня довжина черги на диску залишалася на рівні нуля, що свідчило про відсутність затримок.

Таким чином, розділ підтвердив ефективність обраної моделі адміністрування та моніторингу системи Patch Management у домені kostiuk.net. Збережені звіти, CSV-логи та шаблони моніторингу створили основу для подальшого аналізу продуктивності та оптимізації системи в рамках наступного етапу проєкту.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				117
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 4 ТЕСТУВАННЯ, ОЦІНКА ПРОДУКТИВНОСТІ ТА АНАЛІЗ ЕФЕКТИВНОСТІ СИСТЕМИ

4.1 Перевірка застосування базових групових політик (GPO)

Для забезпечення коректної роботи доменної інфраструктури kostiuk.net було проведено перевірку застосування базових групових політик (GPO), налаштованих раніше, як описано у п. 2.3.5, одразу після їхнього створення. Ця перевірка охопила клієнтську машину Win-10-1-KOST, а також сервери WSUS-PRIM-2019 і DC-SRV-2022, що дало змогу підтвердити ефективність політик у сфері безпеки, доступу до ресурсів і централізованого керування. Такий підхід забезпечив стабільність системи перед її подальшим використанням.

Політика паролів PasswordPolicy-Branch-1. Політика PasswordPolicy-Branch-1 була створена для клієнтських машин у філії Branch-21-7-1 і встановлює мінімальну довжину пароля на рівні 10 символів. Її мета полягає у підвищенні безпеки домену шляхом ускладнення підбору паролів, що захищає облікові записи від несанкціонованого доступу. Перевірка цієї політики проводилася на машині Win-10-1-KOST шляхом спроби змінити пароль на інший, менший за 10 символів, що завершилося невдачею, підтвердивши коректність застосування вимоги.

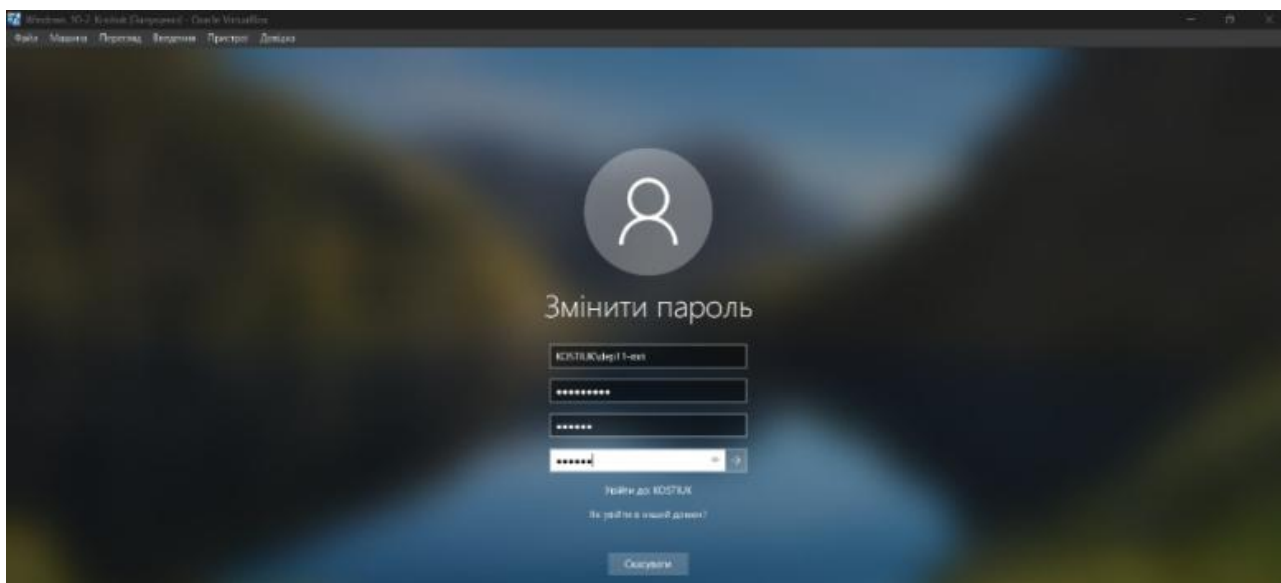


Рис. 4.1 – Спроба зміни пароля.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				118
Змн.	Арк.	№ докум.	Підпис	Дата		

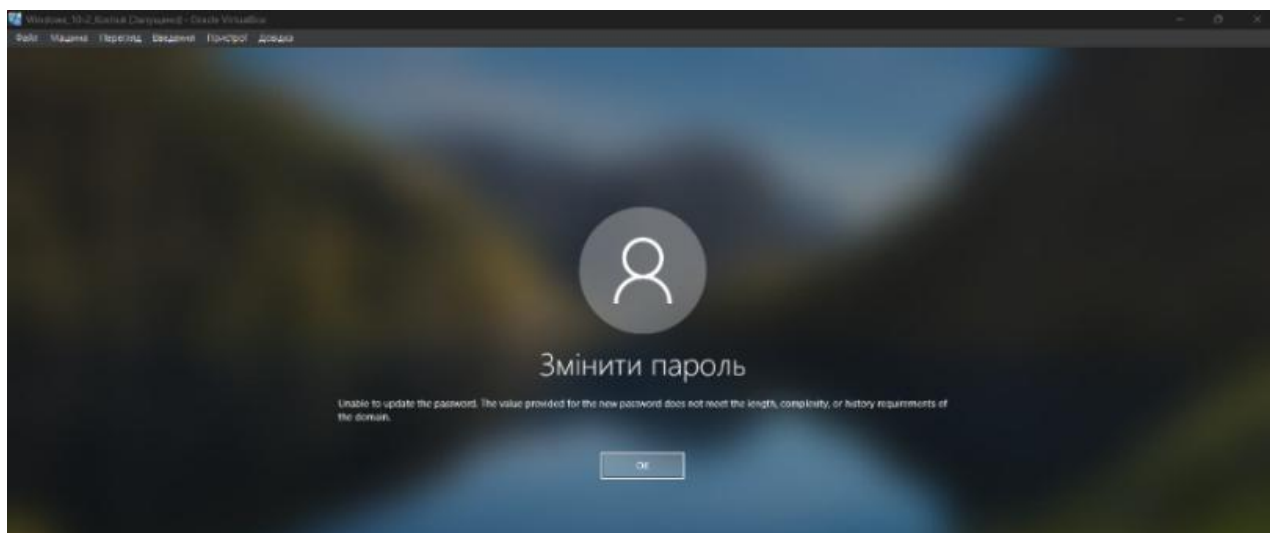


Рис. 4.2 – Заборона зміни пароля, через невідповідність умовам.

Політика обмеження входу Default Domain Policy. Політика Default Domain Policy, застосована до всього домену, встановлює ліміт спроб входу та обмеження розблокування облікових записів лише адміністратором. Її призначення — захистити інфраструктуру від атак методом грубої сили та забезпечити централізований контроль доступу. Перевірка проводилася на Win-10-1-KOST шляхом введення трьох неправильних паролів поспіль, після чого обліковий запис заблокувався, а його розблокування було виконано вручну адміністратором, що підтвердило коректність налаштувань.

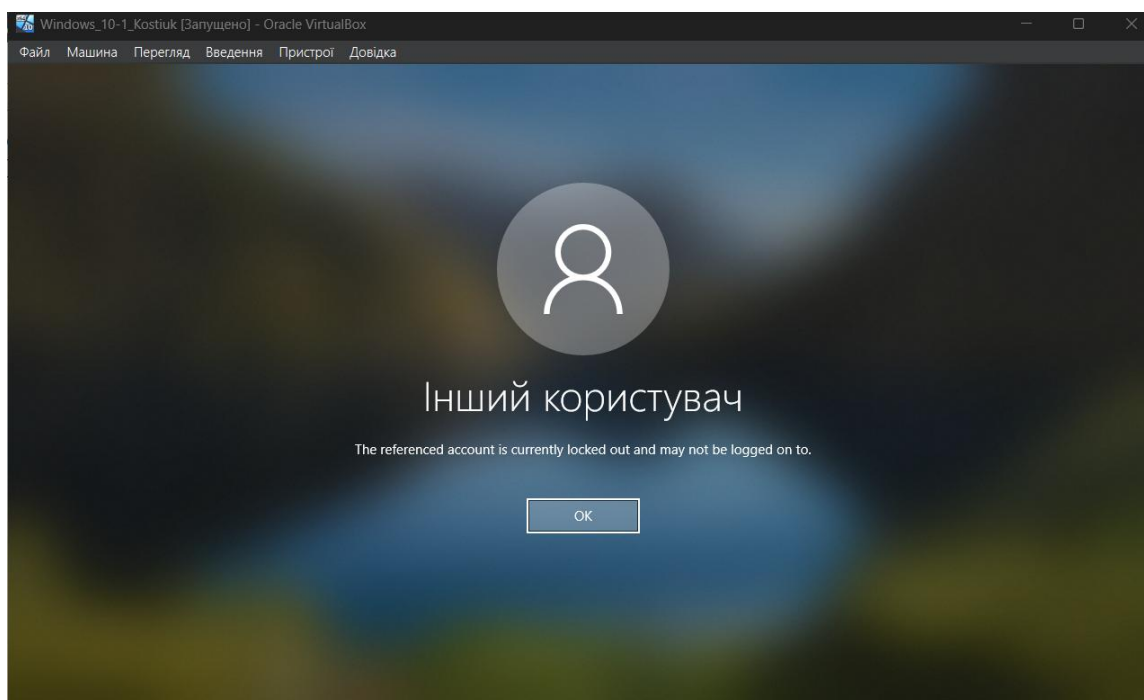


Рис. 4.3 – Блокування облікового запису через 3 невдалі спроби.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				119
Змн.	Арк.	№ докум.	Підпис	Дата		

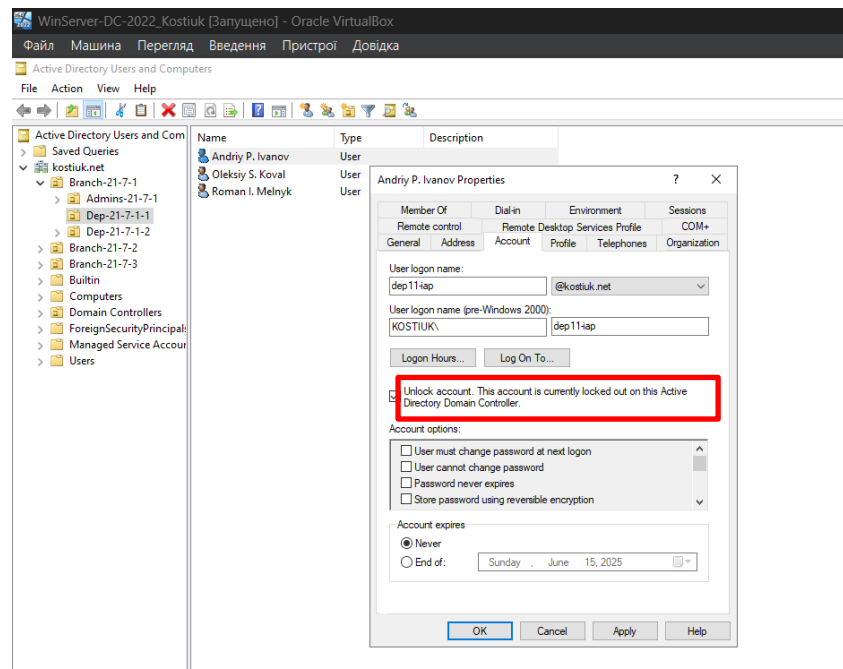


Рис. 4.4 – Ручне розблокування облікового запису.

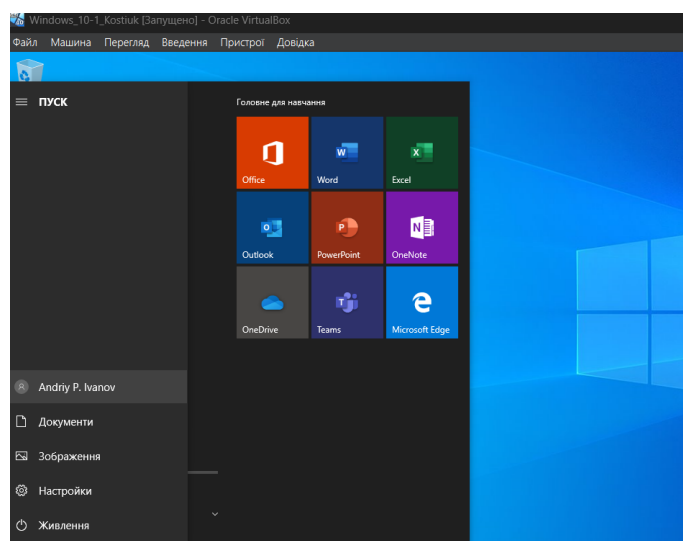


Рис. 4.5 – Перевірка працездатності облікового запису.

Політики доступу до мережевих дисків MapDrive-Admin і MapDrive-ALL. Політики MapDrive-Admin і MapDrive-ALL призначені для організації доступу до мережевих дисків у філіях Branch-21-7-1, Branch-21-7-2 і Branch-21-7-3. MapDrive-Admin забезпечує доступ до певних папок лише для локальних адміністраторів із групи Admins-21-7-1, тоді як MapDrive-ALL надає доступ до іншої папки для всіх користувачів, що сприяє диференційованому управлінню правами. Перевірка здійснювалася на Win-10-1-KOST через тестування доступу до дисків із різних облікових записів: адміністратора з Admins-21-7-1 і звичайного

користувача, що підтвердило наявність і коректний доступ до відповідних дисків.

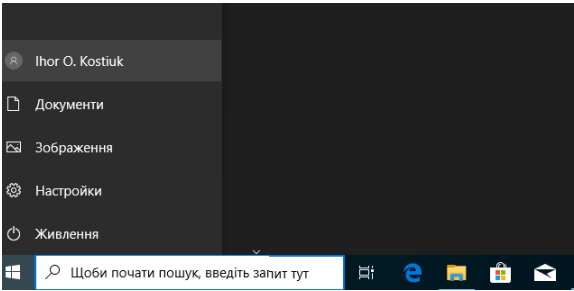


Рис. 4.6 – Вхід в обліковий запис локального адміністратора.

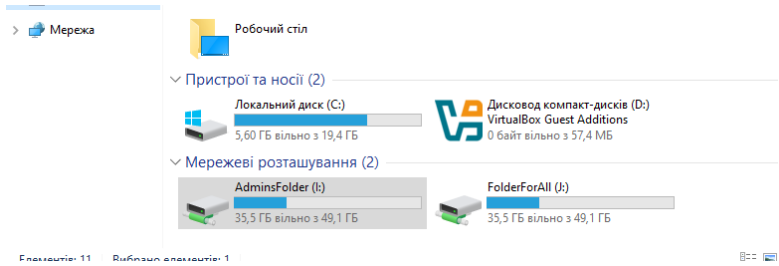


Рис. 4.7 – Наявність обох мережевих дисків.

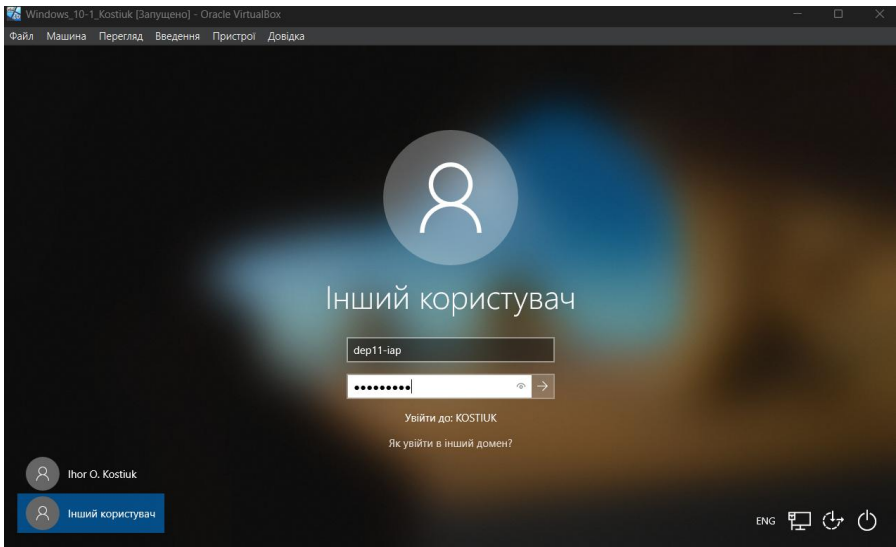


Рис. 4.8 – Вхід з облікового запису звичайного користувача.

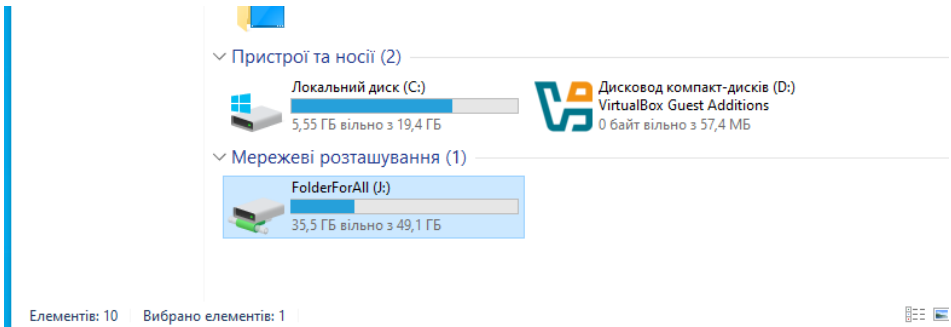


Рис. 4.9 – Наявність лише одного мережевого диску.

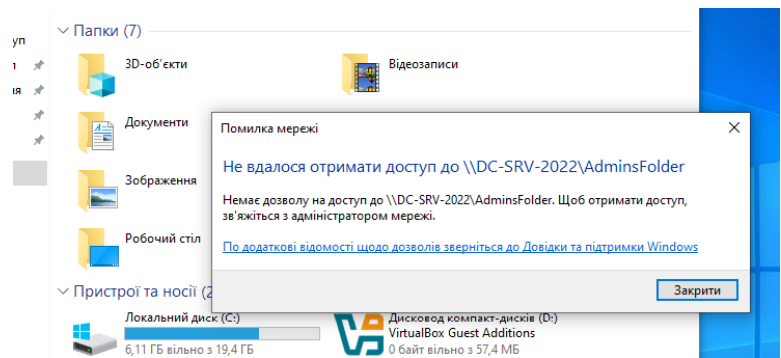


Рис. 4.10 – Спроба доступу до мережевого диску через адресу.

Політика локального входу на серверах. Політика для серверів, застосована до OU Servers, дозволяє локальний вхід лише членам груп локальних адміністраторів на серверах DC-SRV-2022 і WSUS-PRIM-2019. Її мета — обмежити доступ до серверів і підвищити рівень безпеки інфраструктури. Перевірка проводилася шляхом спроб входу на сервери WSUS-PRIM-2019 і DC-SRV-2022 через обліковий запис адміністратора, що завершився успішно, і через звичайний користувацький запис, який був заблокований, що засвідчило коректність налаштувань.

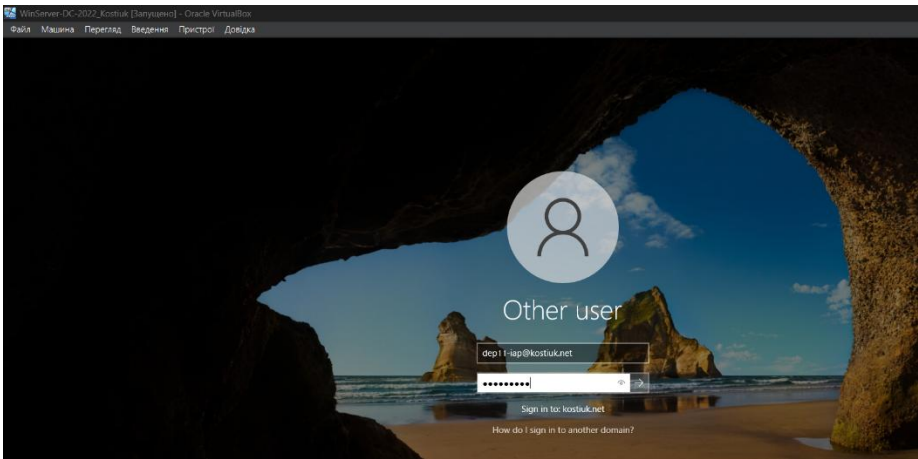


Рис. 4.11 – Введення даних облікового запису звичайного користувача.

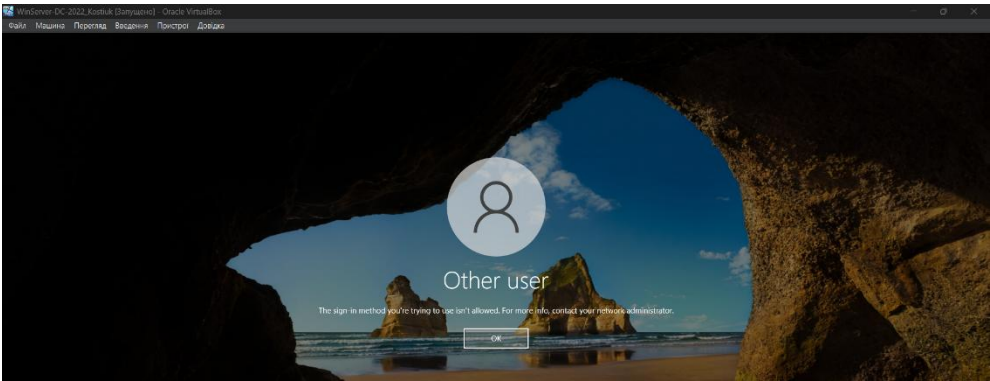


Рис. 4.12 – Заборона доступу до сервера.

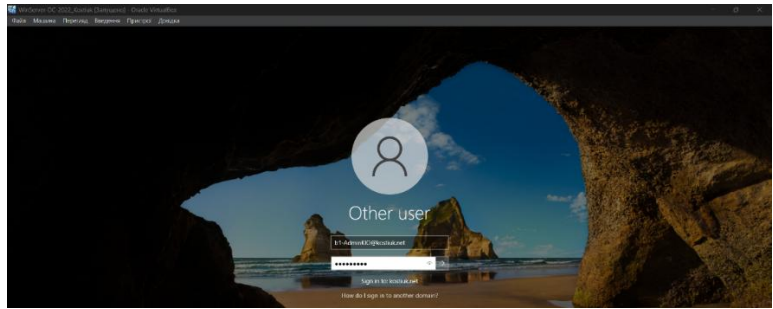


Рис. 4.13 – Введення даних облікового запису локального адміністратора.

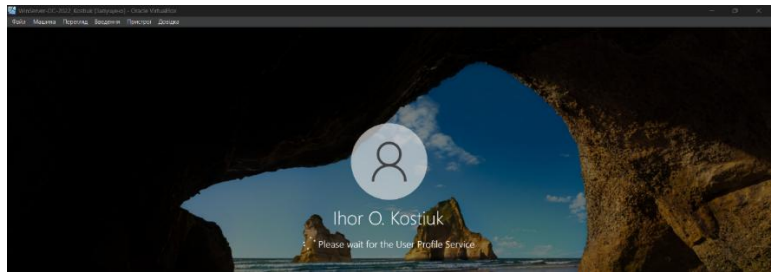


Рис. 4.14 – Успішний вхід до серверу.

Прив’язка GPO до організаційних одиниць. Прив’язка групових політик до відповідних організаційних одиниць, таких як Branch-21-7-1 і Servers, забезпечує їхнє цільове застосування в домені. Ця процедура гарантує, що політики діють лише на призначені об’єкти, що сприяє ефективному управлінню. Перевірка здійснювалася через консоль Group Policy Management, де було підтверджено коректну прив’язку PasswordPolicy-Branch-1 до OU Branch-21-7-1, AdminLogPolicy до OU Servers, а також MapDrive-Admin і MapDrive-ALL до всіх філій.

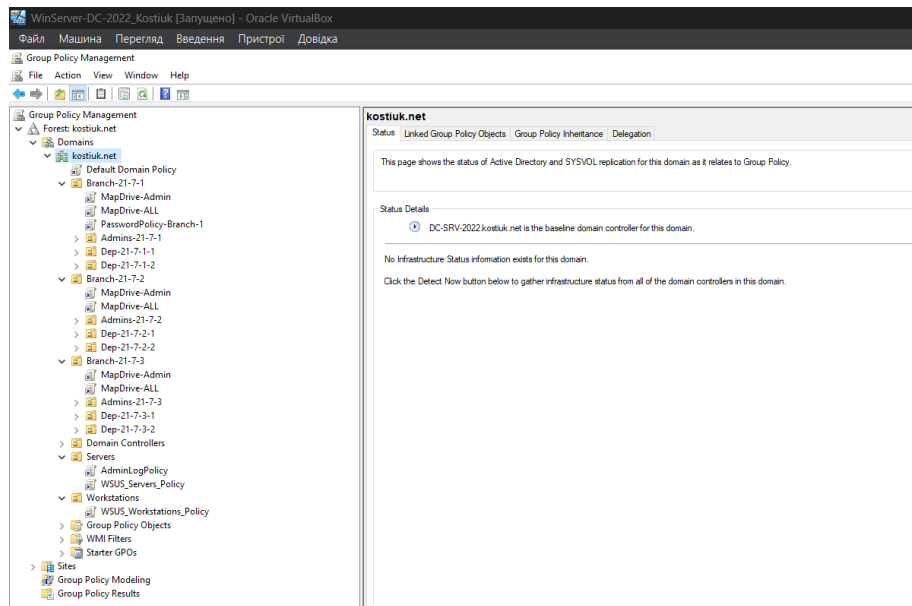


Рис. 4.15 – Перевірка прив’язок GPO.

Отже, результати перевірки свідчать про належну реалізацію GPO, що забезпечує необхідні вимоги безпеки, доступу та управління. Ця конфігурація є придатною до подальшого використання, а також може слугувати базою для масштабування доменної інфраструктури.

4.2 Тестування працездатності оновлень у ключових етапах

4.2.1 Перевірка оновлень після початкового налаштування WSUS

Після завершення базової конфігурації WSUS-сервера WSUS-PRIM-2019 (див. п. 2.4.3) було проведено початкове тестування працездатності системи Patch Management шляхом ручного схвалення та застосування оновлення. Мета полягала у підтвердженні коректної взаємодії між WSUS і клієнтськими пристроями, а також у перевірці доставки та встановлення оновлення в ізольованому середовищі до впровадження HTTPS (п. 2.5) і резервного сервера (п. 2.6). Це дало змогу оцінити базову функціональність системи на ранньому етапі.

Контекст тестування. Тестування проводилося після успішної синхронізації WSUS-PRIM-2019 із Microsoft Update, налаштування групових політик (WSUS_Servers_Policy, WSUS_Workstations_Policy) і появи всіх машин у консолі WSUS. Такий підхід забезпечив готовність інфраструктури до першого етапу розгортання оновлень, спираючись на попередні етапи структуризації груп (п. 3.1).

Вибір оновлення та методика. Для тестування обрано оновлення Security Update KB5058379, яке належить до критичних оновлень безпеки для Windows 10 Pro. Оновлення було вручну схвалено в консолі WSUS для групи Win10-2, що включала лише клієнт Win10-2-KOST. Використання ізольованої групи дало змогу уникнути ризиків для інших пристроїв і перевірити працездатність у контрольованих умовах. Схвалення виконувалося через контекстне меню оновлення (Approve...), із зазначенням цільової групи Win10-2, після чого на клієнті було ініційовано ручну перевірку оновлень.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				124
Змн.	Арк.	№ докум.	Підпис	Дата		

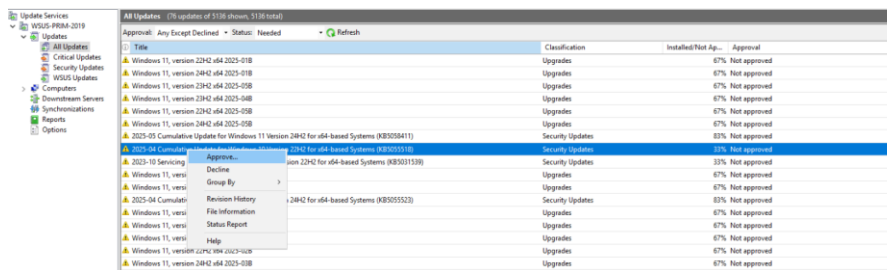


Рис. 4.16 – Схвалення оновлення через контекстне меню.

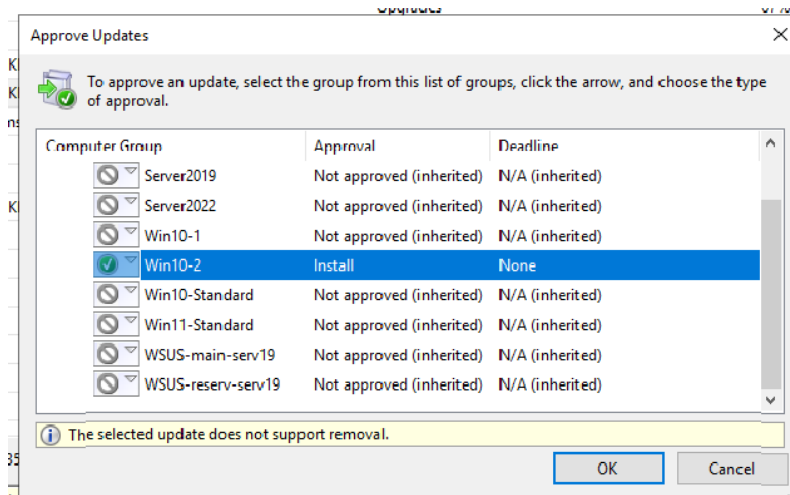


Рис. 4.17 – Вибір групи для схвалення.

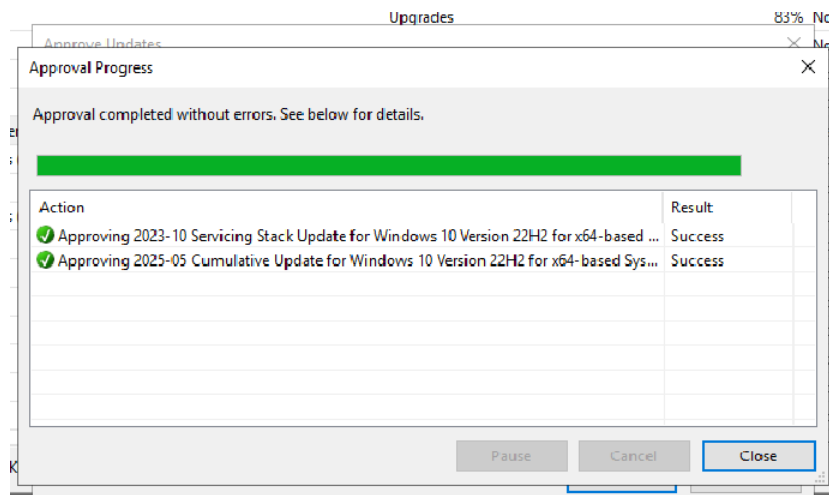


Рис. 4.18 – Повідомлення про успішність операції.

Результати тестування. Перевірка підтвердила успішне застосування оновлення:

- У консолі WSUS статус оновлення KB5058379 для Win10-2-KOST змінився на "Installed".

Title	Classification	Installed/Not Ap...	Approval
Windows 11, version 22H2 x64 2023-04B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2023-05B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2024-01B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2024-12B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2024-01B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2024-02B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2024-02B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2024-03B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2024-03B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2023-12B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2023-11B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2023-07B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2023-06B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2023-08B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2023-09B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2023-10B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2023-11B	Upgrades	83%	Not approved
Windows 11, version 22H2 x64 2023-10B	Upgrades	83%	Not approved
2025-05 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5058379)	Security Updates	3%	Install (1/10)

2025-05 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5058379)

This update supersedes another update. Before you decline any superseded update, we recommend that you verify it is no longer needed by any computers. To do so, approve the superseding update first.

Status:

- Computers with errors: 0
- Computers needing this update: 1
- Computers installed/not applicable: 2
- Computers with no status: 3

MSRC severity: Critical

MSRC number: None

Release date: Tuesday, May 13, 2025

KB article numbers: 5058379

Рис. 4.19 – Оновлення статусу.

- На клієнтському пристрої Win10-2-KOST оновлення з’явилося в Центрі оновлень під час завантаження та встановлення.

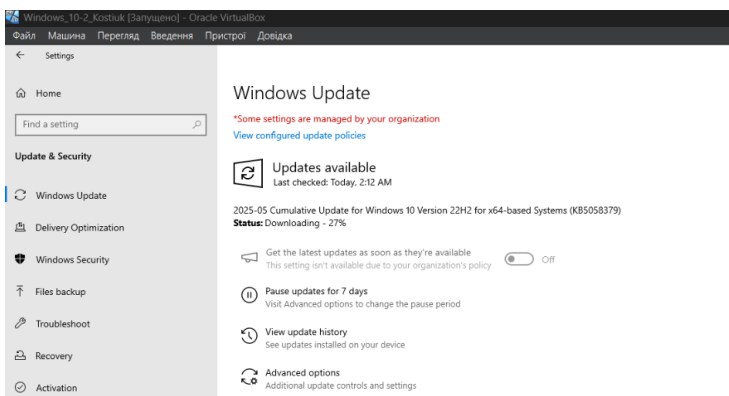


Рис. 4.20 – Проведення оновлення на робочій станції.

- Через звіт Update Tabular Status for Approved Updates було підтверджено, що оновлення належить до класифікації Security, застосовано для групи Win10-2 із статусом INSTALLED.

2025-05 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5058379)

Description:

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

Classification:

Security Updates

Products:

Windows 10, version 1903 and later

MSRC Severity Rating:

Critical

MSRC Number:

None

More Information:

<https://support.microsoft.com/help/5058379>

Approval Summary for: Win10-2

Group	Approval	Deadline	Administrator
Win10-2	Install	None	KOSTIUK\Administrator

Status Summary for 2025-05 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5058379)

The update failed to install on 0 computers

The update is needed by 0 computers

The update is installed/not applicable on 1 computers

The update has no status for 0 computers

Рис. 4.21 – Звіт про вдале встановлення оновлень.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				126
Змн.	Арк.	№ докум.	Підпис	Дата		

- Після встановлення оновлення дані про його статус оновлено під час наступної планової синхронізації з сервером.

All Computers (6 computers of 6 shown, 6 total)				
Status: Any Refresh				
Name	IP Address	Operating System	Installed/Not Applicable Percentage	Last Status Report
win-10-1-kost.kostiuk.net	192.168.7.100	Windows 10 Pro	32%	5/21/2025 10:34 PM
wsus-repl-2019.kostiuk.net	192.168.7.21	Windows Server 2019 Standard	33%	5/22/2025 12:55 AM
win-11-1-kost.kostiuk.net	192.168.7.101	Windows 10 Pro	33%	5/21/2025 11:07 PM
wsus-prim-2019.kostiuk.net	192.168.7.20	Windows Server 2019 Standard	99%	5/23/2025 2:04 AM
dc-srv-2022.kostiuk.net	192.168.7.10	Windows Server 2022 Standard	100%	5/23/2025 1:35 AM
win-10-2-kost.kostiuk.net	192.168.7.102	Windows 10 Pro	100%	5/23/2025 2:40 AM

Рис. 4.22 – Надання оновленої інформації про стан оновлень.

Ці результати свідчать про коректну роботу WSUS, GPO та служби Windows Update.

Тестування працездатності WSUS після початкового налаштування підтвердило успішну доставку та встановлення оновлення KB5058379 на клієнтському пристрої Win10-2-KOST. Коректна взаємодія між сервером і клієнтом дозволила перейти до наступних етапів впровадження, зокрема налаштування HTTPS і резервного сервера, без необхідності повторної перевірки цього ланцюга на даному етапі.

4.2.2 Перевірка після налаштування HTTPS-з'єднання для WSUS

Після реалізації захищеного з'єднання між WSUS-сервером WSUS-PRIM-2019 і клієнтами (див. п. 2.5) було проведено тестування працездатності системи Patch Management із використанням TLS/SSL-комунікації. Мета полягала у перевірці доставки оновлень через HTTPS на порті 8531 після розгортання самопідписаного TLS-сертифіката та оновлення групових політик. Це дало змогу оцінити стабільність і безпеку каналу зв'язку перед подальшим розширенням інфраструктури, зокрема підключенням резервного сервера (п. 2.6).

Контекст і мета перевірки. Тестування проводилося після завершення налаштувань HTTPS і слугувало логічним продовженням попередньої перевірки працездатності (див. п. 4.2.1). Основна мета полягала у підтвердженні, що оновлення коректно доставляються клієнтам через захищений канал, а звітність залишається стабільною.

Підготовчі дії. Перед тестуванням було виконано низку змін для забезпечення HTTPS-з'єднання. Зокрема, на WSUS-PRIM-2019 встановлено самопідписаний TLS-сертифікат, який розгорнуто через групові політики для всіх клієнтів у домені kostiuk.net. У параметрі "Specify intranet Microsoft update service location" групової політики WSUS_Servers_Policy змінено адресу з `http://wsus.kostiuk.net:8530` на `https://wsus.kostiuk.net:8531`. Для застосування змін на клієнтських машинах виконано команду `gpupdate /force`. Такий підхід забезпечив безпечну передачу даних і сумісність із новими налаштуваннями.

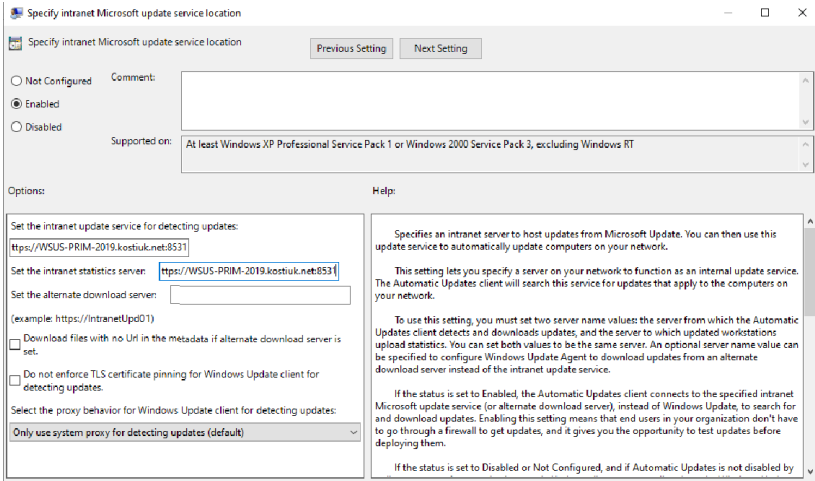


Рис. 4.23 – Оновлення адреси в "Specify intranet Microsoft update service location".

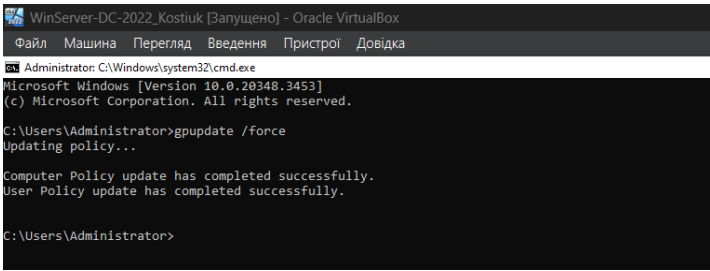


Рис. 4.24 – Примусове оновлення групових політик.

Вибір оновлення і групи. Для тестування обрано оновлення Security Update KB5003711, яке належить до критичних оновлень безпеки. Оновлення було схвалено вручну через інтерфейс WSUS-консолі (пункт Approve...) для групи Server2019, що включає сервери WSUS-PRIM-2019 і WSUS-REPL-2019. Перевірка проводилася на обох серверах, зокрема WSUS-REPL-2019, щоб оцінити стабільність HTTPS-з'єднання в умовах критичних вузлів. Вибір серверної групи дозволив перевірити працездатність у реальних умовах експлуатації.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				128
Змн.	Арк.	№ докум.	Підпис	Дата		

Методика перевірки. Схвалення оновлення здійснювалося через інтерфейс WSUS-консолі шляхом вибору пункту Approve... і призначення його групі Server2019. Перевірка доставки включала:

- Аналіз статусу оновлення в консолі WSUS.
- Спостереження за завантаженням і встановленням через Центр оновлень Windows на WSUS-REPL-2019.
- Підтвердження результатів через звіт Update Tabular Status for Approved Updates.

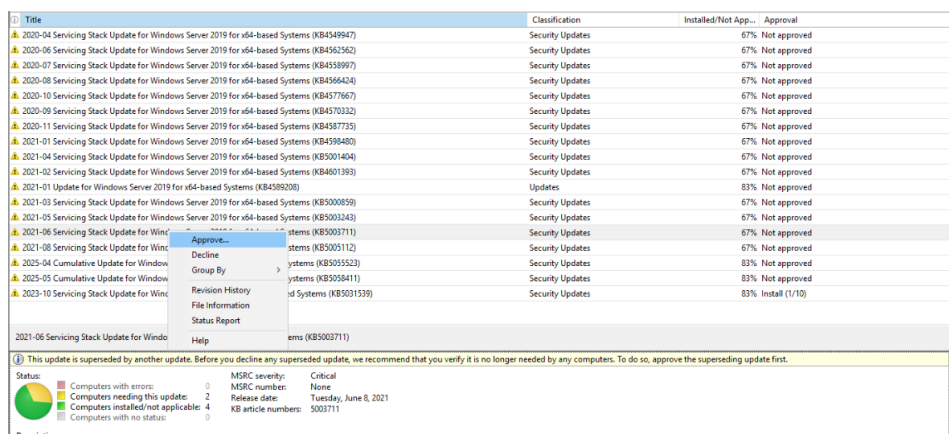


Рис. 4.25 – Схвалення оновлення через контекстне меню.

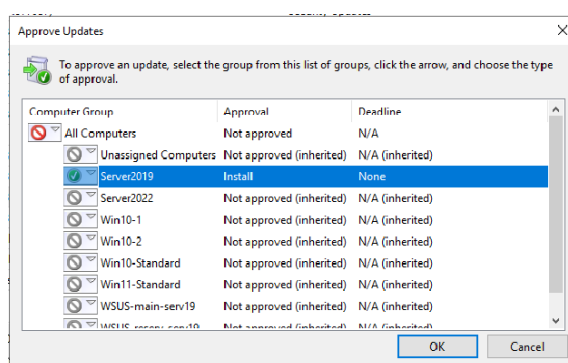


Рис. 4.26 – Вибір групи для схвалення.

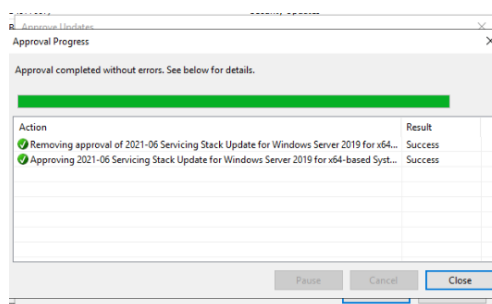


Рис. 4.27 – Повідомлення про успішність операції.

Результати. Тестування засвідчило коректну роботу WSUS у режимі HTTPS:

- Оновлення KB5003711 було завантажено та успішно встановлено на обох серверах групи Server2019.



Рис. 4.28 – Встановлення оновлень на резервному WSUS сервері.

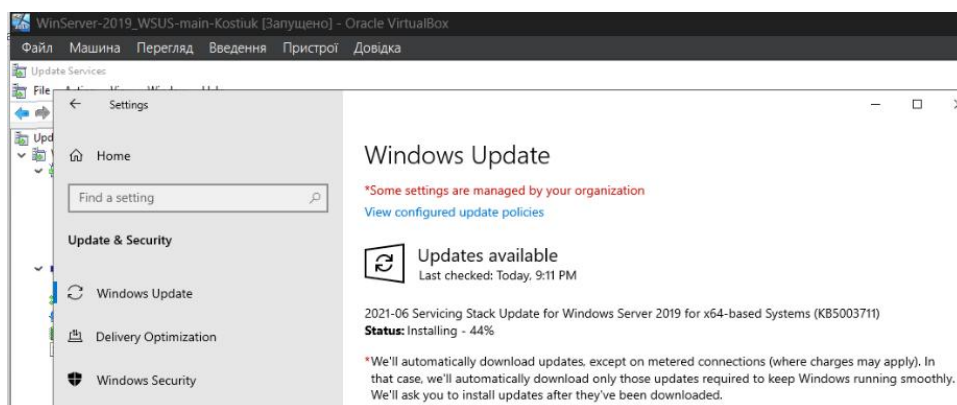


Рис. 4.29 – Встановлення оновлень на основному WSUS сервері.

- У консолі WSUS статус оновлення для WSUS-PRIM-2019 і WSUS-REPL-2019 змінився на "Installed".

All Updates (5139 updates of 5154 shown, 5154 total)				
Approval: Any Except Declined		Status: Any		Refresh
Title	Classification	Installed/Not Appl.	Approval	
2021-06 Servicing Stack Update for Windows 10 Version 1909 for x64-based Systems (KB5003974)	Security Updates	100%	Not approved	
2021-06 Servicing Stack Update for Windows 10 Version 1909 for x86-based Systems (KB5003710)	Security Updates	100%	Not approved	
2021-06 Servicing Stack Update for Windows 10 Version 1909 for x86-based Systems (KB5003974)	Security Updates	100%	Not approved	
2021-06 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB5003711)	Security Updates	100%	Install (1/10)	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows 10 Version 1809 for ARM64 (KB5004228)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for ARM64 (KB5004228)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1909 (KB5003539)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1909 for ARM64 (KB5003539)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1909 for x64 (KB5003539)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 2004 (KB5003537)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 20H2 for ARM64 (KB5003537)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 20H2 for x64 (KB5003537)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H1 (KB5003537)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H1 for ARM64 (KB5003537)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 21H1 for x64 (KB5003537)	Updates	100%	Not approved	
2021-07 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1809 (KB5004228)	Updates	100%	Not approved	
2021-06 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB5003711)	Updates	100%	Not approved	

Рис. 4.30 – Оновлення статусу.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		130

- У звіті Update Tabular Status for Approved Updates підтверджено статус INSTALLED, класифікацію "Security Updates" і цільову групу Server2019.

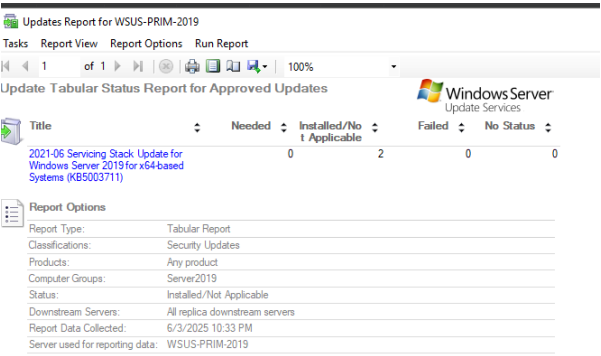


Рис. 4.31 – Звіт про вдале встановлення оновлень.

- Зв’язок через HTTPS залишився стабільним, без попереджень про недійсний сертифікат чи з’єднання, що свідчить про коректне розгортання самопідписаного TLS-сертифіката.
- Час встановлення відповідав очікуваним часовим рамкам стандартного Windows Update-циклу.

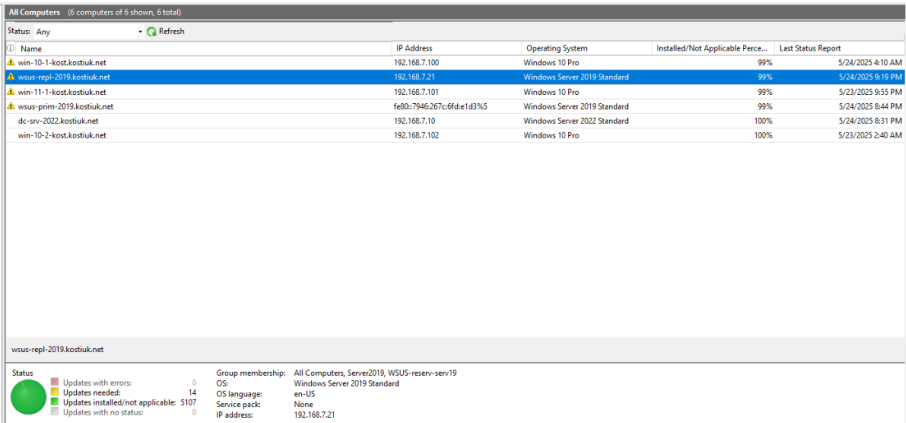


Рис. 4.32 – Надання оновленої інформації про стан оновлень.

Тестування після налаштування HTTPS-з’єднання підтвердило стабільну роботу WSUS у домені kostiuuk.net із використанням захищеного каналу зв’язку на порті 8531. Успішна доставка оновлення KB5003711 на сервери групи Server2019, включно з WSUS-PRIM-2019 і WSUS-REPL-2019, засвідчила правильність розгортання групових політик та сумісність із самопідписаним TLS-сертифікатом. Відсутність проблем із з’єднанням чи довірою до сертифіката дозволила перейти до наступного етапу — підключення резервного сервера (п. 4.2.3).

4.2.3 Тестування після підключення резервного WSUS-сервера

Після налаштування резервного сервера WSUS-REPL-2019 у режимі реплікації основного WSUS-PRIM-2019 (див. п. 2.6) було проведено тестування її працездатності як джерела оновлень для клієнтів у домені kostiuk.net. Мета полягала у перевірці здатності клієнтів, підключених до репліки, отримувати схвалені оновлення та передавати звіти про їхній статус у консоль WSUS-REPL-2019. Це дало змогу переконатися у відмовостійкості інфраструктури перед її подальшим масштабуванням.

Контекст тестування. Тестування проводилося після завершення налаштувань HTTPS (п. 2.5, 4.2.2) і реплікації (п. 2.6), коли WSUS-REPL-2019 було налаштовано як репліку в режимі read-only, а клієнти перенаправлено на нього для отримання оновлень. Цей етап став логічним завершенням трьохфазного тестування працездатності, що охопило базову конфігурацію, HTTPS і реплікацію.

Підготовчі дії. Перед тестуванням внесено зміни до групової політики WSUS_Workstations_Policy: параметр "Specify intranet Microsoft update service location" оновлено на <https://wsus-repl-2019.kostiuk.net:8531>. Групу Win11-Standard, до якої належить клієнт Win-11-1-KOST, призначено для отримання оновлень через репліку. Для застосування змін виконано команду `gpupdate /force` на клієнтських машинах, після чого очікувалася поява звітів у консолі WSUS-REPL-2019. Такий підхід дозволив перенаправити клієнтів на резервний сервер, щоб перевірити коректність реплікації в реальних умовах.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				132
Змн.	Арк.	№ докум.	Підпис	Дата		

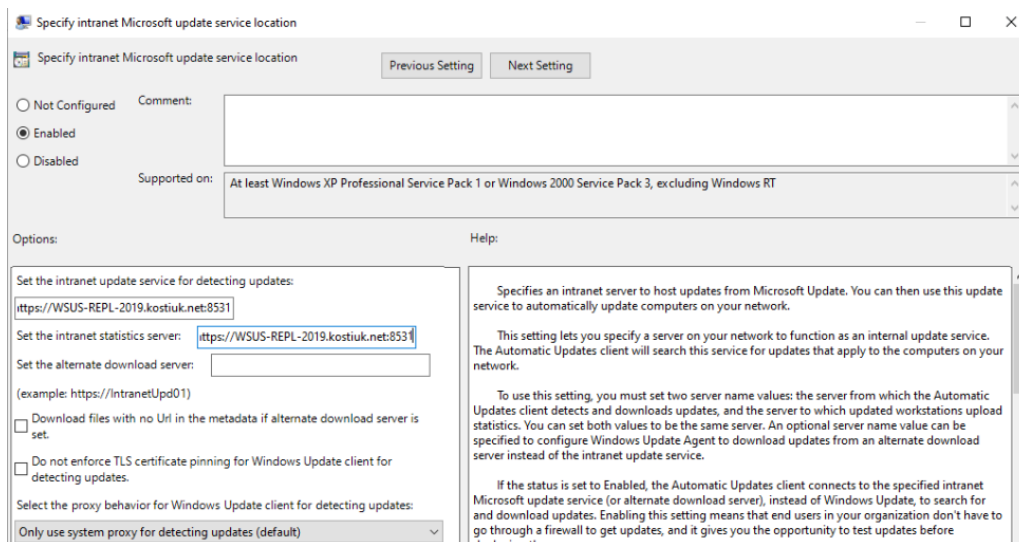


Рис. 4.33 – Оновлення адреси в групових політиках.

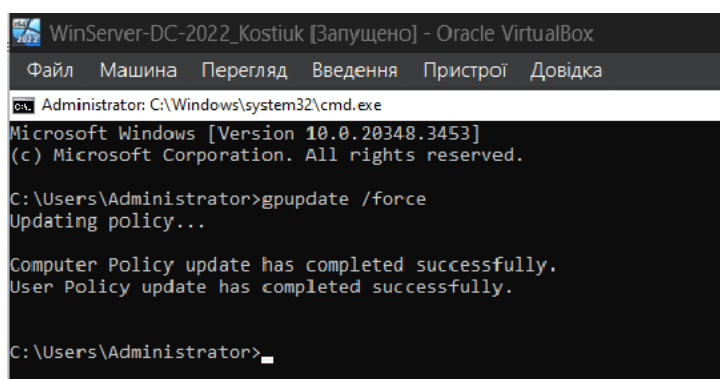


Рис. 4.34 – Примусове оновлення групових політик.

Вибір оновлення для перевірки. Для тестування обрано оновлення Security Updates KB5058411, яке належить до критичних оновлень безпеки для Windows 11. Оновлення було відфільтровано за статусом "Needed" у консолі WSUS-PRIM-2019 і схвалено для групи Win11-Standard. Вибір клієнта з Windows 11 уможливив оцінку роботи репліки в контексті однієї з ключових операційних систем домену.

Методика перевірки

Оскільки WSUS-REPL-2019 працює в режимі read-only, схвалення оновлення здійснювалося на WSUS-PRIM-2019 через інтерфейс WSUS-консолі (пункт Approve... → Win11-Standard). Методика перевірки включала:

- Очікування синхронізації між WSUS-PRIM-2019 і WSUS-REPL-2019.
- Аналіз появи оновлення в консолі WSUS-REPL-2019.

- Перевірку статусу клієнта Win-11-1-KOST у звіті Update Tabular Status for Approved Updates на WSUS-REPL-2019.
- Спостереження за завантаженням і встановленням оновлення через Центр оновлень Windows на Win-11-1-KOST.
- Перегляд дат синхронізації через WSUS GUI.

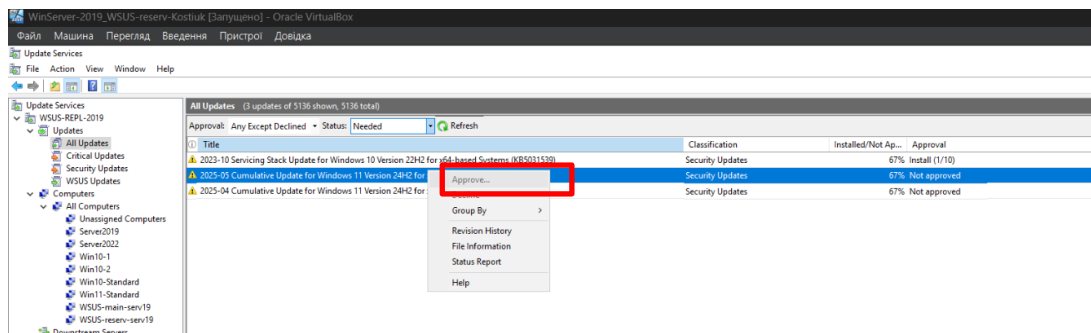


Рис. 4.35 – Перевірка працездатності режиму «read-only».

Результати перевірки. Тестування засвідчило коректну роботу реплікації:

- Після схвалення на WSUS-PRIM-2019 оновлення KB5058411 з'явилося в консолі WSUS-REPL-2019.

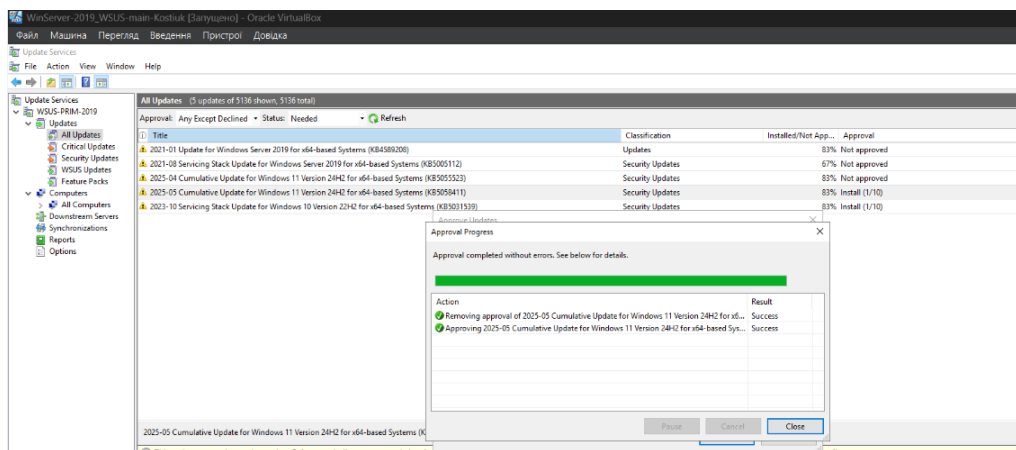


Рис. 4.36 – Схвалення оновлення через основний сервер.

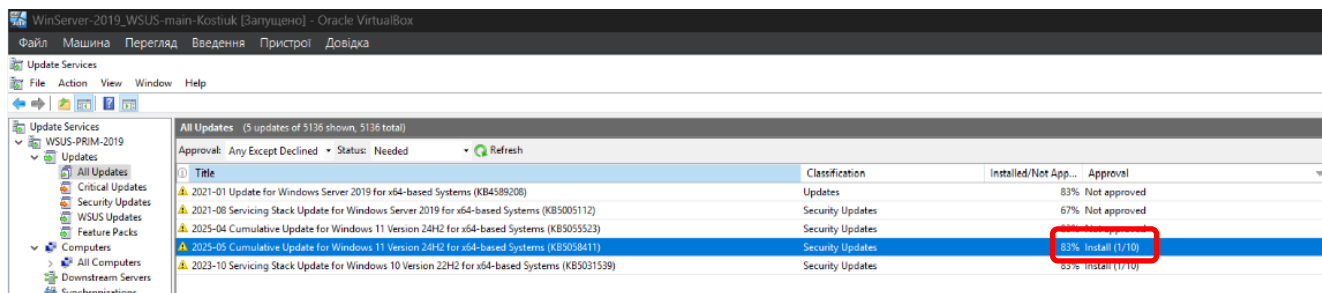


Рис. 4.37 – Перевірка схвалення оновлення на резервному сервері.

- Клієнт Win-11-1-KOST, підключений до репліки, успішно завантажив і встановив оновлення.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				134
Змн.	Арк.	№ докум.	Підпис	Дата		

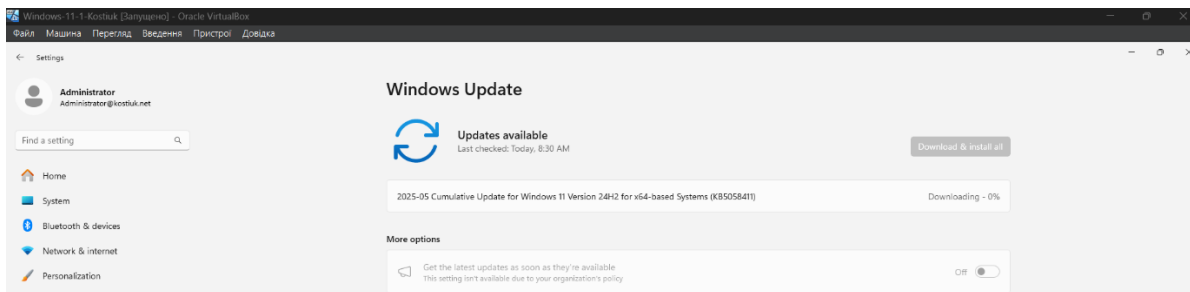


Рис. 4.38 – Завантаження оновлення на робочій станції Win-11-1-KOST.

- У звіті Update Tabular Status for Approved Updates на WSUS-REPL-2019 статус оновлення змінився на "Installed" із прив'язкою до групи Win11-Standard.

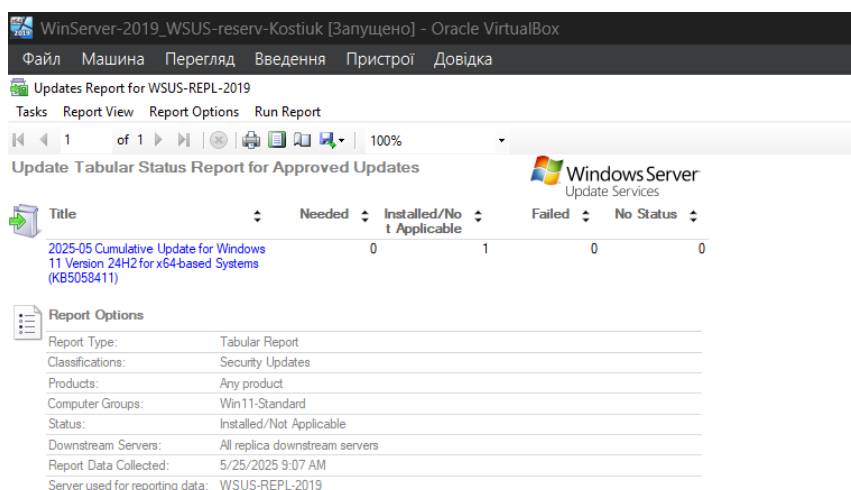


Рис. 4.39 - Звіт про вдале встановлення оновлень.

- Дати LastSync і LastReported, переглянуті через WSUS GUI, оновилися, що підтвердило стабільну синхронізацію.

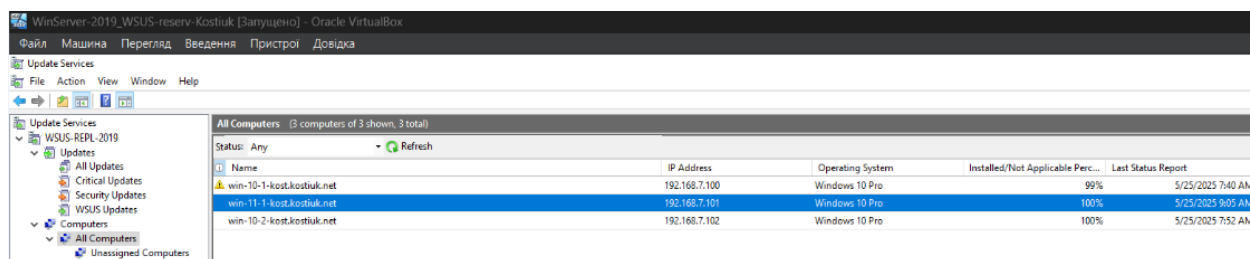


Рис. 4.40 - Надання інформації про стан оновлень на резервний сервер.

- Після встановлення оновлення дані про його статус оновилися на WSUS-REPL-2019, після чого синхронізувалися з WSUS-PRIM-2019, де також було оновлено інформацію.

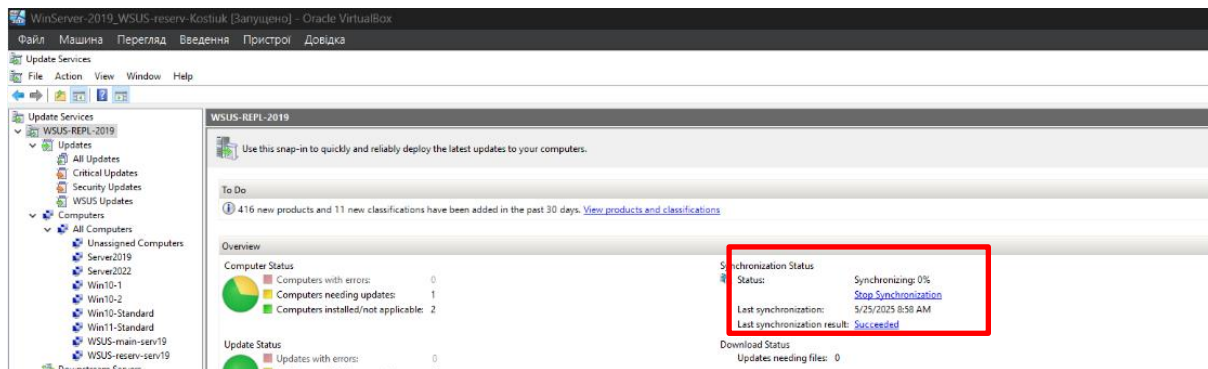


Рис. 4.41 – Проведення синхронізації з основним сервером.

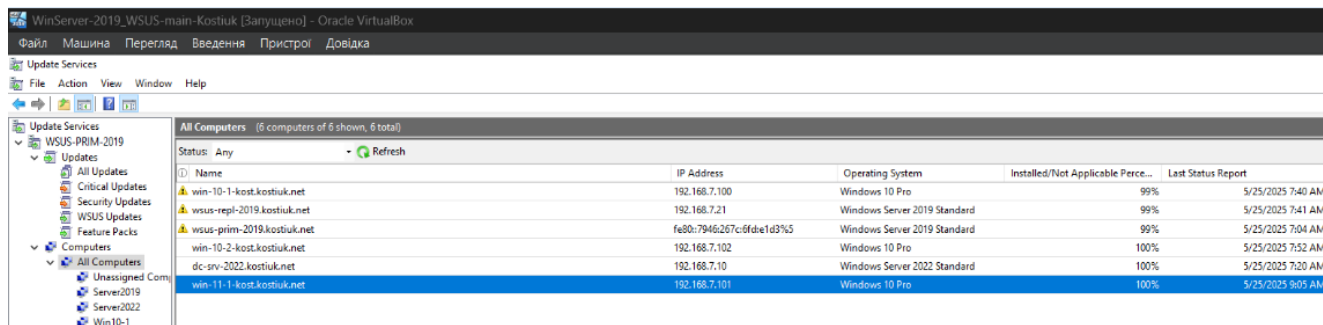


Рис. 4.42 - Надання інформації про стан оновлень на основний сервер.

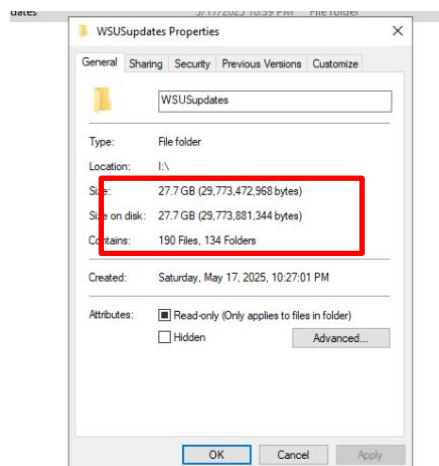


Рис. 4.43 – Перевірка завантаження оновлень на дисковий простір серверів.

Проведене тестування підтвердило, що WSUS-REPL-2019 у режимі read-only повноцінно виконує функції джерела оновлень для клієнтів у домені kostiuk.net. Схвалене на основному сервері оновлення KB5058411 було коректно синхронізоване з реплікою, а клієнт Win-11-1-KOST успішно отримав і встановив його без затримок. Стабільна звітність клієнта в репліку, оновлення статусів і синхронізація даних із основним сервером підтвердили правильність налаштування інфраструктури. Це завершило трьохетапну перевірку працездатності си-

стеми Patch Management (див. п. 4.2.1–4.2.2) і підтвердило готовність до подальшого масштабування, зокрема розподілу навантаження між серверами, зберігаючи централізоване керування оновленнями через основний сервер.

4.3 Оцінка ефективності продуктивності після впровадження

4.3.1 Показники продуктивності до запуску оновлень

Перед початком масового схвалення та розгортання оновлень у домені kostiuk.net було проведено базове тестування продуктивності WSUS-серверів WSUS-PRIM-2019 та WSUS-REPL-2019 з використанням Performance Monitor (Perfmon). Метою цього етапу було зафіксувати типові значення навантаження системних ресурсів у стані відсутності активних оновлень, щоб у наступних підпунктах порівняти їх із результатами активної фази розгортання. Це дало змогу встановити еталонні показники для оцінки впливу оновлень на інфраструктуру.

Контекст і методика. Моніторинг проводився до запуску оновлень. Обидва сервери були повністю налаштовані, із увімкненими HTTPS, груповими політиками та реплікою, але перебували в стані "спокою", коли оновлення не схвалювалися й не доставлялися клієнтам. Збір даних здійснювався через Perfmon із використанням двох підходів: моніторингу в реальному часі та Data Collector Sets, основний аналіз базувався на CSV-логах (C:\PerfLogs).

Цілі моніторингу. Основна мета полягала у реєстрації базових значень навантаження на процесор, пам'ять, диск, мережу, а також активності служб WSUS, IIS і SQL Server. Отримані дані мали слугувати еталоном для подальшого порівняння з показниками під час розгортання оновлень, що дозволило оцінити їхній вплив на продуктивність серверів.

Збір даних. Для моніторингу обрано наступні лічильники, вибрані з урахуванням ключових аспектів роботи WSUS:

- **Стан процесора:** % Processor Time (WsusService, w3wp, _Total) — для оцінки навантаження на процесор службами.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				137
Змн.	Арк.	№ докум.	Підпис	Дата		

- **Пам'ять:** Available MBytes — для контролю вільної оперативної пам'яті; Working Set (w3wp, WsusService, sqlservr) — для аналізу використання пам'яті процесами.
- **SQL Server:** Page Life Expectancy — для оцінки ефективності кешу; Batch Requests/sec — для вимірювання рівня запитів.
- **Диск:** Avg. Disk Queue Length — для виявлення затримок у роботі диска.
- **Мережа:** Bytes Total/sec — для моніторингу мережевої активності.
- **IIS/WSUS:** Active Requests, Requests/sec — для оцінки навантаження на веб-сервер.

Спостереження проводилося на WSUS-PRIM-2019 і WSUS-REPL-2019, результати збережено у CSV-логах, доповнених скріншотами графіків Perfmon.

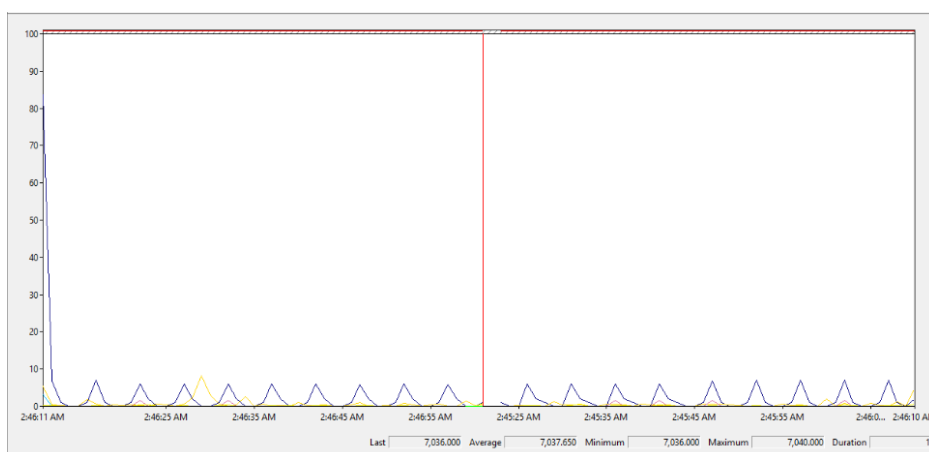


Рис. 4.44 – Графік моніторингу для основного сервера.



Рис. 4.45 – Графік моніторингу для резервного сервера.

Результати. Тестування показало наступні типові значення:

- **WSUS-PRIM-2019:**
 - Available MBytes: 7019 МБ — висока доступність пам'яті.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				138
Змн.	Арк.	№ докум.	Підпис	Дата		

- w3wp Working Set: 198 МБ; WsusService Working Set: 60 МБ — помірне використання пам'яті службами.
- Page Life Expectancy: 14498 сторінок; Batch Requests/sec: 0 — низька активність SQL.
- Bytes Total/sec: 0 Б/с — відсутність мережевої передачі.
- % Processor Time (WsusService, w3wp): 0%; _Total: 1.39% — низьке навантаження на процесор.
- Active Requests: 0 — ненавантажений IIS.

\\WSUS-PRIM-2019			
Memory			
Available MBytes	7,071.000		
Network Interface	Intel[R] PRO_1000 MT Desktop Adapter	Intel[R] PRO_1000 MT Desktop Adapter_2	
Bytes Total/sec	0.000		0.000
PhysicalDisk	_Total		
Avg. Disk Queue Length	0.001		
Process	w3wp	WsusService	
% Processor Time	0.000	0.000	
Working Set	198,688,768.000	60,162,048.000	
Processor	_Total		
% Processor Time	1.393		
SQLServer:Buffer Manager			
Page life expectancy	14,322.000		
SQLServer:SQL Statistics			
Batch Requests/sec	1.993		
W3SVC_W3WP	5260_WsusPool		
Active Requests	---		
File Cache Misses / sec	---		

Рис. 4.46 – Перегляд навантаження у вигляді звіту.

- **WSUS-REPL-2019:**
 - Available MBytes: 4078 МБ — достатня кількість вільної пам'яті.
 - w3wp Working Set: 252 МБ; WsusService Working Set: 135 МБ; sqlservr Working Set: 462 МБ — стабільне використання пам'яті.
 - % Processor Time (WsusService, w3wp, sqlservr): 0%; _Total: 1.5% — мінімальне навантаження.
 - Avg. Disk Queue Length: ≈ 0 — відсутність затримок на диску.

\\WSUS-REPL-2019			
Memory			
Available MBytes	4,014.000		
PhysicalDisk			
Avg. Disk Queue Length	_Total		
	0.003		
Process			
% Processor Time	sqlservr	w3wp	WsusService
	0.000	0.000	0.000
Working Set	462,925,824.000	252,755,968.000	135,819,264.000
Processor			
% Processor Time	_Total		
	1.509		
W3SVC_W3WP	4540_WsusPool		
Active Requests	---		
Requests / Sec	---		

Рис. 4.47 – Перегляд навантаження у вигляді звіту.

Візуально графіки Perfmon демонстрували стабільні мінімальні значення, без значних піків, що підтверджено логами.

Зібрані дані засвідчили, що до запуску оновлень інфраструктура WSUS-PRIM-2019 і WSUS-REPL-2019 функціонувала в стабільному та ненавантаженому режимі. Низькі показники використання ресурсів (CPU 1.39–1.5%, Queue Length ≈ 0 , SQL і IIS ненавантажені) відображають базовий стан системи. Отримані значення, збережені в CSV-логах і графіків, слугуватимуть еталонним для порівняння з результатами активного розгортання оновлень у підпунктах 4.3.2 і 4.3.3.

4.3.2 Навантаження під час розгортання оновлень

Для оцінки продуктивності інфраструктури під час активного етапу розгортання було проведено моніторинг навантаження на сервери WSUS-PRIM-2019 і WSUS-REPL-2019 під час доставки оновлення Security Updates KB5031539 для групи Win10-1. Це дало змогу дослідити поведінку системи під реальним навантаженням і виявити критичні ресурси, які зазнають пікового навантаження в процесі оновлення клієнта Win-10-1-KOST.

Контекст і мета. Тестування проводилося в період із 01:33 до 01:37 за локальним часом. Оновлення KB5031539 було схвалено для групи Win10-1 на WSUS-PRIM-2019, після чого репліка WSUS-REPL-2019 синхронізувалася, щоб забезпечити доставку оновлення клієнту Win-10-1-KOST. Метою було зафіксувати зміну навантаження під час доставки та встановлення оновлення, порівняти ці дані з базовими значеннями (див. п. 4.3.1) і визначити потенційні вузькі місця. Такий підхід дозволив оцінити готовність інфраструктури до масштабування.

Методика збору даних. Моніторинг розпочато через Perfmon на обох серверах перед схваленням оновлення, із використанням реального часу та Data Collector Sets, результати збережено у CSV-логах (C:\PerfLogs). Процес включав схвалення оновлення KB5031539 для групи Win10-1 через консоль WSUS-PRIM-2019 та спостереження за ключовими лічильниками.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				140
Змн.	Арк.	№ докум.	Підпис	Дата		

Результати. Тестування зафіксувало зміни навантаження на обох серверах у порівнянні з базовими значеннями (див. п. 4.3.1):

Таблиця 4.1. Результати тестування на WSUS-PRIM-2019

WSUS-PRIM-2019		
Параметр	Значення	Коментар
CPU (% Processor Time)	до 35%	Пік під час активної доставки оновлення.
Avg. Disk Queue Length	до 0.385	Невелике зростання, без критичних значень.
Bytes Total/sec (мережа)	до 13 477 Байт/с	Активна передача оновлень.
w3wp Working Set	до 303 МБ	Збільшення пам'яті IIS.
Available MBytes	до 6 473 МБ	Просідання на ~546 МБ.
Page Life Expectancy	до 1 209	Підвищене навантаження на кеш.
Batch Requests/sec	до 3.015	Зростання активності SQL.

Таблиця 4.2. Результати тестування на WSUS- REPL-2019

WSUS-REPL-2019		
Параметр	Значення	Коментар
CPU (% Processor Time)	до 6.3%	Помірне зростання.
w3wp Working Set	до 239 МБ	Активність IIS підвищена.
sqlservr Working Set	до 311 МБ	Зростання пам'яті SQL.
WsusService Working Set	до 87 МБ	Підвищене навантаження на службу WSUS.
Available MBytes	4 189 МБ	Помітне, але не критичне зниження.
Avg. Disk Queue Length	0	Відсутність затримок на диску.

Пікові значення спостерігалися на WSUS-PRIM-2019 у 01:33–01:36 і на WSUS-REPL-2019 у 01:34–01:37, що узгоджується з логами.

Графіки / логи. Результати візуалізовані у скріншотах графіків Perfmon і CSV-логах (C:\PerfLogs), які відображають час пікового навантаження.

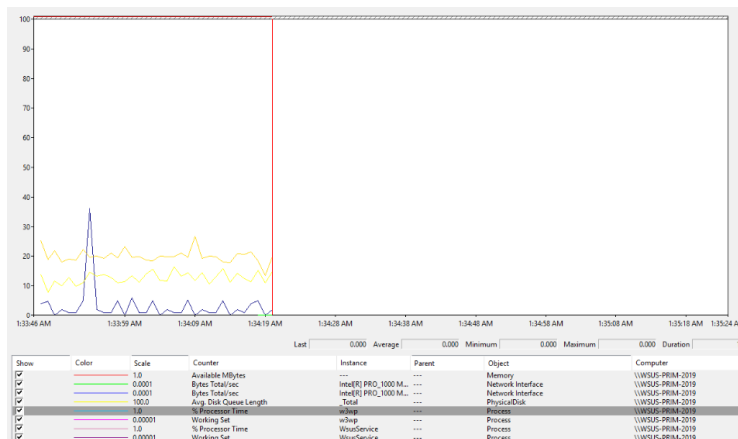


Рис. 4.48 – Перегляд графіку Perfmon для WSUS-PRIM-2019

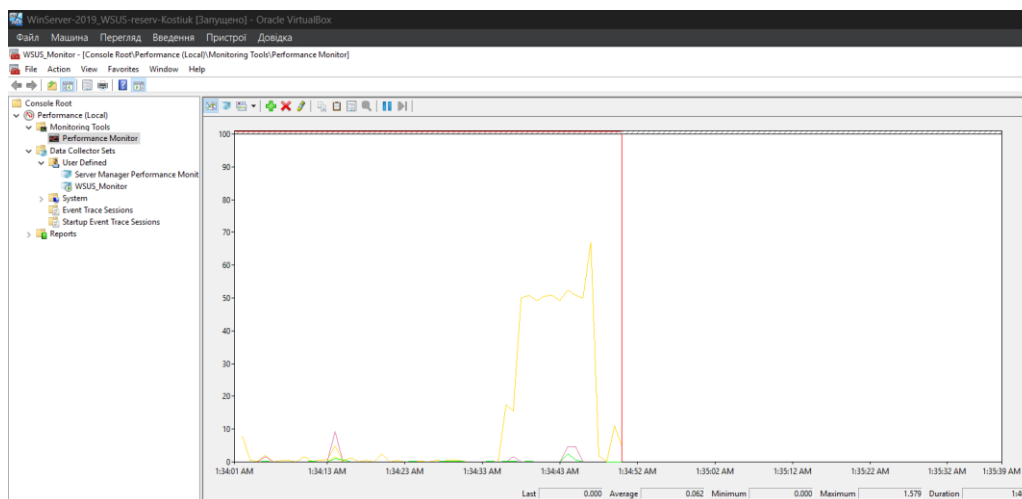
\\WSUS-PRIM-2019			
Memory			
Available MBytes	6,502,000		
Network Interface			
Bytes Total/sec	Intel[R] PRO_1000 MT Desktop Adapter	Intel[R] PRO_1000 MT Desktop Adapter_2	
	0.000	0.000	
PhysicalDisk			
			_Total
Avg. Disk Queue Length			0.078
Process			
	w3wp	WsusService	
% Processor Time	0.000	0.000	
Working Set	303,341,568.000	57,257,984.000	
Processor			
			_Total
% Processor Time			17.887
SQLServer:Buffer Manager			
Page life expectancy	1,252.000		
SQLServer:SQL Statistics			
Batch Requests/sec	1.983		
W3SVC_W3WP			
Active Requests	5260	WsusPool	---
File Cache Misses / sec			---

Рис. 4.49 – Перегляд моніторингу у вигляді звіту для WSUS-PRIM-2019

[illegible]

Рис. 4.50 – Перегляд вмісту створеного CSV-лога для WSUS-PRIM-2019

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росинський Ю.М.				142
Змн.	Арк.	№ докум.	Підпис	Дата		



\WSUS-REPL-2019			
Memory			
Available MBytes	4,189,000		
PhysicalDisk			
	_Total		
Avg. Disk Queue Length	0.000		
Process			
	sqlservr	w3wp	WsusService
% Processor Time	0.000	0.000	0.000
Working Set	311,898,112.000	239,579,136.000	87,920,640.000
Processor			
	_Total		
% Processor Time	6.343		
W3SVC_W3WP			
	4540_WsusPool		
Active Requests	---		
Requests / Sec	---		

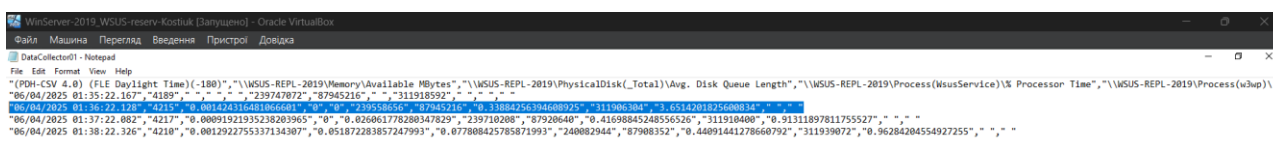


Рис. 4.53 – Перегляд вмісту створеного CSV-лога для WSUS- REPL-2019

Результати тестування підтвердили, що інфраструктура витримала навантаження під час розгортання оновлень. WSUS-PRIM-2019 продемонстрував значне зростання навантаження (CPU до 35%, мережа до 13 477 Байт/с), що пов'язано з роллю основного джерела оновлень, тоді як WSUS-REPL-2019 показав помірне підвищення (CPU до 6.3%), відображаючи синхронізацію та підтримку клієнта. Просідання Page Life Expectancy до 1209 на WSUS-PRIM-2019 вказує на підвищене використання кешу, але без критичних затримок. Отримані дані свідчать про стабільну роботу системи в умовах типового розгортання і будуть використані для оцінки стану після завершення оновлень у п. 4.3.3, підтверджуючи готовність до масштабування

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієвський Ю.М.				143
Змн.	Арк.	№ докум.	Підпис	Дата		

4.3.3 Стан системи після розгортання оновлень

Після завершення активного етапу розгортання оновлень у домені kostiuk.net (див. п. 4.3.2) було виконано завершальне тестування продуктивності серверів WSUS-PRIM-2019 і WSUS-REPL-2019. Мета полягала у фіксації стану ресурсів після встановлення оновлення KB5031539 на клієнта Win-10-1-KOST, порівнянні цих даних із базовими (п. 4.3.1) і піковими значеннями (п. 4.3.2), а також перевірки, чи повернулася інфраструктура до стабільного стану. Це дозволило оцінити, наскільки швидко система відновлюється після навантаження та чи фіксується тривале навантаження на ресурси.

Контекст і методика. Тестування проводилося о 02:30–02:31 за локальним часом, тобто через приблизно 55 хвилин після початку розгортання оновлення (01:33–01:37). На момент моніторингу доставка оновлення була завершена, а клієнт повернувся в режим очікування. Дані збиралися через Performance Monitor (Perfmon) із використанням реального часу та Data Collector Sets, результати збережено у CSV-логах.

Для коректного порівняння було використано ті самі лічильники.

Результати. Через 55 хвилин після завершення розгортання оновлення зафіксовано наступні значення:

Таблиця 4.3. Результати тестування на WSUS-PRIM-2019

WSUS-PRIM-2019		
Параметр	Значення	Коментар
CPU (% Processor Time)	11.3%	Зниження після пікового навантаження.
Avg. Disk Queue Length	0.001	Диск у спокійному стані.
w3wp Working Set	330 МБ	Залишилося трохи підвищеним..
Page Life Expectancy	4 656	Відновлюється після падіння.
Batch Requests/sec	1.8	Помірна SQL-активність.

Таблиця 4.4. Результати тестування на WSUS- REPL-2019

WSUS-REPL-2019		
Параметр	Значення	Коментар
CPU (% Processor Time)	0.61%	Дуже низьке навантаження.
w3wp Working Set	240 МБ	Стабільне значення.
WsusService Working Set	105 МБ	Залишилося стабільним.
Available MBytes	4 251 МБ	Без значних змін..
Avg. Disk Queue Length	0.001	Диск у режимі очікування.

Примітка: Пікові значення наведено за результатами CSV-логів і Perfmon-графіків.

Порівняння з попередніми етапами показало, що система повертається до стабільного стану. На WSUS-PRIM-2019 CPU знизився з пікового значення 35% (п. 4.3.2) до 11.3%, що все ще вище базового 1.39% (п. 4.3.1), але свідчить про значне зменшення навантаження. Page Life Expectancy відновилося з 1209 (п. 4.3.2) до 4656, хоча ще не досягла базового значення 14498 (п. 4.3.1). Available MBytes зросла з 6473 (п. 4.3.2) до 6619, наблизившись до початкового 7019 (п. 4.3.1). На WSUS-REPL-2019 CPU знизився з 6.3% (п. 4.3.2) до 0.61%, що навіть нижче базового 1.5% (п. 4.3.1), а пам'ять залишилася стабільною (4251 проти 4078 у п. 4.3.1).

Графіки / логи. Графіки Perfmon демонструють повернення до мінімальних коливань, подібних до базових показників у п. 4.3.1. CSV-логи (C:\PerfLogs) містять повні сесії спостереження.

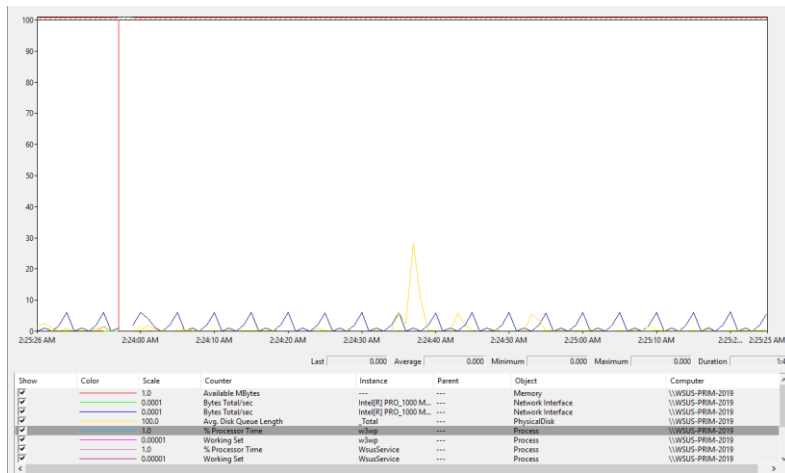


Рис. 4.54 – Перегляд графіку Perfmon для WSUS-PRIM-2019.

\\WSUS-PRIM-2019			
Memory			
Available MBytes	6,630.000		
Network Interface			
Bytes Total/sec	Intel[R] PRO_1000 MT Desktop Adapter	0.000	Intel[R] PRO_1000 MT Desktop Adapter_2
			0.000
PhysicalDisk			
Avg. Disk Queue Length	_Total		
	0.001		
Process			
% Processor Time	w3wp	0.000	WsusService
Working Set	330,629,120.000	0.000	57,487,360.000
Processor			
% Processor Time	_Total		
	4.621		
SQLServer:Buffer Manager			
Page life expectancy	4,338.000		
SQLServer:SQL Statistics			
Batch Requests/sec	1.018		
W3SVC_W3WP			
5260_WsusPool			
Active Requests	---		
File Cache Misses / sec	---		

Рис. 4.55 – Перегляд моніторингу у вигляді звіту для WSUS-PRIM-2019.

File Edit Format View Help	
06/04/2025 02:36:51.289", "6435", "13.267157551490873", "0", "0.0007886889213482702", "0", "331722752", "0.02834706502469671", "57516032", "0", "5016", "1.8000666824642913", "0", "0"	
06/04/2025 02:37:56.218", "6619", "4.833230053590413", "0", "0.0008667215976521421", "0", "331722752", "0.02334531273414441", "57516032", "0", "45671847919406", "5075", "1.7999608781854498", "0", "0"	
06/04/2025 02:38:05.999", "6620", "1.0671398204559597", "0.7083105071742235", "0.00075999436455438326", "0", "331718656", "0.028522972142546836", "57524224", "0", "5136", "1.9175168648818024", "0", "0"	
06/04/2025 02:40:01.827", "6621", "13.114757136169711", "0", "0.00064820633594491741", "0", "331718656", "0", "57516032", "12.00405222649289", "5196", "1.7997379551541663", "0", "0"	
06/04/2025 02:40:54.850", "6621", "1.0666406530788726", "0", "0.00049364996212773762", "0", "331718656", "0", "57516032", "5.255", "1.78328984186624", "0", "0"	
06/04/2025 02:42:01.091", "6626", "17.162724789246155", "0.0408708238039964", "0.0004566872193103492", "0", "331681792", "0", "57509280", "9.4173922924345464", "5316", "1.799586676930665", "0", "0"	
06/04/2025 02:42:55.715", "6627", "1.0668941284948616", "0", "0.001259584633553228", "0", "331653120", "0.028604544356455486", "57516032", "0", "5375", "1.8003838418350793", "0", "0"	
06/04/2025 02:44:25.020", "6737", "253.64312716413102", "1.4003381138210322", "0.0047125450071596343", "0", "331784192", "0.08748187981524691", "57561088", "33.048367739795239", "5435", "2.517260085592364", "0", "0.13336561"	
06/04/2025 02:45:26.002", "6706", "200.8181747646803", "2.8000210234911846", "0.0013976118769186521", "0", "331739136", "0", "57602048", "2.6352076586871442", "5406", "1.8000135151014758", "0", "0"	
06/04/2025 02:46:25.778", "6732", "8.99082608633616152", "0.69998647150470233", "0.0013724481669346031", "0", "331685808", "0.052331106802091545", "57528320", "0", "5556", "1.7166334898634192", "0", "0"	
06/04/2025 02:47:25.482", "6734", "8.9957566715921544", "0", "0.00098727298015075828", "0", "331694080", "0.026170796254172343", "57532416", "0", "5616", "1.799151343184309", "0", "0"	
06/04/2025 02:48:21.971", "6736", "12.76648999722554", "0.8998768405376563", "0.00078441546186775325", "0", "331694080", "0", "57532416", "0", "5676", "1.7999750913446944", "0", "0"	
06/04/2025 02:49:15.137", "6737", "10.067245784900447", "0.700004026981652112", "0.001234423740052678", "0.054665507314756542", "331718656", "0.02732735367378271", "57536512", "0", "5736", "1.9167769292595223", "0", "0"	
06/04/2025 02:50:19.119", "6737", "5.4648718653414499", "0", "0.0007481934841467255", "0", "331759616", "0", "57528320", "0.006590468561973312", "5706", "1.78313903560113", "0", "0"	
06/04/2025 02:51:20.135", "6737", "3.532393340520254", "0", "0.00087376418838592304", "0", "331710464", "0.051216070359270602", "57528320", "1.8700091916375228", "5856", "1.8009799814982016", "0", "0"	
06/04/2025 02:52:20.176", "6737", "4.1166744746259205", "0", "0.00116446652490627", "0", "331710464", "0.026023912199554019", "57528320", "0.1982967147034427", "5915", "1.8000034140064753", "0", "0"	
06/04/2025 02:53:19.942", "6737", "8.99757359737385", "0", "0.0011700987867002107", "0", "331689984", "0.052807847320823637", "57528320", "0", "5976", "1.79951470387846575", "0", "0"	
06/04/2025 02:54:19.751", "6737", "9.2316401582119152", "0.04925732571389004", "0.001136311491778646", "0.02612484359683135", "331788288", "0.0522496871936627", "57556992", "0", "6036", "2.5162851694765331", "0", "0.13338871"	
06/04/2025 02:55:20.921", "6704", "526.07181308442716", "4.902222283575961", "0.001267336261801877", "0", "331722752", "0.051087634485745582", "57552896", "2.887515606462315", "6095", "1.80008163490687203", "0", "0"	
06/04/2025 02:56:21.358", "6729", "0.2.59890413088721", "0.0017063444482114723", "0", "331784192", "0.051706755703063628", "57528320", "0.92985407293007977", "6156", "1.7659220391580285", "0", "0"	
06/04/2025 02:57:21.237", "6732", "9.403890811233535", "0", "0.001142095204702236", "0", "331720944", "0.078281212297918222", "57008128", "0.011576849012307355", "6216", "1.8007164138085995", "0", "0"	
06/04/2025 02:58:21.042", "6731", "8.3625429204972734", "6.9965498613323795", "0.0011205108350522939", "0", "331730944", "0.05225257166214801", "57012224", "0", "6274", "1.799112821485469", "0", "0"	
06/04/2025 02:59:20.748", "6734", "127.42490434244584", "0.69967917144498959", "0.0011878987750273159", "0", "331673600", "0", "57028416", "0", "6336", "1.9157882075279475", "0", "0"	
06/04/2025 03:00:20.531", "6734", "0.0072680730866662", "0", "0.001207731791073923", "0", "331755200", "0.052301164282996339", "57012224", "0", "6396", "1.8014521746173213", "0", "0"	
06/04/2025 03:01:19.007", "6734", "0.0002046807904504", "0", "0.0011040486311463261", "0", "331714560", "0.026720374739080542", "57044092", "0", "6455", "1.8000402973080099", "0", "0"	
06/04/2025 03:02:14.108", "6734", "0.06786957523574", "0", "0.0013019236298800357", "0", "331710464", "0.056713713199267761", "57008128", "0", "6516", "1.800215086999173", "0", "0"	
06/04/2025 03:03:10.831", "6734", "8.9978206828415122", "0", "0.0011288314845538487", "0", "331644928", "0.082638962863615606", "57008128", "0", "6576", "1.7995641365683026", "0", "0"	
06/04/2025 03:04:10.008", "6734", "13.1124151566497", "0", "0.0012913100764596999", "0", "331812864", "0.15826161011102398", "57001856", "0", "6635", "2.5158509087930616", "0", "0.13329024059854783"	
06/04/2025 03:05:07.472", "6708", "1.009.665911200979", "3.3018219152006958", "0.0027086218863802311", "0", "331755200", "0.001658177306546472", "57024512", "0", "6696", "1.917353805880112", "0", "0"	
06/04/2025 03:06:06.763", "6730", "17.166942539433276", "4.050055084545909", "0.0012988501531403531", "0", "331722752", "0", "57008128", "0", "6756", "1.7833619919605441", "0", "0"	
06/04/2025 03:07:03.460", "6729", "330.62289763819444", "0", "0.0009543219957653958", "0", "331710464", "0.027568345103384649", "57008128", "0", "6815", "1.799580318680073", "0", "0"	
06/04/2025 03:08:04.233", "6732", "16.69943086887347", "4.8958126501485", "0.0008065578198326725", "0", "331722752", "0", "57008128", "1.4017128518900566", "6876", "1.799453626585165", "0", "0"	
06/04/2025 03:09:59.740", "6732", "17.2159340848219897", "2.801086742511738", "0.001819470789498017", "0", "331743232", "0", "57020816", "0", "6936", "1.917353805880112", "0", "0"	
06/04/2025 03:10:02.526", "6731", "147.83963594872122", "1.3999018622131194", "0.00064407640444595713", "0", "331710464", "0.024889433093931979", "57012224", "4.5739135178647921", "6996", "1.7998738228454392", "0", "0"	
06/04/2025 03:10:59.846", "6733", "9.0021951702886156", "0", "0.0008316857032024772", "0.002259145993025043", "331714560", "0", "57012224", "0", "7056", "1.80043903480757232", "0", "0"	
06/04/2025 03:12:01.443", "6734", "0", "0.0008853699533686674", "0", "331714560", "0", "57012224", "2.6381421847306408", "7116", "1.79968087800479574", "0", "0"	
06/04/2025 03:12:57.830", "6733", "8.994675914972877", "0", "0.0007083439856360234", "0", "331685808", "0.13855184016909291", "57012224", "0", "7176", "1.799893512994573", "0", "0"	

Рис. 4.56 – Перегляд вмісту створеного CSV-лога для WSUS-PRIM-2019.

		Костюк І.О.			Арк.
		Росієнський Ю.М.			25.123.07.000 - ПЗ
Змн.	Арк.	№ докум.	Підпис	Дата	146

зниження процесорного навантаження, вивільнення оперативної пам'яті, відновлення метрик SQL і відсутність черг на диску. Жодних тривалих навантажень чи "витікань" ресурсів не виявлено, що підтверджує належну стабільність і оптимальність налаштувань системи. Отримані дані дозволяють рекомендувати цю конфігурацію для подальшого масштабування без необхідності додаткової оптимізації.

4.4 Проблеми та обмеження під час реалізації

4.4.1 Початкова проблема з WID (Windows Internal Database)

Контекст появи проблеми. На початковому етапі впровадження системи WSUS у домені kostiuk.net під час налаштування основного сервера WSUS-PRIM-2019 було обрано використання Windows Internal Database (WID) як бази даних за замовчуванням. Це рішення було прийнято з метою спрощення конфігурації та уникнення окремої інсталяції SQL Server, що мало зменшити витрати часу на підготовку інфраструктури. Проте перша повна синхронізація з Microsoft Update, яка охоплювала оновлення для продуктів, таких як Windows 10, Windows 11, Server 2019 і Office, призвела до виявлення критичної проблеми.

Суть проблеми. Після запуску синхронізації база SUSDB почала стрімко зростати через великий обсяг метаданих. Протягом приблизно 6 годин прогрес синхронізації зупинився на позначці 36%, після чого виникли постійні помилки при зверненні до бази. Консоль WSUS перестала відповідати, а служба WsusService втратила стабільне з'єднання з WID, що свідчило про серйозні збої в роботі системи. Аналіз журналів подій виявив систематичні повідомлення про помилку із кодом Event ID 1105 від джерела MSSQL\$MICROSOFT##WID із текстом: "Could not allocate space for object 'dbo.tbXml'... in database 'SUSDB' because the 'PRIMARY' filegroup is full".

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				148
Змн.	Арк.	№ докум.	Підпис	Дата		

Наслідки для впровадження. Ця проблема спричинила повне припинення процесу налаштування WSUS, що унеможливило завершення синхронізації. Адміністративна консоль стала недоступною, а служба WsusService втратила стабільність, що ускладнило подальше управління оновленнями. Відновлення роботи без кардинальних змін виявилось неможливим, оскільки очищення бази чи її розширення за межі 10 ГБ не підтримуються WID, що вимагало термінового втручання для вирішення ситуації.

Прийняте рішення. У зв'язку з виявленими обмеженнями було прийнято рішення відмовитися від використання WID і здійснити перевстановлення WSUS із прив'язкою до окремого SQL Server, інсталюваного локально на WSUS-PRIM-2019. Такий підхід дозволив усунути обмеження в 10 ГБ, забезпечивши базу SUSDB можливістю розширення, покращив керованість через SQL Server Management Studio та підвищив загальну стабільність системи. Це також унеможливило повторення подібних проблем у майбутньому, створивши надійну основу для подальшої роботи.

Отриманий досвід засвідчив, що Windows Internal Database має суттєві обмеження для використання з WSUS у продуктивному середовищі з великими обсягами оновлень. Для подібних реалізацій рекомендовано застосовувати повноцінний SQL Server навіть на початкових етапах, що забезпечить стабільність і уникнення критичних збоїв.

4.4.2 Обмеження дискового простору та відмова від автоматизації

На етапі розгортання інфраструктури системи оновлень WSUS для домену kostiuk.net основним сервером виступав WSUS-PRIM-2019, розгорнутий у середовищі Oracle VirtualBox на ноутбучі з твердотілим накопичувачем SSD обсягом 1 ТБ. Частина дискового простору була зайнята локальними файлами та програмним забезпеченням, а ще частина була розподілена між віртуальними машинами, такими як DC-SRV-2022, WSUS-REPL-2019 і клієнтські Windows 10/11. У результаті для WSUS-сервера вдалося виділити лише 420 ГБ. Після початкового налаштування WSUS та вибору підтримуваних продуктів і класифікацій, таких

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				150
Змн.	Арк.	№ докум.	Підпис	Дата		

як Windows 10, Windows 11, Server 2019, тощо, перша синхронізація виявила потребу в завантаженні понад 890 ГБ оновлень, що значно перевищувало доступний простір. Це створювало ризик нестабільної роботи віртуальної машини та всієї інфраструктури, що вимагало негайного рішення.

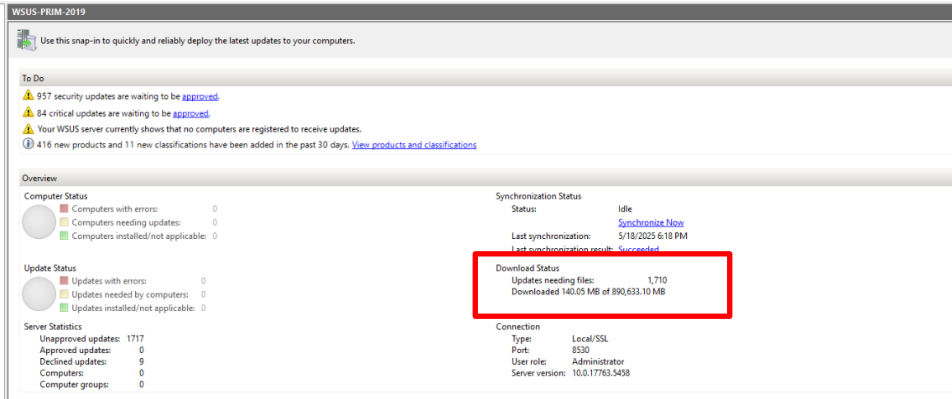


Рис. 4.62 – Спроба встановити всі оновлення на дисковий простір.

Рішення: завантаження лише метаданих. Щоб уникнути перевантаження дискового простору, було вирішено завантажувати лише метадані оновлень, відкладаючи завантаження самих файлів до моменту їхнього схвалення. Це рішення було необхідним для забезпечення стабільності роботи WSUS-сервера в умовах обмежених ресурсів. Завантаження лише метаданих дозволило знизити навантаження на диск до мінімального рівня, надало можливість переглядати список доступних оновлень без зайвого використання простору та забезпечило контроль над тим, які саме оновлення будуть завантажені після ретельного аналізу. Налаштування було виконано під час запуску майстра конфігурації WSUS шляхом зняття позначки з пункту "Download updates to this server only when updates are approved", що відстрочило завантаження файлів до моменту схвалення.

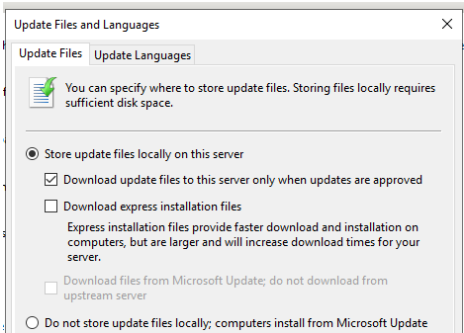


Рис. 4.63 – Налаштування завантаження оновлень лише після схвалення.

Причина відмови від автоматизації. Обмеження дискового простору також зумовило відмову від автоматичного схвалення оновлень. Автоматизація схвалення у WSUS призвела б до негайного завантаження всіх схвалених оновлень на диск, що перевантажило б доступний простір у 420 ГБ. Система WSUS дозволяє налаштовувати автоматичне схвалення за класифікацією чи продуктом, але не має гнучких механізмів фільтрації за релевантністю чи важливістю оновлень. У такому разі автоматичне схвалення могло б спричинити завантаження сотень або тисяч непотрібних оновлень, що було неприйнятним для тестового середовища з обмеженими ресурсами. Цей підхід мав би негативний вплив на стабільність інфраструктури, тому було вирішено уникнути автоматизації.

Натомість було обрано ручне схвалення оновлень після їхньої перевірки, аналізу статусу клієнтів і тестування. Такий підхід дозволив контролювати кожне завантаження, уникаючи накопичення непотрібних або неактуальних оновлень на сервері, що забезпечило стабільність віртуального середовища. Ручне схвалення здійснювалося через консоль WSUS шляхом точкового вибору оновлень для конкретних груп клієнтів, що дало змогу завантажувати лише ті патчі, які були дійсно необхідні для тестування та впровадження.

Обмеження вільного місця на хості, де розгорнуто WSUS, визначило стратегічне рішення — відмову від повного завантаження оновлень і автоматичних правил схвалення. Обрана тактика зосереджена на завантаженні лише метаданих і ручному схваленні оновлень, що забезпечило оптимальний баланс між функціональністю та стабільністю. Такий підхід дозволив масштабувати інфраструктуру в межах доступних ресурсів і уникнути критичних збоїв під час тестування. У продуктивному середовищі з розширеним сховищем ці обмеження можуть бути зняті, що відкриє можливості для повної автоматизації схвалення і завантаження оновлень.

4.4.3 Обмеження WSUS API при роботі з PowerShell

Після налаштування основного WSUS-сервера WSUS-PRIM-2019 у домені kostiuk.net виникла потреба в автоматизації адміністративних завдань, таких як

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				152
Змн.	Арк.	№ докум.	Підпис	Дата		

фільтрація оновлень за класифікацією, аналіз їхнього статусу та формування звітів. Автоматизація мала на меті зменшити час на ручне управління оновленнями та підвищити ефективність адміністрування в тестовому середовищі. Для цього було обрано PowerShell із використанням вбудованого WSUS API через командлет Get-WsusServer, що дозволяло швидко отримувати та обробляти дані про оновлення.

Успішні дії. Початкові дії з PowerShell продемонстрували базову функціональність WSUS API. Підключення до сервера WSUS-PRIM-2019 здійснювалося коректно як через HTTPS (порт 8531), так і через HTTP (порт 8530), що підтвердило доступність сервера. Команда `$wsus.GetUpdates()` успішно повернула список із 5154 оновлень, а `$wsus.GetUpdateClassifications()` надала перелік доступних класифікацій, таких як Critical Updates, Security Updates тощо. Це дозволило виконати базову фільтрацію, наприклад, за допомогою `$criticalUpdates = $wsus.GetUpdates() | Where-Object { $_.UpdateClassificationTitle -eq "Critical Updates" }`, що забезпечило можливість аналізу оновлень за певними категоріями.

Обмеження, з якими зіткнулися. Попри початковий прогрес, подальша робота виявила суттєві обмеження WSUS API при використанні з PowerShell. Спроба отримати класифікацію за ідентифікатором через `$wsus.GetUpdateClassification($classificationId)` завершилася помилкою: "Cannot find an overload for 'GetUpdateClassification' and the argument count: '1'". Це унеможливило точну фільтрацію оновлень за ідентифікатором класифікації, що стало перешкодою для створення гнучких скриптів автоматизації.

Додатковою проблемою стала неконсистентність об'єктів, що повертаються API. Наприклад, властивість `.Classification.Title` часто виявлялася порожньою, змушуючи використовувати альтернативну властивість `.UpdateClassificationTitle`, яка працювала лише в окремих випадках. Властивість `.UpdateClassifications`, будучи масивом, вимагала складної обробки через вкладені цикли або створення конструкцій, таких як `PSCustomObject`, що ускладнювало фільтрацію оновлень за класифікаціями. Недостатня документація

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				153
Змн.	Арк.	№ докум.	Підпис	Дата		

WSUS API додатково ускладнила розробку, змушуючи працювати методом спроб і помилок через відсутність чітких описів методів і структур об'єктів.

Висновок про обмеження WSUS API. Робота з WSUS API через PowerShell виявила його обмежену придатність для складних сценаріїв автоматизації. Через відсутність підтримки методу GetUpdateClassification(id), неконсистентність об'єктів, складність фільтрації та брак документації ефективність скриптів виявилася низькою, а повноцінна автоматизована фільтрація стала неможливою. Наприклад, спроба сортування оновлень за класифікацією завершилася невдачею, що проілюстровано на, де видно відсутність очікуваних оновлень через проблеми з API. У межах тестового середовища використання WSUS API через PowerShell для складних завдань було визнано недоцільним. Проте API може бути корисним для базових сценаріїв моніторингу або інтеграції зі звітністю. Для складніших завдань доцільно застосовувати комбіновані підходи або сторонні модулі з розширеним функціоналом.

4.5 Рекомендації щодо подальшої оптимізації

4.5.1 Автоматизація звітності в системі WSUS

У поточному середовищі системи WSUS для домену kostiuk.net основний акцент робився на ручному аналізі стану оновлень через графічну консоль WSUS. Такий підхід виявився достатнім для тестового впровадження, але у разі масштабування інфраструктури чи збільшення кількості клієнтських машин ручна перевірка стає неефективною. Вона підвищує ризик пропуску критичних проблем, таких як несвоєчасне встановлення оновлень, і потребує значних витрат часу адміністратора. Автоматизація звітності необхідна для оперативного виявлення клієнтів без потрібних оновлень, моніторингу стану синхронізації та результатів встановлення, а також для формування періодичних звітів без ручного втручання, що значно підвищить ефективність керування системою.

Рекомендації щодо використання SQL. Оскільки WSUS-сервер WSUS-PRIM-2019 у домені kostiuk.net використовує повноцінний SQL Server, доцільно

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				154
Змн.	Арк.	№ докум.	Підпис	Дата		

організувати регулярну звітність через SQL-запити до бази SUSDB. Це дозволить отримувати деталізовані дані про стан оновлень і клієнтів, зокрема перелік пристроїв із оновленнями в статусі "Needed", статистику за класифікаціями (наприклад, Security Updates, Critical Updates) та дати останнього підключення клієнтів до сервера. Такі звіти забезпечать адміністраторам точну інформацію для швидкого реагування на проблеми. Рекомендується налаштувати автоматизацію звітів через SQL Server Agent Job, який регулярно виконуватиме запити та експортуватиме результати у формат CSV для подальшої обробки в Excel або у формат HTML для швидкого перегляду через браузер. Для більш динамічного аналізу у майбутньому доцільно інтегрувати звіти з Power BI, використовуючи функцію Scheduled Refresh для оновлення даних.

Рекомендації щодо використання PowerShell. У середовищах, де SQL-звітність менш доступна, альтернативою є використання PowerShell із WSUS API. Це дозволить формувати базові звіти, такі як список оновлень із класифікаціями, аналіз статусу клієнтів за групами чи створення статистики встановлення патчів. PowerShell-скрипти забезпечать експорт даних у формат CSV, зручний для аналізу в Excel, або у формат HTML для веб-перегляду та швидкого ознайомлення. Для регулярності звітів пропонується налаштувати запуск скриптів через Task Scheduler, наприклад, щопонеділка перед початком перевірки стану системи, що дозволить адміністраторам отримувати актуальну інформацію на початку тижня.

Врахування обмежень. SQL-підхід вимагає доступу до бази SUSDB, що неможливо у випадку використання Windows Internal Database (WID), а також знань структури бази для створення коректних запитів. PowerShell із WSUS API має власні обмеження, описані раніше: складність фільтрації через нестабільність властивостей об'єктів, відсутність деяких методів і недостатня документація, що може ускладнити створення деталізованих звітів. Для обох підходів необхідне базове розуміння структури даних WSUS, щоб забезпечити коректність і корисність звітів.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				155
Змн.	Арк.	№ докум.	Підпис	Дата		

Загальні рекомендації. Для середовища із SQL Server, як у домені kostiuk.net, доцільно віддати перевагу SQL-запитам до SUSDB через їхню точність і гнучкість. Для невеликих або початкових етапів можна використовувати PowerShell із збереженням результатів у CSV. Рекомендується розробити шаблони звітів, наприклад, "Клієнти без оновлень" або "Оновлення в статусі Failed", які формуватимуться щотижня. Також доцільно реалізувати тригер-звіт про клієнтів, які не підключалися до сервера понад 7 днів, що дозволить оперативно виявляти проблеми з доступністю пристроїв. У разі розширення інфраструктури варто розглянути інтеграцію з централізованою системою аналітики, такою як Power BI або Excel із Power Query, що використовуватиме SQL-запити до SUSDB для створення інтерактивних звітів.

Автоматизація звітності є важливим кроком для оптимізації системи Patch Management у домені kostiuk.net. Вона дозволить зменшити час на ручні перевірки, підвищити прозорість процесу оновлень і своєчасно реагувати на проблеми. Впровадження регулярних звітів через SQL або PowerShell із подальшою інтеграцією у щотижневий цикл забезпечить ефективне управління системою та підготує її до масштабування.

4.5.2 Розширення ресурсів та реалізація повної автоматизації

У процесі тестового впровадження WSUS-сервера WSUS-PRIM-2019 у домені kostiuk.net (див. п. 4.4.2) було виявлено обмеження дискового простору, що склало 420 ГБ. Ця конфігурація виявилася недостатньою для реалізації повної стратегії Patch Management, оскільки повне завантаження оновлень для обраних продуктів і класифікацій перевищує 890 ГБ, тобто майже вдвічі більше доступного обсягу. Таке обмеження унеможливило завантаження повного каталогу оновлень і змусило вдатися до завантаження лише метаданих із ручним схваленням, що не дозволяє досягти максимальної ефективності системи. Розширення ресурсів є необхідним кроком для переходу до автоматизованого управління оновленнями та забезпечення стабільності інфраструктури.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				156
Змн.	Арк.	№ докум.	Підпис	Дата		

Рекомендація щодо розширення. Для подолання поточних обмежень пропонується розширити дисковий простір WSUS-сервера. Існують кілька варіантів: збільшення обсягу віртуального диску в середовищі VirtualBox, заміна фізичного SSD на хост-машині, підключення зовнішнього накопичувача або перехід на інфраструктуру з віддаленим сховищем. Рекомендований мінімум становить 1 ТБ доступного простору, що включатиме місце для оновлень, а також резерв у розмірі 20–25% для логів, майбутніх оновлень і розширення списку продуктів чи класифікацій. Таке розширення дозволить завантажувати повний набір оновлень локально, підвищуючи швидкість доставки клієнтам і зменшуючи залежність від зовнішнього інтернет-каналу.

Завантаження повного каталогу оновлень. Після розширення дискового простору рекомендується змінити налаштування WSUS, увімкнувши опцію повного завантаження оновлень одразу після синхронізації з Microsoft Update. Це здійснюється в майстрі конфігурації WSUS шляхом активації параметра "Store updates locally and download updates from Microsoft Update", що забезпечить локальне зберігання всіх оновлень. Такий підхід дозволить мати всі патчі на локальному диску, що спростить і прискорить їх розгортання на клієнтських машинах. Крім того, це зменшить навантаження на інтернет-канал, усунувши необхідність повторного завантаження при схваленні, і підвищить продуктивність системи завдяки швидкому доступу до файлів.

Налаштування автоматизації. З урахуванням наявності повного каталогу оновлень доцільно налаштувати автоматичне схвалення в консолі WSUS. Рекомендується увімкнути автоматизацію для критичних класифікацій, таких як Security Updates і Critical Updates, а також для основних продуктів, наприклад, Windows 10, Windows 11 і Office, щоб забезпечити своєчасне закриття вразливостей. Для гнучкості управління пропонується розмежувати автоматизацію за групами клієнтів: автоматичне схвалення для робочих станцій і ручна перевірка для серверів перед розгортанням. Це дозволить мінімізувати ризик помилок і адаптувати процес до специфіки різних пристроїв.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				157
Змн.	Арк.	№ докум.	Підпис	Дата		

Результати від повної автоматизації. Повноцінна реалізація автоматизації забезпечить значне зменшення ручної роботи адміністраторів, дозволяючи зосередитися на стратегічних задачах. Регулярне оновлення клієнтів відбуватиметься без участі персоналу, що підвищить ефективність процесу. Автоматизація також сприятиме підвищенню безпеки шляхом швидкого закриття критичних вразливостей, зменшить кількість помилок, спричинених людським фактором, і полегшить масштабування інфраструктури за рахунок автоматичного розгортання оновлень.

Умови доцільності реалізації. Реалізація розширення та автоматизації потребує достатньої пропускної здатності інтернет-каналу для початкового завантаження оновлень і достатнього дискового простору, як зазначено раніше. Перед впровадженням у продуктивне середовище рекомендується провести тестування на ізолюваному полігоні, щоб оцінити стабільність і ефективність системи. Поступове поширення змін на основну інфраструктуру дозволить уникнути ризиків і забезпечить безперебійну роботу домену kostiuk.net.

Розширення дискового простору до 1 ТБ із резервом є ключовим для реалізації повної автоматизації WSUS у домені kostiuk.net. Завантаження повного каталогу оновлень і налаштування автоматичного схвалення за класифікаціями та групами клієнтів дозволять підвищити ефективність, стабільність і безпеку системи. Поступове впровадження з тестуванням на полігоні забезпечить надійний перехід до автоматизованого управління оновленнями. Також реалізація повного завантаження створює передумови для впровадження більш гнучкої системи автоматичної звітності (див. п. 4.5.1), що дозволить централізовано відстежувати статус оновлень і покриття клієнтів.

4.5.3 Використання зовнішнього моніторингу (Zabbix, Grafana)

У процесі впровадження WSUS у домені kostiuk.net (див. п. 4.2.1–4.2.3) моніторинг продуктивності WSUS-серверів здійснювався за допомогою вбудованих інструментів, таких як Performance Monitor (Perfmon) і Task Manager. Хоча ці інструменти дозволили проводити короткостроковий аналіз, вони виявилися

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				158
Змн.	Арк.	№ докум.	Підпис	Дата		

недостатніми для продуктивного середовища. Ручний моніторинг не забезпечує централізованої історії метрик, ускладнює виявлення трендів і не дозволяє оперативно реагувати на проблеми, що виникають у неробочий час, наприклад, пікові навантаження, витік пам'яті чи повільну деградацію продуктивності. Впровадження зовнішнього моніторингу необхідно для забезпечення проактивного контролю за станом WSUS, SQL Server, IIS та інших компонентів інфраструктури, що підвищить надійність системи.

Переваги використання Zabbix або Grafana. Для вирішення зазначених проблем пропонується використовувати системи зовнішнього моніторингу, такі як Zabbix або Grafana із Prometheus. Їхні переваги включають:

- автоматичні сповіщення про критичні події;
- історичний аналіз метрик;
- інтерактивні графіки і дашборди;
- контроль стану служб у реальному часі.

Zabbix забезпечує активне опитування через агентів, автоматичні сповіщення та готові шаблони моніторингу, що дозволяє швидко виявляти проблеми, наприклад, перевищення навантаження на CPU чи зупинку WsusService. Grafana у поєднанні з Prometheus або InfluxDB пропонує гнучку візуалізацію через інтерактивні дашборди, що допомагає аналізувати тренди використання ресурсів, такі як CPU, RAM, черга запитів (Queue Length), кількість помилок HTTP 5xx, з'єднань до SQL Server чи затримки відгуку. Обидві системи дозволяють централізовано відстежувати ключові метрики WSUS-серверів, SQL Server та IIS через агенти, SNMP або HTTP-запити, забезпечуючи комплексний контроль. Наприклад, шаблон моніторингу WSUS у Zabbix може включати: доступність WsusService, середній час відповіді SQL-запитів, кількість невстановлених критичних оновлень, статус порту 8531.

Рекомендації щодо впровадження. Для реалізації моніторингу рекомендується розгорнути Zabbix-сервер або Grafana із Prometheus на окремій віртуальній машині. На серверах WSUS-PRIM-2019 і WSUS-REPL-2019 необхідно встановити Zabbix Agent або Prometheus Node Exporter для збору метрик. Доцільно

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				159
Змн.	Арк.	№ докум.	Підпис	Дата		

створити базові дашборди для відстеження параметрів, таких як використання CPU, RAM, дискового простору, доступність порту 8531 (HTTPS) і стан служб (WsusService, SQL Server, IIS). Налаштування тригерів на критичні події, наприклад, перевищення CPU понад 80%, недоступність SQL-з'єднань або зупинку WsusService, дозволить оперативно виявляти проблеми. Для інформування адміністраторів рекомендується інтегрувати сповіщення з Telegram, Email або Microsoft Teams, що забезпечить швидке реагування на інциденти.

Можливість майбутнього розширення. Впровадження зовнішнього моніторингу відкриває можливості для централізованого контролю всієї доменної інфраструктури, включаючи доменний контролер, DHCP-сервер і клієнтські машини. У майбутньому можна порівнювати продуктивність між різними філіями або групами клієнтів (наприклад, Windows 10 vs Windows 11), а також інтегрувати дані з Power BI для стратегічної аналітики або з CMDB для управління конфігураціями. Такий підхід забезпечить масштабування системи моніторингу відповідно до зростання інфраструктури.

Ризики та бар'єри впровадження. Перед впровадженням слід врахувати потребу в окремому ресурсі для хостингу Zabbix/Grafana, наявність обізнаного адміністратора та захист зібраних метрик. Ці фактори можуть вплинути на швидкість розгортання та безпеку системи, тому їх необхідно оцінити заздалегідь.

Впровадження зовнішнього моніторингу за допомогою Zabbix або Grafana суттєво підвищить контрольованість і надійність системи Patch Management у домені kostiuk.net. Рекомендується розпочати з моніторингу WSUS-серверів, поступово розширюючи охоплення на інші критичні компоненти інфраструктури для забезпечення комплексного контролю.

Висновок до Розділу 4

У розділі 4 досліджено процес тестування, оцінки продуктивності та аналізу ефективності системи Patch Management у доменному середовищі kostiuk.net. Це уможливило всебічне оцінювання її функціональності й стабільності. Перевірка групових політик засвідчила їхню коректну роботу. Поетапне

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				160
Змн.	Арк.	№ докум.	Підпис	Дата		

тестування WSUS засвідчило надійність доставки оновлень клієнтам і серверам на всіх етапах — від початкового налаштування до впровадження HTTPS і резервного сервера.

Моніторинг продуктивності через Performance Monitor виявив здатність системи витримувати навантаження. Пікове використання CPU сягало 35% на WSUS-PRIM-2019, але після завершення доставки показники стабілізувалися до 11.3%. Зростання активності SQL та IIS під час активної фази вказує на потребу в додатковому контролі. Аналіз дозволив виявити технічні обмеження: зокрема, використання WID спричинило збої через ліміт у 10 ГБ. Нестача дискового простору призупинила автоматизацію. Недоліки WSUS API ускладнили звітність через PowerShell. Для вирішення цих проблем запропоновано автоматизувати звітність через SQL-запити або PowerShell, розширити сховище до 1 ТБ і впровадити зовнішній моніторинг за допомогою Zabbix або Grafana.

Дослідження підтвердило працездатність системи Patch Management у домені kostiuk.net. Зібрані дані, CSV-логи та рекомендації створюють основу для подальшої оптимізації, підвищення безпеки й масштабування інфраструктури. Запропоновані заходи відкривають можливості для інтеграції з аналітичними платформами та автоматизованого керування оновленнями в корпоративному середовищі.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				161
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

Дипломна робота була спрямована на проектування, впровадження та тестування централізованої системи управління оновленнями (Patch Management) на основі Windows Server Update Services (WSUS) у доменному середовищі kostiuk.net. До початку дослідження існувала проблема відсутності ефективного рішення для своєчасного оновлення Windows-систем, що створювало ризики вразливостей і кібератак, а також ускладнювало адміністрування в умовах обмежених ресурсів.

Для вирішення цих проблем було реалізовано лабораторне середовище з основним і резервним WSUS-серверами, інтегрованими з Active Directory через групові політики. Впроваджено захищене з'єднання HTTPS, часткову автоматизацію через PowerShell і механізми моніторингу за допомогою звітів WSUS та SQL-запитів. Обмеження, такі як недостатній дисковий простір і залежність від Windows Internal Database, були частково подолані переходом на повноцінний SQL Server і ручним схваленням оновлень, що забезпечило стабільність системи.

Отримані результати підтвердили ефективність розробленої моделі. Система продемонструвала контрольоване навантаження під час розгортання оновлень і стабільне відновлення після активної фази, а тестування працездатності засвідчило коректну доставку патчів клієнтам. Ключові переваги включають економичність, простоту інтеграції з існуючою інфраструктурою, оптимізацію мережних ресурсів і базову автоматизацію.

У майбутньому доцільно впровадити автоматизовану звітність через SQL-запити або PowerShell, розширити дисковий простір для повного завантаження оновлень і використати зовнішній моніторинг, наприклад, Zabbix або Grafana, для проактивного контролю. Перспективи включають інтеграцію з аналітичними платформами, такими як Power BI, і перехід на хмарні рішення для гібридних інфраструктур.

Таким чином, виконана дипломна робота підтвердила ефективність використання WSUS як основи для побудови централізованої системи управління оновленнями в доменній інфраструктурі. Отримані результати демонструють,

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				162
Змн.	Арк.	№ докум.	Підпис	Дата		

що навіть за умов обмежених ресурсів можна забезпечити стабільну доставку оновлень, забезпечити резервування, часткову автоматизацію та базовий моніторинг. Рекомендовані напрямки оптимізації — автоматизована звітність, повне завантаження оновлень і зовнішній моніторинг — відкривають шлях до масштабування системи з мінімальними витратами. Практична цінність реалізованого рішення полягає в його гнучкості, економічності та у можливості масштабування і простоті впровадження.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				163
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Active Directory Domain Services overview. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
2. Get-WsusServer (UpdateServices). Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/powershell/module/updateservices/get-wsusserver?view=windowsserver2025-ps>
3. Mastering Windows Server 2022: Comprehensive Administration of Your Windows Server Environment. de Gruyter GmbH, Walter, 2023.
4. Microsoft WSUS Patch Management Software | SolarWinds. Observability, Database, and IT Service Management | SolarWinds. URL: <https://www.solarwinds.com/patch-manager/use-cases/microsoft-patch-management-wsus>
5. Nicastro F. Security Patch Management. Taylor & Francis Group, 2019. 284 p.
6. Optimize WSUS client performance - Configuration Manager. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/troubleshoot/mem/configmgr/update-management/optimize-wsus-client-performance>
7. Plan Your WSUS Deployment. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/plan/plan-your-wsus-deployment>
8. Running WSUS Replica mode. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/manage/running-wsus-replica-mode>
9. Simister A. What Is Active Directory and How Does It Work?. Lepide Blog: A Guide to IT Security, Compliance and IT Operations.

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				164
Змн.	Арк.	№ докум.	Підпис	Дата		

URL: <https://www.lepide.com/blog/what-is-active-directory-and-how-does-it-work/>

10. Step 1 - Install the WSUS Server Role. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/1-install-the-wsus-server-role?tabs=server-manager>
11. Step 2 - Configure WSUS. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus>
12. Step 3 - Approve and Deploy Updates in WSUS. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/3-approve-and-deploy-updates-in-wsus>
13. Step 4 - Configure Group Policy Settings for Automatic Updates. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-configure-group-policy-settings-for-automatic-updates>
14. Try Microsoft Intune overview. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/try-intune-overview>
15. TLS/SSL Certificates | What are TLS/SSL Certificates and Why do We Need Them? | DigiCert. TLS/SSL Certificate Authority | Leader in Digital Trust | DigiCert. URL: <https://www.digicert.com/tls-ssl/tls-ssl-certificates>
16. What is WSUS? Microsoft Patch Management Tools. Patch & Endpoint Management Software | Automox. URL: <https://www.automox.com/blog/what-is-wsus>
17. What's new in SQL Server 2022 - SQL Server. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/sql/sql-server/what-s-new-in-sql-server-2022>

		Костюк І.О.			ДУ «Житомирська політехніка». 25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				165
Змн.	Арк.	№ докум.	Підпис	Дата		

18. What's new in Windows Server 2022. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022>
19. Windows Patching: The Quirks of Windows Patch Management & How to Stay Ready for Patch Tuesday | Puppet. *Puppet*. URL: <https://www.puppet.com/blog/windows-patching>
20. Windows Server documentation. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/uk-ua/windows-server/>
21. Windows Server Update Services (WSUS) overview. [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus>
22. Yasar K., Wright G. What is Windows Server Update Services (WSUS)? | Definition from TechTarget. SearchWindows Server. URL: <https://www.techtarget.com/searchwindowsserver/definition/Windows-Server-Update-Services-WSUS>

ДОДАТКИ

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				167
Змн.	Арк.	№ докум.	Підпис	Дата		

Організаційні одиниці, повний список користувачів та їх створення

Створення організаційних одиниць. У домені kostiuk.net було створено структуру організаційних одиниць (OU) для забезпечення логічного поділу користувачів за філіями, департаментами та адміністративними групами. Процес створення OU виконувався через консоль Active Directory Users and Computers (ADUC).

Нижче наведено приклад створення OU для філії Branch-21-7-1:

1. Відкрито консоль ADUC на доменному контролері DC-SRV-2022.
2. У дереві домену kostiuk.net обрано кореневий вузол.
3. Через контекстне меню (правий клік) обрано "New → Organizational Unit".

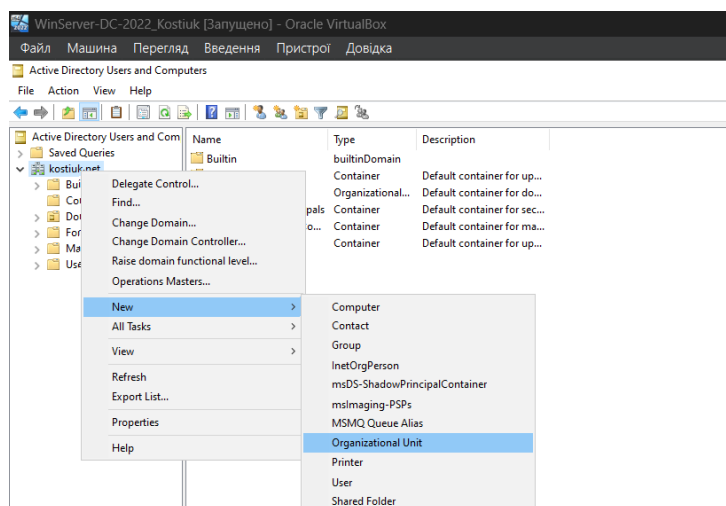


Рис. 1 – Створення нової організаційної одиниці через контекстне меню.

4. У вікні введено назву OU — "Branch-21-7-1" — та обрано прапорець "Protect container from accidental deletion" для захисту від випадкового видалення.
5. Натиснуто "ОК" для створення OU.

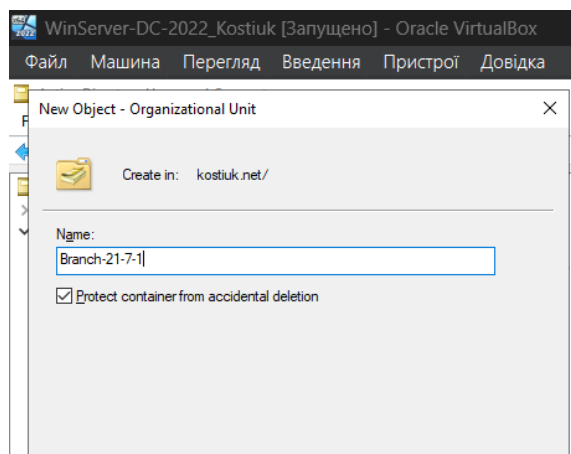


Рис. 2 – Введення назви організаційної одиниці

Аналогічно створено інші OU: Branch-21-7-2, Branch-21-7-3, а також вкладені OU для департаментів (Dep-21-7-X-Y) та адміністраторів (Admins-21-7-X), де X — номер філії (1, 2, 3), Y — номер департаменту (1, 2). Структуру OU зображено на схемі:

- kostiuk.net
 - Branch-21-7-1
 - Dep-21-7-1-1
 - Dep-21-7-1-2
 - Admins-21-7-1
 - Branch-21-7-2
 - Dep-21-7-2-1
 - Dep-21-7-2-2
 - Admins-21-7-2
 - Branch-21-7-3
 - Dep-21-7-3-1
 - Dep-21-7-3-2
 - Admins-21-7-3

Повний список створених користувачів. Нижче наведено список користувачів із логінами, створеними за шаблоном: для користувачів департаментів — "dep(номер_департаменту)-(ініціали)", для адміністраторів — "b(номер_філії)-

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				169
Змн.	Арк.	№ докум.	Підпис	Дата		

Admin(ініціали)". Ініціали формувалися як перші літери прізвища, імені та по батькові (наприклад, для Іванова Андрія Петровича — "іар").

Branch-21-7-1

– **Dep-21-7-1-1:**

- Іванов Андрій Петрович — логін: dep11-iar
- Коваль Олексій Сергійович — логін: dep11-kos
- Мельник Роман Іванович — логін: dep11-mri

– **Dep-21-7-1-2:**

- Шевченко Дмитро Олегович — логін: dep12-shdo
- Бондар Антон Юрійович — логін: dep12-bay
- Сидоренко Артем Володимирович — логін: dep12-sav

– **Admins-21-7-1:**

- Костюк Ігор Олександрович — логін: b1-AdminKIO

Branch-21-7-2

– **Dep-21-7-2-1:**

- Гриценко Богдан Сергійович — логін: dep21-gbs
- Кравчук Владислав Ігорович — логін: dep21-kvi
- Руденко Назар Віталійович — логін: dep21-rnv

– **Dep-21-7-2-2:**

- Мороз Андрій Арсенович — логін: dep22-maa
- Петренко Євген Євгенович — логін: dep22-pee
- Дяченко Микита Вікторович — логін: dep22-dmv

– **Admins-21-7-2:**

- Костюк Сергій Олександрович — логін: b2-AdminKSO

Branch-21-7-3

– **Dep-21-7-3-1:**

- Савченко Юрій Миколайович — логін: dep31-syum
- Захарченко Микола Ростиславович — логін: dep31-zhmr
- Лисенко Олександр Вадимович — логін: dep31-lov

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росініський Ю.М.				170
Змн.	Арк.	№ докум.	Підпис	Дата		

– **Dep-21-7-3-2:**

- Ткаченко Владлена Миколаївна — логін: dep32-tvm
- Кузьменко Артур Ігорович — логін: dep32-kai
- Левченко Богдан Валерійович — логін: dep32-lbv

– **Admins-21-7-3:**

- Костюк Олександр Миколайович — логін: b3-AdminKOM

Нижче наведено описи скріншотів створення кожного користувача через консоль Active Directory Users and Computers (ADUC). Скріншоти демонструють процес створення облікових записів із зазначеними логінами у відповідних OU

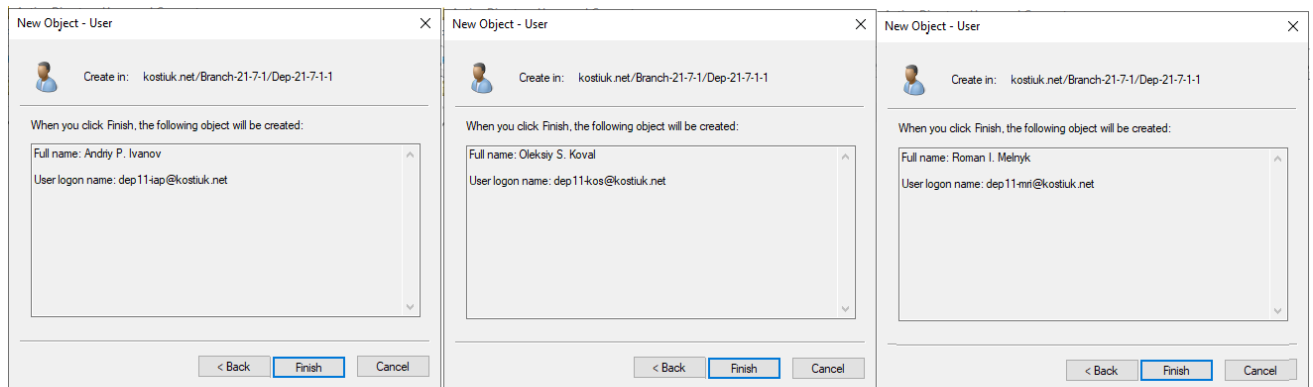


Рис. 3 – Створення користувачів для Dep-21-7-1-1

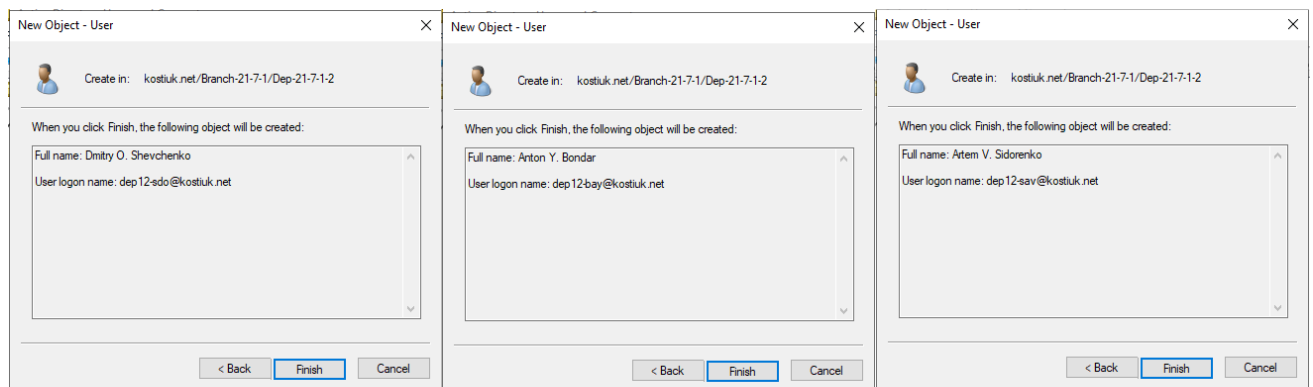


Рис. 4 – Створення користувачів для Dep-21-7-1-2

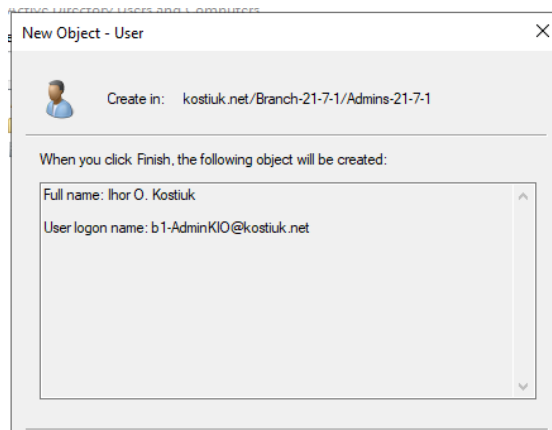


Рис. 5 – Створення користувача для Admins-21-7-1

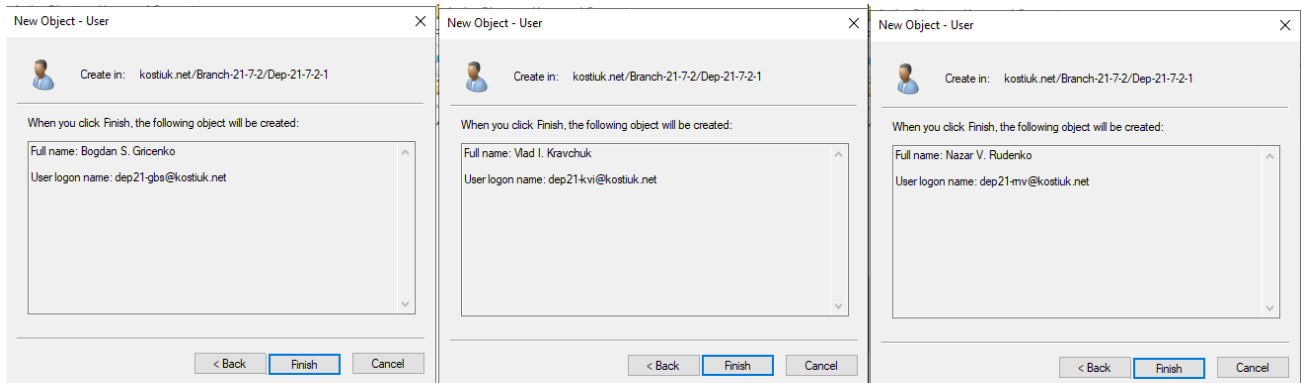


Рис. 6 – Створення користувачів для Dep-21-7-2-1

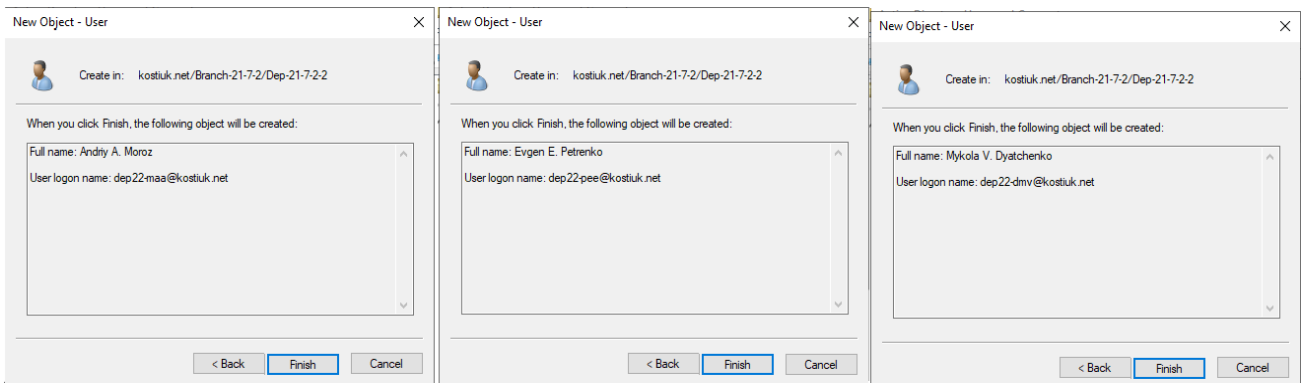


Рис. 7 – Створення користувачів для Dep-21-7-2-2

New Object - User

Create in: kostiuk.net/Branch-21-7-2/Admins-21-7-2

When you click Finish, the following object will be created:

Full name: Serhiy O. Kostiuk
User logon name: b2-AdminKSO@kostiuk.net

Рис. 8 – Створення користувача для Admins-21-7-2

New Object - User

Create in: kostiuk.net/Branch-21-7-3/Dep-21-7-3-1

When you click Finish, the following object will be created:

Full name: Yuri M. Savchenko
User logon name: dep31-sym@kostiuk.net

New Object - User

Create in: kostiuk.net/Branch-21-7-3/Dep-21-7-3-1

When you click Finish, the following object will be created:

Full name: Mikola R. Zaharchenko
User logon name: dep31-zmr@kostiuk.net

New Object - User

Create in: kostiuk.net/Branch-21-7-3/Dep-21-7-3-1

When you click Finish, the following object will be created:

Full name: Alexander V. Lysenko
User logon name: dep31-lav@kostiuk.net

Рис. 9 – Створення користувачів для Dep-21-7-3-1

New Object - User

Create in: kostiuk.net/Branch-21-7-3/Dep-21-7-3-2

When you click Finish, the following object will be created:

Full name: Vladlena M. Tkachenko
User logon name: dep32-tvl@kostiuk.net

New Object - User

Create in: kostiuk.net/Branch-21-7-3/Dep-21-7-3-2

When you click Finish, the following object will be created:

Full name: Artur I. Kusmenko
User logon name: dep32-kai@kostiuk.net

New Object - User

Create in: kostiuk.net/Branch-21-7-3/Dep-21-7-3-2

When you click Finish, the following object will be created:

Full name: Bogdan V. Levchenko
User logon name: dep32-lbv@kostiuk.net

Рис. 10 – Створення користувачів для Dep-21-7-3-2

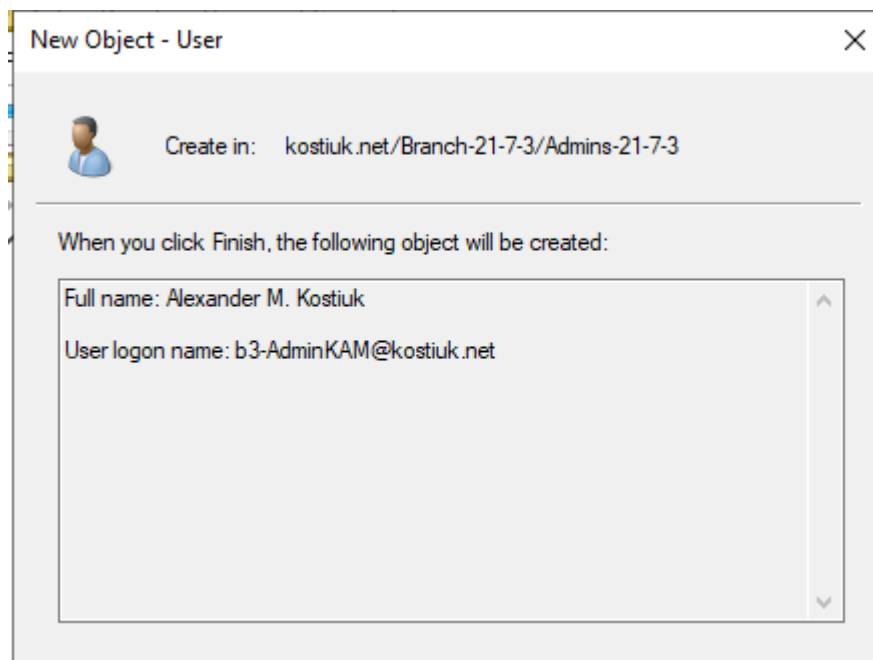


Рис. 11 – Створення користувача для Admins-21-7-3

SQL-запити до бази SUSDB

Список клієнтів. Цей запит витягує основну інформацію про всіх клієнтів, зареєстрованих у WSUS, включаючи доменні імена, IP-адреси та часи останнього звіту й синхронізації. Призначений для оцінки активності та наявності клієнтів у системі.

Лістинг запити:

```
SELECT
    FullDomainName,
    IPAddress,
    LastReportedStatusTime,
    LastSyncTime
FROM
    tbComputerTarget
ORDER BY
    LastReportedStatusTime DESC;
```

	FullDomainName	IPAddress	LastReportedStatusTime	LastSyncTime
1	wsus-prim-2019.kostiuk.net	fe80::7946:267c:6fd:e1d3%5	2025-06-05 00:44:29.020	2025-06-05 00:37:06.010
2	dc-srv-2022.kostiuk.net	192.168.7.10	2025-06-04 01:13:48.737	2025-06-04 01:05:02.107
3	wsus-repl-2019.kostiuk.net	192.168.7.21	2025-06-04 00:27:16.667	2025-06-04 00:27:14.243
4	win-10-1-kost.kostiuk.net	192.168.7.100	2025-06-03 22:33:53.080	2025-06-03 22:33:44.880
5	win-11-1-kost.kostiuk.net	192.168.7.101	2025-05-25 19:17:29.853	2025-05-25 20:54:29.650
6	win-10-2-kost.kostiuk.net	192.168.7.102	2025-05-25 04:52:34.323	2025-05-25 04:43:32.383

Рис. 1 – Результат виконання запиту.

Затверджені оновлення та їхні цільові групи. Запит призначений для аналізу зв'язку затверджених оновлень із відповідними цільовими групами клієнтів. Використовується для перевірки коректності схвалень, хоча в основному аналізі не застосовувався.

Лістинг запити:

```
SELECT
    p.Title,
    tg.TargetID,
    tg.TargetGroupID
FROM
    tbLocalizedProperty p
JOIN
    tbUpdate u ON p.LocalizedPropertyID = u.LocalUpdateID
JOIN
    tbTargetInTargetGroup tg ON tg.TargetID = u.LocalUpdateID
```

```
ORDER BY
    p.Title;
```

	Title	TargetID	TargetGroupID
1	Actualizaciones críticas	7	D374F42A-9BE2-4163-A0FA-3C86A401B7A7
2	Critical Updates	6	7FC38D85-8BA9-45ED-AF3E-4DECDDDFDE73
3	Critical Updates	6	6150123F-50FA-40D0-85C0-919525059F60
4	Důležité aktualizace	2	CC675BF3-76B7-4479-9776-1E580C07F589
5	Vigtige opdateringer	3	F3682C31-B8F3-4DDC-A4B9-661C899FE314
6	Wichtige Updates	4	8DF5C861-B892-4061-B47B-F1635340F09D
7	Wichtige Updates	4	F5CC5F03-8708-4533-830A-F3DE070EE88C
8	Κρίσιμες ενημερωμένες εκδόσεις	5	25669B04-3627-4290-9250-3EA7BC6EA2E6
9	Κρίσιμες ενημερωμένες εκδόσεις	5	6150123F-50FA-40D0-85C0-919525059F60
10	التحديثات الضرورية	1	99E4F46B-6B69-46E8-8D07-E416A8858680
11	التحديثات الضرورية	1	8DF5C861-B892-4061-B47B-F1635340F09D

Рис. 2 – Результат виконання запиту.

Зведена статистика Installed / Needed / NotApplicable. Цей запит обчислює кількість оновлень у статусах "встановлено", "потрібно" та "не застосовується" для кожного клієнта. Призначений для оцінки загального стану оновлень у системі.

Лістинг запита:

```
SELECT
    c.FullDomainName,
    SUM(CASE WHEN s.SummarizationState = 1 THEN 1 ELSE 0 END) AS Installed,
    SUM(CASE WHEN s.SummarizationState = 2 THEN 1 ELSE 0 END) AS Needed,
    SUM(CASE WHEN s.SummarizationState = 3 THEN 1 ELSE 0 END) AS NotApplicable
FROM
    tbUpdateStatusPerComputer s
JOIN
    tbComputerTarget c ON s.TargetID = c.TargetID
GROUP BY
    c.FullDomainName
ORDER BY
    Needed DESC;
```

	FullDomainName	Installed	Needed	NotApplicable
1	wsus-repl-2019.kostiuk.net	0	2	0
2	wsus-prim-2019.kostiuk.net	0	1	0
3	win-10-1-kost.kostiuk.net	0	0	0
4	win-11-1-kost.kostiuk.net	0	0	0
5	win-10-2-kost.kostiuk.net	0	0	0

Рис. 3 – Результат виконання запиту.

Потрібні оновлення. Запит витягує детальний список оновлень зі статусом "потрібно" (SummarizationState = 2), включаючи назви оновлень, клієнтів і час останнього звіту. Призначений для планування подальшого схвалення та розгортання.

Лістинг запити:

```
SELECT
    c.FullDomainName AS [Computer Name],
    lp.Title AS [Update Title],
    s.SummarizationState AS [Status],
    c.LastReportedStatusTime AS [Last Report]
FROM
    tbUpdateStatusPerComputer s
JOIN
    tbComputerTarget c ON s.TargetID = c.TargetID
JOIN
    tbUpdate u ON s.LocalUpdateID = u.LocalUpdateID
JOIN
    tbRevision r ON u.LocalUpdateID = r.LocalUpdateID
JOIN
    tbLocalizedPropertyForRevision lpr ON r.RevisionID = lpr.RevisionID
JOIN
    tbLocalizedProperty lp ON lpr.LocalizedPropertyID = lp.LocalizedPropertyID
WHERE
    s.SummarizationState = 2 -- 2 = Needed
ORDER BY
    c.FullDomainName, lp.Title;
```

	Computer Name	Update Title	Status	Last Report
1	wsus-prim-2019.kostiuk.net	2021-08 Actualización de pila de mantenimiento de Wi...	2	2025-06-05 00:44:29.020
2	wsus-prim-2019.kostiuk.net	2021-08 Actualizarea stivei de servicii pentru Window...	2	2025-06-05 00:44:29.020
3	wsus-prim-2019.kostiuk.net	2021-08 Aggiornamento dello stack di manutenzione p...	2	2025-06-05 00:44:29.020
4	wsus-prim-2019.kostiuk.net	2021-08 Aktualizácia balíka služieb pre Windows Ser...	2	2025-06-05 00:44:29.020
5	wsus-prim-2019.kostiuk.net	2021-08 Aktualizacja stosu obsługi Windows Server 2...	2	2025-06-05 00:44:29.020
6	wsus-prim-2019.kostiuk.net	2021-08 apkalpošanas steka atjauninājums operētājsi...	2	2025-06-05 00:44:29.020
7	wsus-prim-2019.kostiuk.net	2021-08 Atualização da pilha de manutenção do Win...	2	2025-06-05 00:44:29.020
8	wsus-prim-2019.kostiuk.net	2021-08 Ažuriranje servisnog stoga za Windows Serv...	2	2025-06-05 00:44:29.020
9	wsus-prim-2019.kostiuk.net	2021-08 hooldusvima värskendus x64-põhistele süste...	2	2025-06-05 00:44:29.020
10	wsus-prim-2019.kostiuk.net	2021-08 Mise à jour de la pile de maintenance pour W...	2	2025-06-05 00:44:29.020
11	wsus-prim-2019.kostiuk.net	2021-08 Onderhoudsstackupdate voor Windows Serv...	2	2025-06-05 00:44:29.020
12	wsus-prim-2019.kostiuk.net	2021-08 Opdatering af stabelpakke til Windows Serve...	2	2025-06-05 00:44:29.020
13	wsus-prim-2019.kostiuk.net	2021-08 Összegző frissítés Windows Server 2019 ren...	2	2025-06-05 00:44:29.020
14	wsus-prim-2019.kostiuk.net	2021-08 Posodobitev servisnega sklada za Windows ...	2	2025-06-05 00:44:29.020
15	wsus-prim-2019.kostiuk.net	2021-08 Servicing Stack Update for Windows Server ...	2	2025-06-05 00:44:29.020
16	wsus-prim-2019.kostiuk.net	2021-08 Servicing Stack Update für Windows Server ...	2	2025-06-05 00:44:29.020

Рис. 4 – Результат виконання запиту (фрагмент).

Несинхронізовані машини (за останні 3 дні). Цей запит виявляє клієнтів, які не синхронізувалися протягом останніх 3 днів, порівнюючи час останнього

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росіньський Ю.М.				177
Змн.	Арк.	№ докум.	Підпис	Дата		

звіту з поточною датою. Призначений для ідентифікації потенційних проблем, хоча результати виявилися порожніми, що свідчить про активність усіх клієнтів.

Лістинг запита:

```
SELECT
    FullDomainName,
    LastSyncTime,
    LastReportedStatusTime,
    DATEDIFF(day, LastReportedStatusTime, GETDATE()) AS DaysSinceLastReport
FROM
    tbComputerTarget
WHERE
    LastReportedStatusTime < DATEADD(day, -3, GETDATE())
ORDER BY
    LastReportedStatusTime ASC;
```

Results		Messages		
	FullDomainName	LastSyncTime	LastReportedStatusTime	DaysSinceLastReport
1	win-10-2-kost.kostiuk.net	2025-05-25 04:43:32.383	2025-05-25 04:52:34.323	11
2	win-11-1-kost.kostiuk.net	2025-05-25 20:54:29.650	2025-05-25 19:17:29.853	11

Рис. 5 – Результат виконання запиту.

Опис скрипта моніторингу оновлень WSUS

Опис функціональності скрипта. Скрипт розроблено для моніторингу статусу оновлень на резервному WSUS-сервері (за замовчуванням WSUS-REPL-2019) у доменному середовищі kostiuk.net. Його основне призначення — аналіз затверджених критичних і безпекових оновлень для заданих груп комп'ютерів (Win10-Standard, Win11-Standard), виявлення проблемних оновлень (потрібних або невдалих) і збереження результатів у CSV-файл із паралельним логуванням процесу.

Скрипт виконує наступні завдання:

- Ініціалізацію параметрів (сервер, порт, шляхи для логів і CSV, групи для моніторингу) із можливістю їхньої зміни через командний рядок.
- Перевірку і створення директорії для логів (C:\WSUS-Scripts), якщо її не існує.
- Підключення до WSUS-сервера та обробку помилок з'єднання.
- Аналіз оновлень для кожної групи, фільтруючи за типом (Security Updates, Critical Updates), датою (останні 12 місяців), затвердженням і відповідністю ОС (Windows 10 або 11).
- Збір статистики (кількість потрібних, невдалих і встановлених оновлень) із обмеженням попереджень про відсутність даних (максимум 5).
- Експорт результатів у CSV-файл із полями: назва групи, заголовок оновлення, класифікація, продукти, кількість потрібних/невдалих/встановлених оновлень.
- Логування всіх дій у текстовий файл із позначенням розміру лог-файлу.

Алгоритм роботи скрипта. Скрипт працює за наступним алгоритмом:

1. **Налаштування параметрів:** Ініціалізація змінних (сервер WSUS-REPL-2019, порт 8530, шляхи логів і CSV із часовою міткою, групи Win10-Standard і Win11-Standard).

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				179
Змн.	Арк.	№ докум.	Підпис	Дата		

2. **Підготовка середовища:** Створення директорії C:\WSUS-Scripts і початок логування через Start-Transcript.
3. **Підключення до WSUS:** Використання Get-WsusServer для з'єднання; при помилці скрипт завершується з повідомленням.
4. **Аналіз груп:** Для кожної групи викликається функція Get-UpdateStatus, яка:
 - Знаходить групу за назвою.
 - Перевіряє кількість комп'ютерів у групі.
 - Фільтрує оновлення за критеріями (тип, дата, затвердження, ОС).
 - Збирає статистику встановлення для кожного оновлення.
5. **Обробка результатів:** Збір даних у масив \$allResults, фільтрація проблемних оновлень і експорт у CSV.
6. **Діагностика та завершення:** Перевірка невдалих оновлень, виведення розміру лог-файлу, завершення логування через Stop-Transcript.

Лістинг скрипта:

```
# Налаштування параметрів
param (
    [string]$wsusServer = "WSUS-REPL-2019", # Змініть на ваш резервний сервер
    [int]$port = 8530,
    [string]$logPath = "C:\WSUS-Scripts\MonitorUpdatesLog_$(Get-Date -Format
'yyyyMMdd_HH:mm:ss').txt",
    [string]$csvPath = "C:\WSUS-Scripts\MonitorUpdatesResults_$(Get-Date -Format
'yyyyMMdd_HH:mm:ss').csv",
    [string[]]$groupsToMonitor = @("Win10-Standard", "Win11-Standard")
)
$maxWarnings = 5 # Максимальна кількість попереджень

# Створення директорії для логів, якщо її немає
if (-not (Test-Path "C:\WSUS-Scripts")) {
    New-Item -Path "C:\WSUS-Scripts" -ItemType Directory
}

# Початок логування
Start-Transcript -Path $logPath
```

```

Write-Output "Підключення до WSUS-сервера $wsusServer о $(Get-Date)..."
$wsus = Get-WsusServer -Name $wsusServer -PortNumber $port

if (-not $wsus) {
    Write-Error "Не вдалося підключитися до WSUS!"
    Stop-Transcript
    exit
}

# Функція для отримання статусу оновлень для групи
function Get-UpdateStatus {
    param ($groupName)
    $group = $wsus.GetComputerTargetGroups() | Where-Object { $_.Name -eq $groupName }
    if (-not $group) {
        Write-Warning "Група '$groupName' не знайдена. Пропускаємо..."
        return @()
    }

    # Перевірка кількості комп'ютерів у групі
    $computers = $wsus.GetComputerTargets() | Where-Object { $_.ComputerTarget-
GroupIds -contains $group.Id }
    Write-Output "Група '$groupName' містить $($computers.Count) комп'ютерів."
    if ($computers.Count -eq 0) {
        Write-Warning "У групі '$groupName' немає комп'ютерів. Пропускаємо..."
        return @()
    }

    Write-Output "Аналіз оновлень для групи '$groupName'..."
    $updates = $wsus.GetUpdates() | Where-Object {
        $_.UpdateClassificationTitle -in @("Security Updates", "Critical Updates")
    -and
        $_.CreationDate -ge (Get-Date).AddYears(-1) -and
        $_.IsApproved -eq $true -and
        (
            ($groupName -eq "Win10-Standard" -and $_.ProductTitles -contains "Win-
dows 10") -or
            ($groupName -eq "Win11-Standard" -and $_.ProductTitles -contains "Win-
dows 11")
        )
    }

    Write-Output "Знайдено $($updates.Count) затверджених оновлень для аналізу в
групі '$groupName'..."

    $results = @()
    $warningCount = 0
    foreach ($update in $updates) {
        try {
            $installationInfo = $update.GetUpdateInstallationInfoPerComputerTar-
get($group)

```

		Костюк І.О.			ДУ «Житомирська політехніка».25.123.07.000 - ПЗ	Арк.
		Росієнський Ю.М.				181
Змн.	Арк.	№ докум.	Підпис	Дата		

```

        if (-not $installationInfo) {
            if ($warningCount -lt $maxWarnings) {
                Write-Warning "Інформація про встановлення для '$($update.Title)' відсутня."
                $warningCount++
            }
            elseif ($warningCount -eq $maxWarnings) {
                Write-Warning "Додаткові попередження про відсутність інформації приховані (загалом більше $maxWarnings випадків)."
                $warningCount++
            }
            continue
        }

        $neededCount = ($installationInfo | Where-Object { $_.UpdateInstallationState -eq "Needed" }).Count
        $failedCount = ($installationInfo | Where-Object { $_.UpdateInstallationState -eq "Failed" }).Count
        $installedCount = ($installationInfo | Where-Object { $_.UpdateInstallationState -eq "Installed" }).Count

        if ($neededCount -gt 0 -or $failedCount -gt 0) {
            $productsString = ($update.ProductTitles -join ", ").Substring(0, [Math]::Min(100, ($update.ProductTitles -join ", ").Length))
            $results += [PSCustomObject]@{
                Group           = $groupName
                Title            = [string]$update.Title
                Classification    = [string]$update.UpdateClassificationTitle
                Products         = $productsString
                NeededCount      = $neededCount
                FailedCount      = $failedCount
                InstalledCount    = $installedCount
                IsApproved       = $update.IsApproved
            }
        }
    }
    catch {
        Write-Warning "Помилка при обробці оновлення '$($update.Title)': $_"
    }
}

Write-Output "Завершено аналіз для групи '$groupName'. Знайдено $($results.Count) проблемних оновлень."
return $results
}

# Збір даних для всіх груп
$allResults = @() # Очищаємо $allResults
foreach ($group in $groupsToMonitor) {
    $groupResults = Get-UpdateStatus -groupName $group
    if ($groupResults -and $groupResults.Count -gt 0) {
        $allResults += $groupResults
    }
}

```

```

    }
    Write-Output "Обробка групи '$group' завершена."
}

# Діагностика $allResults
Write-Output "Діагностика: Загальна кількість елементів у allResults: $($allResults.Count)"
if ($allResults.Count -gt 0) {
    Write-Output "Перший елемент у allResults:"
    Write-Output ($allResults[0] | Format-List | Out-String)
}

# Виведення результатів і експорт у CSV
if ($allResults.Count -eq 0) {
    Write-Output "Жодних проблемних або потрібних оновлень не знайдено."
} else {
    Write-Output "Знайдено $($allResults.Count) оновлень, які потребують уваги."
    Write-Output "Експортуємо результати в CSV: $csvPath"
    $allResults = $allResults | Where-Object { $_ -ne $null }
    if ($allResults.Count -gt 0) {
        $allResults | Export-Csv -Path $csvPath -NoTypeInfoInformation -Encoding UTF8
    } else {
        Write-Warning "Після фільтрації allResults порожній. Експорт у CSV не виконано."
    }
}

# Перевірка невдалих оновлень для сповіщень
$failedUpdates = $allResults | Where-Object { $_ -ne $null -and $_.FailedCount -gt 0 }
if ($failedUpdates) {
    Write-Warning "Знайдено $($failedUpdates.Count) невдалих оновлень. Перевірте CSV для деталей."
}

# Перевірка розміру лог-файлу
$logSize = (Get-Item $logPath).Length / 1KB
Write-Output "Розмір лог-файлу: $logSize KB"

# Повідомлення про завершення
Write-Output "Скрипт завершено о $(Get-Date)."

# Завершення логування
Stop-Transcript

```

```
Administrator: Windows PowerShell
PS C:\Users\Administrator.KOSTIUK> cd C:\WSUS-Scripts
PS C:\WSUS-Scripts> .\Monitor-WSUS-Updates.ps1
Transcript started, output file is C:\WSUS-Scripts\MonitorUpdatesLog_20250602_222609.txt
Підключення до WSUS-сервера WSUS-REPL-2019 о 06/02/2025 22:26:09...
Обробка групи 'win10-Standard' завершена.
Обробка групи 'win11-Standard' завершена.
Діагностика: Загальна кількість елементів у allResults: 8
Перший елемент у allResults:
Група 'win10-Standard' містить 2 комп'ютерів.

Знайдено 8 оновлень, які потребують уваги.
Експортуємо результати в CSV: C:\WSUS-Scripts\MonitorUpdatesResults_20250602_222609.csv
Розмір лог-файлу: 1.296875 KB
Скрипт завершено о 06/02/2025 22:26:28.
Transcript stopped, output file is C:\WSUS-Scripts\MonitorUpdatesLog_20250602_222609.txt
PS C:\WSUS-Scripts>
```

Рис. 1 – Перевірка виконання скрипта

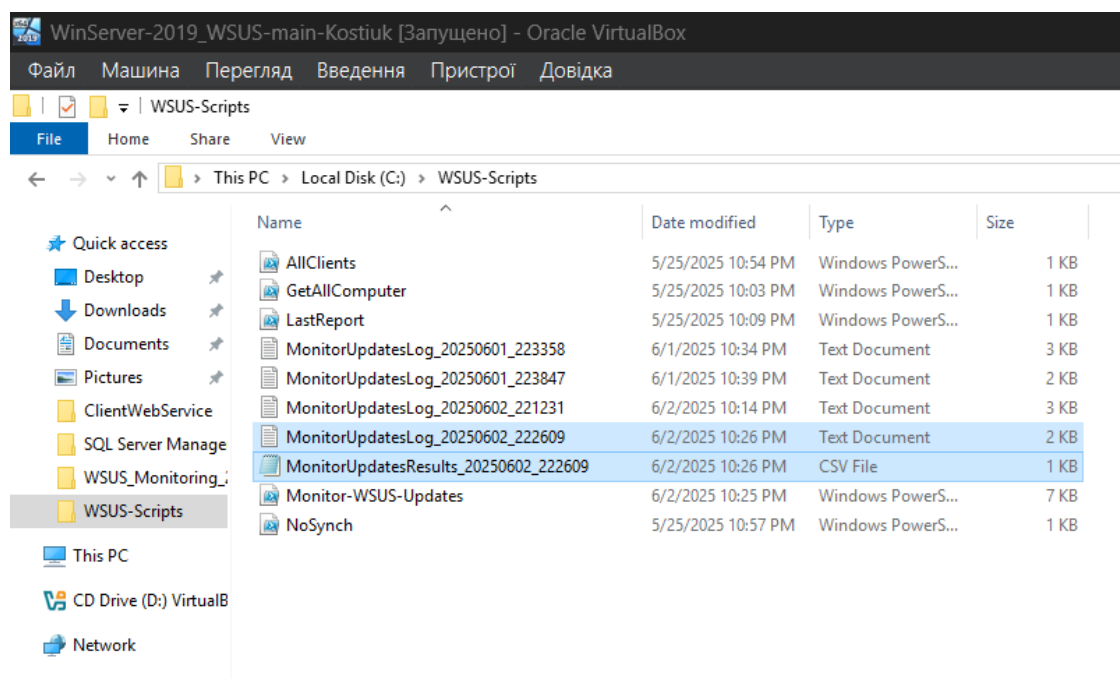


Рис. 2 – Перевірка створення логів.

Файл

Машина

Перегляд

Введення

Пристрої

Довідка

MonitorUpdatesLog_20250602_222609 - Notepad

File Edit Format View Help

Windows PowerShell transcript start

Start time: 20250602222609

Username: KOSTIUK\Administrator

RunAs User: KOSTIUK\Administrator

Configuration Name:

Machine: WSUS-PRIM-2019 (Microsoft Windows NT 10.0.17763.0)

Host Application: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe

Process ID: 4092

PSVersion: 5.1.17763.7309

PSEdition: Desktop

PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.7309

BuildVersion: 10.0.17763.7309

CLRVersion: 4.0.30319.42000

WSManStackVersion: 3.0

PSRemotingProtocolVersion: 2.3

SerializationVersion: 1.1.0.1

Transcript started, output file is C:\WSUS-Scripts\MonitorUpdatesLog_20250602_222609.txt

Підключення до WSUS-сервера WSUS-REPL-2019 о 06/02/2025 22:26:09...

Обробка групи 'Win10-Standard' завершена.

Обробка групи 'Win11-Standard' завершена.

Діагностика: Загальна кількість елементів у allResults: 8

Перший елемент у allResults:

Група 'Win10-Standard' містить 2 комп'ютерів.

Знайдено 8 оновлень, які потребують уваги.

Експортуємо результати в CSV: C:\WSUS-Scripts\MonitorUpdatesResults_20250602_222609.csv

Розмір лог-файлу: 1.296875 KB

Скрипт завершено о 06/02/2025 22:26:28.

Windows PowerShell transcript end

End time: 20250602222628

Рис. 3 – Перевірка вмісту логу.