

О.В. СУБОТИН, О.В. РАЗЖИВІН
О.О. КОЙФМАН, В.П. АМЕЛІН

ДОСЛІДЖЕННЯ І РОЗРОБКА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ УСТАНОВИ

Навчальний посібник



ОДІ
П/НОЗ

ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«МЕТІНВЕСТ ПОЛІТЕХНІКА»

**ДОСЛІДЖЕННЯ І РОЗРОБКА
ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ
СИСТЕМИ УСТАНОВИ**

Навчальний посібник

Одеса • 2026 • Олді+

УДК 004.7+004.2(075.8)
Д70

Автори:

О. В. Суботін, О. В. Разживін, О. О. Койфман, В. П. Амелін

Рецензенти:

Д. Ю. Захаренков – доктор філософії, доцент, завідувач кафедри кібербезпеки та захисту інформації, ПВНЗ «Європейський університет», м. Київ;

О. Ф. Тарасов – доктор технічних наук, професор, завідувач кафедри комп'ютерних інформаційних технологій, Донбаська державна машинобудівна академія, м. Краматорськ;

Ю. С. Білоіваненко – начальник відділу комп'ютерно-інтегрованих систем, ТОВ «САНРАЙЗ ЕНЕРГЕТИКА», м. Житомир;

А. В. Голоядов – головний спеціаліст з ІТ-технологій ПРАТ «КАМЕТ-СТАЛЬ», м. Кам'янське

Рекомендовано до друку Вченою радою

ТОВ «Технічний університет «Метінвест політехніка»

(протокол № 10 від 07.07.2026 р.)

Д70

Дослідження і розробка інформаційно-телекомунікаційної системи установи : навчальний посібник / О. В. Суботін, О. В. Разживін, О. О. Койфман, В. П. Амелін ; ТОВ «Технічний університет «Метінвест Політехніка». – Одеса : Олді+, 2026. – 156 с.

ISBN 978-617-8555-09-2

У навчальному посібнику розглядаються питання, які стосуються дослідження і розробки інформаційно-телекомунікаційної системи установи з метою підвищення надійності її роботи. Проводиться аналіз існуючої інформаційно-телекомунікаційної системи установи, сформульовано вимоги до неї, показано побудову нової системи на базі застарілої. Також проводиться аналіз вимог до програмного забезпечення, наведені державні стандарти побудови системи. В якості прикладу проектується й будується нова топологія мережі, розробляється план IP-адресації, створюються програмні коди конфігурації активного мережевого обладнання, створюється домен на базі ОС Windows Server, розподіляється між серверами й розгорнуто ролі AD, DNS, DHCP, FS, WDS, VPN, WSUS, Print. Показано організацію централізованого антивірусного захисту в домені, розробку механізмів резервного копіювання і зберігання даних, централізованого оновлення програмного забезпечення, контролю переміщення складових системи в межах установи, а також обслуговування інформаційної інфраструктури. Наведено аналіз законодавчих змін щодо захисту інформації.

Посібник може бути використаний при вивченні дисциплін «Комп'ютерні мережі», «Технологія проектування комп'ютерних систем», «Проектування та дослідження комп'ютерних систем та мереж», «Мережі та протоколи систем автоматизації», «Технології захисту даних і інформаційної безпеки», при виконанні курсових та випускових кваліфікаційних робіт. Також викладений матеріал може бути корисним як довідковий матеріал для професіоналів, які проєктують або супроводжують інформаційно-телекомунікаційні системи.

УДК 004.7+004.2(075.8)

ISBN 978-617-8555-09-2

© О. В. Суботін, О. В. Разживін, О. О. Койфман, В. П. Амелін, 2026

© ТОВ «Технічний університет «Метінвест Політехніка», 2026

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ	6
ВСТУП	9
1. АНАЛІЗ НАЯВНОЇ МЕРЕЖЕВОЇ ТА ОБЧИСЛЮВАЛЬНОЇ ІНФРАСТРУКТУРИ УСТАНОВИ	13
1.1. Визначення установи. Структура, штат, програмне забезпечення. Характеристика споживаних мережевих послуг	13
1.2. Наявна інформаційно-телекомунікаційна інфраструктура установи (топологія, мережа передачі даних та її характеристика)	16
1.3. Розрахунок поточних характеристик мережі	17
1.4. Висновки, цілі і завдання модернізації ІТС	24
2. ВИМОГИ ДО ПРОЄКТУВАННЯ І ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ В УСТАНОВІ	27
2.1. Система захисту інформації в установі	28
2.2. Вимоги до програмного забезпечення та типи ліцензій	35
2.3. Планування мережевої інфраструктури	38
2.4. Закупівля обладнання, оплата послуг та робіт з монтажу і налагодження системи згідно із затвердженим планом та діючим законодавством України	44
2.5. Підсумок загальних витрат	50

3. РОЗГОРТАННЯ	
ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ	
В УСТАНОВІ	53
3.1. Побудова мережі	53
3.2. Побудова домену Windows	75
3.3. Антивірусний захист у домені Windows	104
3.4. Сервіси обміну інформацією між користувачами	110
3.5. Virtual Private Network (VPN) під Hyper-V в домені Windows	111
3.6. Система охорони та контролю доступу до приміщення, система відеоспостереження	116
4. ПРАКТИЧНІ РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ	
СИСТЕМИ	119
4.1. Розрахунок навантаження та аналіз ефективності спроектованої мережі	119
4.2. Оновлення ПЗ	120
4.3. Обслуговування ІТС	123
4.4. Контроль наявності та переміщення техніки в межах установи	123
ВИСНОВКИ	129
ЛІТЕРАТУРНІ ДЖЕРЕЛА	132
ДОДАТКИ	138
Додаток А. Структура та штатна чисельність установи ..	138
Додаток Б. Програмне забезпечення, яке використовується установою	140
Додаток В. Топологія мережі ДУ	141
Додаток Г. Загальний трафік в установі в розрізі програмного забезпечення	142

Додаток Д. Кількість користувачів у розрізі програмного забезпечення й поверхів (топології)	143
Додаток Е. Нова топологія мережі ДУ	144
Додаток Ж. План будівлі	145
Додаток И. Файл конфігурації маршрутизатора R1	148
Додаток К. Скрипт контролю авторизації користувачів	154

ПЕРЕЛІК СКОРОЧЕНЬ

ІТС – інформаційно-телекомунікаційна система. Організаційно-технічна сукупність, що складається з автоматизованої системи та мережі передачі даних.

ДУ – установа державної форми власності.

КУ – комерційні установи різних форм власності та підпорядкування.

КП ДВ – комп'ютерна програма з діловодства. Клієнт-серверний додаток для здійснення електронного документообігу в межах установи, організації або підприємства.

ОЗ – засідання або нарада в режимі онлайн.

ВКЗ – сервіс відеоконференцзв'язку. Використовується в установах для проведення засідань або нарад в режимі онлайн з використанням засобів мультимедіа.

Зал ОЗ – Зал засідання або Актова зала. Спеціальне приміщення для проведення ОЗ, яке обладнане засобами мультимедіа, системою фіксації ОЗ (запису аудіо та відео).

ПЗ – програмне забезпечення.

БД – база даних.

БФП – багатофункціональний пристрій. Офісне обладнання, де функції друку, сканера і копіра поєднано в одному пристрої.

КСЗІ – комплексна система захисту інформації. Це сукупність організаційних і інженерно-технічних заходів, програмно-апаратних засобів, які забезпечують захист інформації у відповідності до нормативно-правових документів в галузі захисту інформації, та дозволяють обробляти інформацію, до якої, відповідно до її призначення, правового статусу та грифу обмеження доступу, висуваються вимоги

по забезпеченню її конфіденційності, цілісності та доступності в ході її обробки.

КСЗІ – служба захисту інформації. Спеціально створений структурний підрозділ установи, який відповідає за КСЗІ.

ТЗІ – технічний захист інформації. Термін включає як програмну, так і апаратну складову.

КЕКВ – код економічної класифікації видатків. Бюджетна класифікація видатків, призначена для чіткого розмежування видатків бюджетних установ та одержувачів бюджетних коштів за економічними характеристиками операцій, що здійснюють відповідно до функцій держави та місцевого самоврядування.

КШ – комунікаційна шафа. Закрита конструкція для зручного та безпечного кріплення комунікаційного обладнання, в даному конкретному випадку – комутаторів і патч-панелей до яких надходять лінії зв'язку.

ДСК – гриф документу «Для службового користування». Накладається як цифрові так і паперові носії.

ВМ – віртуальна машина. Екземпляр обчислювального пристрою, створеної шляхом віртуалізації ресурсів: процесора, оперативної пам'яті, пристроїв зберігання та вводу і виводу інформації тощо.

AD – Active Directory (або активний каталог) – ієрархічна структура де зберігаються відомості про мережу. Служби каталогу (наприклад – AD DS) надають методи зберігання даних каталогу і передачі цих даних користувачам і адміністраторам.

ДНСР – Dynamic Host Configuration Protocol це протокол прикладного рівня для автоматичного отримання параметрів мережі в тому числі IP-адреси. Процесом керує ДНСР-сервер.

DNS – Domain Name System є сервісом, який призначений для відповідей на DNS-запити за відповідним протоколом.

ОС – операційна система. Базовий комплекс програм, що виконує керування апаратною складовою комп'ютера або віртуальної машини, забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем.

GPO – Group Policy Object або об'єкт групової політики.

WSUS – Windows Server Update Services. Сервіс оновлень для операційних систем і продуктів Microsoft. Дозволяє адміністраторам керувати розповсюдженням оновлень в корпоративній мережі.

СОКД – система охорони і контролю доступу. Комплекс технічних та програмних засобів безпеки, що здійснює регулювання входу / виходу та переміщень людей чи транспортних об'єктів на територіях, які знаходяться під охороною.

ВСТУП

З початку 2000-х років електронні сервіси впевнено витісняють паперовий документообіг та переводять надання інформаційних та адміністративних послуг населенню у цифровий формат. Стрімке зростання попиту на цифрові послуги призводить не тільки до критичного збільшення навантаження на системи обробки і передачі інформації, але й до зростання навантажень на працівників, які задіяні в підтримці існуючої застарілої цифрової інфраструктури, що, в свою чергу, негативно впливає на кінцевий результат роботи установи. Вирішення питання відповідності інформаційної системи до обсягу даних, які обробляються в цій системі, питання відповідності пропускну здатності каналів зв'язку до необхідного обсягу трафіку, а також перерозподіл робочого часу персоналу з ремонту й підтримки на вдосконалення і втілення інновацій – витрушується шляхом побудови сучасної інформаційно-телекомунікаційної системи (надалі – ІТС), яка в цілому відповідатиме задачам установи.

Після прийняття Закону України «Про Національну програму інформатизації» [1] в 1998 році й набрання чинності Указу Президента України від 14.07.2000 № 887/2000 «Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади» [2], подальшого розвитку ідеї цифрової трансформації країни, яка була відображена у Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації, введеною в дію розпорядженням Кабінету міністрів України від 17 січня 2018 р. № 67-р [3], суттєво змінився підхід до організації процесу функціонування державних установ всіх рівнів підпорядкування. Наразі триває масштабна реформа

законодавства у сфері захисту інформації та кібербезпеки, спрямована на реальне управління ризиками й синхронізації з європейськими стандартами.

Отже, впровадження інформаційно-телекомунікаційних систем в державних установах має кілька відмінностей від процесу розгортання аналогічних корпоративних системи, які використовуються комерційними підприємствами. Насамперед розбіжності в методах побудови ІТС полягають у дотриманні державних стандартів, спрямованих на: захист інформації; стандартизацію методів обміну інформацією між ІТС суміжних установ; використанні сертифікованих каналів зв'язку та програмного забезпечення. В посібнику наведено аналіз ключових законодавчих змін та нововведень, що стосуються створення систем захисту інформації в державних установах.

У рамках загальнодержавних вимог до побудови і використання ІТС існують вимоги та стандарти затверджені центральним органом, на рівні міністерств, а також регіональні, і далі по низхідній – локальні. Впроваджуючи ІТС в установі, інженерам, системним адміністраторам, фахівцям служб матеріально-технічного забезпечення слід брати до уваги всю існуючу нормативну базу, яка стосується інформаційно-технічної інфраструктури певної установи, нормативну базу органу, якому вона підпорядковується та, безпосередньо – Конституцію України, закони України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки», «Про інформацію», та ін.

Представлені в посібнику матеріали виконано згідно вимог Національної програми інформатизації на 2022–2024 роки, затвердженої постановою Верховної Ради України від 08.07.2022 року №2360-IX [4].

Побудова працездатної, ефективної, здатної до масштабування, гнучкої, керованої, прозорої, надійної та самостійної ІТС в державній установі складається з двох компонентів – дотримання державних стандартів на етапі проектування і етапі

закупівлі обладнання, та використання сучасних технологій на етапі впровадження. Кожна з перелічених вище властивостей є важливою складовою грамотної побудови ІТС – *здатність до масштабування* передбачає можливість збільшення потужності та розширення ІТС без суттєвих додаткових витрат на зміну інфраструктури, *гнучкість* та *керованість* дозволяє виконувати переналаштування системи згідно умов та обставин, які мають тенденцію змінюватися з часом, *прозорість* допомагає своєчасно виявляти помилки в роботі і несанкціоновані втручання, *надійність* зменшує витрати часу на підтримку працездатності системи, що зберігає час на її удосконалення, *самостійність* передбачає довгострокову автоматизовану роботу системи без безпосередньої участі обслуговуючого персоналу, тобто зменшує вплив людського фактору, який, в свою чергу, впливає на кількість потенційних помилок в процесі функціонування ІТС та на кількість витраченого на виправлення вищевказаних помилок часу.

Мета даної роботи – побудувати саме таку ІТС на базі існуючої, але незадовільно працюючої системи на прикладі установи державної форми власності (ДУ) згідно державних стандартів та сучасного законодавства.

Слід зазначити, що розглянута у поточній роботі ІТС є універсальною. Тобто вона може бути побудована і впроваджена в будь-якій іншій установі України без змін в конфігурації обладнання та переробки програмних складових системи.

Отже об'єктом дослідження є типова інформаційно-телекомунікаційна система, яка використовується в діючій установі.

Приймається, що мережева складова ІТС будується на базі обладнання Mikrotik, яке, на даний момент не має експертного висновку про відповідність до вимог технічного захисту інформації. Автори роботи сподіваються, що незабаром Державна служба спеціального зв'язку та захисту інформації України проведе дослідження мережевих пристроїв латвійського виробника й позитивно оцінить рівень їх захищеності. На особисту думку авторів роботи мережеве обладнання Mikrotik й операційна

система RouterOS, під керуванням якої пристрої діють, є гідним рішенням на світовому ринку для побудови мережевої інфраструктури на даний момент. Натомість, описані в роботі принципи, методи і конфігурації цілком можуть бути використані для розгортання ІТС на базі с, які мають позитивний експертний висновок.

Оскільки матеріали, що наводяться в посібнику успішно реалізовано у діючій державній установі, всі мережеві імена серверів й внутрішні IP-адреси було змінено на схожі з міркувань безпеки. Також на рисунках і схемах прихована або змінена інформація, яка може бути використана задля завдання шкоди безпеці ІТС ДУ.

1. АНАЛІЗ НАЯВНОЇ МЕРЕЖЕВОЇ ТА ОБЧИСЛЮВАЛЬНОЇ ІНФРАСТРУКТУРИ УСТАНОВИ

Аналіз наявної мережевої та обчислювальної інфраструктури дає змогу реалізувати розумний підхід до питання модернізації. Перш за все, будь-які витрати коштів, особливо державних, мають бути обґрунтованими та доцільними, саме тому першим кроком на шляху до втілення інновацій є дослідження існуючої бази обладнання, яке дає відповідь на питання що треба змінити, що перебудувати або переналаштувати без здійснення зайвих закупівель. Аналіз надає інформацію щодо вузьких місць, так званих «bottleneck», де процес вводу, обробки, виводу чи передачі інформації створює чергу, уповільнюючи загальний процес виконання завдань [5, 6].

1.1. Визначення установи.

Структура, штат, програмне забезпечення.

Характеристика споживаних мережевих послуг

Установа державної форми власності (надалі – ДУ) – це місцевий вищий навчальний заклад (ВНЗ) з підпорядкуванням Міністерству освіти і науки України. Аналізована установа – це освітньо-науковий заклад, який діє відповідно до законодавства про освіту і реалізує освітні програми вищої освіти, забезпечує навчання, виховання і професійну підготовку осіб відповідно до їхніх інтересів та нормативних вимог у галузі вищої освіти, а також здійснює науково-дослідну та науково-технічну діяльність.

ВНЗ розташовано в окремії чотириповерховій будівлі. Електричне живлення, водопостачання, опалення – центральні. Кількість залів засідань, актових та конференцзалів (надалі – залів ОЗ) дорівнює восьми, з них п'ять обладнано системами відеоконференцз'язку (надалі – ВКЗ). Всі зали ОЗ знаходяться на першому поверсі будівлі. Вхід у приміщення установи здійснюється через пост Служби охорони.

Штатна чисельність установи наведена у *Додатку А* та становить: 167 науково-педагогічні працівники і допоміжний персонал та 50 працівників відділів і служб – загалом 217 осіб. Структура складається із керівництва установи, восьми відділів та служб, трьох факультетів з профільними кафедрами. Відповідальних за ОЗ призначають з викладачів кафедр, за якими ці зали закріплені. Доступ до електронних сервісів мають 208 працівників установи. Дев'ять осіб із штату є обслуговуючим персоналом та не мають доступу до інформації, що циркулює в межах установи.

В установі функціонують чотири сервери: файловий сервер 1 на базі Intel Xenon E1225 / 16Gb RAM/Raid10 із загальним масивом 14,5Tb; файловий сервер 2 на базі Intel Xenon E5-2407 / 16Gb RAM/Raid10 із загальним масивом 2Tb; сервер баз даних на базі Intel Xenon E5-2620 X 2 / 64Gb RAM / Raid10 із загальним масивом 1Tb; сервер додатків на базі Intel Xenon E5-2609 / 16Gb RAM / Raid10 з масивом 512Gb. Сервери мають інсталювану ліцензійну операційну систему (надалі – ОС) Windows Server 2019 з необхідною кількістю клієнтських ліцензій користувача. Потужності серверного обладнання достатньо для обслуговування поточних завдань, які виконує ДУ.

Робочі місця працівників обладнано комп'ютерами та ноутбуками достатньої потужності. Вся комп'ютерна техніка має мережеві адаптери з підтримкою стандартів Gigabit Ethernet 1000BASE-T, ліцензійну операційну систему Windows 10 Pro, необхідний для роботи набір офісних додатків.

Програмне забезпечення (надалі – ПЗ), яке використовуються у процесі освітньої, науково-педагогічної та науково-технічної

діяльності, разом із кількістю користувачів окремих програмних продуктів та сервісів надано у *Додатку Б*.

Слід зазначити, що кількість одночасних клієнтських підключень до система електронного документообігу (надалі – СЕД) не може дорівнювати 183 як вказано у *Додатку Б*, а обмежена 30, що є умовою ліцензійної угоди між установою та власником і розробником системи. Тобто пікове навантаження на мережу та сервер бази даних (надалі – БД) MS SQL, яке викликане використанням системи електронного документообігу, має бути розраховане з урахуванням вказаного обмеження.

З інформації, яка міститься у *Додатку Б* витікає, що на продуктивність локальних каналів передачі даних, а також завантаженість сервера БД найбільший вплив має процес функціонування комп'ютерної програми з діловодства (надалі – КП ДВ), де кількість одночасно підключених користувачів може сягати 194 та Web-сервіс EasyCon.

Особливістю сервісу ВКЗ EasyCon, який може бути одночасно запущено у п'яти залах ОЗ, є передача відео- та аудіопотоку на зовнішній сервер через мережу Інтернет, що суттєво впливає на навантаження як локальних так і зовнішніх каналів передачі даних через щільність і високий обсяг інформації, що передається в обидві сторони. Паралельно із процесом ВКЗ, який триває в залах ОЗ, в системі можуть бути присутні до 45 користувачів, відповідальних за ОЗ, які працюють з документацією, пов'язаною із минулими ОЗ, що були проведені в режимі ВКЗ.

Інші програмні продукти, котрі використовуються установою, теж займають серверні потужності і мають вплив на канали передачі даних, але вплив не такий суттєвий, як перелічені вище.

Зовнішній канал Інтернет має перепускну здатність 150 Мбіт/с та використовується для обміну даними між локальним та центральним рівнем, для проведення ОЗ в режимі ВКЗ та для поточних потреб працівників установи. Зокрема, пріоритет на зовнішнє Інтернет-з'єднання мають Сервіс підтримки КП ДВ, сервіс EasyCon та Web-сервіс електронної пошти.

ІТС установи має відповідати її потребам у швидкості обробки та передачі інформації як в межах ДУ та і поза її межі. Далі буде проаналізовано існуючу ІТС на предмет відповідності нагальним потребам [7, 8].

1.2. Наявна інформаційно-телекомунікаційна інфраструктура установи (топологія, мережа передачі даних та її характеристика)

Поточна топологія мережі наведена у *Додатку В*, де наведені: P1 – маршрутизатор MikroTik RB4011iGS+RM (рис. 1.1); K1–K11 – комутатори D-Link DES-3200-26 (рис. 1.2);



Рисунок 1.1 – Маршрутизатор MikroTik RB4011iGS+RM



Рисунок 1.2 – Маршрутизатор D-Link DES-3200-26

Маршрутизатор P1 під'єднано до п'яти серверів, зовнішнього каналу Інтернет та до трьох комутаторів (K2, K7 і K11) за топологією зірка з використанням стандарту Gigabit Ethernet 1000BASE-T (IEEE 802.3ab). В свою чергу, комутатори K2, K7 та K11 мають лінки із іншими комутаторами мережі за принципом послідовного з'єднання через порти стандарту

1000BASE-T. Клієнтські підключення здійснюються через комутатори K1...K11 за технологією Fast Ethernet 100BASE-T. Для поєднання всіх складових мережі використовується мідна кручена пара UTP п'ятої категорії.

На підставі швидкого аналізу топології можна зробити висновок, що швидкість передачі даних, при використанні даної топології мережі, падає по низхідній від K11 до K8, від K7 до K3 та від K2 до K1. В найбільш складному випадку, пакет даних, який надійшов на клієнтський порт комутатора K3 і має бути доставлено до клієнтського порту комутатора K8, має пройти комутатори K4, K5, K6, K7, маршрутизатор P1, комутатори K11, K10, K9, K8. Більш за те, швидкість проходження кадрів даних через ланцюги комутаторів суттєво залежить від поточного навантаження на кожен з них, що негативно впливає на перепускную здатність мережі в цілому.

1.3. Розрахунок поточних характеристик мережі

Зробимо розрахунок поточного навантаження на мережу та коефіцієнту використання мережі. Затребуваність ширини внутрішніх та зовнішніх каналів зв'язку, щільність абонентів тощо [9].

Для здійснення розрахунку навантаження на мережу було виконано контрольні заміри трафіку у розрізі ПЗ, результати яких представлено у *Додатку Г*. Заміри здійснювалися з використанням внутрішньої утиліти Windows «Відомості про використання даних», ПЗ «Microsoft Network Monitor 3.4» та «Моніторинг ресурсів Windows».

Показник загального навантаження на локальну мережу розраховується за формулою:

$$V_{nw} = \sum V_i \text{ (Мб/сек)},$$

де V_i дорівнює навантаженню окремого ПЗ на мережу та обчислюється за формулою: $V_i = n_i \cdot T_i$ (Мб/сек), де n_i – кількість вузлів

(користувачів ПЗ), T_i – трафік, який генерує та споживає окреме ПЗ. Значення T_i були знайдені експериментальним шляхом та перелічені в *Додатку Д* разом із кількістю активних користувачів ПЗ – n_i .

Розрахунок навантажень виглядає так:

$$\begin{aligned} V_{dss} &= 194 \cdot \frac{48}{3600} = 2,59 \text{ Mb/s}, & V_{spd} &= 1 \cdot \frac{187}{3600} = 0,05 \text{ Mb/s}, \\ V_{lig} &= 30 \cdot \frac{76}{3600} = 0,63 \text{ Mb/s}, & V_{isp} &= 4 \cdot \frac{94}{3600} = 0,10 \text{ Mb/s}, \\ V_{med} &= 3 \cdot \frac{21}{3600} = 0,02 \text{ Mb/s}, & V_{avz} &= 9 \cdot \frac{15}{3600} = 0,04 \text{ Mb/s}, \\ V_{eas} &= 5 \cdot \frac{11\,450}{3600} = 15,90 \text{ Mb/s}, & V_{vkz} &= 3 \cdot \frac{33}{3600} = 0,03 \text{ Mb/s}, \\ V_{kad} &= 5 \cdot \frac{35}{3600} = 0,05 \text{ Mb/s}, & V_{other} &= 208 \cdot \frac{106}{3600} = 6,12 \text{ Mb/s}. \end{aligned}$$

Загальне навантаження $V_{nw} = 25,53 \text{ (Mb/s)}$.

Максимальна теоретична швидкість проходження пакетів між двома клієнтами мережі стандарту Fast Ethernet 100BASE-T становить 12,5 Мб/с [10]. На практиці, досягти теоретичного максимуму в мережі, що складається з трьох і більше вузлів, неможливо. В комп'ютерній мережі неминучі колізії, циркулюють пакети різноманітної довжини, службова інформація робочої групи або домену, тощо.

Довжина кадру Fast Ethernet (тобто пакета без преамбули) має бути не менш 512 бітових інтервалів [10] та не більшою за 12 144 бітових інтервалів що є граничною величиною подвійного часу проходження в мережі Fast Ethernet. З них 18 байтів (144 біти) займає службова інформація, а розмір корисних даних може змінюватись від 46 до 1 500 байт. Тобто розмір кадру передачі інформації може варіюватися від $46 + 18 = 64$ байтів до $1\,500 + 18 = 1\,518$ байтів, що тягне за собою висновок: частка

корисної інформації в кадрі мінімальної довжини дорівнює $\frac{46}{64} = 0,72$ від загального об'єму переданої інформації, а кадру максимальної довжини $\frac{1500}{1518} = 0,99$. Тобто корисний трафік суттєво залежить від довжини кадру передачі інформації.

Довжина преамбули в пакеті може змінюватися після проходження комутаторів та маршрутизатора, тому для розрахунку буде використовуватися середнє значення – 8 байт (64 біти).

Для стандарту Fast Ethernet із заявленою виробником швидкістю 100Мбіт/с один бітовий інтервал (час передачі одного біту) дорівнює 0,01 мкс.

Для передачі одного кадру мінімальної довжини разом із преамбулою необхідно:

$$0,01 \cdot (512 + 64) = 5,76 \text{ (мкс)}.$$

Кадр максимальної довжини:

$$0,01 \cdot (12\,144 + 64) = 122,08 \text{ (мкс)}.$$

Міжкадровий інтервал в мережі Fast Ethernet становить 96 бітових інтервалів (0,96 мкс), з чого виходить, що період передачі кадру мінімальної довжини буде дорівнювати:

$$5,76 + 0,96 = 6,72 \text{ (мкс)}.$$

Кадру максимальної довжини:

$$122,08 + 0,96 = 123,04 \text{ (мкс)}.$$

Перепускна здатність найменших кадрів становить:

$$F_{\min} = \frac{10^6}{6,72} = 148\,809 \text{ (кадрів/с)}.$$

Перепускна здатність найбільших кадрів становить:

$$F_{\max} = \frac{10^6}{123,04} = 8\,127 \text{ (кадрів/с)}.$$

Параметри перепускної здатності мережі розраховується як результат передачі максимального об'єму корисної інформації кадрами найменшої та найбільшої довжини в інтервалі однієї секунди:

$$C_{\min} = 46 \cdot 148\,809 = 6\,845\,214 \frac{\text{байт}}{\text{с}} = 6,53 \text{ Мб/с};$$

$$C_{\max} = 1500 \cdot 8\,127 = 12\,190\,500 \frac{\text{байт}}{\text{с}} = 11,63 \text{ Мб/с}.$$

Середня швидкість передачі даних в мережі Fast Ethernet становить:

$$C_{\text{avg}} = (C_{\min} + C_{\max})/2 = 9,08 \text{ Мб/с}.$$

Коефіцієнт використання мережі:

$$P = \frac{Vnw}{C_{\text{avg}}} = \frac{25,53}{9,08} = 2,81.$$

На рис. 1.3 зображено залежність затримок передачі даних T_z від коефіцієнта використання мережі ρ , де спостерігається експонентне зростання кількості затримок із зростанням коефіцієнта в розрізі трьох мережевих технологій.

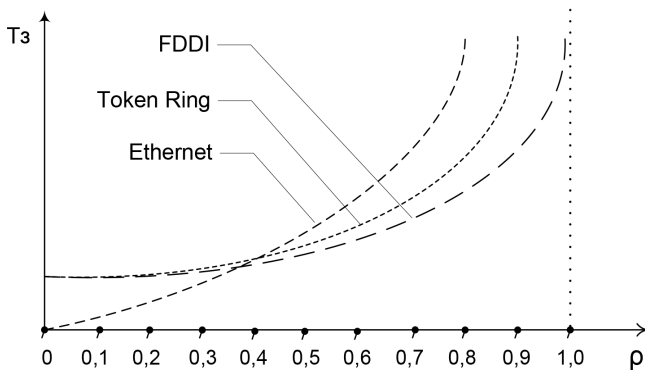


Рисунок 1.3 – Графік залежності затримок передачі даних від коефіцієнта використання мережі

Графік демонструє, що існує поріг після якого поведінка мережі істотно змінюється в гіршу сторону. Для всього сімейства Ethernet це значення полягає між 0,4 та 0,5 [7].

Отриманий в результаті розрахунку – коефіцієнт 2,81 – говорить про повну непрацездатність локальної мережі при використанні всіх сервісів ДУ одночасно. Поліпшує ситуацію передача даних проміж комутаторами та між серверами за допомогою технології Gigabit Ethernet. Але послідовне з'єднання комутаторів один до одного з єдиним магістральним каналом даних на загальний пул унеможливорює нормальний процес передачі даних від найнижчих клієнтів одного пулу до найнижчих клієнтів іншого.

Щоб впевнитися у висновках варто розглянути процес передачі файлу на прикладі клієнта, підключеного до комутатора К3, до іншого клієнта, якого під'єднаного до комутатора К8. Маршрут можна відстежити на схемі топології мережі у *Додатку Г*.

При умові передачі файлу (хай його об'єм становить 1 Гб) мережевий інтерфейс клієнта розпочне передачу даних кадрами найбільшої довжини на швидкості 100 Мбіт/с. Припустимо, що всі порти комутаторів К3...К7 завантажено обміном даних із серверами ДУ. Комутатор К3 (D-Link DES-3200-26) має 24 порти Fast Ethernet і два магістральні порти Gigabit Ethernet, один з яких порожній, другий – приєднано до комутатора К4. Всі двадцять чотири клієнти в цей час поділяють перепускную здатність магістрального порту (1000 Мбіт/с) між собою. Тобто комутатор К3 в змозі забезпечити максимальну швидкість трансферу інформації від одного клієнта за свої межі на рівні: $1000/24 = 41,6$ Мбіт/с. Комутатор К4, приймає пакети, але, з огляду на власне навантаження, може виділити лише 50 % свого магістрального каналу для транзиту даних з К3 на комутатор К5. Швидкість на другому хопі (К4) надає навіпіл, та становить 20,83 Мбіт/с, на третьому (К5), відповідно – 10,41 Мбіт/с, на четвертому (К6) – 5,2 Мбіт/с, на п'ятому (К7) – 2,6 Мбіт/с, що дорівнює 325 Кб/с. Як результат, лише до маршрутизатора Р1 ланцюг комутаторів К3...К7, при ідеальних умовах,

буде передавати файл об'ємом 1Гб понад 53 хвилини. Далі, на маршруті K11...K8, та за умови існуючого навантаження на ці комутатори, швидкість буде падати, а час передачі зростатиме вдвічі на кожному хопі та становитиме 0,16 Мбіт/с або 20,48 Кб/с на цільовому порті K8. Тобто на передачу файлу об'ємом 1Гб, в мережі з даною топологією від комутатора K3 до K8, в ідеальних умовах проходження кадрів, знадобиться понад 14 годин, що є цілком незадовільним результатом.

Зовнішній Інтернет-канал фізично надходить до будівлі ДУ оптичним кабелем і, через медіаконвертор, єднається із маршрутизатором P1 до порту Gigabit Ethernet. Гарантована максимальна швидкість каналу за договором із провайдером ПАТ «Укртелеком» становить 150Мбіт/с. Із *Додатку Е* ясно, що канал має обслуговувати два ресурсномістких сервіси – Сервіс підтримки КП ДВ та EasyCon, в також менш вибагливий до ширини каналу сервіс електронної пошти. Раніше було визначено, що $V_{spd} = 0,05$ Мб/с, $V_{eas} = 15,90$ Мб/с, разом, при повному навантаженні, обидва сервіси потребують швидкість прийому / передачі даних 15,95 Мб/с. Наявне Інтернет-підключення може теоретично забезпечити швидкість каналу 18,75 Мб/с, чого буде достатньо для функціонування обох сервісів, але паралельне використання мережі Інтернет сервісом електронної пошти та іншими користувачами у власних потребах ($V_{other} = 6,12$ Мб/с), буде суттєво впливати на канал в бік зменшення пріоритетного трафіку, та збільшення іншого. В результаті неможливо гарантувати повноцінне функціонування як сервісів, так і клієнтських браузерів, а також операційних систем (мається на увазі автоматичне оновлення OS Windows). Відсутність альтернативного резервного каналу Інтернет робить працездатність системи ненадійною, такою, що залежить від одного провайдера, що ставить роботу всієї установи під сумнів у разі непрацездатності каналів ПАТ «Укртелеком».

Локальна мережа побудована в межах приміщення за допомогою неекранованої крученої пари п'ятої категорії. Підключення комп'ютерів до мережі здійснюється патч-кордами через

розетки стандарту RJ45, які встановлено поруч із робочими місцями працівників. Комутатори розташовано в трьох комунікаційних шафах, які знаходяться на першому, другому та третьому поверхах будівлі. Серверна кімната знаходиться на другому поверсі в окремому захищеному приміщенні, яке обладнано системою кондиціонування повітря. Сервери і маршрутизатор P1 надійно закріплені в серверній стойці. На відміну від топології, серверні, монтажні й периферійні елементи ІТС не викликають питань, мають достатні характеристики для обслуговування системи і не потребують фізичних змін.

Натомість, маршрутизатор P1 має типові налаштування, працює як рядовий комутатор та майже не виконує функції керування потоками даних, хоча має достатньо потужності для обслуговування ІТС.

Окремо від проблем виявлених на каналному, мережевому і, частково, транспортному рівні слід розглянути питання організації прикладного рівня моделі OSI в установі. Локальна мережа функціонує в робочій групі Windows, де кожен із клієнтських комп'ютерів є окремим, самостійним пристроєм. Робоча група не передбачає централізованого керування сервісами локальної мережі, обліковими даними і правами доступу користувачів, політиками, загальними ресурсами, тощо, що в разі ускладнює адміністрування системи в цілому. Неможливість централізованого управління і моніторингу системи не дозволяє налагодити тривалий безперебійний робочий процес й споживає надто багато зусиль та ресурсів на підтримку працездатності ІТС.

Мережеві імена комп'ютерів та серверів не мають логіки, не відображають суті завдань, які вони закликані виконувати, в іменах немає зв'язку із належністю до структурних підрозділів або зв'язку із користувачем, за яким закріплено автоматизоване робоче місце. План IP-адресації відсутній, клієнти мережі мають статичні IP-адреси, які неможливо передбачити, що може призвести (і доволі часто призводить) до помилкової видачі адміністратором дублюючих адрес.

Паразитний трафік служб огляду мережі, який генерується кожним із членів робочої групи при активації мережевих пристроїв, зменшує і без того недостатню швидкість трансферу даних між вузлами, що, в свою чергу, ще раз доводить негативний вплив на нижні рівні моделі OSI з боку хибно побудованих верхніх.

Антивірусний захист здійснюється на кожному окремому комп'ютері різноманітними додатками без локального серверу оновлень. Як результат, це багаторазово збільшує зовнішній трафік і не передбачає централізований моніторинг та аналіз загроз.

Багатофункціональні пристрої (надалі – БФП) з мережевим інтерфейсом, у кількості 37 одиниць, підключено до клієнтських комп'ютерів через USB інтерфейс з наданням загального мережевого доступу всім користувачам робочої групи. Така ситуація ставить у залежність інших користувачів системи від працездатності комп'ютера, до якого під'єднано БФП, виключає централізоване керування чергою друку, не дозволяє раціонально розташувати друкарські пристрої в кабінетах.

Електроживлення серверного та мережевого обладнання організовано безпосередньо від електричної мережі ДУ без використання джерел безперебійного живлення. Така ситуація гарантовано веде до втрати інформації, яка знаходиться на стадії обробки в моменти порушення електропостачання будівлі. Крім того раптове вимкнення електрики може призвести до критичних збоїв як в роботі операційних систем серверів, так і виходу з ладу самого серверного обладнання.

1.4. Висновки, цілі і завдання модернізації ІТС

Ціллю проведеного дослідження було проаналізувати існуючу ІТС установи на предмет відповідності її характеристик нагальним потребам ДУ. Дослідження виявило чисельні недоліки в роботі, побудові, організації інфраструктури як мережевої, так

і прикладної складової. Локальна мережа ДУ не здатна забезпечити достатній для коректної роботи рівень передачі даних, канал Інтернет не в змозі задовільнити потреби у швидкості прийому / передачі інформації зовні/поза межі ІТС. Використання робочої групи Windows на прикладному рівні моделі OSI не надає можливості належним чином адмініструвати і підтримувати робочий стан ІТС. Система є вразливою і незахищеною по декількох напрямках – від загроз зовнішнього вторгнення до втрати інформації з причин неналежного функціонування внутрішніх модулів і складових.

Отже, на основі вищевикладеного, можна зробити такі висновки і окреслити цілі модернізації і перебудови існуючої ІТС:

1. Топологію локальної мережі має бути змінено – кількість магістральних каналів треба збільшити, встановити кореневий комутатор замість маршрутизатора P1, маршрутизатор задіяти по схемі Router on a stick [11] і переналаштувати його на виконання функції керування потоками даних.

2. Активне мережеве обладнання, а саме комутатори K1–K11, потребують заміни на більш технологічні і сучасні з підтримкою технології Gigabit Ethernet по всіх портах.

3. Ширина наявного каналу Інтернет може бути залишена без змін, але має бути задіяно резервний канал (або два канали) зв'язку на базі іншого провайдера, що зробить систему менш вразливою від раптових падінь каналу ПАТ «Укртелеком» а також дозволить перебалансувати зовнішній трафік між користувачами та сервісами ІТС в межах двох (або трьох) каналів зв'язку.

4. Сервери ІТС потребують організації безперебійного живлення достатньої потужності.

5. В мережі має бути побудовано домен під управлінням Windows Server для загального управління та адміністрування ІТС.

6. Мережеві імена комп'ютерів та серверів мають бути змінені за чіткою логікою. Окремо слід розробити план IP-адресації мережевих пристроїв, дотримуватися його при розгортанні і використанні нової ІТС.

7. У систему слід інтегрувати централізований антивірусний захист серверів і клієнтських комп'ютерів.

8. Для організації незалежного і прозорого процесу виводу паперової інформації, в системі треба створити сервер або сервери друку.

Контрольні питання до розділу 1

1. Чому в якості прикладу розглядається провадження інформаційно-телекомунікаційної системи саме в державній установі?

2. Які два основних компоненти передбачається при побудові працездатної, ефективної, здатної до масштабування, гнучкої, керованої, прозорої, надійної та самостійної інформаційно-телекомунікаційної системи в установі?

3. З якою метою проводиться аналіз наявної мережевої та обчислювальної інфраструктури установи?

4. Які особливості розрахунку поточних характеристик мережі?

5. Які цілі модернізації і перебудови існуючої інформаційно-телекомунікаційної системи є типовими для будь-якої установи?

2. ВИМОГИ ДО ПРОЄКТУВАННЯ І ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ В УСТАНОВІ

Як було зазначено, законодавство накладає низьку вимог на проєктування і впровадження ІТС в установі. Вимоги стосуються обладнання, технологій, які використовуються в процесі впровадження та експлуатації ІТС, програмного забезпечення, політики безпеки та інших сторін автоматизації процесу життєдіяльності державних органів.

До недавнього часу головною відмінністю ІТС державної установи від ІТС комерційних організацій була комплексна система захисту інформації, яку кожен державний орган мав побудувати [12].

В Україні триває масштабна реформа законодавства у сфері захисту інформації та кібербезпеки, спрямована на перехід від морально застарілого захисту до реального управління ризиками. Головною метою цих змін є синхронізація з європейськими стандартами (зокрема, директивами ЄС та Регламентом GDPR) і посилення стійкості держави в умовах цифрових загроз [13].

У цьому розділі буде розкрито ключові моменти на які слід звернути увагу відповідальним за впровадження і підтримку ІТС особам в установах різних форм власності.

2.1. Система захисту інформації в установі

Ухвалений парламентом Закон № 4336-IX («Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів...») вніс системні зміни відразу в кілька базових нормативних актів [14].

Відповідно до цих змін відомство Держспецзв'язку закріплено як головний регулятор, який координує та контролює стан захисту державних баз даних та об'єктів критичної інфраструктури. Запроваджується посада CISO (Chief Information Security Officer) в органах державної влади, місцевого самоврядування та на об'єктах критичної інфраструктури (ОКІ) як обов'язкова. Причому посаду директора з інформаційної безпеки або відповідальної особи заборонено суміщати з посадою керівника ІТ-відділу, щоб уникнути конфлікту інтересів. Усі кандидати на цю посаду проходять державну атестацію та погодження. Створюється єдина система обміну даними про кіберінциденти, що зобов'язує установи миттєво інформувати про атаки, а за приховування інформації про інциденти впроваджено адміністративну відповідальність – національна система реагування.

Кабінет Міністрів України своєю Постановою № 712 кардинально змінив підхід до легалізації інформаційних систем [15].

Відповідно до цих змін передбачено, що нова система авторизації замінить застарілі КСЗІ – впроваджується «Авторизація з безпеки». Також запроваджено Порядок розроблення та затвердження профілів безпеки для інформаційних, технологічних та електронно-комунікаційних систем, що базуються на міжнародних стандартах управління ризиками.

Урядом оновлено вимоги до засобів інформатизації – створення, модернізації та функціонування державних цифрових інструментів (зміни до Постанови КМУ № 205) [16].

Відповідно до цих змін встановлено жорсткі Мінімальні вимоги до захисту інформаційних систем, які використовуються у сфері електронного врядування, а також введено суворий

контроль за походженням програмного забезпечення та обладнання, щоб виключити використання технологій країн-агресорів чи пов'язаних із ними компаній.

У межах інтеграції до Європейського Союзу в Україні триває робота над кардинальним оновленням правил обробки особистих даних громадян [17].

Відповідно до цих оновлень Законопроект № 8153 («Про захист персональних даних») має повністю замінити діючий закон 2010 року. Він адаптує українські правила під Загальний регламент про захист даних ЄС (GDPR). Для бізнесу та держави це означатиме появу величезних штрафів за витік даних та суворі умови отримання згоди на обробку інформації. А Законопроект № 6177 передбачає створення незалежного наглядового органу – Національної комісії з питань захисту персональних даних та доступу до публічної інформації, яка перебере на себе функції контролю, що раніше належали Уповноваженому ВРУ з прав людини.

Враховуючи системний підхід до створення комплексної системи захисту інформації, основні її вимоги є сенс використовувати в установах різної форми власності як альтернативу сучасним вимогам кіберзахисту державних ресурсів. Тому далі подається аналіз підходів щодо можливого розгортання комплексної системи захисту інформації в недержавних установах.

Створення комплексної системи захисту інформації (надалі – КСЗІ) в автоматизованій системі передбачається вимогами нормативно-правових актів системи технічного захисту інформації (надалі – ТЗІ) щодо захисту інформації з обмеженим доступом, які формуються згідно вимог низки документів: Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою КМ України від 29.03.2006 № 373 [18] із останніми змінами згідно постанови КМ України від 14.10.2022 № 1171; інструкції «Типова інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації,

що містять службову інформацію», затвердженої постановою КМ України від 19.10.2016 № 736 [19]; нормативних документів ТЗІ; Положення про службу захисту інформації (надалі – СЗІ) та Плану захисту інформації в ІТС.

Таку систему захисту інформації установи називають *комплексною* з тих причин, що впровадження КСЗІ передбачає комплексний підхід до розгортання захищеної ІТС. А саме:

- забезпечення визначених політикою безпеки властивостей інформації (цілісності, доступності) під час створення та експлуатації ІТС;
- своєчасне виявлення та знешкодження загроз для ресурсів ІТС, причин та умов, які спричиняють (можуть привести до) порушення її функціонування та розвитку;
- поєднання програмно-технічних та фізичних засобів, організаційних та інженерно-технічних заходів;
- врахування всього переліку можливих загроз безпеці інформації;
- врахування всього переліку можливих способів, методів та засобів захисту інформації;
- побудову сукупності взаємозв'язаних і взаємодоповнюючих в єдиній системі правових, організаційних, інженерно-технічних заходів та фізичних, технічних й програмно-апаратних засобів захисту інформації, що реалізують задану політику інформаційної безпеки й протидіють означеним загрозам інформації;
- врахування вимог по захисту інформації на всіх етапах життєвого циклу ІТС – розробка, створення, впровадження, функціонування, утилізація;
- визначення вимог до технічних та організаційних заходів захисту веб-сторінки установи в мережі Інтернет.

КСЗІ має забезпечувати наступні види захисту:

- захист від несанкціонованих дій з інформацією (в тому числі захист від несанкціонованого доступу до інформації з обмеженим доступом), при її створенні, обробці та збереженні в автоматизованих системах;

- захист інформації від витоку технічними каналами для інформації, що становить державну таємницю (або для службової інформації за окремим рішенням керівництва);

- захист інформації від спеціальних впливів (за окремим рішенням керівництва);

- антивірусний захист інформації та ресурсів;

- фізичну безпеку об'єктів та ресурсів;

- правове, організаційне та нормативне забезпечення.

Створення КСЗІ включає вирішення наступних завдань:

- виявлення та класифікація інформації, яка підлягає захисту;

- встановлення рівня повноважень користувачів та персоналу;

- встановлення і оформлення правил розмежування доступу, а також правил, що регламентують права доступу суб'єктів до об'єктів;

- вибір профілю захищеності відповідно до особливостей обробки інформації, створення відповідного організаційного та технічного комплексу засобів захисту;

- своєчасне виявлення й знешкодження загроз ресурсам інформаційної системи, дослідження причин та умов які спричиняють, або можуть привести до порушення її нормального функціонування та розвитку;

- створення механізму та умов оперативного реагування на загрози безпеці функціонування ІТС;

- розробка організаційно-технічної і робочої документації, що визначає вимоги і порядок обробки інформації з обмеженим доступом;

- ознайомлення користувачів з переліком відомостей, що захищаються і їх рівнем повноважень, а також із організаційно-розпорядчою і робочою документацією;

- визначення та впровадження технічних засобів фізичної охорони;

- організація служби захисту інформації;

- організація обліку, зберігання, обігу носіїв інформації, яка потребує захисту, здійснення відповідного контролю.

Вирішення зазначених задач складає зміст політики безпеки інформації. Якщо підсумувати все перелічене то можна зробити висновок, що процес побудови ІТС державної установи (на відміну від комерційної організації) включає два додаткові етапи – перший етап це обрання сертифікованого (або сертифікація обраного) ПЗ і обладнання на стадії проєктування ІТС.

Перший етап – актуальний перелік засобів ТЗІ, які вже мають експертний висновок про відповідність до вимог технічного захисту інформації завжди можна завантажити на відповідній сторінці офіційного сайту Державної служби спеціального зв’язку та захисту інформації України [20].

Другий етап – розробка нормативної документації яка доповнює стадію розробки документації перед стадією введення ІТС в експлуатацію і, нарешті, дотримання вимог, які затверджуються розробленими документами на стадії експлуатації ІТС. Детальніше про стадії розгортання ІТС буде викладено в розділі 2.3 «Планування інформаційно-телекомунікаційної інфраструктури».

Мінімальний перелік необхідної супровідної документації КСЗІ ІТС державної установи, який слід розробити і затвердити виглядає так:

- Наказ про призначення відповідальної особи з впровадження КСЗІ;
- Наказ про створення Служби захисту інформації;
- Наказ про затвердження Положення з порядку побудови та впровадження КСЗІ в ІТС установи;
- Наказ про оброблення документів з грифом обмеженого доступу із застосуванням ресурсів ІТС;
- Наказ про створення комісії для проведення детального обстеження та категоріювання об’єктів інформаційної діяльності;
- Наказ про визначення меж контрольованої зони;
- Наказ про затвердження Положення про забезпечення доступу до публічної інформації;
- Наказ про надання доступу до автоматизованих систем (ІТС), які використовує установа;

- Наказ про затвердження інструкцій (і самі інструкції) користувача, адміністратора, адміністратора безпеки, антивірусного захисту, інструкції щодо захисту службової інформації та інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію;

- Положення з порядку побудови та впровадження КСЗІ в ІТС установи;

- Положення про службу захисту інформації;

- Положення про забезпечення доступу до публічної інформації;

- Акти обстеження і акти категоріювання службових приміщень;

- Паспорт-формуляр на кожен одиницю обладнання, яке підключене до ІТС;

- Картка обліку ключів і ліцензій;

- Журнал доступу до серверного приміщення;

- Модель загроз;

- Перелік програмно-технічного, операційного та спеціалізованого програмного забезпечення локальної обчислювальної мережі;

- Перелік категоризованих об'єктів;

- План будівлі;

- План контрольованої зони;

- План захисту інформації в ІТС;

- План технічного захисту інформації;

- Форма подання інформації про результати планової інвентаризації комп'ютерних програм.

Атестат відповідності (або зареєстровану в Державній службі спеціального зв'язку та захисту інформації України декларацію про відповідність КСЗІ вимогам нормативних документів ТЗІ), який засвідчує відповідність побудованої КСЗІ вимогам нормативних документів ТЗІ, можна отримати лише за наявності переліченої вище документації.

Після отримання атестату, комплексна система захисту інформації вводиться в експлуатацію розпорядженням керівника установи.

Також, згідно вимог нормативних документів ТЗІ, розпорядженням керівника установи призначається адміністратор безпеки, який забезпечує функціонування КСЗІ в ІТС. Права та обов'язки адміністратора мають бути перелічені у відповідній інструкції, яка має бути розроблена та затверджена. Всі особи, які беруть участь в процесі обробки інформації засобами ІТС, повинні бути зареєстровані як користувачі системи. Надання доступу до інформації здійснюється згідно зі службовою необхідністю, з урахуванням наданих повноважень, за умови достовірного розпізнавання користувачів в ІТС.

КСЗІ забезпечує можливість своєчасного доступу зареєстрованих користувачів ІТС до відповідної інформації та облік будь-яких дій користувачів в системі.

У процесі обробки інформації в ІТС вона не підлягає неконтрольованому ознайомленню, копіюванню, відновленню та несанкціонованій модифікації. Спроби порушення користувачем порядку доступу до ресурсів ІТС, який встановлено для нього, реєструються в спеціальних журналах. Відповідальні особи повинні мати можливість здійснювати контроль за всіма обліковими подіями, виявляти порушення та блокувати спроби несанкціонованого доступу користувачів до ресурсів ІТС. Перед початком роботи в системі користувачі в обов'язковому порядку під особистий підпис повинні бути ознайомлені з: інструкцією про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію (типова форма інструкції затверджена постановою КМУ від 19.10.2016 № 736 [19]); та інструкцією користувача ІТС.

На стадії експлуатації ІТС, з метою запобігання ненавмисним діям персоналу, які можуть призвести до порушень встановлених правил з обробки інформації в ІТС, мають здійснюватися профілактичні заходи, які включають проведення регулярних інструктажів та занять щодо підвищення кваліфікації персоналу.

2.2. Вимоги до програмного забезпечення та типи ліцензій

Для програмного забезпечення, яке використовується установою, висуваються такі ж самі вимоги, що й до обладнання. Тобто ПЗ повинно мати експертний висновок про відповідність до вимог технічного захисту інформації [21]. Наприклад, станом на жовтень 2022 року, перелік засобів ТЗІ на офіційному сайті містить операційну систему Microsoft Windows 10 і серверну ОС Microsoft Windows Server 2019, що робить побудову ІТС на базі таких систем трохи простішою – можна оминати етап державної експертизи. Натомість, для використання в структурі ІТС новітніх клієнтських операційних систем таких як Microsoft Windows 11 і серверних систем Microsoft Windows Server 2022 треба мати (або отримати) експертний висновок на зазначене ПЗ.

Вочевидь, що використовувати безкоштовні операційні системи на базі Linux на терміналах ІТС значно вигідніше ніж купувати ліцензійне ПЗ, але перелік операційних систем, які використовує установа, обумовлюється переліком спеціалізованого програмного забезпечення з яким вона працює. Наприклад, операційна система Ubuntu вже має готовий експертний висновок і розповсюджується вільно, але у випадку ОАС використання ОС на базі Linux для клієнтських терміналів неможливе через сумісність ПЗ Ліга-Закон та СЕД лише із продуктами Microsoft.

Ліцензування ОС клієнтських терміналів ІТС здебільшого не викликає питань. Як правило, ліцензійні операційні системи Windows для персональних комп'ютерів закуповуються разом із технікою по OEM (Original Equipment Manufacturer) схемі, тобто ліцензійну ОС вже інстальовано на комп'ютер. Слід лише впевнитися, що версія ОС, яка йде в комплекті, не нижча за Professional, бо інакше приєднати новий комп'ютер до домену Windows (тим самим інтегруючи його в ІТС) буде неможливо. Окрім того, можна самостійно здійснити закупівлю ліцензій й не лише за повною вартістю, але й в розрізі різноманітних програм. Наприклад, корпорація Microsoft пропонує досить

значні знижки на свої продукти установам державного сектору, навчальним закладам, ІТ-компаніям, тощо.

Ліцензування серверних операційних систем має трохи складнішу логіку. Для фізичних серверів ліцензування серверної ОС здійснюється шляхом ліцензування кожного окремого ядра на кожному процесорі сервера, але за умови використання не менш ніж однієї 16-ти ядерної ліцензії на один фізичний сервер. Взагалі-то, можна придбати ліцензійні ключі на 2, 8, 16, 32, 64 ядра. Наприклад, придбавши ключ на 16-ти ядерну ліцензію можна ліцензувати один фізичний сервер із одним восьмиядерним процесором. Або один сервер із двома такими процесорами. Або один сервер із одним процесором на шістнадцять ядер. Але на сервер із двома процесорами, кожен з яких має по 10 ядер, вже треба купувати одну ліцензію на 16 ядер + дві двоядерні ліцензії. Також можна придбати один ключ на 64 ядра і ліцензувати їм чотири серверні ОС фізичних серверів, при умові, що кількість фізичних ядер на кожному з них не перевищує 16. Політика Microsoft не передбачає ліцензування віртуальних ядер фізичних серверів, тобто вони не враховуються в процесі розрахунку кількості потрібних ліцензій для серверних операційних систем.

Слід також мати на увазі, що використання клієнт-серверної архітектури сервісів ІТС на базі продуктів Microsoft вимагає додаткових фінансових витрат. Неможна, не порушуючи чинного законодавства про інтелектуальну власність, просто придбати ліцензії для операційних систем Microsoft, побудувати ІТС і користуватися мережевими сервісами. Згідно схеми ліцензування Microsoft для корпоративних мереж, окрім звичайних ліцензій (що купуються на кожен екземпляр ОС як серверного так і термінального парку) треба здійснити закупівлю Client Access License (CAL) – ліцензій клієнтського доступу.

Ліцензії клієнтського доступу надають користувачам та/або пристроям законне право доступу до ПЗ Microsoft на сервері а також до серверних ресурсів і сервісів таких як: активний каталог, мережеві диски, групові політики тощо. Сама по собі, ліцензія

серверної ОС не надає дозволу на підключення користувачів або пристроїв до сервера – для цього на кожного користувача (або на кожен пристрій) на сервері має бути зареєстрована CAL-ліцензія. Таким чином, кількість ліцензій клієнтського доступу обумовлює кількість користувачів, які мають змогу легально працювати в ІТС або кількість пристроїв, які задіяні в роботі. Даний тип ліцензії надається серверній ОС окремо від ліцензій на фізичні ядра і забезпечує легітимне підключення користувачів до сервера.

Принципові відмінності типів CAL-ліцензій зображено на рис. 2.1.



Рисунок 2.1 – Ліцензії клієнтського доступу користувачів (ліворуч) і пристроїв (праворуч)

Якщо кількість користувачів ІТС перевищує кількість обладнання, яке приєднано до мережі (включаючи БФП), то є сенс придбати CAL-ліцензії на пристрої. При цьому кількість CAL ліцензій, які слід закупити, дорівнює кількості всіх пристроїв в мережі, окрім серверів і активного мережевого обладнання (маршрутизатори, комутатори, тощо).

У разі якщо кількість користувачів менша за кількість обладнання – купуються користувацькі CAL ліцензії кожному користувачеві ІТС. В державних установах здебільшого використовуються саме користувацькі CAL ліцензії, натомість в бізнесі більш розповсюджені CAL ліцензії на мережеві пристрої.

Відмінності обумовлені тим, що переважна більшість установ державного сектору працює за фіксованим графіком,

що не передбачає спільного використання обладнання другою або третьою зміною персоналу.

Тільки після активації всіх зазначених ліцензій (ліцензій локальних ОС, серверних ОС та ліцензій клієнтського доступу) в достатній кількості, можна вважати, що сам процес експлуатації ІТС не порушує норми законодавства щодо інтелектуальної власності. При цьому не має значення де розгорнуто ІТС: в державній установі чи комерційній структурі – закони діють на території всієї держави безвідносно юрисдикції чи рівня підпорядкованості установи, організації, підприємства, тощо.

2.3. Планування мережевої інфраструктури

Планування робіт, пов'язаних із модернізацією або створенням ІТС є обов'язковою і першочерговою складовою процесу втілення інновацій в робочий процес. Створення поетапної стратегії запобігає виникненню помилок, що раптово виявляються на етапі впровадження, і які можуть призвести (і доволі часто призводять) до марнування часу на втручання у вже побудовані складові системи з метою усунення проблем сумісності модулів системи.

Процес створення інформаційно-телекомунікаційної системи – це сукупність робіт від формування вхідних вимог до введення системи в експлуатацію. Діючий (на підставі наказу Державного підприємства «Український науково-дослідницький і навчальний центр проблем стандартизації, сертифікації та якості» від 29.12.2018 № 546 [22]) міждержавний стандарт ГОСТ 34.601–90 «Автоматизовані системи. Стадії створення» [23] визначає такі стадії створення інформаційної системи:

1. Формування вимог до інформаційної системи.
2. Розробка концепції інформаційної системи.
3. Технічне завдання.
4. Ескізний проєкт.
5. Технічний проєкт.

6. *Робоча документація.*
7. *Введення в дію.*
8. *Супроводження інформаційної системи.*

Стандартом допускається відмова від четвертої стадії, але за умови об'єднання її із п'ятою та шостою для нескладних систем, які впроваджуються на підставі проєктних рішень.

Результати опрацювання попередніх стадій є сигналом для початку робіт над наступними. Зокрема, початком першої стадії є рішення, прийняте на центральному рівні чи рішення керівника установи стосовно створення або модернізації існуючої інформаційної системи або її елементів.

Підсумком виконання першої та другої стадій можна вважати звіти відповідальних за формування вимог і розробку концепції осіб. Основні *вимоги* до інформаційної системи поділяються на такі групи:

- а) до інформаційної системи *в цілому*;
- б) до *функцій* інформаційної системи;
- в) до підготовленості *персоналу*;
- г) до видів *програмного забезпечення*;
- д) до *безпеки* інформаційної системи.

Загальний опис вимог до ІТС *в цілому*, як правило, здійснюється фахівцями Державної служби спеціального зв'язку та захисту інформації України на замовлення органів центрального рівня на підставі потреб у інформаційно-технічному забезпеченні. Далі загальні вимоги надходять до центральних органів, поширюються серед підпорядкованих установ та є обов'язковими до врахування при побудові власних систем.

В свою чергу, вимоги до *функцій* ІТС можуть бути висунуті на всіх рівнях: від молодших спеціалістів до керівництва. На етапі формування очікувань від впровадження системи слід ретельно дослідити потреби всіх майбутніх користувачів ІТС. Існує безліч методів дослідження попиту на послуги і сервіси. Зокрема, опитування, анкетування, збір і обробка статистичних даних, прямі пропозиції окремих структурних підрозділів, письмові

зауваження і службові листи, тощо. Всі ці методи, або їх частка, можуть бути реалізовані на шляху до збору даних, з яких формуються вимоги до функціоналу ІТС, яка проектується.

Останнім часом, вимоги до підготовленості *персоналу* відображено у посадових інструкціях державних службовців або осіб місцевого самоврядування. Зокрема, в кожній установі проводяться навчання з опанування основ комп'ютерних технологій, а для працівників відділів інформаційних технологій існують відомчі курси підвищення кваліфікації спрямовані на підготовку адміністраторів інформаційних систем саме тих сфер державного управління, де розгорнута (або тільки плануються впровадження) ІТС.

Також слід враховувати моменти сумісності *програмного забезпечення* й протоколів обміну даними із організаціями що підпорядковуються установі і таким установам чи органам до яких підпорядкована установа.

Щодо питання планування *безпеки* ІТС, воно здебільшого стосується побудови КСЗІ, вимоги до якої детально викладено у розділі 2.1 «Комплексна система захисту інформації в установі» й на сайті Служби спеціального зв'язку та захисту інформації України [21].

Отже, *концепцію* та *вимоги* до ІТС, яка має бути побудована, вже сформовано у першому розділі цієї роботи. Технічне завдання, за фактом, надано у висновках до першого розділу, згідно яких можна скласти перелік обладнання та послуг, які необхідні для здійснення модернізації системи.

Оформлений та затверджений належним чином перелік обладнання та послуг зі схемою складових системи і є *ескізним проектом* ІТС, який, із додаванням планів комунікацій, планів розміщення модулів системи, детальним описом конфігурації обладнання, скриптами і налаштуваннями перетворюється на *технічний проект* ІТС. Додавши інструкції користувача, адміністратора, нормативні документи, плани захисту інформації, акти категоріювання і огляду робочих приміщень та інші документи КСЗІ – отримаємо *робочу документацію* на ІТС.

Кінцевим результатом є введення в дію – тобто приймання ІТС в промислову експлуатацію. На останній із стадій – стадії *супроводження*, виконуються роботи відповідно до гарантійних зобов'язань (якщо такі були), а також післягарантійне обслуговування (за умови укладання договору) та підтримка працездатності системи штатними фахівцями. Рішення про розвиток, модернізацію чи зняття системи з експлуатації приймається на підставі результатів аналізу експлуатації інформаційної системи. Усі результати робіт, які виконуються на різних стадіях реалізації системи, оформлюють у вигляді проєктних і організаційно-розпорядчих документів [24].

У *Додатку Ж* надано проєктну топологію мережі ДУ, з якої витікає необхідність здійснити закупівлю загалом дванадцяти комутаторів – одного кореневого K0 та одинадцять комутаторів (K1...K11) у комунікаційні шафи. Окремо слід наголосити на важливості вибору кореневого комутатора. Мережевий стандарт, який підтримують порти комутатора K0, впливає на тип комунікацій які слід прокласти до комунікаційних шаф з серверної кімнати, де буде розташовано кореневий комутатор. Для задоволення поточних потреб установи магістральні канали може бути побудовано за технологією Gigabit Ethernet 1000BASE-T із використанням неекранованої крученої пари п'ятої категорії. Більш затратний але більш ефективний варіант організації магістральних каналів може бути реалізовано за допомогою стандарту 10GBASE-T (IEEE 802.3ap-2006) із використанням крученої пари категорії шість А, або стандарту 10GBASE-SR із використанням оптичного волокна для здійснення трансферу даних між комутаторами. Для реалізації першого запропонованого варіанту достатньо закупити 12 комутаторів типу Mikrotik CRS326-24G-2S+RM (рис. 2.2), один з яких буде виконувати функцію кореневого, та протягнути відносно дешеву кручену пару від комутатора K0 до комунікаційних шаф.

Другий варіант можна реалізувати використовуючи Mikrotik CRS326-24S+2Q+RM (рис. 2.3) як кореневий комутатор (і навіть маршрутизатор).



Рисунок 2.2 – Комутатор MikroTik CRS326-24G-2S+RM



Рисунок 2.3 – Комутатор MikroTik CRS326-24S+2Q+RM

Але слід враховувати, що магістральні порти SFP+ потребують використання і, відповідно, закупівлі SFP+ модулів (дві одиниці для кожного лінка), що вкупі збільшує витрати на вдосконалення мережі в декілька разів.

З огляду на поточне навантаження, економію бюджетних коштів, а також можливість здійснити модернізацію магістральних каналів у майбутньому шляхом заміни кореневого комутатора та магістральних ліній, для модернізації телекомунікаційної складової було обрано перший варіант із магістральними каналами на базі крученої пари й підтримкою стандарту Gigabit Ethernet 1000BASE-T.

Для забезпечення стабільного живлення серверного обладнання, кореневого комутатора, медіаконверторів оптичних каналів мережі Інтернет було запропоновано задіяти інверторне джерело безперебійного живлення LogicPower LPY-W-PSW-5000VA до якого має бути послідовно під'єднано чотири акумуляторні батареї LogicPower LPM-MG 12V 80AH (рис. 2.4).

Після розгляду ескізного проєкту, на нараді керівництва установи із начальниками структурних підрозділів та відповідальними за модернізацію ІТС особами, були обговорені питання і деталі процесу розгортання нової системи в ДУ а також схвалені та прийняті наступні рішення:



Рисунок 2.4 – Джерело безперебійного живлення
LogicPower LPY-W-PSW-5000VA
та акумуляторні батареї LPM-MG 12V 80AH

1. Відділу контролю за використанням державного майна:

- здійснити спрощену процедуру придбання необхідного обладнання в електронній системі публічних закупівель «ProZorro»;
- забезпечити укладання договору із додатковим провайдером доступу до мережі Інтернет;
- забезпечити укладання договору між ДУ та постачальником систем антивірусного захисту;
- надати технічну підтримку відділу інформаційних технологій з прокладання телекомунікацій та монтажу обладнання.

2. Відділу інформаційних технологій та адміністративних послуг:

- підготувати технічний проєкт ІТС;
- згідно проєкту реалізувати мережеву топологію;
- здійснити налаштування активного мережевого обладнання, враховуючи додаткові зовнішні канали Інтернет;
- забезпечити безперебійне живлення серверного та критичного мережевого обладнання;
- організувати централізований антивірусний захист всіх складових системи;
- виконати всі необхідні на прикладному рівні роботи з підвищення безпеки та ефективності ІТС.

3. Відділу бухгалтерського обліку та фінансових ресурсів:
– забезпечити фінансову підтримку реалізації проєкту.

2.4. Закупівля обладнання, оплата послуг та робіт з монтажу і налагодження системи згідно із затвердженим планом та діючим законодавством України

Перш за все слід зазначити, що кошти, які знаходяться на рахунках установи, використовуються згідно із річним планом за кодами економічної класифікації видатків (надалі – КЕКВ). Здійснити оплату послуг провайдерів Інтернет можна лише з ресурсів, акумульованих на рахунках за КЕКВ 2240 – «Оплата послуг (крім комунальних)». Придбання мережевого обладнання, вартість якого не перевищує 20 тис. грн за одиницю, фінансується за КЕКВ 2210 – «Предмети, матеріали, обладнання та інвентар». Якщо вартість обладнання перевищує 20 тис. грн оплата за договорами здійснюється згідно КЕКВ 3110 – «Придбання обладнання і предметів довгострокового користування» [25]. Облік матеріальних цінностей, що було придбано у відповідності певних КЕКВ, теж має свої особливості, але його опис виходить за рамки цієї роботи тому розглядатися не буде.

2.4.1 Розрахунок вартості модернізації ІТС

Розрахунок потреби установи у фінансових ресурсах для реалізації проєкту модернізації ІТС в розрізі кодів економічної класифікації видатків виглядає наступним чином.

Комунікації

Додаток Ж містить план будівлі ДУ за виключенням четвертого поверху, який не впливає на розрахунки. Висота стелі

на кожному поверсі дорівнює 2,9 метрам, товщина перекриття 0,4 метри. Серверне приміщення розташоване на другому поверсі в кабінеті з позначкою 33. Комунікаційна шафа (надалі – КШ) першого поверху із комутаторами К1 і К2 займає приміщення з позначкою 13. На другому поверсі у кабінеті з позначкою 30 розташовано КШ другого поверху (комутатори К3...К7) і безпосередньо над нею, на третьому поверсі, встановлено КШ, яка обслуговує третій і четвертий поверхи через комутатори К8...К11. Всі магістральні канали прокладено під навісними стелями центральних коридорів в кабель-каналах, які були побудовані в рамках капітального ремонту будівлі. Вихід комунікацій з серверної кімнати на перший і третій поверхи реалізовано за допомогою вертикальної комунікаційної шахти, яка розташована безпосередньо в серверному приміщенні.

Виходячи із плану та опису плану комунікацій, довжина магістрального каналу від К0 до К1 дорівнює:

$$M_1 = 5 + 5,45 + 1,63 + 1,1 + 0,4 + (39,67 - 2 - 2,25 - 1,5) + \\ + 1,1 + 0,4 + 5 = 54 \text{ м.}$$

До розрахунку додано по п'ять технологічних відрізків на кожному з кінців магістрального кабелю. За висоту спуску проміж поверхами прийняте значення 1,63 метри (висота від комутатора К0, закріпленого у серверній стойці, до кабель-каналу під стелею першого поверху). Оскільки лінк між Р1 та К1 старої топології вже було прокладено і він працює, оновлення топології потребує прокладання лише однієї додаткової магістральної лінії на перший поверх.

Довжина магістрального каналу другого поверху:

$$M_2 = 5 + 5,45 + 1,1 + 0,4 + 0,4 + 2,72 + 0,4 + 5,83 + 0,2 + \\ + 12,62 + 0,5 + 5 = 39,62 \text{ м.}$$

За новою топологією в КШ другого поверху має бути прокладено чотири магістральні канали. Якщо округлена довжина

одного каналу дорівнює 40 метрам, на прокладання чотирьох буде витрачено 160 метрів крученої пари.

Довжина магістрального каналу до КШ третього поверху M_3 більша за M_2 на висоту стелі плюс перекриття й відрізок від К0 до отвору шахти в перекритті:

$$M_3 = M_2 + 2,9 + 0,4 + 1,7 = 44,62 \text{ м.}$$

На три магістральні канали треба 135 метрів крученої пари. Загальні витрати кабелю становлять:

$$L = 54 + 160 + 135 = 349 \text{ м.}$$

Також слід враховувати, що одна стандартна бухта крученої пари містить 305 метрів кабелю. Мінімальна довжина цілого необхідного відрізка становить 40 метрів – для каналу другого поверху. Тобто, якщо придбати одну бухту кабелю і 44 додаткові метри, то може не вистачити крученої пари на один канал (якщо починати прокладання з найдовших ліній) або на два канали (якщо починати прокладання з найкоротших). Така ситуація могла б скластися, якщо б не було додатково враховано по 10 технологічних метрів на кожен ліній зв'язку. Однак, в жодному разі, прокладати кручену пару з бухти рекомендується починаючи з найдовших ділянок, щоб уникнути описаної вище ситуації, а ділянку у 44 метри, що поза бухтою, використати для прокладання лінії другого поверху, де додаткові 10 технологічних метрів (по п'ять на кожне кінцеве приміщення) відшкодують необхідні 62 сантиметри довжини. Отже, для втілення нової топології достатньо закупити 349 метрів крученої пари. Середня вартість одного метра якісного кабелю п'ятої категорії на момент оголошення відкритої закупівлі – 20 гривень. Максимальна сума витрачених на кабель коштів за КЕКВ 2210 дорівнює 6 980,00 гривень. На обидва кінця кабелю має бути встановлено конектори стандарту 8P8C. Приблизна вартість одного конектора – 2 гриві. З урахуванням того, що конектори одноразові та можуть бути ненавмисно

пошкоджені в момент обжимання кабелю, рекомендується придбати 20 одиниць замість необхідних 16, витративши 40,00 грн. за КЕКВ 2210.

Активне мережеве обладнання

Середня ринкова вартість комутатора Mikrotik CRS326-24G-2S+RM (див. рис. 2.2) становить 6500,00 грн. Максимальна сума витрачених на дванадцять комутаторів коштів за КЕКВ 2210 становить 78 000,00 гривень.

Джерело безперебійного живлення

Рекомендована LogicPower ціна на пристрій LPY-W-PSW-5000VA (див. рис. 2.4) складає 26 тис. гривень. Оскільки вартість одиниці товару перевищує 20 тисяч гривень, кошти будуть витрачатися за КЕКВ 3110 та становитимуть 26 000,00 гривень у своєму максимальному значенні.

Акумуляторні батареї

Рекомендована LogicPower ціна на батарею LPM-MG 12V 80AH (див. рис. 2.4) становить 7 850 грн. Чотири одиниці може бути придбано за 31 400,00 грн. за КЕКВ 2210.

Канали Інтернет

Середня вартість каналу Інтернет для юридичних осіб з гарантованою швидкістю 100 Мбіт/с та статичною IP-адресою дорівнює 1250,00 гривень/місяць. Витрати на рік становлять 15 тис грн за КЕКВ 2240.

Антивірусний захист

Спеціальна пропозиція для Судової влади України на продукти безпеки Словацької компанії ESET встановлює вартість захисту одного робочого місця / сервера у 290 гривень на рік. Для 225-ти робочих місць та 4-ох серверів потрібно 229 річних клієнтських ліцензій. Сума необхідних на реалізацію централізованого антивірусного захисту коштів, для придбання системи безпеки ESET Protect, становить 66 410,00 гривень.

Інше

Як правило, весь необхідний для монтажу інструмент є у наявності й не підлягає закупівлі.

2.4.2 Електронна система закупівель «ProZorro»

Сфера публічних закупівель регулюється Законом України «Про публічні закупівлі» [26]. Згідно закону, з 19 квітня 2020 року всі державні закупівлі, вартість яких сягає 50-ти тисяч гривень і більше в розрізі позицій «Єдиного закупівельного словника» ДК 021:2015 [27], мають бути виконані через електронну систему закупівель – «ProZorro».

При цьому, якщо сума сягає двохсот тисяч гривень (окрім деяких категорій) має бути проведено тендерну процедуру закупівлі. В іншому разі – спрощену.

Кожен лот електронного аукціону класифікується за ДК 021:2015 до п'ятого знаку. Наприклад, «мережеві кабелі»

Розділ 32000000-3 РАДІО-, ТЕЛЕВІЗІЙНА, КОМУНІКАЦІЙНА, ТЕЛЕКОМУНІКАЦІЙНА ТА СУПУТНИА АПАРАТУРА Й ОБЛАДНАННЯ		
	Код	Назва
	32400000-7	Мережі
—	32420000-3	Мережеве обладнання
	32421000-0	Мережеві кабелі
	32422000-7	Мережеві компоненти
	32423000-4	Мережеві концентратори
	32424000-1	Мережеві інфраструктури
	32425000-8	Мережеві операційні системи
	32426000-5	Мережеві видавничі системи
	32427000-2	Мережеві системи
	32428000-9	Модернізація мереж
	32429000-6	Обладнання для телефонних мереж

Рисунок 2.5 – Єдиний закупівельний словник ДК 021:2015

за кодом 32421000-1 належать до підгрупи 32420000-3 «Мережеве обладнання», яка, в свою чергу, входить до складу групи 32400000-7 «Мережі» розділу 32000000-3 «РАДІО-, ТЕЛЕВІЗІЙНА, КОМУНІКАЦІЙНА, ТЕЛЕКОМУНІКАЦІЙНА ТА СУПУТНЯ АПАРАТУРА Й ОБЛАДНАННЯ» (рис. 2.5). Тобто класифіковані у словнику товари або послуги, які належать до групи із п'ятьма спільними знаками, мають бути об'єднані в одну пропозицію і, якщо очікувана вартість цієї пропозиції сягає суми в 50 тисяч гривень, мають бути придбані лише на відкритих торгах через систему «ProZorro».

Отже, всі товари чи послуги, які потребують закупівлі в рамках проекту модернізації ІТС, підлягають обов'язковій класифікації за ДК 021:2015. Результат класифікації надано у табл. 2.1.

Таблиця 2.1 – Класифікація необхідного для модернізації ІТС обладнання за ДК 021:2015

Найменування	Кіл	Вартість	Сума	Код за ДК 021:2015
Кручена пара	385	20,00	6 980,00	32421000-0 Мережеві кабелі
Конектори 8P8C	20	2,00	40,00	32422000-7 Мережеві компоненти
Комутатор Mikrotik CRS326-24G-2S+RM	12	6 500,00	78 000,00	32423000-4 Мережеві концентратори
LogicPower LPY-W-PSW-5000VA	1	26 000,00	26 000,00	31154000-0 Джерела безперебійного живлення
LogicPower LPM-MG 12V 80AH	4	7 850,00	31 400,00	31440000-2 Акумуляторні батареї
Додатковий канал мережі Інтернет	12	1 250,00	15 000,00	72411000-4 Постачальники Інтернет-послуг
ESET Protect	229	290,00	66 410,00	48761000-0 Пакети антивірусного програмного забезпечення

Як видно з таблиці, виділені перші п'ять знаків коду класифікації є унікальними для кожної позиції, тобто співпадаючи до п'ятого знаку коду класифікації, які мають бути об'єднані в одну пропозицію, в табл. 2.1 відсутні. З таблиці зрозуміло, що суми, які перевищують ліміт у 50 тис. грн (виділено червоним) буде витрачено на придбання дванадцяти комутаторів Mikrotik CRS326-24G-2S+RM та комплексної системи антивірусного захисту ESET Protect. За законом, здійснити закупівлю цих комутаторів і програмного забезпечення можна лише через систему електронних закупівель по спрощеній процедурі.

Інші позиції можуть бути придбані як у системі, так і шляхом укладання прямого договору із постачальниками товарів чи послуг без використання «ProZorro», але, у будь-якому випадку, договір із постачальником має бути опубліковано в системі.

2.5. Підсумок загальних витрат

Після проведеного аналізу можна розрахувати максимальну вартість модернізації ІТС, яка дорівнює:

$$S_{\max} = 6,98 + 0,04 + 78 + 26 + 31,4 + 15 + 66,41 = 223,83 \text{ тис. грн.}$$

За задумкою, «ProZorro» є аукціоном, який сприяє зменшенню корупційної складової в сфері державних закупівель шляхом нормалізації ціни товару чи послуги на відкритих торгах. Але за фактом система дозволяє суттєво економити державні кошти тому реальна сума, яка буде витрачена, буде меншою за максимальну. Передбачити переможця торгів і вартість його пропозиції неможливо, але розпочати процедуру можна лише за умови наявності окреслених максимальною очікуваною вартістю коштів на рахунках установи.

Також річний фінансовий план установи (в даному випадку – ОАС) має дозволяти такі видатки в розрізі кодів економічної класифікації:

- за КЕКВ 2210: $6,98 + 0,04 + 78 + 31,4 = 116,42$ тис. грн;
- за КЕКВ 3110: 26 тис. грн;
- за КЕКВ 2240: $15 + 66,41^* = 81,41$ тис. грн.

За виконанням всіх умов, оголошується (в даному випадку – спрощена) процедура закупівлі в системі «ProZoggo». Державна установа формує технічне завдання, встановлює характеристики товару або послуг які потребують закупівлі. Постачальники товарів / послуг висувають пропозиції щодо конкретних товарів / послуг, які відповідають встановленим умовам та характеристикам, їх ціни, термінів гарантійного обслуговування тощо.

Переможець відкритих торгів визначається комісією із складу відповідальних осіб установи, а протокол обрання переможця публікується в системі електронних закупівель та може бути оскаржений іншими учасниками торгів у встановлений законом термін.

Кінцевий договір постачання товарів / послуг також публікується у системі та знаходиться у вільному доступі. При цьому неважливо за якою процедурою було придбано товар чи послуги. Навіть договір, який було укладено безпосередньо, без використання системи публічних закупівель, має бути опубліковано.

Досвід використання системи електронних закупівель «ProZoggo» вказує на те, що можливо економити 10-15% планових коштів, шляхом зменшення первинної ціни пропозиції відносно її середньої ринкової вартості в процесі аукціону. Тому автори роботи рекомендують здійснювати всі державні закупівлі через систему, незважаючи на поріг у 50 тис. грн.

Планування та фінансовий аналіз проєкту модернізації дозволяє уникнути багатьох помилок на стадіях реалізації проєкту після прийняття рішення, спрямованого на втілення цифрових інновацій в державному секторі. Над концепцією модернізації й на стадії формування вимог до ІТС працює майже весь штат організації, а, починаючи зі стадії технічного проєкту,

* Позначене програмне забезпечення, хоч і не є послугою, за законом завжди проходить за КЕКВ 2240.

відповідальність та робота з реалізації проєкту фактично покладається на три структурні підрозділи – інформаційні технології, бухгалтерський облік (або економічний відділ), та матеріально-технічний. Лише сумісна й злагоджена робота означених структурних підрозділів дає змогу у визначені терміни, якісно реалізувати проєкт створення або модернізації ІТС.

Контрольні питання до розділу 2

1. Чого стосуються основні вимоги при проєктуванні і впровадженні інформаційно-телекомунікаційної системи в державній установі?
2. Головна відмінність інформаційно-телекомунікаційної системи державної установи від комерційних організацій?
3. З яких причин систему захисту інформації державної установи називають комплексною?
4. Які два додаткові етапи передбачає процес побудови інформаційно-телекомунікаційної системи державної установи (на відміну від комерційної організації)?
5. Які основні вимоги до програмного забезпечення та типи ліцензій?
6. Які стадії передбачає процес створення інформаційно-телекомунікаційної системи?
7. Які основні групи вимог ставляться до інформаційної системи?
8. Які вимоги ставить діюче законодавство України до закупівлі обладнання, оплати послуг та робіт з монтажу і налагодження системи?
9. Що включає в себе розрахунок вартості модернізації інформаційно-телекомунікаційної системи?

3. РОЗГОРТАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ В УСТАНОВІ

Коли вже проведено аналіз, висунуто вимоги, окреслено потреби, розроблено технічний проєкт та здійснено закупівлю необхідного для модернізації ІТС обладнання – постає питання втілення результатів теоретичних опрацювань.

Першим етапом практичної реалізації проєкту можна назвати прокладання запланованих комунікацій. В даному випадку – магистральних каналів зв'язку між активним мережевим обладнанням. Процес не складний, за умови наявності шахт та кабель-каналів, тому не потребує окремого опису [28].

Наступним етапом є налаштування активного обладнання, яке, навпаки, потребує особливої уваги і має бути детально розкритим.

3.1. Побудова мережі

Насправді, навіть невеликі за розміром установи доволі часто використовують не одну, а декілька мереж. Так, головною є локальна мережа, яка, насамперед, забезпечує виконання основної функції організації. Але у більшості установ також розгорнуті й допоміжні мережі – бездротові WiFi: захищена для персоналу та гостьова для відвідувачів; дротові відокремлені: для циркуляції інформації з грифом «Для службового користування» (надалі – ДСК) або «Таємно». Обробка інформації із зазначеними грифами має свої особливості [29], може

проводитися лише у фізично відокремленій від основної інфраструктури мережі, а використання VLAN-ів для розмежування доступу до інформації в такому разі заборонене – лише окреме фізичне середовище. У випадку побудови ІТС в установі мова може йти про розгортання основної локальної мережі та бездротових мереж – відомчої та загального доступу. Інформація ДСК в межах ОАС обробляється лише у паперовому вигляді відділами з управління персоналом та державної служби і документообігу та архівної роботи, тому використання VLAN-ів цілком можливе. З’ясуємо можливість такого в даному випадку.

3.1.1 Топологія та IP-план

Із топології мережі, яка надана у *Додатку Ж* зрозуміло, що комп’ютери та сервери ДУ використовують 230 IP-адрес. Ще 37 адрес потрібно для підключення БФП через мережевий інтерфейс. Загалом, мінімальна потреба кількості адрес дорівнює 267 одиницям. Але буде доречно виділити IP-адреси для активного мережевого обладнання, сервера внутрішнього спілкування, який можна інстальовати в установі, сервера обладнання системи контролю доступу, додаткових серверів відеоспостереження та запланувати резервні адреси на випадок настання потреби розширення ІТС.

Вочевидь, що стара задіяна адресація мережі 192.168.0.0/24 не зможе бути використана в новій ІТС ДУ бо на підключення БФП через Ethernet інтерфейс не вистачає 13 IP-адрес для хостів. Маска підмережі / 23 може цілком виправити ситуацію, адже дозволяє вже 510 адрес, але використання пулу адресів 192.168.0.0/23 (так само як і старого 192.168.0.0/24) порушує внутрішній стандарт установи, на замовлення якої Державне підприємство «Інформаційні системи» (надалі – ДП «ІС») займається розробкою єдиної інформаційно-телекомунікаційної

системи мережі подібних закладів, що згодом включить до свого складу всі існуючі ІТС окремих установ. Для інтеграції ІТС ДУ у майбутню глобальну ІТС на центральному рівні було розроблено план ІР-адресації, згідно якого кожній установі було виділено свій локальний ІР простір обов'язковий до використання. ДУ, яка розглядається в даній роботі, за планом має використовувати діапазон адрес 10.16.14.0/24. До речі, це є цілком логічним, що для побудови корпоративної мережі використовується блок адрес 10/8, який має набагато ширшу адресацію ніж 172.16/12 або 192.168/16. Але виділені 254 локальні адреси були не в змозі задовільнити потребу ДУ, тому після звернення до ДП «ІС» було надано дозвіл на використання установою діапазону 10.16.14.0/23.

Далі треба вирішити питання сегментації мережі. Кожна локальна мережа може бути сегментована на підмережі. Доступ із однієї підмережі до пристроїв іншої потребує маршрутизації.

Є два плюси використання сегментації: по-перше сегментація це важливий інструмент захисту інформації, який зменшує площу атаки при проникненні у мережу зловмисника; по-друге це засіб захисту мережі в цілому від широкомовного шторму (broadcast storm) – явища, коли обладнання (або його надмірна кількість), яке знаходиться в одному широкомовному домені, призводить до експоненційного зростання широкомовних запитів (на другому рівні моделі OSI), що призводить до втрати працездатності мережі.

Найпоширенішою причиною широкомовного шторму є петля (кільце), коли одним лінком помилково з'єднують два порти одного мережевого пристрою, або два порти одного пристрою із двома портами другого без використання технології STP (Spanning Tree Protocol). В плоскій мережі broadcast storm може з'явитися як результат неможливості своєчасної обробки всіх широкомовних запитів обладнанням. Нові запити зберігаються у кеші активного обладнання та чекають на обробку,

кеш переповнюється, запити ширяться та мережа втрачає свою працездатність. Чіткої рекомендації граничної кількості комп'ютерів, які можуть працювати в одному сегменті мережі немає, але загальний досвід говорить, що якщо кількість пристроїв перевищує 510 одиниць (тобто діапазон IP-адрес за маскою / 23) введення сегментації мережі стає обов'язковою. Також кількість широкомовних запитів в мережі не має перевищувати 10 відсотків від загального об'єму циркулюючої інформації. У разі перевищення цього показника мережа також має бути сегментована.

Для, так би мовити, хрестоматійного налаштування локальної мережі установи треба виділити в окремі VLANи такі сегменти:

а) *управління* – підмережа із доступом до функцій налаштування активного мережевого обладнання;

б) *сервери* – підмережа серверної інфраструктури ДУ;

в) *сервери відеоспостереження* – окрема віртуальна мережа для відеоспостереження;

г) *БФП* – підмережа для пристроїв друку;

д) *зали ОЗ* – окремий VLAN для систем фіксації засідання в онлайн форматі;

е) *викладачі* – комп'ютери викладачів;

ж) *апарат* (або *відділи*) – комп'ютери інших працівників установи.

Аналізуємо шляхи даних від одного комп'ютера мережі до іншого в сегментованій та несегментованій мережі у розрізі топології із *Додатка Ж*.

У плоскій (несегментованій) мережі кадри даних направляються до місць призначення з мінімально необхідною кількістю передач між комутаторами, або навіть в межах одного комутатора. В самих складних випадках пакет на другому хопі досягає кореневого комутатора K0, звідти відправляються напряму на сервер (якщо він є отримувачем пакета) або на інший комутатор, після якого гарантовано досягає пункту призначення – іншого комп'ютера. В такому разі, тільки зовнішній трафік регулюється

маршрутизатором P1, однак всією мережею ширяться широко-мовні запити від кожного комутатора.

У випадку використання сегментованої мережі процес виглядає інакше. Щоб об'єднати мережу і керувати доступом, для кожної підмережі має бути створено і налаштовано віртуальний інтерфейс, який за фактом є шлюзом підмережі. Всі дані поза межі VLANa йдуть через шлюз віртуального інтерфейсу маршрутизатора P1 незалежно від порту їх відправлення і призначення, навіть якщо отримувача і відправника під'єднано до того ж самого комутатора. Отже, лінк між P1 та K0 з пропускною здатністю 1 Гбіт/с має обслуговувати не лише зовнішній трафік, а й внутрішній. Окрім того діапазоні 10.16.14.0/23 не вистачає адрес для сегментації мережі на сім підмереж. Згоди на використання діапазону 10.16.8.0/21, який може надати вісім підмереж, досягти не вдалось з тієї причини, що частина простору вже використовується іншими установами, яких вже інтегровано у єдину інформаційно-телекомунікаційну систему мережі закладів.

З огляду на ситуацію, яка склалася та її аналіз, який проведено вище, приймається рішення будувати плоску мережу в рамках виділеного для використання діапазону, безпеку та розмежування доступу до даних проводити на прикладному рівні, а підключення обладнання до оновленої мережі здійснювати лише за затвердженим планом IP-адресації, з внесенням відповідних змін у план в разі потреби.

У табл. 3.1 перелічено заплановані адреси серверного обладнання та об'єктів критичної мережевої інфраструктури. У табл. 3.2 наведено заплановані адреси активного мережевого обладнання. У табл. 3.3 містяться заплановані адреси інших мережевих пристроїв.

Для стабільної і контрольованої роботи ІТС слід мати на увазі, що всі поточні та майбутні роботи щодо модернізації, розширення, переналаштування ІТС мають здійснюватися лише в межах запропонованого та затвердженого плану адресації мережі.

Таблиця 3.1 – План IP-адресації серверів

Адреса	Обладнання
10.16.14.1	Шлюз (маршрутизатор P1)
10.16.14.2	Сервер додатків
10.16.14.3	DC2 (додатковий контролер домену)
10.16.14.4	DB1 (сервер баз даних)
10.16.14.5	Зарезервовано (віртуальний сервер VPN)
10.16.14.6	Сервер відеоспостереження
10.16.14.7	Зарезервовано
10.16.14.8	Сервер внутрішнього спілкування та обміну
10.16.14.9	Кореневий комутатор
10.16.14.10	DC1 (головний контролер домену)
10.16.14.25– 10.16.14.29	Статичні адреси для DELL iDRAC (Integrated Dell Remote Access Controller) та HP iLO (HPE Integrated Lights Out) – мережеві сервіси керування серверами HP та DELL
10.16.14.254	Сервер обладнання системи контролю доступу

Таблиця 3.2 – План IP-адресації комутаторів

Адреса	Обладнання
10.16.14.11	Комутатор K1
10.16.14.12	Комутатор K2
10.16.14.13	Зарезервовано (додатковий комутатор першого поверху)
10.16.14.14	Комутатор K3
10.16.14.15	Комутатор K4
10.16.14.16	Комутатор K5
10.16.14.17	Комутатор K6
10.16.14.18	Комутатор K7
10.16.14.19	Зарезервовано (додатковий комутатор другого поверху)
10.16.14.20	Комутатор K8
10.16.14.21	Комутатор K9
10.16.14.22	Комутатор K10
10.16.14.23	Комутатор K11
10.16.14.24	Зарезервовано (додатковий комутатор третього / четвертого поверхів)

Таблиця 3.3 – План IP-адресації інших мережевих пристроїв

Адреса	Обладнання
10.16.14.30– 10.16.14.33	Статичні адреси комп'ютерів відділу інформаційних технологій та технічних засобів
10.16.14.34– 10.16.14.36	Статичні адреси комп'ютерів відділу бухгалтерського обліку та фінансових ресурсів
10.16.14.37– 10.16.14.39	Зарезервовані статичні адреси
10.16.14.40– 10.16.14.240	Пул DHCP сервера, з якого адреси надаються в оренду всім іншим користувачам ІТС
10.16.14.241– 10.16.14.248	Адресний простір для обладнання залів засідання або нарад в режимі онлайн (ОЗ)
10.16.14.249– 10.16.14.253	Зарезервовані на випадок розширення ІТС-адреси
10.16.15.1– 10.16.15.149	Резервний пул DHCP сервера
10.16.15.150– 10.16.15.254	Статичні адреси БФП та інших офісних пристроїв

3.1.2 Налаштування активного мережевого обладнання

До складу типового налаштування керованих комутаторів входить присвоєння їм (за потреби) статичних адрес, активізація вбудованих механізмів контролю петлі та, саме, організація комутації VLANів. Оскільки в даній роботі мова йде про плоску мережу, в окремому описі налаштування комутаторів K1...K11 немає сенсу, натомість належне налаштування маршрутизатора P1 є головною задачею. Повний лістинг конфігурації маршрутизатора надано у *Додатку И*. З міркувань безпеки реальні MAC-адреси інтерфейсів, логіни, паролі, зовнішні IP – змінено на символи XXX, код виділено курсивом, а на рисунках ці елементи закриті кольором. При використанні наданої конфігурації у своїх потребах виділені кольором символи слід змінити на власні дані.

Конфігурація передбачає використання трьох незалежних каналів Інтернет (так званий Multivan), де окремі групи користувачів отримують доступ до мережі Інтернет через певні канали в залежності від задач та повноважень. За проєктом система мала використовувати два відокремлені один від одного канали, але, після укладання договору з ПАТ «Укртелеком» про надання послуг Інтернет-зв'язку, виявилось, що у пакет додатково входить резервний канал із пропускнуою здатністю 100 Mbit/s. Використовувати цей канал саме як резервний не має сенсу, адже він обслуговується тим самим провайдером на єдиному обладнанні разом із основним каналом, ще й фізично надходить до будівлі тим самим оптичним кабелем. Тому було вирішено використовувати згаданий «резервний канал» ПАТ «Укртелеком» як відокремлену лінію зв'язку для залів ОЗ. Договір про надання окремого (справжнього резервного) каналу було укладено із ТОВ «САТЕЛІТ НЕТ СЕРВІС».

Загальні налаштування

Конфігурація налаштування маршрутизатора P1 дозволяє при втраті зв'язку через лінію основного каналу автоматично змінити маршрутизацію через резервний. І навпаки, коли працездатність головного каналу відновлено, користувачів буде автоматично повернуто на головний канал.

Як можна побачити, з десяти Ethernet портів маршрутизатора MikroTik RB4011iGS+RM використовуються чотири. Перший порт – основний канал Інтернет від ПАТ «Укртелеком» із тарифною швидкістю 150 Mbit/s:

```
/interface ethernet
set [find default-name=ether1] name="1 UkrTelecom"
```

Другий порт, згідно із топологією із Додатка Е, під'єднано до кореневого комутатора K0:

```
set [find default-name=ether2] name="2 DU Network"
```

Третій і четвертий порти зарезервовано на той випадок, якщо у майбутньому все ж таки доведеться сегментувати мережу

на VLANи. Як вже було обговорено, лінк між P1 та K0 в такому разі почне обслуговування внутрішнього трафіка мережі. Щоб уникнути перенавантаження цього з'єднання достатньо прокинути патч-корди, якими порти 3 і 4 буде з'єднано із портами кореневого комутатора K0. Після обов'язкових окремих налаштувань, пов'язаних із розмежуванням трафіка через додаткові лінки, пропускна здатність з'єднання P1-K0 збільшиться майже втричі. В поточній конфігурації порти 2–4 а також SFP-порт об'єднано в Bridge, що не є обов'язковим:

```
/interface bridge port
add bridge=bridge1 ingress-filtering=no interface="2 DU Network"
add bridge=bridge1 ingress-filtering=no interface=ether3
add bridge=bridge1 ingress-filtering=no interface=ether4
add bridge=bridge1 ingress-filtering=no interface=
sfp-sfpplus1
```

До п'ятого порту надходить трафік від резервного провайдера:

```
set [find default-name=ether5] name="5 Satellite Net Service"
```

Порти з шостого по дев'ятий теж у резерві. Їх можна використовувати як для задач згаданих вище, так і для інших – наприклад приєднати ще декілька Інтернет-каналів.

Десятий порт використовується для додаткового каналу «Укртелеком»:

```
set [find default-name=ether10] name="10 UkrTelecom Reserved"
```

На рис. 3.1 зображено, як виглядає перелік інтерфейсів маршрутизатора P1 в штатному інструменті для налаштування активного мережевого обладнання Mikrotik під керуванням RouterOS – WinBox.

Для підключення до резервного провайдера використовується мережевий протокол другого рівня PPPoE:

```
/interface pppoe-client
add allow=chap,mschap1,mschap2 disabled=no interface=
"5 Satellite Net Service" keepalive-timeout=60 max-mru=1480
max-mtu=1480 mrru=1600 name=sns user=XXXXXXXXXXXX
```

Session: 10.16.14.1

Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (s/n)	Rx Packet (s/n)	FP Tx	FP Rx	FP Tx Packet (s/n)	FP Rx Packet (s/n)
1	UkrTelecom	1500	1500	0	0	0	0	0	0	0	0
10	UkrTelecom	1500	1500	187.1 kbps	345.4 kbps	84	112	0	0	0	112
11	UkrTelecom	1500	1500	738.8 kbps	47.8 kbps	89	75	0	0	45.4 kbps	0
12	UkrTelecom	1500	1500	0	0	0	0	0	0	0	0
13	Bridge	1500	1500	157.2 kbps	679.5 kbps	75	104	0	0	674.4 kbps	0
14	Bridge	1500	1500	0	0	0	0	0	0	0	0
15	Bridge	1500	1500	0	0	0	0	0	0	0	0
16	Bridge	1500	1500	0	0	0	0	0	0	0	0
17	Bridge	1500	1500	0	0	0	0	0	0	0	0
18	Bridge	1500	1500	0	0	0	0	0	0	0	0
19	Bridge	1500	1500	0	0	0	0	0	0	0	0
20	Bridge	1500	1500	0	0	0	0	0	0	0	0
21	Bridge	1500	1500	0	0	0	0	0	0	0	0
22	Bridge	1500	1500	0	0	0	0	0	0	0	0
23	Bridge	1500	1500	0	0	0	0	0	0	0	0
24	Bridge	1500	1500	0	0	0	0	0	0	0	0
25	Bridge	1500	1500	0	0	0	0	0	0	0	0
26	Bridge	1500	1500	0	0	0	0	0	0	0	0
27	Bridge	1500	1500	0	0	0	0	0	0	0	0
28	Bridge	1500	1500	0	0	0	0	0	0	0	0
29	Bridge	1500	1500	0	0	0	0	0	0	0	0
30	Bridge	1500	1500	0	0	0	0	0	0	0	0
31	Bridge	1500	1500	0	0	0	0	0	0	0	0
32	Bridge	1500	1500	0	0	0	0	0	0	0	0
33	Bridge	1500	1500	0	0	0	0	0	0	0	0
34	Bridge	1500	1500	0	0	0	0	0	0	0	0
35	Bridge	1500	1500	0	0	0	0	0	0	0	0
36	Bridge	1500	1500	0	0	0	0	0	0	0	0
37	Bridge	1500	1500	0	0	0	0	0	0	0	0
38	Bridge	1500	1500	0	0	0	0	0	0	0	0
39	Bridge	1500	1500	0	0	0	0	0	0	0	0
40	Bridge	1500	1500	0	0	0	0	0	0	0	0
41	Bridge	1500	1500	0	0	0	0	0	0	0	0
42	Bridge	1500	1500	0	0	0	0	0	0	0	0
43	Bridge	1500	1500	0	0	0	0	0	0	0	0
44	Bridge	1500	1500	0	0	0	0	0	0	0	0
45	Bridge	1500	1500	0	0	0	0	0	0	0	0
46	Bridge	1500	1500	0	0	0	0	0	0	0	0
47	Bridge	1500	1500	0	0	0	0	0	0	0	0
48	Bridge	1500	1500	0	0	0	0	0	0	0	0
49	Bridge	1500	1500	0	0	0	0	0	0	0	0
50	Bridge	1500	1500	0	0	0	0	0	0	0	0
51	Bridge	1500	1500	0	0	0	0	0	0	0	0
52	Bridge	1500	1500	0	0	0	0	0	0	0	0
53	Bridge	1500	1500	0	0	0	0	0	0	0	0
54	Bridge	1500	1500	0	0	0	0	0	0	0	0
55	Bridge	1500	1500	0	0	0	0	0	0	0	0
56	Bridge	1500	1500	0	0	0	0	0	0	0	0
57	Bridge	1500	1500	0	0	0	0	0	0	0	0
58	Bridge	1500	1500	0	0	0	0	0	0	0	0
59	Bridge	1500	1500	0	0	0	0	0	0	0	0
60	Bridge	1500	1500	0	0	0	0	0	0	0	0
61	Bridge	1500	1500	0	0	0	0	0	0	0	0
62	Bridge	1500	1500	0	0	0	0	0	0	0	0
63	Bridge	1500	1500	0	0	0	0	0	0	0	0
64	Bridge	1500	1500	0	0	0	0	0	0	0	0
65	Bridge	1500	1500	0	0	0	0	0	0	0	0
66	Bridge	1500	1500	0	0	0	0	0	0	0	0
67	Bridge	1500	1500	0	0	0	0	0	0	0	0
68	Bridge	1500	1500	0	0	0	0	0	0	0	0
69	Bridge	1500	1500	0	0	0	0	0	0	0	0
70	Bridge	1500	1500	0	0	0	0	0	0	0	0
71	Bridge	1500	1500	0	0	0	0	0	0	0	0
72	Bridge	1500	1500	0	0	0	0	0	0	0	0
73	Bridge	1500	1500	0	0	0	0	0	0	0	0
74	Bridge	1500	1500	0	0	0	0	0	0	0	0
75	Bridge	1500	1500	0	0	0	0	0	0	0	0
76	Bridge	1500	1500	0	0	0	0	0	0	0	0
77	Bridge	1500	1500	0	0	0	0	0	0	0	0
78	Bridge	1500	1500	0	0	0	0	0	0	0	0
79	Bridge	1500	1500	0	0	0	0	0	0	0	0
80	Bridge	1500	1500	0	0	0	0	0	0	0	0
81	Bridge	1500	1500	0	0	0	0	0	0	0	0
82	Bridge	1500	1500	0	0	0	0	0	0	0	0
83	Bridge	1500	1500	0	0	0	0	0	0	0	0
84	Bridge	1500	1500	0	0	0	0	0	0	0	0
85	Bridge	1500	1500	0	0	0	0	0	0	0	0
86	Bridge	1500	1500	0	0	0	0	0	0	0	0
87	Bridge	1500	1500	0	0	0	0	0	0	0	0
88	Bridge	1500	1500	0	0	0	0	0	0	0	0
89	Bridge	1500	1500	0	0	0	0	0	0	0	0
90	Bridge	1500	1500	0	0	0	0	0	0	0	0
91	Bridge	1500	1500	0	0	0	0	0	0	0	0
92	Bridge	1500	1500	0	0	0	0	0	0	0	0
93	Bridge	1500	1500	0	0	0	0	0	0	0	0
94	Bridge	1500	1500	0	0	0	0	0	0	0	0
95	Bridge	1500	1500	0	0	0	0	0	0	0	0
96	Bridge	1500	1500	0	0	0	0	0	0	0	0
97	Bridge	1500	1500	0	0	0	0	0	0	0	0
98	Bridge	1500	1500	0	0	0	0	0	0	0	0
99	Bridge	1500	1500	0	0	0	0	0	0	0	0
100	Bridge	1500	1500	0	0	0	0	0	0	0	0

Рисунок 3.1 – Перелік інтерфейсів у вікні WinBox

```
Далі надаються IP-адреси зовнішнім інтерфейсам (див. рис. 3.2):

/ip address
add address=10.16.14.1/23 interface=bridge1 network=10.16.14.0
add address=192.168.XXX.XX2/30 interface="1 UkrTelecom" network=192.168.XXX.XX0
add address=192.168.XXX.XX8/30 interface="10 UkrTelecom Reserved" network=192.168.XXX.XX6
```

Надання мережевих налаштувань клієнтам мережі буде здійснювати сервер DHCP, розгорнутий в домені Windows. Ту саму функцію може виконувати P1. Але треба усвідомлювати, що два DHCP сервери в одній мережі (чи її сегменті) із єдиним пулом

Address	Network	Interface
10.16.14.1/23	10.16.14.0	bridge1
192.168.XXX.XX2	192.168.XX0	1 UkrTelecom
192.168.XXX.XX8	192.168.XX6	10 UkrTelecom Reserved

4 items (1 selected)

Рисунок 3.2 – Перелік зовнішніх IP у вікні WinBox

адресації не можуть існувати. Тому DHCP сервер маршрутизатора, хоч і налаштовується, але обов'язково вимикається для запобігання дублювання IP-адрес у мережі. Увімкнути його можна у тому випадку, коли основний і резервний сервери DHCP домену виведені з ладу або знаходяться на обслуговуванні, з метою збереження загальної працездатності мережі:

```
/ip pool
    add name=" DU Pool" ranges=10.16.14.40-10.16.14.240
/ip dhcp-server
    add address-pool="DU Pool" interface=bridge1 name=" DU DHCP"
/ip dhcp-server network
    add address=10.16.14.0/23 dns-server=10.16.14.3,8.8.8.8
domain= DU.Local gateway=10.16.14.1 netmask=23
```

Network Address Translation

Налаштування механізму трансляції мережевих адресів для транзитних пакетів або Network Address Translation (NAT) дозволяє зв'язати внутрішню мережу з Інтернетом (див. рис. 3.3).

```
/ip firewall nat
    add action=masquerade chain=srcnat out-interface=
"1 UkrTelecom"
    add action=masquerade chain=srcnat out-interface=
"10 UkrTelecom Reserved"
    add action=masquerade chain=srcnat out-interface=sns
```

#	Action	Chain	Src Address	Dest Address	Proto	Src Port	Dest Port	In Inter.	Out Inter.	In Inter.	Out Inter.	Src Ad.	Dest Ad.	Bytes	Packets
0	*net	dstnat			6 (tcp)		1 UkrT...							0.0	0
1	*net	srcnat			6 (tcp)		1 UkrT...							204.3 KB	2 383 687
2	*net	srcnat			6 (tcp)		10 Ukr...							18.0 KB	304
3	*net	srcnat			6 (tcp)		ans							173.7 KB	2 659 313
4	*net	dstnat			6 (tcp)		22	ans						0.0	0
5	*net	dstnat			6 (tcp)		80	ans						1098.5 KB	23 536
6	*net	dstnat			6 (tcp)		443	ans						19.2 MB	390 356
7	*net	dstnat			6 (tcp)		3000	ans						26.0 KB	601
8	*net	dstnat			6 (tcp)			ans						0.0	0
9	*net	dstnat			6 (tcp)			ans						0.0	0
10	*net	dstnat			6 (tcp)		3389	ans						672 B	14

Рисунок 3.3 – Ланцюг трансляції мережевих адресів у вікні WinBox

Додатково, в цьому ж блоці, налаштовується доступ до певних сервісів внутрішньої мережі доступ до яких потрібен зовні. Наприклад, сервер внутрішнього спілкування може використовуватися поза межами локальної мережі. В такому разі порти цього сервісу мають бути доступні з Інтернету:

```
add action=netmap chain=dstnat comment=»RocketChat Server
SSH« disabled=yes \
    dst-port=22 in-interface=sns protocol=tcp
to-addresses=10.16.14.8 to-ports=22
add action=netmap chain=dstnat comment=»RocketChat HTTP«
dst-port=80 \
    in-interface=sns protocol=tcp
to-addresses=10.16.14.8 to-ports=80
add action=netmap chain=dstnat comment=»RocketChat SSL«
dst-port=443 \
    in-interface=sns protocol=tcp
to-addresses=10.16.14.8 to-ports=443
add action=netmap chain=dstnat comment=RocketChat
dst-port=3000 in-interface=\
    sns protocol=tcp to-addresses=10.16.14.8 to-ports=3000
```

Тобто, при зверненні по протоколу TCP до зовнішньої IP-адреси інтерфейсу SNS з мережі Інтернет по портах 22, 80, 443 та 3 000 запит переадресується на сервер внутрішнього спілкування та обміну з локальною адресою 10.16.14.8 по відповідних портах. У той же спосіб можна, наприклад, керувати сервером за допомогою протоколу RDP через вбудований в операційну систему Windows інструмент Remote Desktop Connection, який за замовченням працює на 3389 порті TCP. Оскільки відкривати всьому світові свій резервний контролер домену (10.16.14.3) не варто, слід вказати конкретну зовнішню адресу з якої доступ буде дозволено. В даному випадку реальна зовнішня адреса прихована, тобто замість XXX.XXX.XXX.XXX треба вказати потрібну. Звернення з інших адрес будуть ігноруватися:

```
add action=netmap chain=dstnat dst-port=3389
in-interface=sns protocol=tcp src-address=XXX.XXX.XXX.XXX
to-addresses=10.16.14.3 to-ports=3389
```

Маршрутизація

Попередня маршрутизація (PreRouting) надає змогу маркувати пакети від/до певних мережових адрес. Маркування надає змогу відокремити трафік певних груп користувачів для подальшої маршрутизації. Для роботи ІТС, яка розглядається, треба створити дві маркерні групи: «MarkVIP» та «MarkZal» (див. рис. 3.4). Перша група IP-адрес буде використовувати резервний канал Інтернет як власний основний, друга група буде використовувати додатковий канал ПАТ «Укртелеком» в той же спосіб. Згідно плану IP-адресації (див. табл. 3.1, 3.2, 3.3) адреси 10.16.14.10 та 10.16.14.3 належать контролерам домену, 10.16.14.8 – серверу внутрішнього спілкування та обміну. Діапазон 10.16.14.30–10.16.14.39 – це виділені статичні адреси для обладнання двох відділів. Пакети даних, де відправником є одна з перелічених адрес, отримують марку «MarkVIP». Пакети від комп'ютерного обладнання залів ОЗ (10.16.14.241 – 10.16.14.248) будуть промарковані «MarkZal»:

```
/routing table
  add fib name=MarkVIP
  add fib name=MarkZAL
/ip firewall mangle
  add action=mark-routing chain=prerouting comment="VIP"
new-routing-mark=MarkVIP \
  passthrough=no src-address=10.16.14.30-10.16.14.39
  add action=mark-routing chain=prerouting comment=DNS2
new-routing-mark=\
  MarkVIP passthrough=no src-address=10.16.14.10
  add action=mark-routing chain=prerouting comment=RocketChat
new-routing-mark=\
  MarkVIP passthrough=no src-address=10.16.14.8
  add action=mark-routing chain=prerouting comment=DNS1
new-routing-mark=\
  MarkVIP passthrough=no src-address=10.16.14.3
  add action=mark-routing chain=prerouting comment="Zal OZ"
new-routing-mark=\
  MarkZAL passthrough=yes src-address=10.16.14.241-10.16.14.248
```

#	Action	Chain	Src. Address	Out. Address	Proto	Sec. Port	Out. Port	In. Inter.	Out. Int.	In. Inter.	Out. Int.	Sec. Ad.	Out. Ad.	Bytes	Packets
0	mar...	input	10.16.14.30-10.16.14.39											74.1 GB	81 425 064
1	mar...	input	10.16.14.10											0 B	0
2	mar...	input	10.16.14.8											0 B	0
3	mar...	input	10.16.14.3											1726.7 MB	11 620 527
4	mar...	input	10.16.14.241-10.16.14.248											3535.9 KB	46 012

Рисунок 3.4 – Попередня маршрутизація у вікні WinBox

Далі надаються саме маршрути з урахуванням попереднього маркування пакетів. Для пакетів із маркою «MarkVIP» використовувати шлюз «sns»:

```
/ip route
add disabled=no distance=3 dst-address=0.0.0.0/0 gateway=sns
routing-table=
MarkVIP suppress-hw-offload=no
```

Але, якщо кінцевим отримувачем пакету є сервіс, який розташований в ІТС державного рівня (ДСА), трафік від «MarkVIP» буде направлятися на шлюз основного каналу ПАТ «Укртелеком»:

```
add comment=Replication disabled=no dst-address=
10.1.10.0/24 gateway=\
192.168.XXX.XX1 routing-table=MarkVIP suppress-hw-offload=no
```

Далі створюється маршрут для основного каналу:

```
add comment=ISP1 disabled=no distance=5 dst-address=
0.0.0.0/0 gateway=192.168.XXX.XX1
```

І вимкнутий за замовченням маршрут резервного каналу:

```
add comment=ISP2 disabled=yes distance=2 dst-address=
0.0.0.0/0 gateway=sns
```

Прокладається маршрут до сервера DNS корпорації Google через основний канал:

```
add comment=GOOGLE disabled=no dst-address=8.8.4.4/32 gateway=192.168.XXX.XX1
```

Якщо є потреба, можна організувати доступ до певних ресурсів через канали певних провайдерів. Код, наведений нижче, дозволяє всім користувачам ІТС відвідувати сайт Укрпошти й сайт Верховної Ради України виключно через шлюз резервного каналу:

```
add comment=ukrposhta.ua disabled=yes dst-address=91.209.214.17/32 gateway=sns
add comment=zakon.rada.gov.ua disabled=yes dst-address=193.19.153.66/32 gateway=sns
```

А сайт Державного реєстру і поштовий сервер Верховної Ради України через основне з'єднання для пакетів промаркованих «MarkVIP»:

```
add comment=EDR,MAIL disabled=no distance=1 dst-address=212.90.190.0/24 \
gateway=192.168.XXX.XX1 pref-src=0.0.0.0 routing-table=MarkVIP scope=30 \
suppress-hw-offload=no target-scope=10
```

Остання команда спрямовує весь трафік с залив ОЗ із маркою «MarkZal» через шлюз додаткового каналу ПАТ «Укртелеком»:

```
add comment=Reserv disabled=no distance=4 dst-address=0.0.0.0/0 gateway=\
192.168.XXX.XX7 routing-table=MarkZAL
```

Для того, щоб задіяти механізм автоматичного перемикання маршруту з основного каналу на резервний при втраті працездатності першого, активується вбудований в RouterOS інструмент NetWatch.

З інтервалом в 30 секунд маршрутизатор відстежує доступність сервера DNS корпорації Google з адресою 8.8.4.4 через провайдера основного каналу зв'язку. У разі відсутності доступу

до сервера маршрут із коментарем IPS2 автоматично активується. Як тільки доступ відновлюється, резервний маршрут знов вимикається:

```
/tool netwatch
  add down-script="/ip route enable [find comment=\"ISP2\"]"
  host=8.8.4.4 \
    interval=30s    up-script="/ip route disable [find
  comment=\"ISP2\"]"
```

Для тих самих дій можна відстежувати активність інтерфейсу Ethrt1 з ім'ям «1 UkrTelecom» («LinkUp» або «LinkDown»), але доволі часто трапляються випадки, коли лінк до провайдера працює, але інтернет-зв'язок відсутній. За настанням таких обставин автоматична перемаршрутизація працювати не буде, що є недоцільним. Також замість сервера DNS Google з адресою 8.8.4.4 можна використовувати будь-який, що викликає довіру.

Важливу роль в маршрутизації пакетів відіграє параметр «Distance», який обумовлює черговість застосування маршруту. Маршрути з нульовою дистанцією створюються автоматично для всіх зовнішніх інтерфейсів. Пакет даних проходить ланцюг по низхідній і, якщо умови направлення пакету співпадають із заданим маршрутом, здійснюється його направлення адресатові.

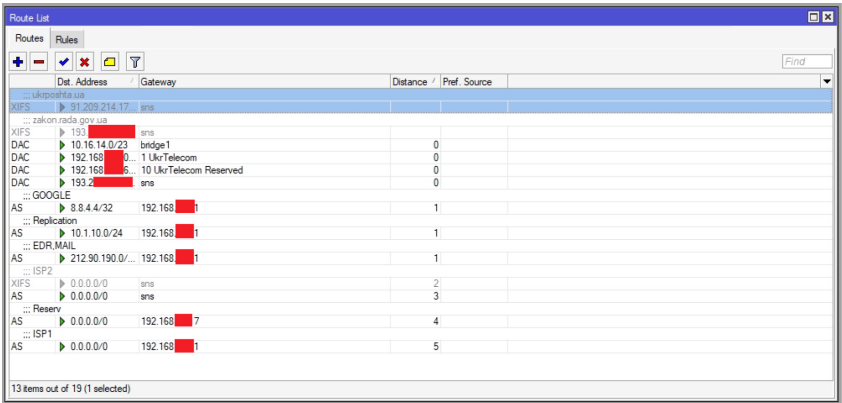


Рисунок 3.5 – Маршрутизація пакетів у вікні WinBox

На рис. 3.5 відображено налаштовану маршрутизацію.

На рисунку маршрут із параметром Distance = 2 є маршрутом резервного каналу, а маршрут з Distance = 5 основного каналу.

При втраті з'єднання із мережею Інтернет на інтерфейсі Ethrt1 автоматично активується маршрут де Distance = 2. Таким чином всі пакети починають рухатися через резервний канал зв'язку. І навпаки, при дезактивації маршруту з Distance = 2 (після відновлення працездатності основного каналу) система продовжує працювати в штатному режимі. Маршрути з Distance = 1, в реалізованій конфігурації, обумовлюють використання певних ресурсів через певних провайдерів й застосовуються незалежно від механізму перемикання каналів, бо мають параметр Distance = 1, що обумовлює їх першочергове виконання. Маршрут із Distance = 3 використовується для всіх пакетів, що мають марку «MarkVIP», а з Distance = 4 – «MarkZal».

Сервіси

Безпека від зовнішнього вторгнення в конфігурацію маршрутизатора P1 здійснюється шляхом заборони всіх сервісних з'єднань із маршрутизатором із зовні. Також вимикаються незадіяний в роботі функціонал (disabled=yes):

```
/ip service
set telnet address=10.16.14.0/23 disabled=yes
set ftp address=10.16.14.0/23 disabled=yes
set www address=10.16.14.0/23
set ssh address=10.16.14.0/23 disabled=yes port=222
set www-ssl address=10.16.14.0/23
set api address=10.16.14.0/23
set winbox address=10.16.14.0/23
set api-ssl address=10.16.14.0/23
```

Для захисту внутрішніх ресурсів здійснюється налаштування фільтрів файрволу. Правила прописуються для трьох ланцюгів фільтрації: вхідних, вихідних та транзитних пакетів. Кожен ланцюг є окремим, але порядок правил в рамках певного ланцюга має значення. Правила застосовуються послідовно, також діє принцип: що не має заборони – є дозволим. Тобто принцип

організації ланцюгів файерволу передбачає, що останнім фільтром у ланцюзі буде тотальна заборона – drop, а попередні правила фільтрації дадуть дозвіл на обробку безпечних та очікуваних пакетів.

Firewall. Ланцюг вхідних пакетів

Дозволяються всі встановлені й раніш схвалені вхідні з'єднання:

```
/ip firewall filter
    add action=accept chain=input comment="Allow Related
Connections" connection-state=established,related
```

Блокуються вхідні пакети із статусом «invalid»:

```
    add action=drop chain=input comment="Drop all Invalid input"
connection-state=invalid
```

Дозволяються вхідні з'єднання з зовнішніх IP-адрес з переліку «Allowed Input» який можна налаштувати за потреби:

```
    add action=accept chain=input comment="Allowed Input
IP list" src-address-list="Allowed Input"
```

Надається дозвіл на надходження пакетів ping зовні. Суперечливий пункт з міркувань безпеки, але необхідний для моніторингу працездатності ІТС установи контролюючим органом або підприємством.

```
    add action=accept chain=input comment="Allow Ping Mikrotik"
protocol=icmp
```

Блокуються всі інші вхідні з'єднання окрім тих, що надходять із внутрішньої мережі (по всіх інтерфейсах окрім bridge1):

```
    add action=drop chain=input comment="Drop all other Input"
in-interface=!bridge1
```

Firewall. Ланцюг транзитних пакетів

Заборона транзиту пакетів від певного пристрою внутрішньої мережі із певною MAC адресою. Використовується

за потреби задля: обмеження доступу до Інтернету деяких комп'ютерів, блокування зовнішнього трафіка БФП, відеореєстраторів тощо:

```
add action=drop chain=forward comment=»Block some user
by MAC» out-interface=\
    "1 UkrTelecom" src-mac-address=D0:XX:XX:XX:XX:A6
```

У той же спосіб можна обмежити певний IP або цілий перелік IP:

```
add action=drop chain=forward comment=»Block some user
by IP» disabled=yes \
out-interface=sns src-address=10.16.14.XXX
```

Заборона транзиту пакетів сервісів віддаленого доступу, таких як TeamViewer, AnyDesk та інших, для діапазону локальних адрес, потребує окремого налаштування фільтрації протоколу сьомого рівня, яке буде розглянуте нижче:

```
add action=reject chain=forward comment=TeamViewer disabled=
yes \
    layer7-protocol=team reject-with=icmp-network-unreachable
src-address=\
    10.16.14.40-10.16.14.254
add action=reject chain=forward comment=TeamViewer
disabled=yes \
    layer7-protocol=team1 reject-with=icmp-network-
unreachable src-address=\
    10.16.14.40-10.16.14.254
add action=reject chain=forward comment=AllOtherRemote
disabled=yes \
    layer7-protocol=Other reject-with=icmp-network-
unreachable src-address=\
    10.16.14.40-10.16.14.254
add action=drop chain=forward comment=TeamViewer disabled=yes
dst-port=5938 \
    protocol=tcp src-address=10.16.14.40-10.16.14.254
add action=drop chain=forward comment=TeamViewer disabled=yes
dst-port=5938 \
    protocol=udp src-address=10.16.14.40-10.16.14.254
```

Далі за аналогією налаштувань ланцюга Input дозволяються транзит пакетів для віх встановлених й раніш схвалених з'єднань та блокуються зіпсовані пакети:

```
add action=accept chain=forward comment="Allow Related Forward" connection-state=established,related
add action=drop chain=forward comment="Drop invalid connections My Network" connection-state=invalid
```

Блокуються змоги шахрайського проникнення до внутрішньої мережі шляхом підміни адресів по всіх зовнішніх інтерфейсах:

```
add action=drop chain=forward comment="Drop all from WAN not DSTNATED" connection-nat-state=!dstnat \
    connection-state=new in-interface="1 UkrTelecom"
add action=drop chain=forward comment="Drop all from WAN not DSTNATED" connection-nat-state=!dstnat connection-state=new in-interface="10 UkrTelecom Reserved"
add action=drop chain=forward comment=" Drop all from WAN not DSTNATED " connection-nat-state=!dstnat connection-state=new in-interface=sns
```

Відкриваються порти необхідних для функціонування ІТС сервісів:

```
add action=accept chain=forward comment="Allow DNS" dst-port=53 in-interface=bridge1 protocol=udp
add action=accept chain=forward comment="GLOBAL Allow TCP" dst-port=80,443,7680 in-interface=bridge1 protocol=tcp
add action=accept chain=forward comment="GLOBAL Allow UDP" dst-port=123,443 in-interface=bridge1 protocol=udp
add action=accept chain=forward comment="Replication SPD SRV-BASE" dst-port=21,25,110,5000,8090 in-interface=bridge1 protocol=tcp src-address=10.16.14.4
add action=accept chain=forward comment="Allow TCP MEDok MAIL" dst-port=465,993 in-interface=bridge1 protocol=tcp src-address=10.16.14.2
add action=accept chain=forward comment="ZOOM TCP" dst-port=8801,8802 in-interface=bridge1 protocol=tcp
add action=accept chain=forward comment="ZOOM UDP" dst-port=3478,3479,8801-8810 in-interface=bridge1 protocol=udp
add action=accept chain=forward comment="Allow TCP EasyCon"
```

```
dst-port=3478,5349,8443,8444,8958      in-interface=bridge1
out-interface="10 UkrTelecom Reserved" protocol=tcp
add action=accept chain=forward comment="Allow UDP
EasyCon" dst-port=3478,5349,31001-65535 in-interface=bridge1
out-interface="10 UkrTelecom Reserved" protocol=udp
add action=accept chain=forward comment="Allow TCP
EasyCon SNS" disabled=yes dst-port=3478,5349,8443,8444,8958
in-interface=bridge1 out-interface=sns protocol=tcp
add action=accept chain=forward comment="Allow UDP
EasyCon SNS" disabled=yes dst-port= 3478,5349,31001-65535
in-interface=bridge1 out-interface=sns protocol=udp
```

Всі інші транзитні пакети блокуються:

```
add action=drop chain=forward in-interface=bridge1
out-interface="1 UkrTelecom"
add action=drop chain=forward in-interface=bridge1
out-interface="10 UkrTelecom Reserved"
add action=drop chain=forward in-interface=bridge1
out-interface="sns"
```

Firewall. Ланцюг вихідних пакетів

Дозволено обробку пакетів ping протоколу icmp для контролю працездатності основного каналу і заборона проходження їх через резервний:

```
add action=accept chain=output comment="Google DNS ping
Allow" dst-address=8.8.4.4 out-interface="1 UkrTelecom"
protocol=icmp src-address=192.168.XXX.XX2
add action=drop chain=output comment="Google DNS ping Drop"
dst-address=8.8.4.4 out-interface=sns
```

отже, таблиця файерволу виглядає так, як зображено на рис. 3.6.

Для коректної роботи фільтрації протоколу сьомого рівня залишається обумовити його правила:

```
/ip firewall layer7-protocol
add name=team regexp=»^(post|get) /d(out|in).
aspx\\?.*client=dyngate»
add name=team1 regexp=»^\\x17»
add name=Other regexp="^.(anydesk|ammy|aerodesk|teamviewe
r|relays.net.anydesk.com).*$"
```

#	Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter.	Out. Inter.	In. Inter. IP	Out. Inter. IP	Src. Ad.	Dst. Ad.	Bytes	Packets
0	allow	input												474.8 MB	9 114 961
1	drop	input												1352.4 KB	26 429
2	allow	input												0 B	0
3	allow	input												3632.2 KB	64 533
4	allow	input												0 B	0
5	drop	input												43.6 MB	832 433
6	drop	forward												0 B	0
7	drop	forward												0 B	0
8	drop	forward												0 B	0
9	drop	forward												0 B	0
10	allow	forward	10.16.14.2											0 B	0
11	allow	forward	10.16.14.2											0 B	0
12	allow	forward	10.16.14.2											0 B	0
13	allow	forward	10.16.14.2											0 B	0
14	allow	forward	10.16.14.2											0 B	0
15	allow	forward												292.6 GB	338 413
16	drop	forward												3174.1 KB	58 952
17	drop	forward												0 B	0
18	drop	forward												0 B	0
19	drop	forward												0 B	0
20	allow	forward												97.1 MB	1 405 095
21	allow	forward												206.9 MB	4 149 954
22	allow	forward												191.2 MB	289 952
23	allow	forward	10.16.14.4											0 B	0
24	allow	forward	10.16.14.2											1040 B	20
25	allow	forward												0 B	0
26	allow	forward												885.9 KB	14 140

Рисунок 3.6 – Таблиця файерволу у вікні WinBox

На цьому налаштування маршрутизатора P1 та активного мережевого обладнання можна вважати завершеним.

Дану конфігурацію маршрутизатора P1 з Додатку И було розроблено й успішно імплементовано в ІТС ДУ. Конфігурація дозволяє блокувати несанкціоновані зовнішні підключення, в тому числі з метою перехорлення керуванням обладнанням. Також фільтруються пакети, які надходять з локальної мережі в мережу Інтернет по нестандартних протоколах або від груп пристроїв / користувачів, які не мають прав на використання сервісів, що взаємодіють через такі порти і протоколи. У разі відсутності доступу до Інтернету, конфігурацію передбачено автоматичну зміну маршруту пакетів через резервний канал, а також прописані статичні маршрути для деяких зовнішніх корисних сервісів.

Слід нагадати, що перегляд файлів журналів акивного мережевого обладнання дозволяє виявити спроби несанкціонованого вторгнення до ІТС й заздалегідь прийняти низку заходів щодо усунення загрози і поліпшення системи захисту ІТС.

3.2. Побудова домену Windows

Домен Windows це сукупність мережевих пристроїв з встановленими операційними системами Microsoft, які мають єдиний центр керування (контролер домену), єдину базу даних Active Directory (надалі – AD), єдину групову і локальну політику та єдині параметри безпеки (для кожної окремої групи). Домен дозволяє керувати безпосередньо всією корпоративною комп'ютерною інфраструктурою через сервіси контролера домену, який, в свою чергу, контролює всі мережеві пристрої за виключенням комутаторів та маршрутизатора.

3.2.1. Рекомендації щодо найменувань комп'ютерів у домені

Мережеві імена комп'ютерів і серверів є не лише набором символів, але й ідентифікатором пристрою в мережі. Взагалі, завдяки службам DNS, мережеві імена виконують ту ж саму функцію, що й локальні IP-адреси, тому не слід відноситися до процесу найменувань техніки зневажливо. Не існує єдиних стандартів надання імен, але існує єдина рекомендація – імена мають вкладатися в систему. Ім'я може відображати структуру, географію, ПІБ користувача, спеціальні ідентифікатори і все що завгодно, але, за потреби, по імені пристрою адміністратор має ідентифікувати місцезнаходження обладнання або його володаря/користувача.

Отже, на стадії проєктування ІТС було вирішено, що ім'я сервера має відображати його спрямованість і починатися з префіксу «SRV-». Тобто, в ДУ будуть використовуватися чотири основні сервери з такими іменами: SRV-MAIN, SRV-DOMAIN, SRV-BASE, SRV-SOFT. А віртуальні сервери отримають префікс «VSRV-»: VSRV-VPN, VSRV-DU.

В той же час, ім'я комп'ютера, який підпорядковується контролеру домена, має починатися з префіксу, який вказує на його фактор, його належність до структурного підрозділу та прізвища

користувача, за яким закріплено робоче місце – після префіксу. Літерні префікси означають наступне:

«СХХ-» – персональні комп'ютери відділів установи, де ХХ це номер структурного підрозділу.

«S-» – персональні стаціонарні комп'ютери відповідальних ОЗ.

«А-» – персональні стаціонарні комп'ютери начальників підрозділів та відділів.

«J-» – персональні стаціонарні комп'ютери членів ректорату.

«Z-» – комплекси фіксації онлайн засідання, встановлені в спеціалізованих аудиторіях.

«ZAL-» – комплекси фіксації онлайн засідання (в тому числі комплекси відеоконференцзв'язку), які використовуються в залах ОЗ.

Розглянемо *приклади* можливих найменувань:

– в імені підпорядкованого контролерові домену терміналу «С08-PETRENKO» префікс «С08-» означає, що термінал є стаціонарним персональним комп'ютером, який належить до структурного підрозділу із кодом «08» – відділу статистики та звітності, і його закріплено за користувачем із прізвищем Петренко;

– «J-GOLOVA» – персональний комп'ютер члена ректорату з прізвищем Голова;

– «ZAL-102» – комплекс фіксації онлайн засідання, розташований у конференц-залі ОЗ № 102;

– для найменування портативних і персональних терміналів, що мають форм-фактор типу ноутбук, встановлюється префікс «NB-» після якого слідує послідовність літер, яка відображає прізвище користувача: «NB-SADOVA» – ноутбук, який закріплено за користувачем із прізвищем Садова.

3.2.2. Розподіл ролей між серверами домену

Інформаційно-телекомунікаційну інфраструктуру ДУ обслуговують чотири основні фізичні сервери.

Найкращим шляхом для побудови будь-якої взаємопов'язаної ІТ-структури є використання таких інструментів хмарних технологій як віртуальні машини (надалі – ВМ). Взагалі, на наявному обладнанні і ліцензійному ПЗ можна побудувати дванадцять серверів під керуванням Windows Server 2019: 4 фізичні й 8 віртуальних. Їх кількість обумовлена обмеженням ліцензійної угоди на використання Windows Server 2019 Standard.

Аналіз апаратної складової серверного обладнання ДУ виділяє один фізичний сервер на базі Intel Xenon E5-2620, який має достатні характеристики для виконання ролі сервера віртуальних машин Hyper-V. Але, згідно стандартів цифрової інфраструктури ДУ, цей сервер єдиний з усіх чотирьох відповідає вимогам і може використовуватися як сервер бази даних комп'ютерної програми з діловодства КП ДВ. З іншої сторони, ніхто не забороняє використовувати його як сервер БД і, в той же час, як сервер Hyper-V. Але, з міркувань стабільності ІТС, розташування контролера домену і сервера БД в одному фізичному середовищі небажане.

Окрім того, установа має достатню кількість фізичних серверів щоб розгорнути збиткову (або надлишкову – redundant) доменну структуру. Якщо ДУ мала би лише два сервери, побудувати повноцінну і захищену доменну структуру було б неможливо без використання ВМ.

Наразі серверів чотири, тому головні ролі фізичних пристроїв було вирішено розподілити так:

- головний контролер домену;
- додатковий контролер доменну;
- сервер БД (із роллю сервера Hyper-V);
- сервер додатків.

Інші ролі і доменні сервіси розподіляються між чотирма серверами згідно з їх потужнісними характеристиками.

Головний контролер домену. Сервер на базі Intel Xenon E1225 / 16Gb RAM / Raid10 із загальним масивом 14,5Tb. Мережеве ім'я – «SRV-MAIN». IP-адреса (див. табл. 3.1): 10.16.14.10/23. Ролі сервера (див. рис. 3.7): Активний Каталог (AD), DHCP

(первинний), DNS, Hyper-V (реплікація і відпрацювання відмови), WDS, Сервер сертифікатів, Сервер друку, Файловий сервер резервних копій, а також сервер Windows Server Update Services для централізованого зберігання і розповсюдження оновлень операційних систем Microsoft серед членів домену.

Фактично, SRV-MAIN є головним сервером, який здатен самостійно керувати процесами життєдіяльності ІТС, навіть при умові втрати зв'язку із всіма іншими серверами. Але, якщо із будь-яких причин зв'язок терміналів ІТС із сервером SRV-MAIN буде втрачено, доменна структура припинить своє існування. Щоб запобігти виникненню згаданих проблем, в структуру домену треба ввести додатковий контролер домену. В той же час, процес реплікації дозволить тримати дані активного каталогу в актуальному стані одразу на обох серверах. І хоча володарем домену залишиться SRV-MAIN, при відсутності зв'язку із ним, резервний контролер буде виконувати всі функції головного сервера. Також, при фізичній втраті головного контролера, існують механізми для передачі його ролі резервному контролерові.

Додатковий контролер домену. Сервер на базі Intel Xeon E5-2609 / 16Gb RAM/Raid10 з масивом 512Gb. Мережеве ім'я – «SRV-DOMAIN». IP-адреса (див. табл. 3.1): 10.16.14.3/23. Ролі сервера (див. рис. 3.8): Активний Каталог (AD), DHCP

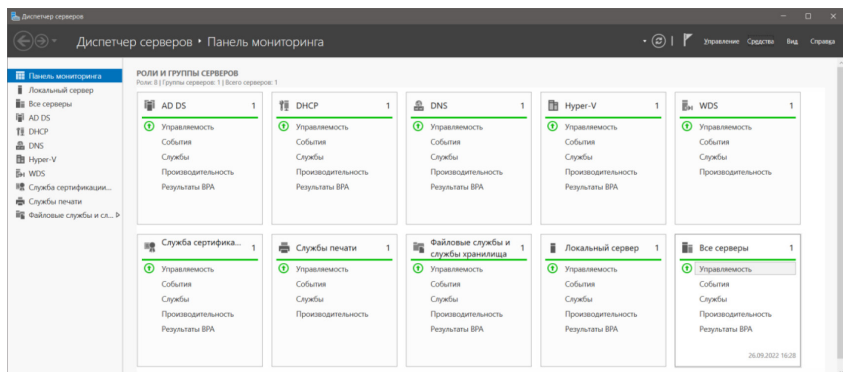


Рисунок 3.7 – Ролі головного контролера домену

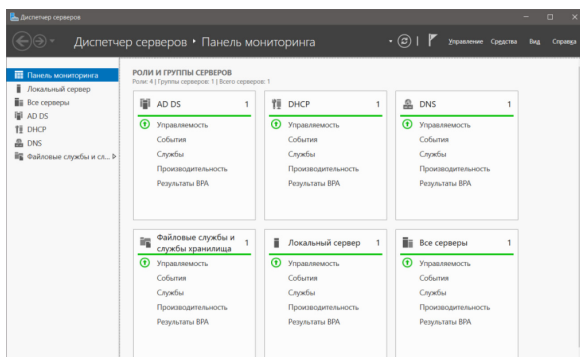


Рисунок 3.8 – Ролі додаткового контролера домену

(відпрацювання відмови), DNS, Сервер системи безпеки ESET Protect, Файловий сервер захищеної інформації. Як було зазначено вище, виконує дублюючу роль головного контролера домену і забезпечує користувачів ІТС низкою власних сервісів.

Сервер баз даних. Сервер на базі Intel Xenon E5-2620 X 2 / 64Gb RAM / Raid10 із загальним масивом 1Tb. Мережеве ім'я – «SRV-BASE». IP-адреса (див. табл. 3.1): 10.16.14.4/23. Ролі сервера (див. рис. 3.9): Сервер Hyper-V, Сервер Firebird, Сервер реплікації КР ДБ.

Сервер додатків. Сервер на базі Intel Xenon E5-2407/16Gb RAM/ Raid10 із загальним масивом 2Tb. Мережеве ім'я – «SRV-SOFT». IP-адреса (див. табл. 3.1): 10.16.14.2/23. Ролі сервера: Файловий

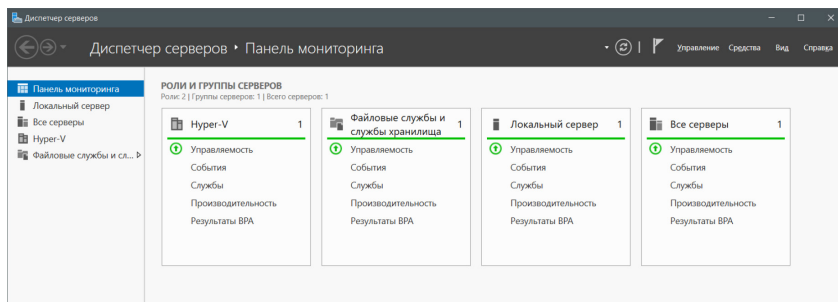


Рисунок 3.9 – Ролі сервера БД та гіпервізора

сервер загальної інформації, MS SQL Server, Сервер M.E.Doc, Сервер ISPro, Сервер «Ліга закон».

Розподіл ролей між фізичними серверами є фундаментом, на якому базуються майбутні сервіси ІТС. Тому вкрай важливо раціонально розподілити серверні потужності між складовими запланованої інфраструктури. Сервери із значним об'ємом дискового масиву використовуються як файлові сховища, багатопроцесорні платформи із великою кількістю ядер якнайкраще підходять на роль гіпервізорів, малоядерні але швидкі сервери із декількома мережевими картами – найкращі кандидати на роль контролерів домену.

Треба ще раз наголосити, що для еталонної побудови ІТС для кожного сервісу слід використовувати окрему віртуальну машину. Тобто, сервер додатків мав бути сервером з однією єдиною роллю – Нурер-V. Далі, на базі гіпервізору, мали б бути розгорнуті окремі ВМ, кожна з яких обслуговувала б лише один сервіс. Тобто одна ВМ для MS SQL Server, друга для сервера M.E.Doc і т.д. Але, для ДУ вимагається, що, програмне забезпечення сторонніх виробників має знаходитися в окремому фізичному середовищі, а ліцензії Windows Server типу «standard» достатньо лише для розгортання двох ВМ в гіпервізорі. Окрім ліцензійних обмежень серверові «SRV-SOFT» не вистачає обчислювальних потужностей для віртуалізації всіх сторонніх сервісів. Лише за цих обставин була прийнята й втілена модель розподілу ролей між фізичними серверами аналізованої установи, яка розглядається вище.

За інших обставин (наприклад у комерційній структурі) вся інфраструктура прикладного рівня ІТС (навіть на базі розглянутого обладнання) була б побудована на віртуальних машинах.

3.2.3. Активний каталог Active Directory

У мережі Інтернет існує безліч статей й інструкцій з інсталяції і налаштування Windows Server 2019 корпорації Microsoft – від покрокових мануалів [30, 31, 32] до навчальних відео на платформах

YouTube [33], тому весь процес інсталяції серверних систем, їх ролей і компонентів та типових налаштувань не потребує опису. Розглядатимуться лише нюанси, яким було приділено особливу увагу та оригінальні рішення, які було реалізовано на шляху побудови ІТС у вищому навчальному закладі.

Активний каталог містить структуровану інформацію про користувачів і комп'ютери мережі, про групи безпеки і права. Після розгортання ролі Active Directory (надалі – AD) на майбутньому контролері домену слід підвищити його рівень до доменного контролера (рис. 3.10) і створити новий ліс імен, якщо мова йде про головний контролер домену, або додати контролер до існуючого домену, якщо йдеться про додатковий (рис. 3.11).

При створенні нового домену необхідно визначитися з його ім'ям. Доменне ім'я буде додаватися до імені будь-якого мережевого пристрою, робота якого підпорядкована контролерові домена. Ще одна важлива особливість – у разі коли домен локальний (а саме такий було побудовано в ДУ) після імені домену слід позначити це, вказавши «.Local» наприкінці доменного імені. Наприклад, для локального домену Office треба вказати ім'я Office.Local для домену DU–DU.Local.

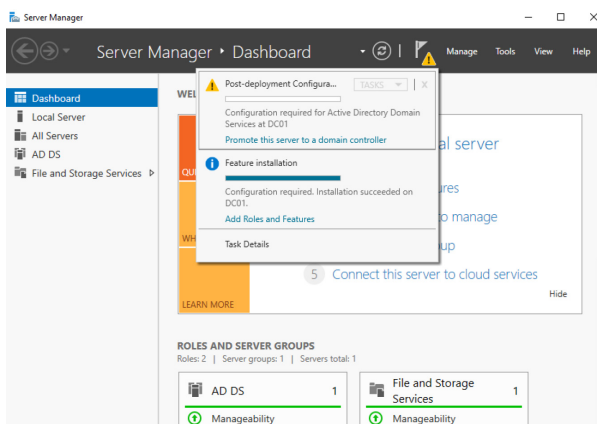


Рисунок 3.10 – Підвищення сервера до рівня контролера домену

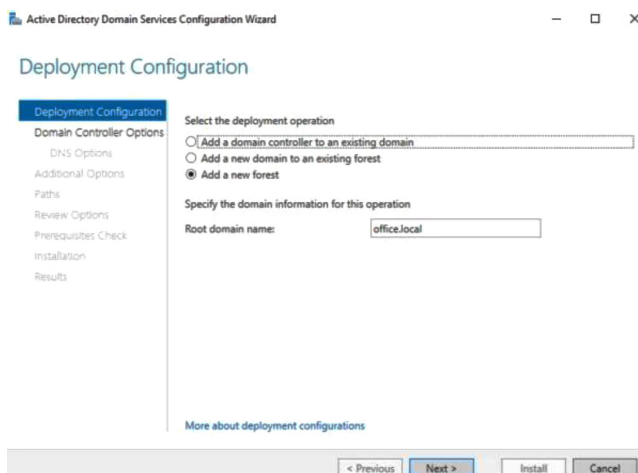


Рисунок 3.11 – Створення нового локального домену

У рамках поточної роботи створено домен DU.Local й додано до нього додатковий контролер домену. Після створення домену, повне доменне ім'я головного контролера домену, або FQDN (від англ. Fully Qualified Domain Name), буде визначатися як SRV-MAIN. DU.Local.

Однією з фундаментальних речей при організації доменної структури є принцип організації активного каталогу. Active Directory, за фактом, є ієрархічним лісом і визначення його структури обумовлює подальшу долю активного каталогу. Оскільки ДУ розташовано у приміщенні, яке має номери кабінетів, а кабінети, в свою чергу, належать структурним підрозділам установи, логічним кроком є побудова змішаної географічно-штатної моделі активного каталогу, де об'єктами вищого рівня є підрозділи або відділи ДУ, яким підпорядковуються контейнери-приміщення, які, в свою чергу, зберігають об'єкти AD – користувачів й пристрої. Така модель побудови AD дозволяє застосовувати доменні політики по низхідній: від організації в цілому, до підрозділу і кожного окремого кабінету. Зокрема, така структура забезпечує достатній рівень прозорості при переміщенні технічних засобів

в межах установи, що дозволяє посилити й спростити облік матеріальних цінностей.

На рис. 3.12 зображено активний каталог ДУ, де на прикладі кабінету № 209, який входить до складу групи «Відділи та служби», яка підпорядковується контейнерові «DU» у складі лісу «DU.Local» можна побачити створену ієрархічну структуру.

Контейнери створюються за допомогою контекстного меню об'єкта вищого рівня. Об'єкти комп'ютерів з'являються автоматично при введенні комп'ютера в домен і додаються у групу найвищого рівня «Computers» звідкіль їх потрібно перетягнути у цільовий підрозділ. Також існує можливість створити об'єкт-комп'ютер самостійно в потрібному підрозділі, а вже потім ввести комп'ютер з відповідним ім'ям до домену.

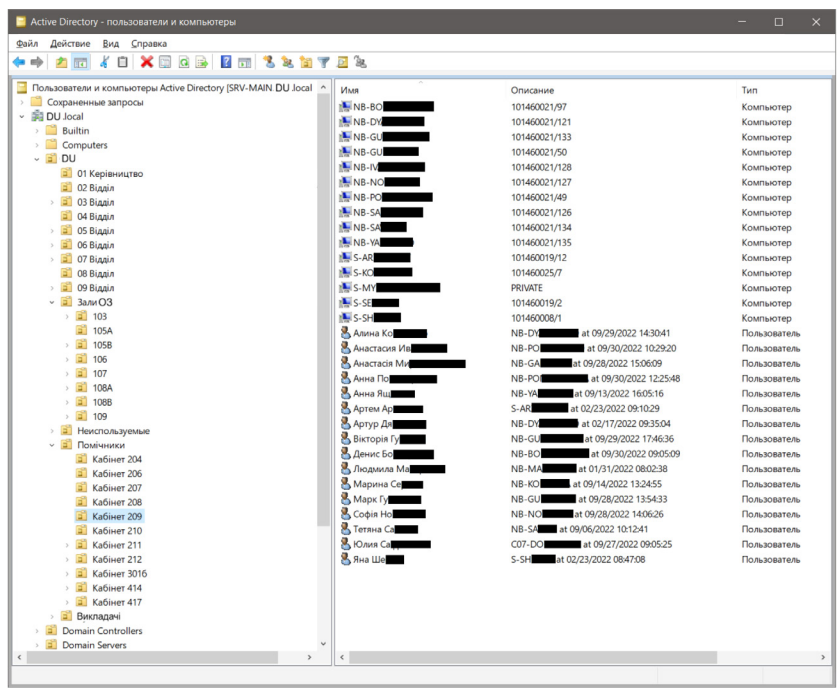


Рисунок 3.12 – Активний каталог ДУ

Групи безпеки активного каталогу надають змогу згрупувати користувачів за рівнем і правами доступу. Отже, для ДУ було створено групи: «J», «A» й «S», які відповідно включають до свого складу членів ректорату, керівників відділів та служб і відповідальних за ОЗ. Також створено групи безпеки для кожного структурного підрозділу ДУ і службові групи такі, як група безпеки віддаленого робочого стола (для забезпечення доступу по протоколу RDP) й група керівників відділів для доступу до певної мережевої теки лише окресленим особам.

На рис. 3.13 наведений перелік груп безпеки й підрозділів АД, які було створено в активному каталозі ДУ.

Окрім перелічених вище об'єктів, структура АД наповнюється інформацією про користувачів. Користувачі створюються у контейнерах підрозділів / кабінетів до яких вони належать. Кожен користувач має логін і належить, як мінімум, до однієї групи безпеки або є членом декількох груп одночасно. Як приклад, начальник структурного підрозділу є членом обох груп – свого підрозділу і групи керівників.

На початку наповнення АД бажано впровадити систему логізації користувачів, котра допоможе систематизувати облікові дані. Логін може містити код підрозділу, номер приміщення

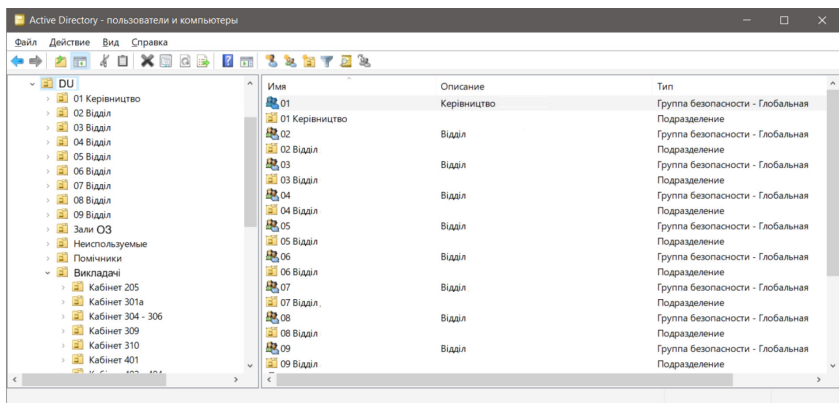


Рисунок 3.13 – Групи безпеки активного каталогу

користувача, його ім'я, прізвище або лише частину його імені та/або прізвища. В рамках цієї роботи, в ДУ була розроблена система логінізації користувачів, але вона не може розголошуватися задля зберігання кібербезпеки.

Групи безпеки визначають межі повноважень користувача. Всі комп'ютери установи мають бути налаштовані таким чином, щоб здійснити вхід до системи мав змогу лише користувач структурного підрозділу, до якого належить пристрій. Наприклад, на локальному комп'ютері відповідального ОЗ, в консолі «Керування комп'ютером» в меню «Локальні користувачі і групи» до групи «Користувачі» слід включити групу безпеки «S», а всі інші записи вилучити. Як результат, здійснити вхід на цей комп'ютер зможуть лише ті користувачі, яких включено до групи «S» активного каталогу, тобто відповідальні ОЗ.

Для терміналів, на яких зберігається інформація із обмеженим доступом можна замість груп безпеки використовувати персональний доступ користувача. Наприклад, право входу на комп'ютер викладача має лише певний користувач із складу відповідного структурного підрозділу – володар терміналу. Не слід додавати всю групу «J» до групи «Користувачі», треба додати лише об'єкт певного користувача. У той самий спосіб регулюється доступ до загальних мережевих ресурсів, про що буде згодом.

На рис. 3.14 зображено властивості AD об'єкту користувача, який належить контейнерові «02 Відділ з управління персоналом» – Катерина М., яка є членом групи безпеки «02». У сусідньому вікні маємо властивості групи безпеки «02», де відображено всіх членів групи.

Два AD об'єкти користувачів зі складу групи безпеки «02» – «Вікторія» та «Марія Сав.» відключено, про що свідчить піктограма із стрілкою. В обов'язок адміністратора безпеки служби захисту інформації входить відключення або вилучення користувачів при звільненні та у випадках тривалих відпусток / відраджень.

Варто зазначити, що видалення користувача або комп'ютера з AD позбавляє можливості входу в доменний

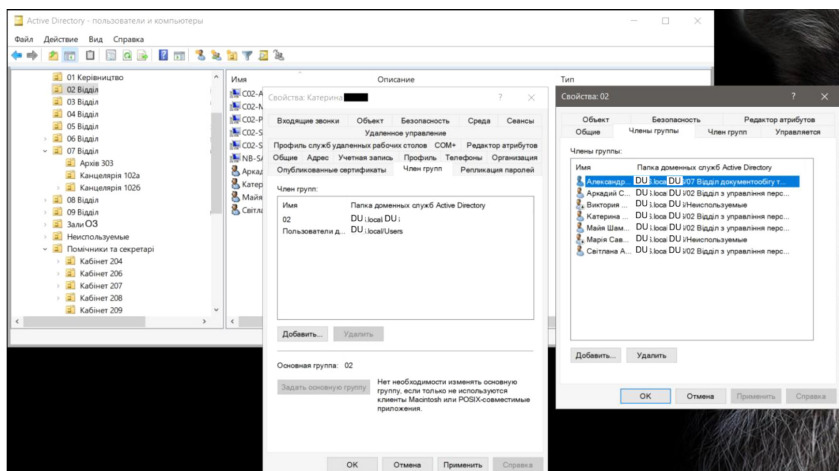


Рисунок 3.14 – Властивості активного каталогу об’єкта користувача

профіль клієнтського терміналу певному користувачеві чи виключає комп’ютер з домену відповідно. Для відновлення доступу доведеться створювати нового користувача (що не є правильним, бо в журналах безпеки користувач ідентифікується за унікальним кодом, який у нового користувача буде іншим) або знов вводити комп’ютер в домен.

Тому рекомендується замість видалення об’єктів AD вимикати їх (функція доступна в контекстному меню об’єкта) і, після дезактивації, переміщати до спеціально створеного для таких випадків контейнеру вищого рівня, наприклад «Відключені», «Незадіяні» або «Кошик». Назва не принципова і залежить лише від фантазії адміністратора безпеки / домену. Відключення об’єкту має такі самі наслідки як і вилучення, але у разі потреби знов задіяти об’єкт достатньо увімкнути його, замість витрачання часу на створення нового.

Окрім того, спеціальний контейнер вищого рівня для відключених об’єктів може зберігати комп’ютери (і їхні інвентарні номери) які є неприцездатними або підлягають списанню. Наразі, для тих самих цілей можна створити окремий об’єкт, наприклад – «Склад».

3.2.4. Ролі DHCP і DNS

Служби Dynamic Host Configuration Protocol (надалі – DHCP) видають в оренду IP-адреси і параметри мережевих сервісів пристроям ІТС у яких мережевий інтерфейс налаштовано на автоматичне отримання вказаних даних. У випадку аналізованої ДУ, майже всі клієнтські термінали, окрім комп'ютерів залів ОЗ та окремих комп'ютерів двох відділів, отримують IP-адреси від серверів DHCP (див. табл. 3.3). Як видно з рис. 3.7 та рис. 3.8, роль DHCP виконують два сервери: SRV-MAIN який налаштовано як основний сервер, та SRV-DOMAIN який виконує роль резервного сервера з відпрацюванням відмови.

Після розгортання ролі DHCP в першу чергу було налаштовано діапазон IP-адрес які видаються клієнтам. Згідно із планом IP-адресації (див. табл. 3.3) в оренду здається пул адрес 10.16.14.40–10.16.14.240.

Потім встановлюються параметри, які видаються клієнтам: шлюз (маршрутизатор), сервер часу, DNS і т. д. в залежності від мережевих сервісів які використовуються.

В останню чергу увімкнено відпрацювання відмови, що передбачає наступний механізм: коли основний сервер, з будь-яких причин не може виконати свою функцію, адреси починає видавати резервний DHCP. При цьому за резервним сервером бронюється 20 відсотків діапазону адрес. Якщо основний сервер не відновлює працездатність на протязі 5 хвилин, весь діапазон переходить у власність резервного сервера, який виконує функцію основного до моменту повернення зв'язку із основним. На рис. 3.15 приведено налаштування ролі DHCP на сервері SRV-MAIN. При налаштуванні відмови замість імені резервного серверу SRV-DOMAIN використовується його IP-адреса (10.16.14.3) що не принциповим.

Пункт меню «Орендовані адреси» дозволяє переглянути перелік мережевих пристроїв, які отримали оренду і строк її закінчення.

Як було зазначено в п. 3.1.2 «Налаштування активного мережевого обладнання», у разі виходу з ладу обох серверів функцію

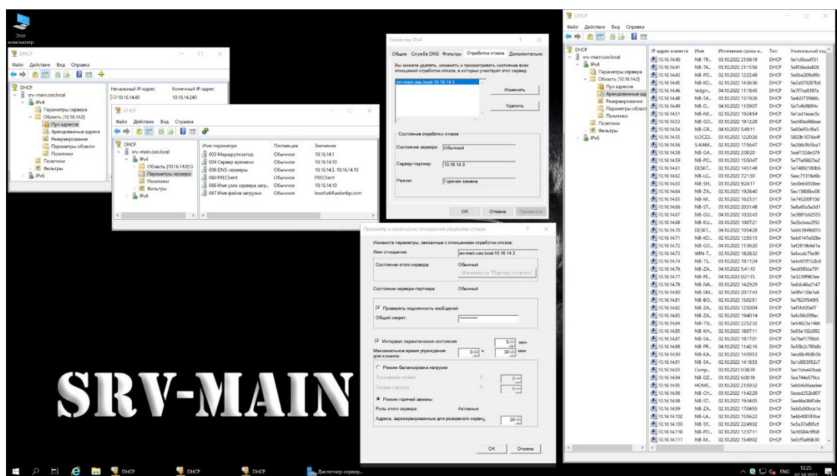


Рисунок 3.15 – Налаштування ролі DHCP

DHCP може виконувати маршрутизатор P1. Таким чином досягається безвідмовне функціонування служб DHCP в ІТС ДУ.

Domain Name System (надалі – DNS) зв’язує IP-адреси із іменами мережевих інтерфейсів і навпаки – імена з адресам. Іншими словами, це механізм ведення динамічного довідника, де записи додаються або змінюються в залежності від присутності / відсутності пристроїв в мережі. Налаштування ролі DNS передбачає окреслення зон прямого і зворотного огляду і створення статичних записів для тих інтерфейсів, які мають статичні адреси. Сервери DNS в домені здійснюють обмін інформацією один з одним задля підтримки інформації в актуальному стані. Цей процес схожий на процес обміну між контролерами домену і теж має назву реплікація.

Для співставлення імен з адресами була створена зона «DU. Local» а для зворотного процесу службі надано дві зони «14.16.10.in-addr.arpa» та «15.16.10.in-addr.arpa». Необхідність окреслення двох зон зворотного огляду витікає із використання IP діапазону ІТС 10.16.14.0/23 в якому задіяні адресні простори 10.16.14.XXX та 10.16.15.XXX. Обидві зони мають бути надані службі DNS.

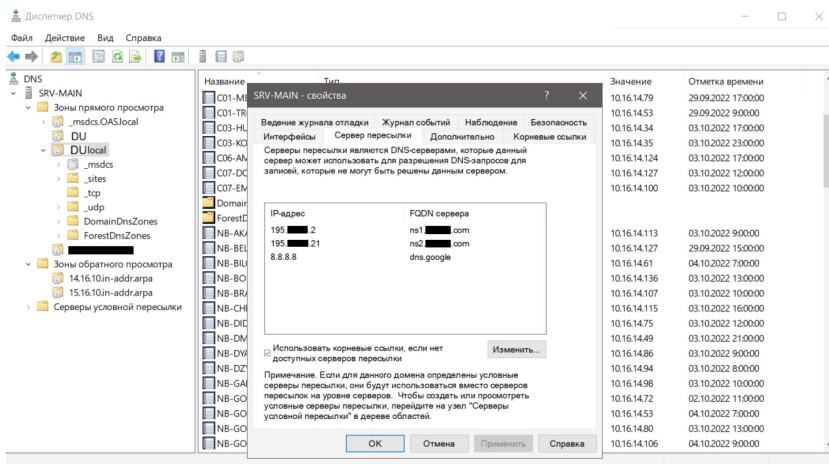


Рисунок 3.16 – Налаштування ролі DNS

Записи DNS на внутрішніх серверах відповідають інформації із внутрішньої мережі. Для співставлення адресів і доменних імен Інтернету слід використовувати зовнішні DNS сервери. Як правило, в ролі зовнішніх серверів використовуються власні DNS сервери провайдерів мережі Інтернет, але також можна прописати й публічні сервери, наприклад – 8.8.8.8 (DNS сервер корпорації Google). Якщо запитуване мережеве ім'я або IP-адреса відсутні в базі даних служби DNS, сервіс звертається до зовнішніх DNS серверів, які обов'язково слід прописати у вкладці «Сервери пересилання».

На рис. 3.16 наведений перелік зон огляду мережі і налаштування серверів пересилання запитів DNS.

3.2.5. Сервер друку

У державному секторі, де робота доволі часто пов'язана із паперовими носіями інформації, принтери та БФП експлуатуються досить активно. Техніка потребує постійних

профілактичних робіт, іноді – ремонту, тому доволі часто переміщується в межах установи: резервні друкарські пристрої займають місце тимчасово непрацездатних, поки ті знаходяться в сервісі, а після повернення з обслуговування основний пристрій стає резервним і чекає на інсталяцію. Таким чином пристрої друку циркулюють в межах установи, що ускладнює їх відстеження і облік. В мережі, де не розгорнуто сервер друку або не використовуються мережеві принтери / БФП адміністратору доводиться витратити багато часу на підключення і відключення пристроїв, інсталяцію і деінсталяцію драйверів, подолання інших проблем пов'язаних із сумісністю й обліком. Сервер друку Microsoft систематизує і значно полегшує керування всіма друкарськими мережевими пристроями в установі.

Для розгортання серверу друку в ДУ на сервері SRV-MAIN було додано роль «Служби друку», завантажено драйвери всіх БФП що використовуються в роботі, а самі друкарські пристрої інстальовано на сервер. Покрокові дії з інсталяції Microsoft Print Server 2019 можна знайти у статті «How to Install and Configure a Print Server in Windows Server 2019» [34].

На рис. 3.17 зображено налаштований сервер друку. Для коректної роботи всі драйвери, що зберігаються на сервері, мають бути підписані видавником ПЗ, тобто завантажувати драйвери слід з офіційних джерел.

Підключення засобів друку до клієнтських терміналів здійснюється через групову політику. Саме поле «Об'єкт групової політики» вказує на певну пов'язану політику. Процес розгортання принтера за допомогою GPO буде детально описано в п. 3.2.8 «Групова політика (GPO) домену». В якості імені політики використовується номер приміщення, що дозволяє миттєво визначити де в даний момент розташовано БФП.

Мережеві імена принтерів теж бажано систематизувати. У випадку досліджуваної ДУ було вирішено, що ім'я складається з покоління БФП, його інвентарного номеру і кабінету,

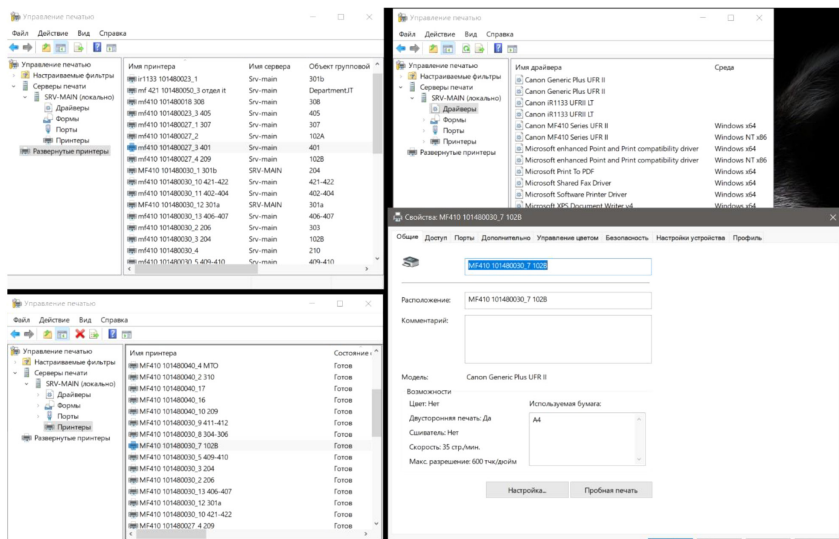


Рисунок 3.17 – Сервер друку

в якому початково було інстальовано принтер. Але згодом, у процесі експлуатації, БФП мігували до інших місць розташування внаслідок дій, що описані вище (цей процес можна чітко відстежити на рис. 3.17). Тому використання номерів приміщень як частки мережевих імен БФП (в цьому конкретному випадку) неможна назвати вдалою ідеєю.

За допомогою сервера друку можна не лише керувати окремими друкарськими пристроями, але й створювати розподілені принтери, коли під єдиним мережевим ім'ям знаходиться пул БФП. В такому разі друк буде здійснюватися з урахуванням загальної черги та вільних пристроїв. Це є доцільним коли в одному приміщенні знаходиться декілька БФП, які постійно завантажені. Оскільки умови роботи установи не потребують використання розподілених принтерів, кожен фізичний пристрій установи має один розгорнутий на сервері мережевий екземпляр.

3.2.6. Файлові сервери

Роль «Файлові служби та служби сховища» забезпечує функціонування загальних файлових ресурсів і надає до них доступ користувачам із певними правами. Існує два методи організації файлового обміну. Перший передбачає створення й використання розподіленої файлової хмари, другий базується на експлуатації мережеских ресурсів загального користування. Перший метод зручніший, надійніший але й більш небезпечний (у разі використання сторонніх хмарних сервісів), другий простіший, і, при налаштуванні резервного копіювання інформації, не менш надійний. Оскільки безпека інформації, власником якої є держава, має бути на першому місці при виборі методів організації файлового сховища, в ДУ застосовується другий метод побудови.

Для обміну файлами було створено низьку мережеских тек:

1. «*Файловий архів*». Містить теки структурних підрозділів, теки із інформацією загального характеру, теки обміну й теки окремих користувачів мережі.

2. «*Штат ДУ*». Тека з обмеженим доступом, яка використовується для зберігання конфіденційної інформації працівників установи. Доступ налаштовується індивідуально до окремої іменної теки, яка зберігається всередині ресурсу «Штат ДУ».

3. «*Скановані додатки*». Тека містить скановані документи й матеріали, які мають бути оброблені.

4. «*Scanner*» – тека внесена до налаштувань кожного БФП як точка зберігання сканованих документів. Організована для мережевого сканування паперових носіїв інформації.

5. «*Інсталяції*» – адміністративна тека для зберігання інсталяційних пакетів програмного забезпечення.

6. «*Конвертація PDF в Word*» мережевий ресурс для сервісу конвертації документів.

Права користувачів на використання теки визначаються стандартними методами адміністрування – через властивості теки і консоль «Загальні ресурси». Для надання прав використовуються

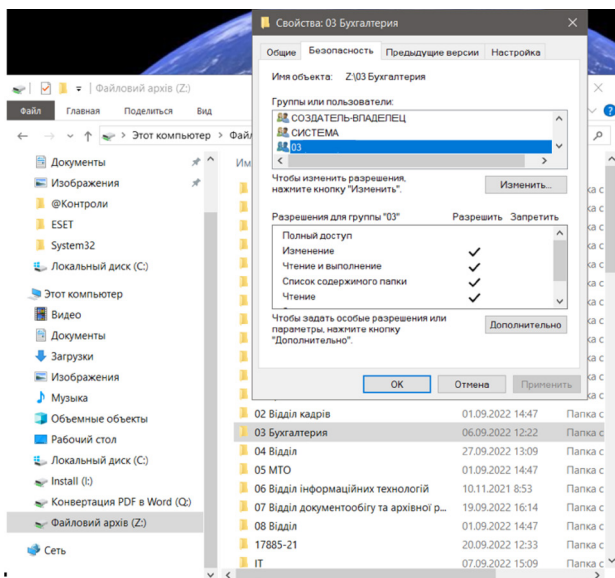


Рисунок 3.18 – Налаштування прав доступу

групи безпеки AD що, на прикладі теки «Бухгалтерія», демонструє рис. 3.18.

У залежності від прав доступу, кожен користувач ІТС отримує масив мережевих дисків, які пов’язані із необхідними для виконання роботи загальними ресурсами файлових серверів. Мережеві диски розгортаються на клієнтських терміналах за допомогою групової політики. Процес буде розглянуто у п. 3.2.8 «Групова політика (GPO) домену».

3.2.7. Сервер Microsoft Hyper-V

Гіпервізор це низькорівнева оболонка яка забезпечує одночасне виконання декількох операційних систем на віртуальних машинах в одному фізичному середовищі, ізолюючи ВМ (та їхні ОС) одну від одної і розподіляючи ресурси між ними, а також

надає засоби зв'язку й взаємодії між ВМ. Нурер-V є вбудованим в операційні системи Microsoft гіпервізором.

Встановлення ролі Нурер-V надає можливість використовувати віртуальні машини, які, за фактом, є екземплярами або інших серверних операційних систем (не обов'язково Microsoft), або звичайними користувацькими ОС.

Надзвичайною особливістю віртуальних машин є легкість копіювання, перенесення, розгортання, резервного зберігання машини в цілому. Вбудований механізм реплікації дозволяє зберігати копії працюючих ВМ майже в реальному часі, і в будь-який момент можна відпрацювати відмову певної ВМ просто запустивши резервну репліку. Для перенесення ВМ в інший гіпервізор, на інший сервер чи навіть у хмарне середовище достатньо скопіювати файл віртуального жорсткого диска машини і її службові файли в нове розташування і запустити її. При цьому, скопійована машина буде не клонованим екземпляром, а точною копією оригіналу з усіма ідентифікаторами безпеки, MAC-адресами інтерфейсів, налаштуваннями ОС і файловою системою. Ще однією особливістю ВМ є контрольні точки, які зберігають стан машини в певний момент часу і можуть бути використані для відкату стану машини. Точки можна створювати в будь-який час і вони, так само як і батьківська машина, можуть реплікуватися на резервні сервери. Керування всіма процесами здійснюється через Диспетчер Нурер-V.

В установі було створено дві віртуальні машини: VSRV-VPN відповідає за VPN підключення користувачів до віртуальної приватної мережі, VSRV-OAS використовується як майданчик для експериментів. При виникненні потреби в експлуатації VPN, достатньо запустити потрібну віртуальну машину в диспетчері. Коли необхідність у використанні VPN сервісу зникає – вимкнути ВМ. Це є однією з корисних властивостей технології ВМ і її суть полягає в тому, що машину можна зупинити (у разі якщо вона не потрібна) і вивільнити ресурси для інших ВМ, або власне для сервера. У той самий спосіб використовується ВМ із тестовою

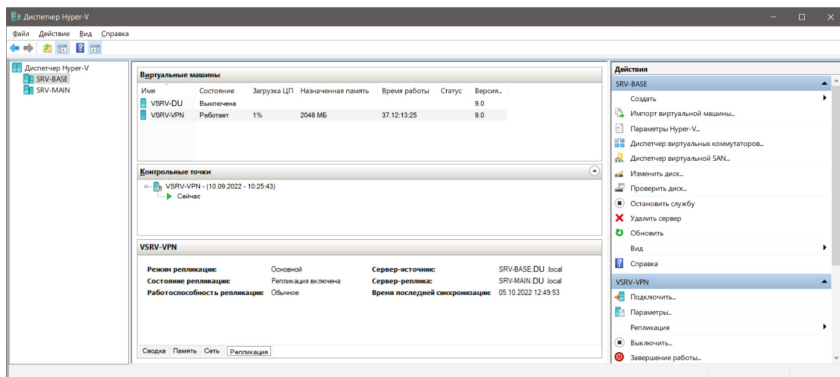


Рисунок 3.19 – Диспетчер Нурег-V з двома віртуальними машинами

серверною ОС, на якій можна протестувати оновлення операційної системи, нове ПЗ, скрипти, вплив політик і багато іншого, а потім, за потреби, виконати відкат машини до первісного стану єдиним кліком миші й завершити її роботу. Стосовно VPN слід підкреслити, що використання віддаленого доступу до ІТС державної установи, без державної експертизи всіх засобів встановлення зв'язку, є порушенням законодавства України щодо захисту інформації. Тому тримати несертифікований сервер VPN в ІТС можна лише на випадок настання надзвичайних обставин.

Як було зазначено, керування віртуальними машинами здійснюється в Диспетчері Нурег-V (див. рис. 3.19).

Налаштування і особливості експлуатації VPN сервера в державній установі буде детально розглянуто в п. 3.5 «Virtual Private Network (VPN) під Нурег-V в домені Windows».

3.2.8. Групова політика (GPO) домену

Групова політика і її об'єкти Group Policy Object (Надалі – GPO) є потужними інструментами адміністратора доменної інфраструктури, які дозволяють централізовано керувати налаштуваннями

клієнтських терміналів, віртуальних машин і серверів, що функціонують в домені Windows. Зокрема GPO також відповідає за розповсюдження ПЗ.

Об'єкти групової політики, пов'язані із контейнерами AD, впливають на певні групи користувачів або комп'ютерів – членів груп активного каталогу – та застосовуються суворо ієрархічно наслідуючи політики всіх батьківських об'єктів. Таким чином, досягається стандартизація налаштувань для всіх підпорядкованих домену об'єктів інфраструктури. Керування об'єктами здійснюється за допомогою утиліти «Управління груповою політикою». Розглянемо об'єкт групової політики на прикладі політики, яка застосовується для кабінету №304.

Сама по собі політика «304» впливає на всі об'єкти типу «користувач», які містяться в контейнері AD – «304». Політика підключає користувачеві БФП з інвентарним номером 101480040/9. А також під'єднає мережевий диск «S», який вказує на загальний ресурс сканованих документів файлового сервера.

З рис. 3.20 видно, що об'єкт GPO з назвою «304» збережено у контейнері «304» активного каталогу, який належить контейнерові AD «Кабінет 304-306» (з яким пов'язаний об'єкт політики «304-306»), що, в свою чергу, входить до складу контейнера «Викладачі» із об'єктом групової політики «Judges Global». Контейнер «Викладачі» зберігається в контейнері «DU», який пов'язаний з політикою «DU Users». Найвищим рівнем лісу є контейнер «DU.Local» із політикою «DU Global» і він містить всі об'єкти активного каталогу. Таким чином, політика «304» успадковує всі налаштування політики «304-306», «Judges Global», «DU Users» і «DU Global».

На рис. 3.20 зазначені політики виділені червоними стрілками, де розмір стрілки демонструє рівень підпорядкованості об'єкта GPO. Тобто, «304» успадковує цілу низьку налаштувань з об'єктів GPO (див. рис. 3.21).

Фізично кабінет 304 (разом із кабінетами 305 і 306) знаходиться у тамбурі, який обладнано БФП загального користування

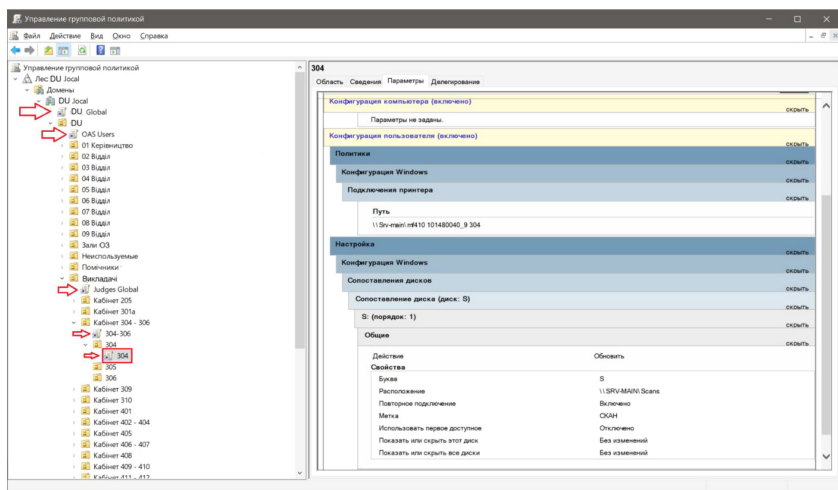


Рисунок 3.20 – Об’єкт групової політики «304»

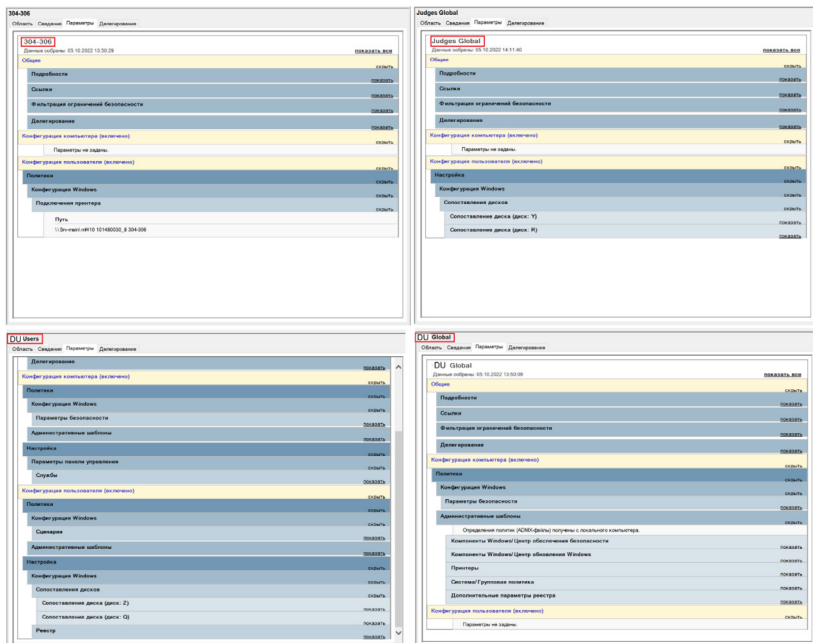


Рисунок 3.21 – GPO, які успадковує «304»

з інвентарним номером 101480030/8. Політика «304–306» розгортає цей друкарський пристрій всім користувачам контейнера «304–306», тобто всім викладачам із кабінетів 304, 305 й 306. «Judges Global» підключає два мережеві диски «Y» (захищене персональне файлове сховище) та «R» (скановані матеріали або документи). Політика «DU Users» впливає на всі об'єкти установи, окрім об'єктів серверного обладнання і контейнер «Незадіяні», де зберігаються відключені об'єкти. Вона містить багато налаштувань, пов'язаних із специфічним ПЗ, безпекою, програмами і скриптами котрі виконуються при вході користувача до системи, а також приєднує ще два мережеві диски – «Z» (файловий архів загального користування) та «Q» (мережева папка сервісу конвертації PDF в DOCX). Політика вищого рівня «DU Global» втілює перелік загальних налаштувань для всіх без виключення членів домену.

Отже викладач, котрий під своїми обліковими даними входить в систему, автоматично отримує пару підключених, налаштованих і готових до роботи БФП, п'ять мережевих дисків, які вказують на певні ресурси файлових серверів, встановлене програмне забезпечення і налаштування операційної системи. У процесі входу виконуються контрольні скрипти, які змінюють поля «опис» об'єктів AD: користувача (викладача) й можливо терміналу (комп'ютер викладача), де прописуються облікові дані, час, дата входу і мережеве ім'я комп'ютера, з якого користувач здійснив вхід (скрипт детально буде розглянуто згодом).

За допомогою Редактора об'єктів групової політики (див. рис. 3.22) можна редагувати будь-які об'єкти GPO в процесі налаштування.

Політики можуть застосовуватися до об'єктів типу «комп'ютер» та/або до об'єктів типу «користувач».

Якщо політика націлена на користувача, то *не має значення з якого терміналу* користувач увійде до системи – він отримає свій набір політик, які під'єднують йому звичні й необхідні для роботи сервіси, ПЗ і налаштовують систему. У тому разі, якщо

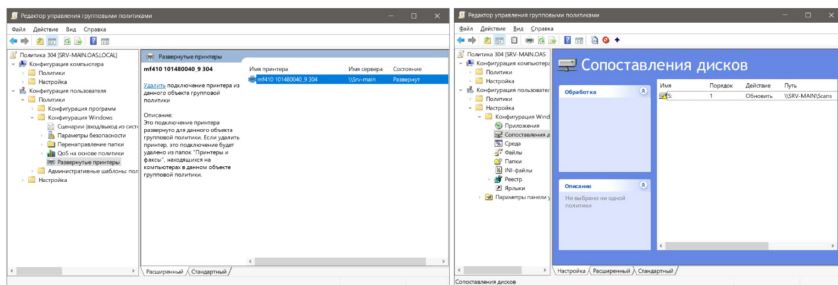


Рисунок 3.22 – Редактор GPO

політика націлена на комп'ютер, то не має значення який користувач здійснить вхід на певний комп'ютер – він отримає набір сервісів певного комп'ютера.

В установі механізм GPO було налаштовано таким чином, що конфігурація комп'ютера містить параметри безпеки, а параметри користувача – все інше: розгортання сервісів, принтерів, ПЗ а також персональні налаштування.

3.2.9. WDS (Windows Deployment Services)

У процесі використання мережі, яка підпорядкована доменній структурі, набагато легше розгортати операційні системи клієнтських терміналів централізовано. Наразі, комп'ютери певних партій закупівлі мають, як правило, однакові модулі, які потребують однакових драйверів та ПЗ. Значно заощадити час системного адміністратора в такому разі допомагає служба розгортання Windows (англійською Windows Deployment Services. Надалі – WDS).

На рис. 3.23 зображено консоль керування службами WDS.

Роль WDS встановлюється на серверну операційну систему так само, як і інші ролі через меню керування сервером. На сервері зберігаються еталонні образи вже налаштованих операційних систем, які призначені для розгортання. Створити

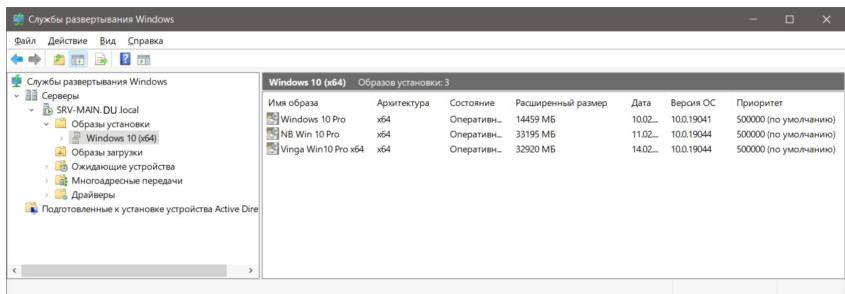


Рисунок 3.23 – Службы розгортання Windows

образи можна як із дистрибутива ОС та і шляхом клонування ОС налаштованого термінала. До складу WDS входить служба PXE (англ. Preboot eXecution Environment) яка є середою для завантаження комп'ютера за допомогою мережевої карти без використання локальних носіїв даних. Після мережевого завантаження можна піти двома шляхами – клонувати ОС терміналу або розгорнути на терміналі одну з підготовлених та збережених на сервері WDS операційних систем. При тому кількість терміналів, що можуть одночасно розгортати ОС, обмежена лише пропускною здатністю мережі.

Для служби WDS вищого навчального закладу було створено три образи операційної системи: для комп'ютерів викладачів, для ноутбуків викладачів і для систем фіксації онлайн засідання, що можна побачити на рис. 3.23. Використання WDS дозволило розгорнути повністю налаштовану і готову до роботи операційну систему на двохстах терміналах за лічені години.

3.2.10. Резервне копіювання даних

Резервне копіювання даних запобігає втраті службової інформації в результаті нештатних ситуацій або некваліфікованих дій користувачів. Сервери ДУ налаштовано на використання масивів пристроїв зберігання інформації за технологією

Raid 10, що є достатнім для надійного збереження даних. Навіть якщо один з чотирьох жорстких дисків серверного масиву остаточно вийде з ладу, втрати інформації не відбудеться, що зрозуміло зі схеми на рис. 3.24, яка демонструє принцип роботи технології.

Але більшість випадків втрати інформації пов'язані не з обладнанням, а з діями користувачів. Для нейтралізації цієї проблеми було вирішено створити архіви службової інформації мережевих ресурсів загального доступу серверів SRV-SOFT і SRV-DOMAIN на сервері SRV-MAIN. Додатково, на SRV-MAIN, було вирішено копіювати і зберігати записи з усіх діючих систем фіксації онлайн засідань з подальшим автоматичним розгортанням загального мережевого ресурсу цих записів через GPO для використання в роботі викладачів, здобувачів та відповідальних ОЗ.

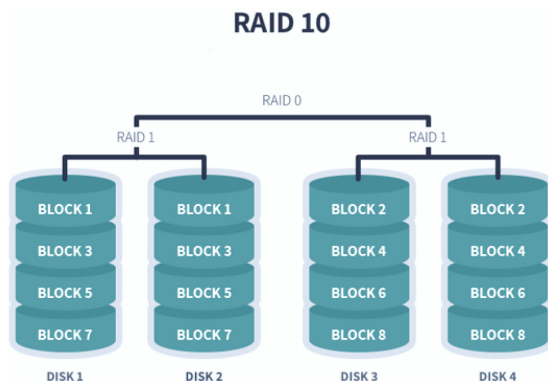


Рисунок 3.24 – Схема, що демонструє технологію Raid 10

Рішення було реалізоване через командні файли, які виконуються за розкладом з диспетчера завдань Windows на сервері SRV-MAIN. Проблема постала із кодом. Стандартна команда *сору* копіює весь об'єм інформації незважаючи на присутність у місці призначення ідентичних файлів. Можна визначити лише атрибут перезапису або пропуску файлу, якщо файл з таким ім'ям вже існує. Перезапис великих об'ємів даних

займає багато часу, завантажує мережу і зменшує ресурс жорстких дисків, тому не розглядався як варіант взагалі. Натомість, пропуск файлів з ідентичними іменами призводить до ситуації, коли в резервну копію потрапляють лише найперші версії документів, а, після внесення змін до оригіналу, нова версія документа не копіюється бо такий файл вже існує в дзеркальній теці. Більш функціональна команда *xcopy* хоч і має розширені можливості, але теж не може ідентифікувати різні за наповненням файли з однаковими іменами. Проблема була вирішена за допомогою *robocopy* – маловідома команда яка з'явилася як частина Windows Resource Kit серверної ОС Windows Server 2008 й інтегрована в подальші продукти Microsoft. Команда є розширеною версією *xcopy* і має потужний функціонал саме для резервного копіювання файлів та каталогів. Для реалізації резервного копіювання цілого мережевого ресурсу достатньо однієї строки:

```
robocopy "\\Srv-domain\C$\Документи викладачів"  
C:\Архів\Викладачі *.doc *.docx *.rtf *.xls *.xlsx *.pdf  
*.txt /E /Z /XA:H /XO /MAX:102400000 /R:3 /W:5 /MT:48 /LOG+:  
"C:\Tasks\Протоколи\Judges.log"
```

Команда перевіряє ідентичність вмісту оригінальної теки «\\Srv-domain\C\$\Документи викладачів» і її репліки «C:\Архів\Викладачі» зі всіма вкладеними файлами та теками (за наданим команді шаблоном *.doc *.docx... і т. ін.) й копіює лише нові або відредаговані файли в каталог дзеркала. Таким чином, досягається не лише резервне копіювання, коли із архіву можна завжди підняти найсвіжішу версію файлу – в теці репліки зберігається вся видалена з оригінальної теки інформація котра була знищена після реплікації. Тобто вилучена інформація загального ресурсу (якщо вона хоча б одного разу була реплікована) буде недоторканно зберігатися в теці репліки. Важливою особливістю *robocopy* є здатність працювати у кількох потоках. Далі надається опис використаних ключів:

/E – копіювати вкладені теки, навіть порожні;
/Z – дозволити продовжити копіювання при відновленні втраченого з'єднання з місця зупинки;
/XA:N – виключити з копіювання файли із атрибутом «hidden»;
/XO – не копіювати файл, якщо в теці репліки є більш свіжа версія;
/MAX:102400000 – максимальний розмір файлу, який підлягає реплікації в байтах;
/R:3 – кількість спроб скопіювати файл у разі помилки;
/W:5 – кількість секунд перед наступною спробою скопіювати файл у разі помилки;
/MT:48 – кількість потоків копіювання;
/Log+:»C:\Tasks\Протоколи\Judges.log» – додати журнал реплікації до вказаного файлу.

Більше інформації щодо ключів команди robocopy містить опис команди на сайті Microsoft [35]. Запуск командних файлів для реплікації загальних ресурсів було налаштовано на нічний час, коли ресурси ІТС максимально вільні.

Записи систем фіксації засідань копіюються у схожий спосіб, але протягом робочого часу – коли системи увімкнено. Всього було створено вісім задач (по кількості залів) розподілених у часі. Далі, як приклад, наведена команда, яка копією дані з системи, яка встановлена в залі №103:

```
robocopy \\Za1103\d$\CФC3\Записи "C:\Court Records\103"  
/E /Z /XO /R:3 /W:5 /MT:16 /LOG+:»C:\Tasks\Протоколи\103.log"
```

Команди для окремих залів або аудиторій виконуються послідовно з інтервалом у півгодини раз на добу, щоб зменшити вплив трансферу даних локальною мережею на робочій процес. Оскільки інформація містить не тільки текстову складову, але й аудіо- і відеозаписи онлайн засідань, її об'єм є суттєвим. Кожен викладач, здобувач або відповідальний за запис після входу в домен Windows, через групові політики, отримує мережевий диск, який посилається на загальний ресурс записів ОЗ на сервері. Користувачі мають права на читання інформації і не в змозі змінити або видалити

її. Отже, разом із механізмом резервного копіювання важливої інформації, користувачі отримують зручний і корисний сервіс для використання в роботі.

3.3. Антивірусний захист у домені Windows

Основні правила безпеки при роботі в інформаційній системі викладені в інструкціях користувача, адміністратора безпеки і системного адміністратора. Інструкції містять перелік заходів, виконання котрих значно зменшує ризик несанкціонованого доступу до службової інформації, її витоку, пошкодженню, тощо. Три перелічені документи є невід’ємною часткою нормативної бази комплексної системи захисту інформації, інструкції затверджуються наказом очільника установи и підлягають безумовному виконанню користувачами ІТС. Але, як загальновідомо, людський фактор є найбільш поширеною причиною зламу інформаційно-телекомунікаційних мереж. Для мінімізації впливу дій користувачів на безпеку середовища використовується антивірусне програмне забезпечення, яке в автоматичному режимі стежить за всіма процесами, які протікають на окремій складовій ІТС (комп’ютері / сервері) на всіх рівнях моделі OSI окрім фізичного. Існує досить багато розробників антивірусного програмного забезпечення. Навіть Microsoft розробила і інтегрувала в свої операційні системи антивірусний захист, який здійснює окрема складова операційної системи – Windows Defender. На жаль, зазначений антивірус задовільно працює лише на прикладному рівні, але роботи по вдосконаленню захисту ОС тривають і можна сподіватися, що згодом команда розробників Windows Defender наблизить якість свого ПЗ до якості продуктів своїх найближчих конкурентів – словацької компанії ESET та американської NortonLifeLock. Одними із найкращих продуктів в сфері підтримки безпеки інформаційно-телекомунікаційних систем є ESET Protect, який має позитивний експертний висновок

Державної служби спеціального зв'язку та захисту інформації України, що робить його одним з найкращих варіантів для впровадження при виборі системи організації безпеки в державній установі.

ESET Protect це клієнт-серверна система і це означає, що головний модуль ПЗ розгорнуто на сервері, а клієнтські додатки працюють на терміналах мережі і постійно підтримують зв'язок із сервером. Використання саме клієнт-серверних продуктів значно підвищує рівні керованості процесами і прозорості системи, заощаджує зовнішній трафік через локальні оновлення клієнтських баз антивірусного захисту і модулів захисту самих клієнтів.

У рамках реалізації технічного проєкту побудови ІТС в ДУ, було здійснено закупівлю ліцензійного ПЗ ESET Protect для забезпечення захисту інформаційної інфраструктури установи. В якості сервера безпеки було вирішено використовувати SRV-DOMAIN. З покроковою інструкцією з інсталяції і налаштування системи ESET Protect можна ознайомитися на офіційному сайті компанії ESET, де існує цілий розділ присвячений цій темі [36].

Для зберігання внутрішньої інформації Protect використовує систему керування базами даних Microsoft SQL Server або Oracle. Оскільки сервер баз даних Microsoft вже розгорнуто в установі для серверних модулів бухгалтерського ПЗ «IS Pro» й системи контролю доступу на об'єкт «STOP-Net 4», керування базою даних ESET Protect було реалізовано через Microsoft SQL Server.

З тієї причини, що адміністрування системи антивірусного захисту здійснюється через Web інтерфейс, інсталяційний пакет системи містить свій власний Apache сервер, який теж розгортається в ІТС.

Однією з найкорисніших функцій ESET Protect є інтеграція з доменом Windows. Protect знаходить об'єкти типу «комп'ютер» в активному каталозі і додає в свою базу даних.

Таким чином, зсередини консолі антивірусного захисту завжди можна отримати інформацію стосовно всіх складових

ІТС, які підлягають захисту, навіть якщо на них не встановлено клієнтське ПЗ – достатньо лише встановити агента.

Інсталяція клієнтських модулів (як і агента) виконується віддалено в автоматичному режимі, через консоль, без необхідності фізичного доступу до терміналів, після чого система готова до роботи.

ESET Protect надає безліч аналітичних даних щодо стану безпеки ІТС.

Загальну інформацію адміністратор отримує одразу після авторизації в консолі керування з панелі моніторингу, яка зображена на рис. 3.25 та рис. 3.26.

У даному випадку скріншоти панелі моніторингу демонструють загрозливу ситуацію із безпекою в ІТС.

Докладніше про причини загроз можна дізнатися з переліку меню «Комп'ютери», що наведено на рис. 3.27.

Обравши будь-який термінал, що потребує уваги адміністратора, можна отримати повну інформацію про нього і поради щодо усунення загрози. Зокрема, звідсіля також можна виконати певні дії із обраним терміналом або групою терміналів (див. рис. 3.28).

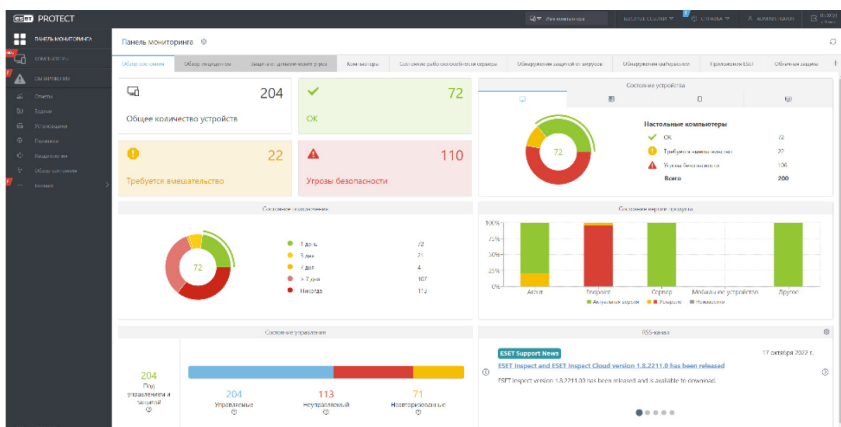
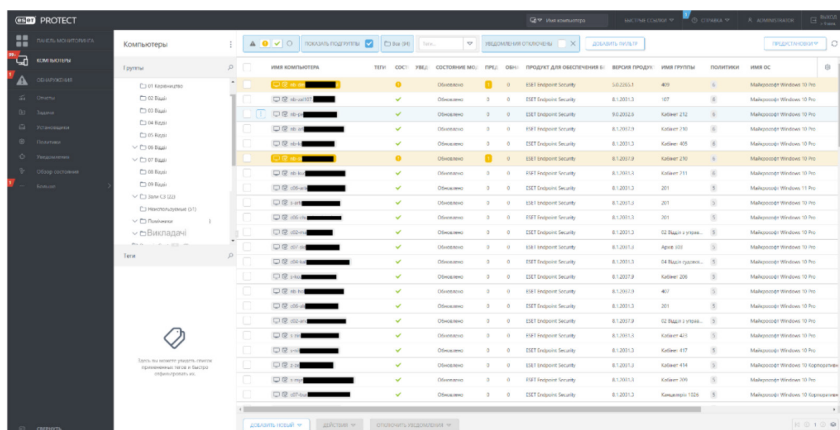
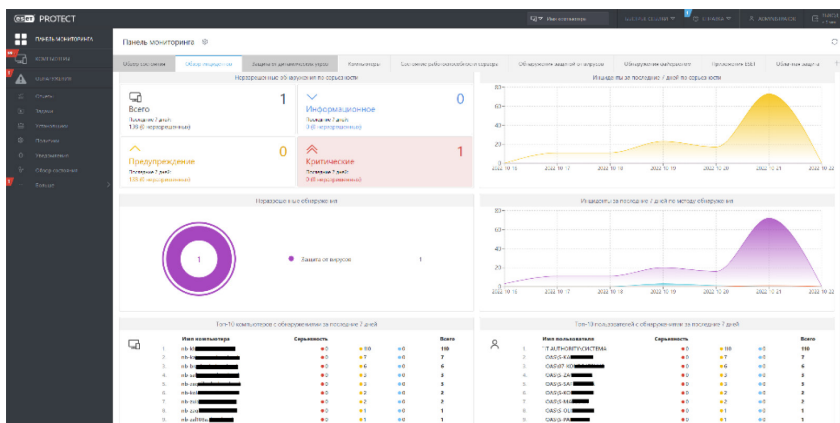


Рисунок 3.25 – Панель 1 моніторингу ESET Protect



Глобальний перелік виявлених загроз в розрізі всієї ІТС, або її окремого підрозділу (контейнера AD), теж можливо переглянути і проаналізувати (див. рис. 3.29).

Вбудовані звіти, а також можливість створити звіти користувачські, (див. рис. 3.30) допомагають більш щільно проаналізувати стан безпеки як ІТС в цілому, так і окремих її елементів.

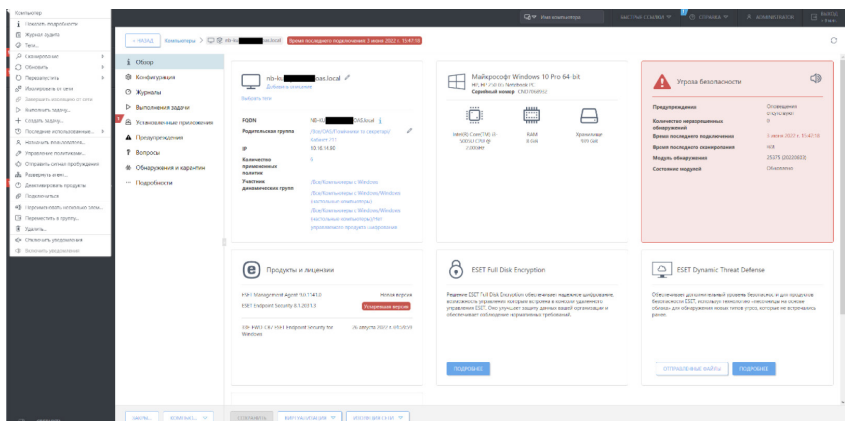


Рисунок 3.28 – Детальна інформація про термінал

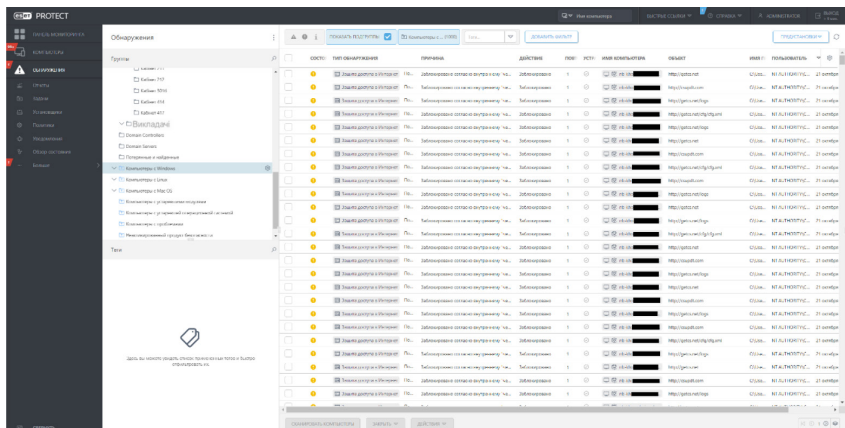


Рисунок 3.29 – Загальний перелік виявлених загроз

Слід підкреслити, що згідно пукну 6 і 7 Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 26.03.2007

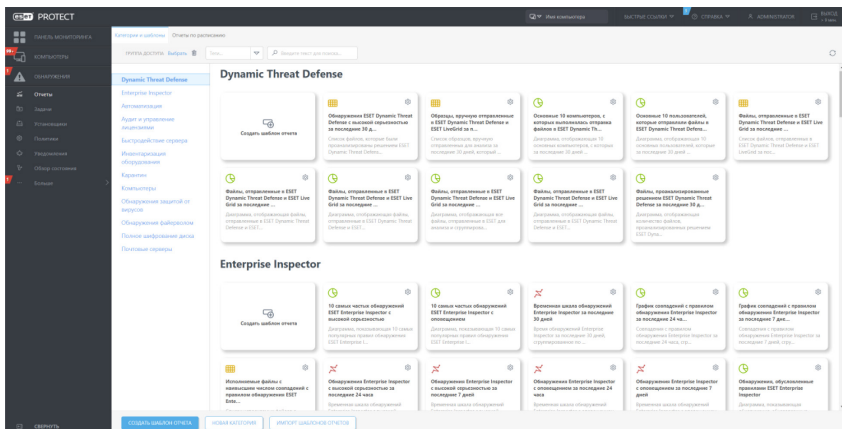


Рисунок 3.30 – Звіти ESET Protect

№ 45 [37] – оновлення АВПЗ (антивірусного програмного засобу) здійснюється шляхом організації та забезпечення процесу отримання та впровадження в АВПЗ антивірусних оновлень. Оновлення АВПЗ, який пройшов державну експертизу та має позитивний експертний висновок Адміністрації Державної служби спеціального зв'язку та захисту інформації України, здійснюється з використанням антивірусних оновлень, які розміщуються на веб-сайті www.cazi.dssz.gov.ua. Іншими словами, оновлення для серверних частин систем безпеки (які також містять оновлені бази даних вірусних сигнатур для клієнтів) дозволяється завантажувати лише з вказаного сайту, що є специфікою використання антивірусного програмного забезпечення в установах, які уповноважені на виконання функцій держави.

Після розгортання системи безпеки ESET Protect в ДУ, було відзначено, що система знешкоджує понад три тисячі зловмисних спроб втручання в роботу ІТС щомісяця. У разі відсутності такої інтегрованої системи, або її аналогів, ІТС установи неможливо вважати достатньо захищеною.

3.4. Сервіси обміну інформацією між користувачами

У сучасному світі неможливо уявити роботу будь-якого офісу без засобів миттєвого зв'язку, сповіщення та обміну інформацією серед користувачів чи груп користувачів. Найпростішими прикладами сервісів обміну є месенджери Viber, WhatsApp, Telegram та інші.

Використання кросплатформеного сервісу обміну дозволяє миттєво пересилати файли і повідомлення в офісному середовищі на будь-які пристрої – комп'ютери, планшети, мобільні телефони, інформаційні кіоски, інші термінали, які мають операційні системи і під'єднані до Інтернету. В державному секторі, використання вказаних як приклад месенджерів для передачі інформації володарем якої є держава – заборонене. Причина полягає не лише у відсутності сертифіката державної експертизи на ПЗ, але й в тому, що серверні частини цих месенджерів розташовані невідомо де. Тобто інформація, потенційно, може бути використана третіми особами. Але у разі коли сервер обміну розташовано в серверній кімнаті установи, а в якості платформи використовується така, що має відкритий код і вільну ліцензію, використання месенджеру стає можливим і є вкрай ефективним інструментом, що підвищує рівень комунікації в установі.

Після тривалого пошуку було знайдено два варіанти клієнт-серверних систем, які підпадають під окреслені умови: перший це сервер OpenFire і його клієнт Spark, і другий – RocketChat.

У ДУ було вирішено використовувати RocketChat. Сервер було розміщено на окремій віртуальній машині під керуванням операційної системи CentOS, клієнтське ПЗ RocketChat для ОС Windows було завантажено з сайту команди розробників (<https://www.rocket.chat>) а мобільні додатки легко інсталиються з Google Play для ОС Android та App Store для iOS / macOS.

Окрім обміну приватними повідомленнями RocketChat дозволяє створювати приватні або публічні групи, канали обговорення, надає можливість обміну файлами, підтримує

відеоконференцзв'язок, аудіострімінг, push-повідомлення (для економії трафіка мобільних клієнтів), має безліч безкоштовних плагінів для розширення функціоналу.

3.5. Virtual Private Network (VPN) під Hyper-V в домені Windows

Зазвичай, віддалений доступ до робочих місць державних установ не дозволено. Точніше, щоб реалізувати такий доступ установі треба пройти процедуру державної сертифікації програмного забезпечення і каналів зв'язку через які встановлюються віддаленні з'єднання із відомчою ІТС. Але у певних випадках, при настанні надзвичайних обставин, коли належне виконання функцій установи перевищує ризик інформаційної небезпеки, використання віддаленого доступу стає безвихідною необхідністю. При цьому, при використанні стороннього ПЗ з прихованим кодом або коли серверна частина знаходиться поза межами контрольованої установою зони – заборона зберігається. Такі програмні продукти як Ammyu Admin, TeamViewer, AnyDesk та аналогічні за своєю суттю рішення використовувати неможливо. Єдиним більш-менш прийнятним інструментом організації віддаленого доступу є механізм віртуальних приватних мереж або VPN. Оскільки необхідність у віддаленому доступі є засобом подолання форс мажорних обставин (які трапляються не лише раптово але й зрідка) та частково несе загрозу інформаційній безпеці, тримати такий сервіс в ІТС установи постійно розгорнутим немає сенсу. В такому разі, ідеальним за суттю рішенням є інсталяція сервера VPN на віртуальну машину, яку при необхідності можна активізувати, а у разі подолання форс мажорних обставин – знов вимкнути і тримати в такому стані на всяк випадок.

Більшість рекомендацій, щодо вибору VPN сервісу, стосуються OpenVPN сервера. Програмне забезпечення має відкритий код, вільну ліцензію, для нього розроблені інструкції з інсталяції

і налаштування. Все перелічене, а також дистрибутиви ПЗ, розташовано на офіційному сайті проєкту <https://openvpn.net>. До недоліків можна віднести відсутність графічного інтерфейсу безкоштовної версії, що вимагає від адміністратора роботи в консольному режимі, але й теоретично зменшує кількість задіяних ресурсів серверного обладнання. Натомість, існує менш відомий та більш зручний (і теоретично більш швидкий завдяки використанню нового протоколу) програмний продукт, який було розроблено на базі OpenVPN в національному університеті Цукуби (<https://www.tsukuba.ac.jp/english/>) в Японії – SoftEther VPN. На відміну від OpenVPN, SoftEther VPN має графічний інтерфейс і має механізм обходу файерволу (точніше його складової – NAT), тобто може використовуватися в ІТС, які не мають статичної зовнішньої IP-адреси. Для цього віртуальному хабові присвоюється субдоменне ім'я в домені softether.net через яке клієнти VPN мають змогу знайти цільовий сервер. Одночасно зберігається варіант з'єднання із сервером безпосередньо.

Для реалізації можливості віддаленого доступу (при настанні надзвичайних обставин) в ІТС ДУ було розгорнуто віртуальну машину VSRV-VPN під керування ОС Windows Server 2019 на гіпервізорі фізичного сервера SRV-BASE із реплікою на гіпервізор сервера SRV-DOMAIN (див. рис. 3.19). На зазначеній ВМ було встановлено і налаштовано сервер SoftEther VPN.

Процес налаштування серверу SoftEther VPN такий: через консоль керування SoftEther VPN (див. рис. 3.31) на сервері створюється віртуальних хаб (який об'єднує всіх користувачів VPN) та віртуальний брідж (див. рис. 3.32), який єднає між собою хаб віртуальної приватної мережі і внутрішню локальну мережу ДУ.

У налаштуваннях сервера визначаються порти, на яких SoftEther VPN прослуховує з'єднання зовні (див. рис. 3.31), встановлюються протоколи і методи шифрування (див. рис. 3.33).

Далі налаштовується віртуальний хаб, а точніше база динних віртуального хабу наповнюється інформацією про користувачів і методи їх авторизації (див. рис. 3.34).

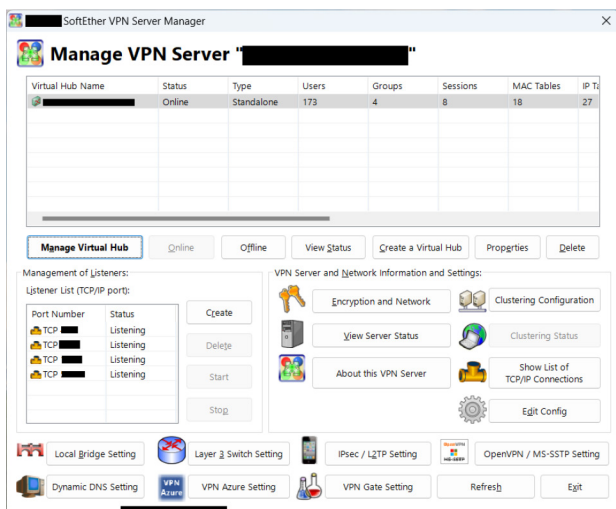


Рисунок 3.31 – Консоль керування сервером SoftEther VPN

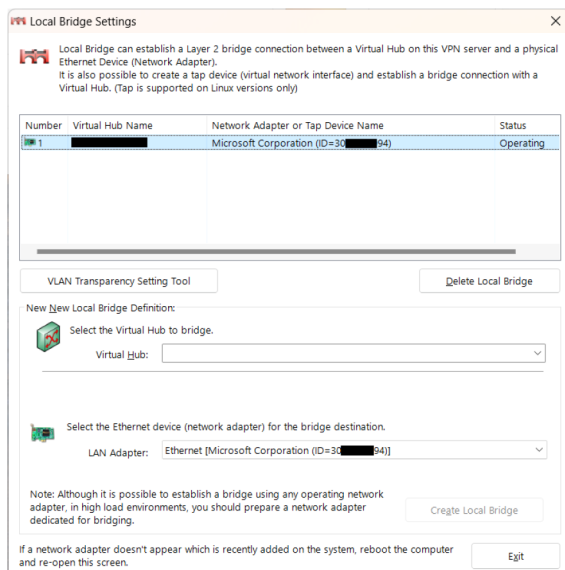


Рисунок 3.32 – Віртуальний бідж SoftEther VPN

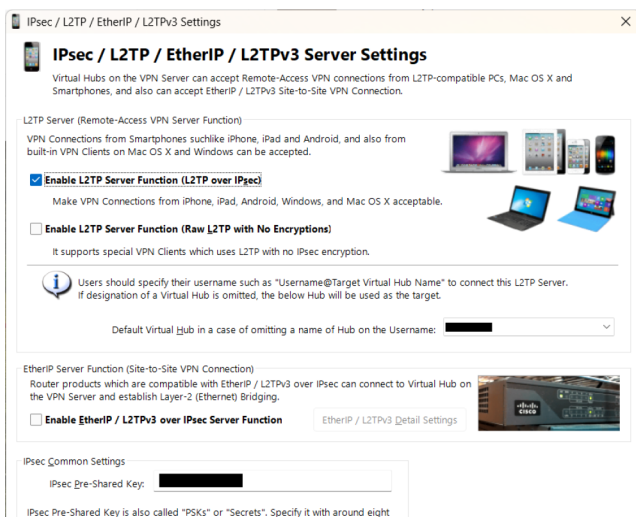


Рисунок 3.33 – Налаштування SoftEther VPN

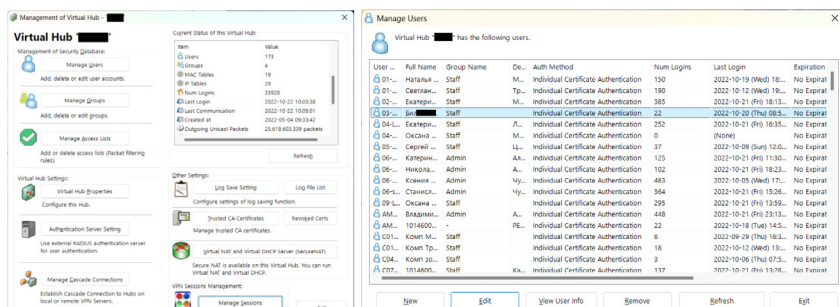


Рисунок 3.34 – Налаштування віртуального хабу і перелік користувачів

Слід прийняти до уваги, що самим надійним методом є авторизація по імені користувача, паролю і сертифікату одночасно. В такому разі, користувач ідентифікується відразу за трьома факторами і трафік між сервером VPN і клієнтським комп'ютером шифрується / дешифрується за допомогою відкритого і закритого ключів сертифіката. Лише у такий спосіб організації авторизації користувачів VPN з'єднання можна вважати досить безпечним для використання.

На комп'ютери користувачів встановлюються клієнти SoftEther VPN (див. рис. 3.35), в процесі чого в автоматичному режимі створюються віртуальні мережеві карти. Користувачам видаються логіни, паролі і закриті ключі шифрування.

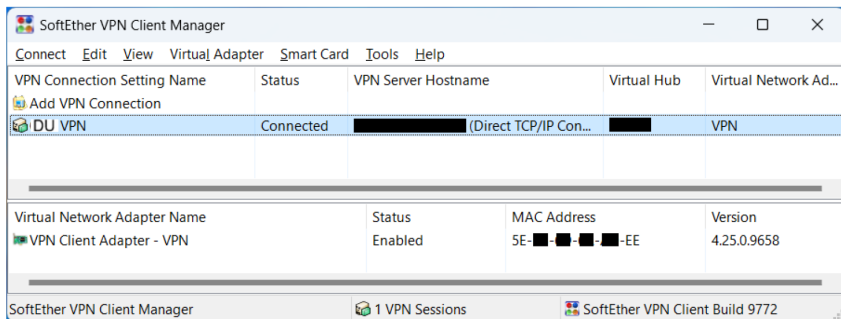


Рисунок 3.35 – Клієнт SoftEther VPN

На цьому етапі всі налаштування можна вважати завершеними. Після підключення до віртуальної приватної мережі користувач може працювати на підготовленому комп'ютері в ІТС установи з будь-якої точки світу так, нібито він знаходиться на робочому місці, але при умові, що його комп'ютер підключено до мережі Інтернет і швидкість з'єднання є достатньою. Всі сервіси ІТС працюватимуть, доменні політики будуть застосовані, специфічне ПЗ інстальоване, ресурси доступні. Але слід мати на увазі, що корисна пропускна здатність каналу при використанні протоколу L2TP поверх IPsec, завдяки шифруванню, падає приблизно навіпіл.

Адміністратор ІТС має засоби контролю за користувачами, трафіком, сесіями через журнали і вбудовані в консоль керування сервером SoftEther VPN інструменти (див. рис. 3.36).

У жодному разі (навіть при настанні надзвичайних обставин) до використання технології віртуальних приватних мереж слід ставитися обережно і розглядати її лише як спосіб збереження працездатності державного органу або установи під час нештатних ситуацій.

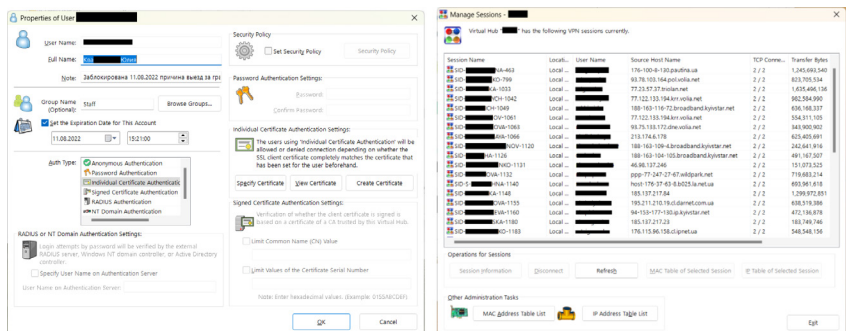


Рисунок 3.36 – Контроль користувачів та їхніх сесій в SoftEther VPN

3.6. Система охорони та контролю доступу до приміщення, система відеоспостереження

Особливістю розгортання ІТС в державній установі, на відміну від комерційної структури, є реалізація комплексної системи захисту інформації, одна із задач якої передбачає фізичну охорону і моніторинг контролюваної установою зони (надано в п. 2.1).

Для здійснення фізичного захисту інформації використовуються системи контролю доступу на територію установи, а для моніторингу – системи відеоспостереження. Вибір обладнання систем відеоспостереження не є принциповим питанням. Можна використовувати як цифрові IP-камери, так і аналогові пристрої, але, якщо вибір став за мережевими технологіями, по-перше слід впевнитися в достатній пропускну здатності мережі, по-друге мережа для відеоспостереження має бути фізично відокремлена від локальної мережі установи. Інакше зловмисник може легко отримати доступ до локальної мережі просто демонтувавши одну із камер й під'єднавши до крученої пари свій пристрій. Сервер відеоспостереження має бути розташований у захищеній серверній кімнаті, доступ до архіву записів має надаватися певним особам за наказом голови установи.

Система охорони і контролю доступу (надалі – СОКД) – це програмно-апаратний комплекс, який допомагає організувати безпечний контрольно-пропускний режим. В мінімальній конфігурації СОКД являє собою сервер обладнання, підключений до нього турнікет, два модуля зчитування ключів (на вході й виході), сервер СОКД і саме засоби підтвердження прав на перетин контрольованої зони (RF-ключі, карти, NFC-чіпи тощо). Тобто на центральному вході до установи встановлюється турнікет, пропуск через який здійснюється лише за наявності певного персонального ключа. Сервер обладнання передає всю інформацію стосовно перетину контрольованої зони серверові СОКД, який веде журнали входу / виходу й на основі них формує звіти про запізнення, не вихід на роботу, завчасне залишення робочого місця тощо.

У розширеному варіанті система додатково бере під охорону і контролює доступ до важливих об'єктів й приміщень. В такому разі до сервера обладнання єднуються магнітні замки і запори, датчики охоронної й пожежної сигналізації, блоки керування шлагбаумами, автоматичними воротами, ґратами, ролетами та інші спеціальні пристрої. У разі пожежі система самостійно відкриває аварійні виходи з будівлі, керує освітленням, сповіщає персонал про небезпеку. Перелік звітів розширеної системи доповнюється журналами доступу до критичних об'єктів, звітами про настання нештатних подій – пожежі, вимкнення електрики, спроб злочинного проникнення тощо.

Система може контролювати не лише персонал, а й відвідувачів за допомогою гостьових ключів для доступу до публічних зон – наприклад до залів ОЗ. Оскільки побудова КСЗІ, окрім переліченої в п.2.1 нормативної бази, вимагає ведення журналу відвідування установи іноземними та іншими делегаціями, то випуск гостьових ключів в разі спрощує контроль і ведення звітності.

ВДУ використовується система контролю доступу «STOP-Net 4», яка здійснює контроль доступу до приміщень не лише штатних працівників, але й відвідувачів. Без СОКД побудувати якісну

і дієву комплексну систему захисту інформації, в будь-якій установі, де кількість персоналу перевищує п'ятдесят осіб, практично неможливо.

Контрольні питання до розділу 3

1. Проаналізуйте основні підходи до побудови та налаштування мережі установи?
2. Які основні етапи треба врахувати при побудові домену Windows?
3. Які основні заходи щодо реалізації антивірусного захисту в домені Windows?
4. Чи є умови для використання сервісу обміну інформацією між користувачами в мережі установи?
5. Як реалізується віддалений доступ до робочих місць державних установ?
6. Що передбачає фізична охорона і моніторинг контрольованої установою зони як елемент комплексної системи захисту інформації?

4. ПРАКТИЧНІ РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ СИСТЕМИ

Після впровадження нової ІТС в досліджуваній установі швидкість процесів обробки інформації значно зросла. Завдяки новій топології мережі, кадри даних рухаються по оптимальних маршрутах, нові комутатори мають на порядок більші швидкісні характеристики щодо передачі даних клієнтським терміналам. Для аналізу ефективності нової мережі буде використано ту ж саму розроблену методику, яка дозволила виявити непрацездатність минулої.

4.1. Розрахунок навантаження та аналіз ефективності спроєктованої мережі

Оскільки функції і задачі установи після модернізації ІТС не змінилися, у нових контрольних замірах трафіку у розрізі ПЗ немає сенсу – можна користуватися результатами минулого дослідження, які перелічено у *Додатку Г* й *Додатку Е* і, вочевидь, загальне навантаження буде те саме:

$$V_{nw} = 25,53 \text{ (Mb/s)}.$$

Натомість максимальна теоретична швидкість проходження пакетів між двома клієнтами змінилася завдяки реалізованому стандарту Gigabit Ethernet 1000BASE-T (або IEEE 802.3ab) якому підпорядковуються з'єднання клієнтських терміналів до комутаторів. Новий стандарт для передачі кадрів використовує всі чотири кручені пари кабелю п'ятої категорії. Кожна пара має заявлену швидкість передачі інформації в обох напрямках

250 Мбіт/с, отже чотири пари можуть здійснити передачу пакетів зі швидкістю 1000 Мбіт/с.

Gigabit Ethernet працює на базі того ж самого протоколу передачі MAC CSMA/CD як і Fast Ethernet, де максимальна і мінімальна довжина кадру була збережена з міркувань сумісності протоколів, але час передачі було скорочено рівно у десять разів. Тобто, з урахуванням зростання швидкості трансляції кадрів на порядок, всі попередні розрахунки можна вважати вірними за умови збільшення кінцевих результатів в десять разів:

$$C_{\min} = 65,3 \text{ Мб/с.}$$

$$C_{\max} = 116,3 \text{ Мб/с.}$$

Тоді середня швидкість передачі даних в мережі Gigabit Ethernet становить:

$$C_{\text{avg}} = (C_{\min} + C_{\max})/2 = 90,8 \text{ Мб/с.}$$

І можна, нарешті, обчислити коефіцієнт використання мережі:

$$P = \frac{Vnw}{C_{\text{avg}}} = \frac{25,53}{90,8} = 0,281.$$

Пам'ятаємо, що графік на рис. 1.3 демонструє поріг після якого поведінка мережі істотно змінюється в гіршу сторону, і який для всього сімейства Ethernet полягає між значенням 0,4 та 0,5. Модернізована ІТС має коефіцієнт використання мережі 0,281, що є показником задовільної роботи мережі.

4.2. Оновлення ПЗ

До того, як ІТС установи була модернізована, оновлення спеціалізованого програмного забезпечення здійснювалося вручну на кожному терміналі. В свою чергу, оновлення

операційних систем клієнтських терміналів взагалі не підлягало контролю. Побудова домену під керуванням Windows Server створило умови для централізованого керування процесом оновлення ПЗ і ОС.

Розповсюдження оновлень спеціалізованого програмного забезпечення здійснюється двома шляхами – через спільні мережеві ресурси та за допомогою групових політик. Встановлення (оновлення) ПЗ через механізм GPO дозволяє підтримувати більшість офісних додатків в актуальному стані. Обмеження стосуються методів пакування інсталяційних пакетів. Для оновлення через GPO цільове ПЗ має являти собою пакет Windows Installer, тобто файл *.msi готовий до розгортання. Нажаль, не всі виробники ПЗ компілюють інсталяційні пакети в потрібний формат.

За даною схемою [38], інсталяція або оновлення ПЗ здійснюється автоматично в момент вмикання комп'ютера або в інтервалі до 120 хвилин, при умові, що комп'ютер було увімкнено раніше ніж була створена відповідна політика. Інтервал 90 ± 30 хвилин обумовлений часом за замовченням, який встановлено на перевірку актуальності об'єктів GPO для клієнтських терміналів. При цьому, звичайно, рядовий користувач не має права на видалення або оновлення встановленого таким чином ПЗ.

Другий варіант має на увазі завантаження інсталяційного пакету на мережевий ресурс загального користування і виконання скриптів засобами GPO для його масового встановлення. Обидва варіанти доповнюють один одного і можуть використовуватися одночасно. Зокрема в досліджуваній установі, оновлення КП ДВ, через відсутність *.msi пакету, було реалізовано за другим варіантом, в той час коли все інше ПЗ оновлюється за першим.

Модернізація ІТС вплинула не лише на процес оновлення ПЗ, але й на оновлення ОС. До втілення інновацій кожен комп'ютер отримував власний пакет оновлень з серверів Microsoft через

Інтернет, що призводило до марного витрачання перепускної здатності зовнішнього каналу, коли більш ніж 200 клієнтських комп'ютерів завантажували одне й теж саме оновлення операційної системи Windows. Після побудови домену в мережі було налаштовано централізований локальний сервіс оновлення Windows Server Update Services (Надалі – WSUS) – який за фактом є серверною роллю Windows Server. WSUS є єдиним центром оновлень Windows в установі. Служби WSUS дозволяють розгортати чи відкладати оновлення ОС, забезпечують часткове оновлення, окреслення кола пристроїв для розгортання оновлень, визначають час доставки оновлень. Також служби WSUS є інструментом контролю над клієнтським компонентом «Центр оновлення Windows».

Процес впровадження сервісу централізованих оновлень розпочинається із встановлення ролі WSUS на одному із серверів домену. У випадку досліджуваної установи для розгортання ролі WSUS було обрано SRV-MAIN з огляду на його наявний найбільший за об'ємом масив носіїв інформації для зберігання пулу оновлень. Для здійснення керуванням оновленнями клієнтських Windows в об'єкті GPO «DU Users» були визначені параметри «Налаштування автоматичних оновлень» і «Розташування служби оновлень Microsoft в інтрамережі». Після чого, окреслені клієнти замість серверів Microsoft почали звертатися до сервера SRV-MAIN для отримання оновлень ОС. Детально процес налаштування WSUS описано у статті [39] «Розгортання оновлень клієнта Windows за допомогою служб Windows Server Update Services (WSUS)». Завдяки впровадженню сервісу централізованих оновлень, навантаження на зовнішні канали значно скоротилося. Хоча контрольні заміри витрат трафіку на оновлення не проводилися, можна впевнено стверджувати, що зовнішній трафік, пов'язаний із оновленнями ОС, було зменшено в 225 разів – саме стільки клієнтських терміналів використовується в роботі установи.

4.3. Обслуговування ІТС

Розгорнута, як практичний результат проведеної роботи, ІТС потребує поточного обслуговування, яке, у більшості випадків, зводиться до моніторингу роботи певних складових системи.

З боку активного мережевого обладнання: комутаторів на предмет відсутності петель, маршрутизатора на предмет відсутності несанкціонованого доступу до ІТС з боку злоумисників. Моніторинг здійснюється шляхом перегляду *.log файлів пристроїв, переліку активних з'єднань маршрутизатора, тощо.

З боку серверного обладнання, до методів контролю працездатності входять перегляд файлів системних журналів Windows Server та дослідження інформації з вбудованих сервісів контролю працездатності серверів, таких як Integrated Dell Remote Access Controller для серверного обладнання Dell та Integrated Lights Out для Hewlett-Packard.

З боку програмної складової, більшість аналітичної інформації надходить від серверу антивірусного захисту, локальних системних журналів комп'ютерів мережі.

У разі виявлення будь-яких проблем стосовно функціонування ІТС, адміністратор ІТС має негайно вжити заходи щодо усунення причин і наслідків позаштатної ситуації, керуючись рекомендаціями, нормативною базою, інструкціями які згадуються у п. 2.1 «Комплексна система захисту інформації (КСЗІ) в установі» даної роботи.

4.4. Контроль наявності та переміщення техніки в межах установи

Як правило, облік матеріальних цінностей державних установ здійснюється фахівцями відділів бухгалтерського обліку та фінансових ресурсів, окремими структурними підрозділами матеріально-технічного забезпечення, регіональними органами

і територіальними галузевими управліннями. Оскільки вартість інформаційно-телекомунікаційної інфраструктури кожної установи є доволі високою, а інформацією про точки інсталяції специфічного обладнання володіють насамперед співробітники відділів інформаційних технологій, до складу інвентаризаційних комісій майже завжди включають фахівців ІТ-відділів. В залежності від умов і рівня здійснення постійного контролю за переміщенням технічних засобів, щорічна інвентаризація може тривати як декілька годин, так і декілька тижнів. Питання організації ефективного контролю за складовими ІТС детермінує часові витрати фахівців інформаційних відділів на фінансово-господарські напрямки роботи. Іншими словами, чим більше часу адміністратор ІТС витрачає на пошук обладнання, тим менше його залишається на обслуговування, моніторинг та вдосконалення ІТС. З метою заощадження і мінімізації часових втрат на інвентаризаційні заходи, було розроблено і інтегровано в ІТС ДУ ефективну систему з контролю розташування складових системи.

Насамперед, місцезнаходження кожного комп'ютера, сервера, друкарського пристрою можна визначити за його місцезнаходженням в контейнері Active Directory. Відразу після приєднання до домену, полю «Опис» кожного комп'ютерного термінала надається значення його інвентарного номера (див. рис. 3.12). Мережеві імена багатофункціональних друкарських пристроїв теж формуються з найменування моделі БФП і інвентарного номеру (див. рис. 3.17). Оскільки перелік ПЗ, мережеві ресурси, під'єднані БФП в ІТС ДУ регулюються лише через активний каталог, фізичне переміщення комп'ютерної техніки без віртуального переміщення між контейнерами AD не має сенсу – користувач, який самостійно перемістив техніку, не отримає необхідних на новій локації сервісів, в той же час, адміністратор, який здійснив фізичне переміщення технічних засобів без віртуальних рухів, незабаром отримає звернення від користувача щодо недоступності необхідних для роботи ресурсів. Таким чином, здійснюється не лише автоматичне налаштування певних конфігурацій обладнання, але

й діє подвійний контроль за переміщенням терміналів і БФП – з боку адміністраторів і з боку користувачів.

Для посилення цього контролю та з метою пошуку «втрачених» терміналів було розроблено скрипт контролю авторизації користувачів, який надано у Додатку К. Скрипт інтегровано в GPO і пов'язано із подією User Logon, тобто він виконується кожного разу коли користувач здійснює вхід під своїми обліковими даними з будь-якої точки входу ІТС. Детально про налаштування виконання скриптів через групові політики викладено в статті «Using Startup, Shutdown, Logon, and Logoff Scripts in Group Policy» [40].

У процесі авторизації скрипт зберігає ПІБ користувача,

```
$user = $env:USERNAME;
```

найменування терміналу входу,

```
$computer = $env:COMPUTERNAME;
```

дату і час входу,

```
$time = [datetime]::Now;
```

шукає об'єкт користувача в активному каталозі та, у поле «опис» об'єкта AD користувача, записує мережеве ім'я терміналу з якого було здійснено вхід, а також дату і час входу:

```
$string = "$computer at $time";  
$Searcher = New-Object DirectoryServices.DirectorySearcher;  
$Searcher.SearchRoot = "LDAP://DC=DU,DC=local";  
$Searcher.SearchScope = 2;  
$Searcher.Filter = "(&(objectCategory=person)(objectClass=user)(SamAccountName=$user))";  
$objUser = [adsisearcher]$Searcher.FindOne().Path;  
$objUser.Put("Description",$string);  
$objUser.SetInfo();
```

Результат роботи цієї частини програмного коду можна побачити на рис. 3.12, де кожен з об'єктів типу «користувач» в полі «опис» має збережені дані щодо найменування терміналу

авторизації й дати / часу входу. Натомість, поле «опис» об'єкту типу «комп'ютер» в активному каталозі вже зберігає його інвентарний номер, тому перезапис в це поле (щодо можливих даних користувача, який здійснив вхід) не виконується. Але, з метою пошуку терміналів які були «втрачені» а також відключені, списані, знаходяться в сервісі або в процесі обслуговування, і які з перелічених вище причин зберігаються в контейнері вищого рівня активного каталогу «Незадіяні» (і лише в ньому!), виконується наступна частина програмного коду скрипта:

```
$string = "$user at $time";  
$Searcher = New-Object DirectoryServices.DirectorySearcher;  
$Searcher.SearchRoot = "LDAP://OU= Незадіяні, OU=DU, DC=DU, DC=local";  
$Searcher.SearchScope = 1;  
$Searcher.Filter = "(&(objectCategory=computer)(name=$computer))";  
$objComp = [adsisearcher]$Searcher.FindOne().Path;  
  
if (-not ([string]::IsNullOrEmpty($objComp)))  
{  
    $objComp.Put("Description",$string);  
    $objComp.SetInfo();  
}
```

Результатом виконання цього скрипту є запис в поле «опис» об'єктів типу «комп'ютер» інформації щодо користувача, який здійснив вхід і час його логіну.

Я результат вжитих заходів, за допомогою вбудованого в серверну систему Windows Server 2019 інструменту «Центр адміністрування Active Directory» (який має функціонал глобального пошуку серед об'єктів активного каталогу) пошук місцезнаходження будь-яких складових ІТС виконується миттєво і точно.

Наприклад, на рис. 4.1 можна побачити результати пошуку клієнтського ноутбука, закріпленого за користувачем, чие прізвище починається на літеру «Б».

Продемонстровані результати містять інвентарні номери всіх пристроїв і їх місцезнаходження в активному каталозі, яке

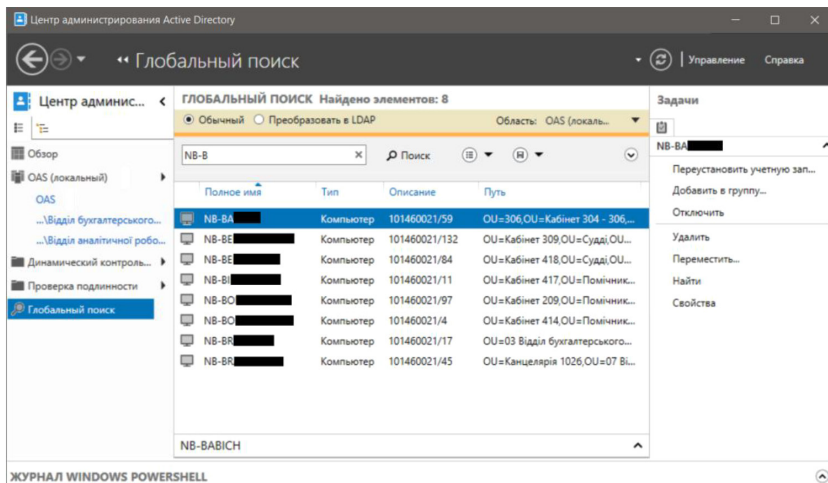


Рисунок 4.1 – Приклад пошуку ноутбуків в активному каталозі

відображає їх фізичне розташування і належність до структурного підрозділу.

Другий приклад пошуку на рис. 4.2 демонструє результати пошуку користувача, чиє прізвище починається на «Аме».

З результатів можна побачити, що в останнє користувач Володимир Амелін входив до ІТС ДУ 29 жовтня 2022 року о 23:47 через віртуальний сервер VSRV-DU. Користувач належить до відділу

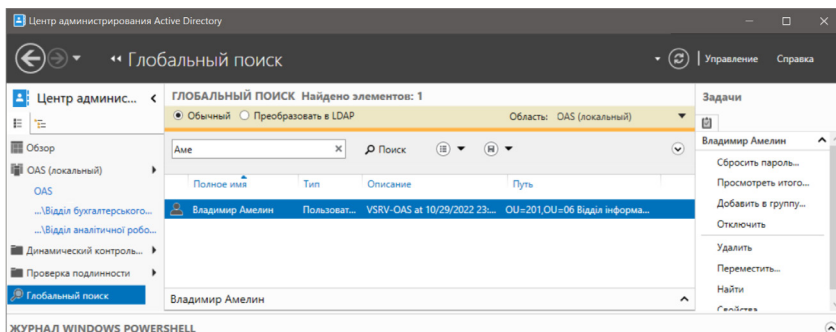


Рисунок 4.2 – Приклад пошуку користувача в активному каталозі

інформаційних технологій та технічних засобів, і має робоче місце в кабінеті № 201.

Введення описаних вище заходів дозволило скоротити час, який фахівці відділу ІТ (у складі комісії) витрачали на проведення щорічної інвентаризації, з одного тижня до одного робочого дня.

Контрольні питання до розділу 4

1. З якою метою робиться розрахунок навантаження та аналіз ефективності спроектованої мережі?
2. Що передбачає поточне обслуговування інформаційно-телекомунікаційної системи установи?
3. У який спосіб можливо реалізувати контроль наявності та розміщення техніки в межах установи?

ВИСНОВКИ

Мета наведеної роботи полягає у побудові *працездатної і ефективної, здатної до масштабування, гнучкої, керованої, прозорої, надійної й самостійної* інформаційно-телекомунікаційної системи на прикладі вищого навчального закладу на базі її діючої, але незадовільно працюючої ІТС.

Для планування модернізації було проаналізовано характеристики задіяного в робочому процесі обладнання, розглянуто план будівлі і комунікацій, проведено дослідження законодавчої і нормативної бази, здійснено розрахунок ефективності існуючої ІТС. На основі переліченого, було зроблено остаточний висновок про цілком незадовільну роботу системи і висунуто вимоги до нової системи, сформовано концепцію, розроблено технічне завдання і ескізний проєкт, який згодом перетворився на технічний проєкт нової, модернізованої ІТС.

У процесі розгортання спроектованої системи було перебудовано топологію локальної мережі, збільшено кількість внутрішніх магістральних каналів і зовнішніх каналів Інтернет, переналаштовано маршрутизатор R1 на виконання функцій керування трафіком і зовнішніми каналами. Паралельно здійснено закупівлю необхідного обладнання, згідно технічного проєкту і в рамках діючого законодавства України, й організовано безпребійне живлення серверної інфраструктури.

На прикладному рівні побудовано домен під управлінням Windows Server для загального управління та адміністрування ІТС, всі мережеві імена пристрів ІТС і логіни користувачів переназначено згідно логіки розробленої системи, створено і узгоджено план IP-адресації, розгорнуто централізований антивірусний захист на базі клієнт-серверної системи ESET Protect, оновлення

клієнтських операційних систем задіяно через локальну службу оновлення Windows, інстальовано сервер обміну службовою інформацією RocketChat, облік матеріально-технічних засобів інтегровано в активний каталог, налаштовано сервер друку, який взяв на себе керування всіма друкарськими пристроями зареєстрованими в ІТС, а сервіс WDS і задачі резервного копіювання разом із використанням технології Raid-10 забезпечили надлишковість процесів обробки і зберігання інформації.

Для забезпечення роботи установи в надзвичайному режимі було розгорнуто сервер віртуальної приватної мережі для віддаленого доступу працівників установи до всіх ресурсів ІТС.

Також розроблена нормативно-документальна база для побудови комплексної системи захисту інформації, що є останнім кроком на шляху до створення еталонної інформаційно-телекомунікаційної системи установи будь-якої форми власності й підпорядкування.

Підсумковий розрахунок ефективності ІТС дає змогу зробити висновок, що побудована система *ефективна і працездатна*. Вона має запас для *масштабування* без будь-якого доопрацювання, більш того, в модернізовану ІТС закладена можливість збільшення кількості магістральних каналів, або навіть перехід на нові стандарти / протоколи передачі даних магістральними каналами зв'язку у разі потреби (після заміни кореневого комутатора К0 на більш сучасний), що робить систему ще більш *гнучкою*. Керування системою можливе з будь-якої точки входу, включаючи віддалені робочі місця приєднані через VPN. Адміністраторам ІТС, за допомогою вбудованих в доменну структуру інструментів і механізмів, надано майже безмежні можливості для вдосконалення і підвищення ефективності ІТС. Журнали мережевого і серверного обладнання, а також спеціальні скрипти інтегровані через GPO організують *прозору* роботу системи з можливістю виявити будь-які відхилення або загрози у її роботі. Завдяки безперебійному живленню серверів і активного мережевого обладнання, резервному копіюванню інформації, а також

через те, що для забезпечення зв'язку із зовнішнім світом використовуються три незалежні канали, систему можна вважати *надійною* і такою, що не залежить від зовнішніх факторів окрім форс мажорних обставин.

ІТС була спроектована і побудована таким чином, щоб зменшити долю участі адміністративного персоналу в процесах налаштувань клієнтських робочих місць, а також оновленні і підтримці працездатності терміналів. Наразі система *самостійно* розгортає потрібні для виконання службових обов'язків ресурси для певного користувача або певного термінала через групові політики, здійснює контроль переміщень обладнання і веде облік дій користувачів і ПЗ, мінімізуючи участь фахівців ІТ у згаданих вище процесах.

Отже робиться висновок, що всі цілі, які було окреслено на початку роботи над проектом з розробки ІТС установи, було досягнуто і реалізовано на практиці.

ЛІТЕРАТУРНІ ДЖЕРЕЛА

1. Про Національну програму інформатизації : Закон України : станов на 01.01.2021р. URL <https://zakon.rada.gov.ua/laws/show/74/98-вр#Text>

2. Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади: Указ Президента України від 14 лип. 2000р. № 887/2000. URL: <https://zakon.rada.gov.ua/laws/show/887/2000#Text>

3. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації : розпорядження Кабінету міністрів України від 17 січ. 2018 р. № 67-р. <https://zakon.rada.gov.ua/laws/show/67-2018-р#Text>

4. Про затвердження завдань Національної програми інформатизації на 2022–2024 роки : постанова Верховної Ради України від 08 липня 2022 р. №2360-IX. <https://zakon.rada.gov.ua/laws/show/2360-20#Text>

5. Амелін В. П., Суботін О. В. Особливості створення інформаційно-телекомунікаційної системи державної установи. *Важке машинобудування. Проблеми та перспективи розвитку* : матеріали XX Міжнародної науково-технічної конференції 01–03 вересня 2022 року / за заг. ред. В. Д. Ковальова. Краматорськ-Тернопіль : ДДМА, 2022. С. 216–217. ISBN 978-617-7889-20-4

6. Суботін О. В., Новіков Д. С. Особливості створення комплексної інформаційної системи управління підприємством. International scientific conference “MININGMETALTECH 2024 – The mining and metals sector: integration of business, technology and education”: conference proceedings (November 28–29, 2024, Riga, the Republic of Latvia). Riga, Latvia : Baltija Publishing, 2024. Vol. 1. Pp. 356–360. DOI <https://doi.org/10.30525/978-9934-26-506-8-119>.

7. Суботін О., Новіков Д. Особливості модернізації інформаційних мереж. *Стан, досягнення і перспективи інформаційних систем і технологій* : матеріали XXV Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 17–18 квітня 2025 р. Одеса, Видавництво ОНТУ, 2025 р. С. 53–55. https://ontu.edu.ua/download/konfi/2025/Conference_abstract-IT-2025.pdf

8. Суботін О. В., Петрухін Я. І. Особливості вибору технічних засобів інформаційної мережі. *Research in Science, Technology and Economics* : Collection of Scientific Papers “International Scientific Unity” with Proceedings of the 2nd International Scientific and Practical Conference. March 5–7, 2025. Luxembourg, Luxembourg. 68–71 p. DOI: <https://doi.org/10.70286/isu-05.03.2025>) – Режим доступу: <https://isu-conference.com/en/archive/research-in-science-technology-and-economics-5-03-25>

9. Суботін О. В., Новіков Д. С., Петрухін Я. І. Особливості розрахунку поточних характеристик інформаційної мережі. *The Importance of Innovation for the Modern World* ‘2025 : conference proceedings. June 20, 2025. Karlsruhe, Germany. 24–31 p. DOI: <https://doi.org/10.30890/2709-1783.2025-39-00>. URL: <https://www.proconference.org/index.php/gec/issue/view/gec39-00/gec39-00>

10. Мережі Ethernet й Fast Ethernet. *UA5.org*. URL: <https://ua5.org/lan/136-merezh-ethernet-jj-fast-ethernet.html>

11. Router on a stick. *Вікіпедія вільна енциклопедія*. URL: https://en.wikipedia.org/wiki/Router_on_a_stick

12. Суботін О. В., Новіков Д. С. Особливості розгортання комплексної системи захисту інформації в установі. *Важке машинобудування. Проблеми та перспективи розвитку* : матеріали XXII Міжнародної науково-технічної конференції 28–30 травня 2024 року / за заг. ред. В. Д. Ковальова. Краматорськ-Тернопіль : ДДМА, 2024. С.175–177.

13. Закон 4336-IX: що змінюється для держустанов і критичної інфраструктури та як до цього готуватися бізнесу. *Журнал NV*. URL: <https://biz.nv.ua>

14. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України : станом на 27.03.2025 р. URL: <https://zakon.rada.gov.ua/laws/show/4336-20#Text>

15. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем: постанова Верховної Ради України від 18 червня.2025 р. № 712. URL: <https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text>

16. Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації : постанова Верховної Ради України від 21 лютого.2025 р. № 205. URL: <https://zakon.rada.gov.ua/laws/show/205-2025-%D0%BF#Text>

17. Новий закон про захист персональних даних в Україні: що очікувати. *Журнал BSO privacy group*. URL: <https://bsoprivacygroup.com>

18. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : постанова Кабінету Міністрів України від 29 березня 2006 р. № 373. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-п#Text>

19. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію : постанова Кабінету Міністрів України від 19 жовтня 2016 р. № 736. URL: <https://zakon.rada.gov.ua/laws/show/736-2016-п#Text>

20. Засоби ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації : Державна служба спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi>

21. Поради (рекомендації) щодо створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет : Державна служба спеціального зв'язку та захисту

інформації України. URL: <https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorenniya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet>

22. Про відновлення дії національного та міждержавних стандартів: наказ Державного підприємства «Український науково-дослідницький і навчальний центр проблем стандартизації, сертифікації та якості» від 29 груд. 2018р. № 546 : Аналітично-правова система ZakonOnline. URL: https://zakononline.com.ua/documents/show/46274__46274

23. ГОСТ 34.601-90. Інформаційна технологія. Комплекс стандартів на автоматизовані системи. Автоматизовані системи. Стадії створення : затв. постановою від 29.12.1990 р. № 3469. URL : http://online.budstandart.com.ua/catalog/doc-page.html?id_doc=53626

24. Недашківський О. Л. Планування та проектування інформаційних систем / О. Л. Недашківський., 2014. 215 с.

25. Про затвердження Інструкції щодо застосування економічної класифікації видатків бюджету та Інструкції щодо застосування класифікації кредитування бюджету : наказ Міністерства Фінансів України від 12 березня 2012 р. № 333. URL: <https://zakon.rada.gov.ua/laws/show/z0456-12#Text>

26. Про публічні закупівлі : Закон України : станом на 16.08.2022 р. URL: <https://zakon.rada.gov.ua/laws/show/922-19#Text>

27. Єдиний закупівельний словник ДК 021:2015. URL: <https://dk21.dovidnyk.info>

28. Мантула М. В., Суботін О. В., Періг О. В. Удосконалення корпоративної мережі підприємства з метою підвищення ефективності роботи. *Сучасні інформаційні технології, засоби автоматизації та електропривод* : матеріали IX Всеукраїнської науково-практичної конференції, 17–19 квітня 2025 року / За заг. ред. О. Ф. Тарасова. Краматорськ-Тернопіль : ДДМА, 2025. С. 81–84. URL: <http://cit.dgma.donetsk.ua/materials.html>

29. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших

матеріальних носіїв інформації, що містять службову інформацію : постанова Кабінету Міністрів України від 19 жовт. 2016 р. № 736. URL: <https://zakon.rada.gov.ua/laws/show/736-2016-п#Text>

30. How To Install Windows Server 2019 Step by Step. URL: <https://computingforgeeks.com/install-windows-server-2019/>

31. Install Active Directory Domain Services in Windows Server 2019. URL: <https://computingforgeeks.com/how-to-install-active-directory-domain-services-in-windows-server/>

32. Windows Server: Installing roles and features in different ways. URL: <https://social.technet.microsoft.com/wiki/contents/articles/52780.windows-server-installing-roles-and-features-in-different-ways.aspx>

33. Windows Server 2019: Installation and Initial Configuration : *Сервіс відеохостингу YouTube*. URL: <https://www.youtube.com/watch?v=k3fZjVOIXnA>

34. How to Install and Configure a Print Server in Windows Server 2019. URL: <https://www.networkinglearning.com/2022/04/how-to-install-and-configure-print.html>

35. Robocopy : *Офіційний сайт корпорації Microsoft*. URL: <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/robocopy>

36. Install the ESET PROTECT Server : *Офіційний сайт компанії ESET*. URL: https://help.eset.com/protect_install/80/en-US/step_by_step.html

37. Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 26 березня 2007 р. № 45. *Сайт Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/z0320-07#Text>

38. Використання групової політики для віддаленого встановлення програмного забезпечення : *Офіційний сайт корпорації Microsoft*. URL: <https://learn.microsoft.com/ru-ru/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software>

39. Розгортання оновлень клієнта Windows за допомогою служб Windows Server Update Services (WSUS) : *Офіційний сайт корпорації Microsoft*. URL: <https://learn.microsoft.com/ru-ru/windows/deployment/update/waas-manage-updates-wsus>

40. Using Startup, Shutdown, Logon, and Logoff Scripts in Group Policy : *Офіційний сайт корпорації Microsoft*. URL: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn789196\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn789196(v=ws.11))

ДОДАТКИ

Додаток А Структура та штатна чисельність установи

	Назва структурного підрозділу та посад	Кількість штатних одиниць
1	Професорсько-викладацький склад	167
1.1	Ректорат	3
1.2	Факультет інформаційних технологій (кафедри, деканат)	68
1.3	Технічний факультет (кафедри, деканат)	54
1.4	Економічний факультет (кафедри, деканат)	42
2	Відділи та служби	59
2.1	Відділ бухгалтерського обліку та фінансових ресурсів	6
	Начальник відділу	1
	Заступник начальника відділу	1
	Головний спеціаліст	4
2.2	Відділ контролю якості	3
	Начальник відділу	1
	Заступник начальника відділу	1
	Головний спеціаліст	1
2.3	Відділ з управління персоналом	5
	Начальник відділу	1
	Заступник начальника відділу	1
	Головний спеціаліст	3
2.4	Відділ контролю за використанням державного майна	9
	Начальник відділу	1
	Заступник начальника відділу	1
	Головний спеціаліст	1

Продовження додатка А

	Назва структурного підрозділу та посад	Кількість штатних одиниць
	Провідний спеціаліст	1
	Провідний консультант	1
	Водій автотранспортних засобів	2
	Робітник з комплексного обслуговування й ремонту будинків	2
	Прибиральник службових приміщень	5
2.5	Відділ документообігу та архівної роботи	16
	Начальник відділу	1
	Заступник начальника відділу	1
	Головний спеціаліст	5
	Провідний спеціаліст	3
	Провідний консультант	5
	Завідувач архіву	1
2.6	Відділ інформаційних технологій та технічних засобів	6
	Начальник відділу	1
	Головний спеціаліст	4
	Провідний спеціаліст	1
2.7	Відділ аналітичної роботи та правового забезпечення	5
	Начальник відділу	1
	Заступник начальника відділу	1
	Головний спеціаліст	3
2.8	Відділ статистики та звітності	9
	Начальник відділу	1
	Заступник начальника відділу	1
	Головний спеціаліст	7
	Загалом штатна чисельність працівників вищого навчального закладу	217

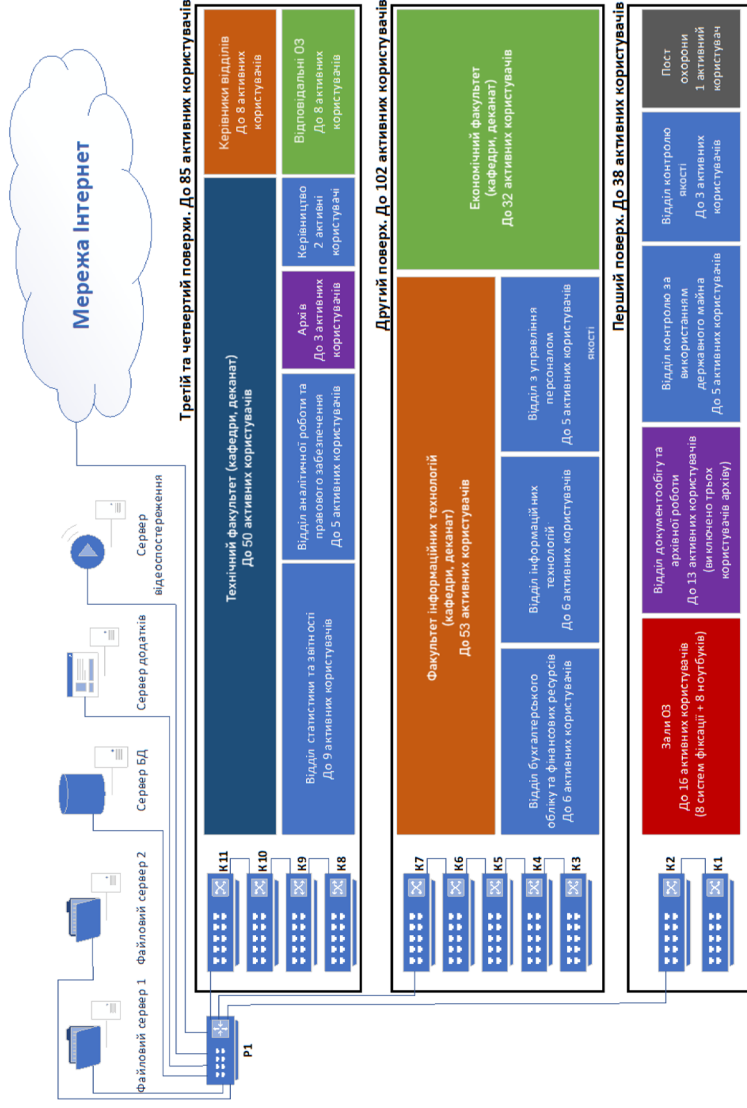
Додаток Б

Програмне забезпечення, яке використовується установою

Назва	Опис	Платформа	Кількість користувачів
КП ДВ	Клієнт-серверний додаток для здійснення електронного документообігу	Firebird	194
Сервіс підтримки КП ДВ	Серверна служба для обслуговування БД КП ДВ та здійснення реплікацій між установами та центральним рівнем	Firebird	1
Інформаційна платформа Ліга-Закон	Клієнт-серверна інформаційно-аналітична і пошукова система законодавства України	MS SQL Server	30/183
ISPro	Клієнт-серверний додаток для ведення всіх ділянок бухгалтерського обліку	MS SQL Server	4
MEDoc	Клієнт-серверний додаток для ведення та надсилання електронної звітності	MS SQL Server	3
АС АРМ-ВЗ	Клієнт-серверний додаток для формування і друку супровідних документів до поштових відправлень, поштових переказів	Firebird	9
EasyCon	Сервіс ВКЗ для проведення ОЗ в режимі відеоконференцій	Web	5/50
Система бронювання майданчиків ВКЗ	Сервіс бронювання залів ОЗ для проведення ОЗ в режимі ВКЗ	Web	3
Кадри Web	Ведення кадрового обліку	Web	5

Топологія мережі Ду

Додаток В



Додаток Г

Загальний трафік в установі в розрізі програмного забезпечення

Назва ПЗ	Трафік окремого з'єднання (Мб/год), Т	Кількість користувачів, n	Загальний трафік у мережі (Мб/год), V
КП ДВ	48	194	9 312
Сервіс підтримки КП ДВ	187	1	187
Інформаційна платформа Ліга-Закон	76	30	570
ISPro	94	4	148
MEDoc	21	3	63
АС АРМ-ВЗ	15	9	135
EasyCon	11 450	5	57 250
Система бронювання майданчиків ВКЗ	33	3	99
Кадри Web	35	5	175
Інші сервіси та ПЗ (електронна пошта, Web, OS Windows, файлові служби тощо)	106	208	22 048

Додаток Д

Кількість користувачів у розрізі програмного забезпечення й поверхів (топології)

Назва ПЗ	Трафік окремого з'єднання (Мб/год)	Кількість користувачів, перший поверх	Кількість користувачів, другий поверх	Кількість користувачів, третій-четвертий поверхи
КП ДВ	48	21	91	82
Сервіс підтримки КП ДВ	187	0	1	0
Інформаційна платформа Ліга-Закон	76	3	25	2
ISPro	94	0	4	0
MEDoc	21	0	3	0
АС АРМ-ВЗ	15	9	0	0
EasyCon	11450	5	0	0
Система бронювання майданчиків ВКЗ	33	0	3	0
Кадри Web	35	0	5	0
Інші сервіси та ПЗ	342	38	102	85

Нова топологія мережі ДУ

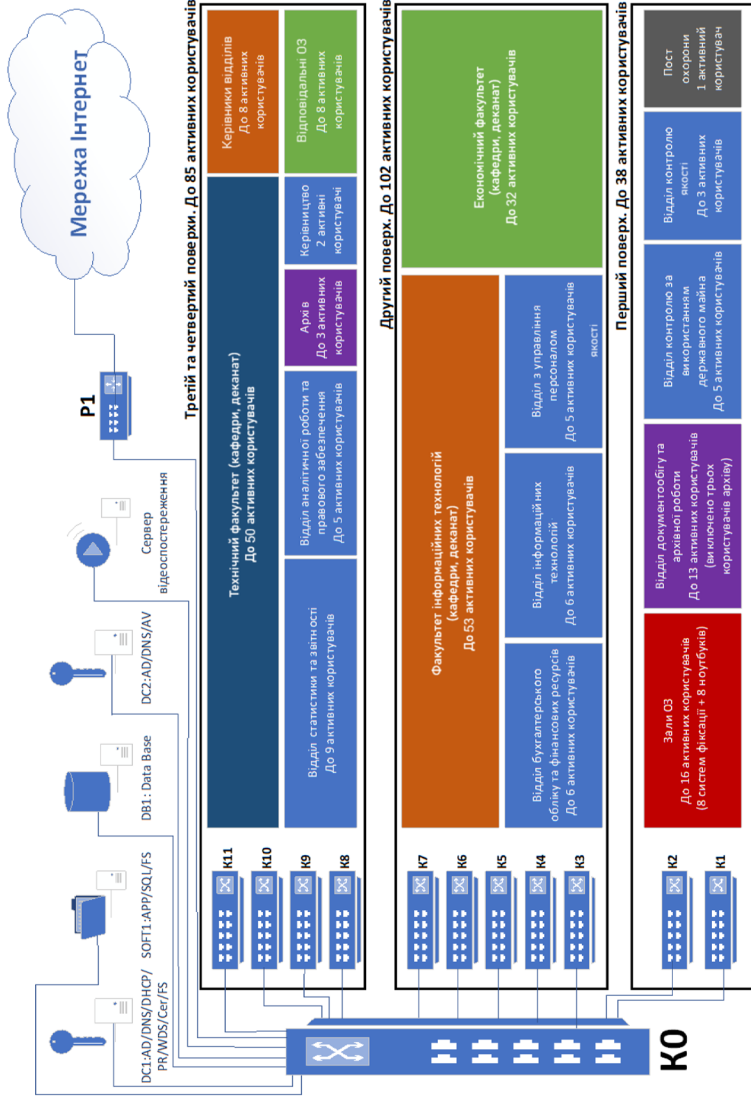


Схема другого поверху будівлі

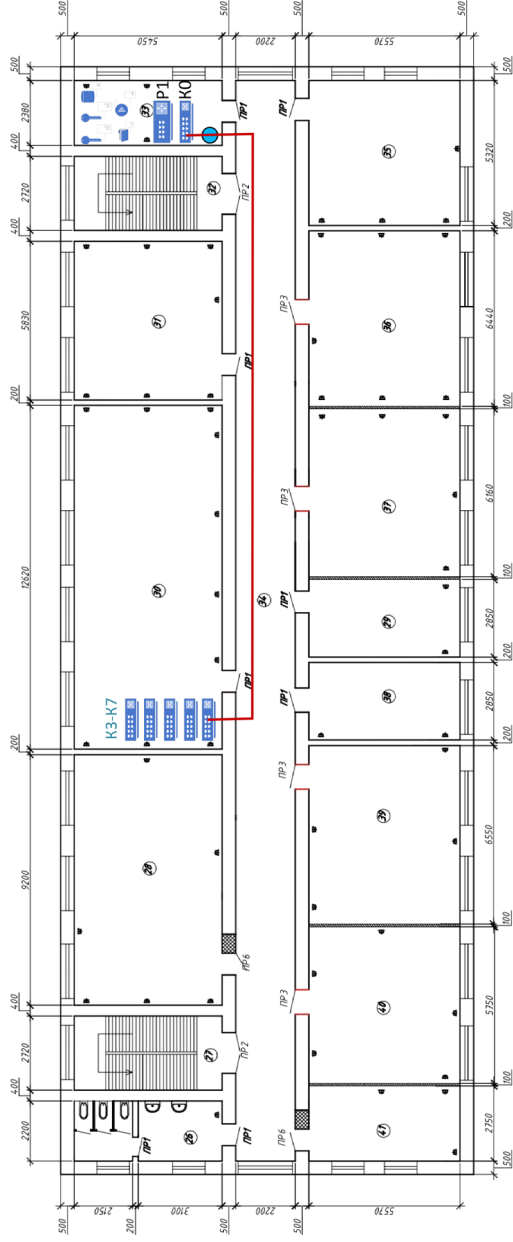
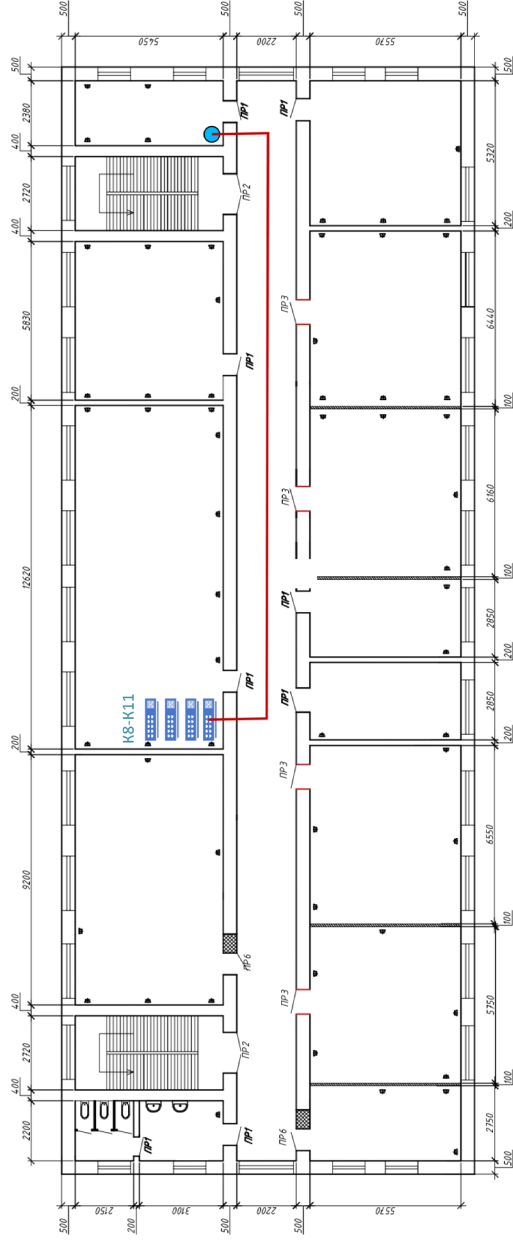


Схема третього поверху будівлі



Додаток И

Файл конфігурації маршрутизатора P1

```
# apr/05/2022 10:34:39 by RouterOS 7.1.3
# software id = XXXX-XXXX
# model = RB4011iGS+
# serial number = XXXXXXXXXXXXX
/interface bridge
    add admin-mac=XX:XX:XX:XX:XX:XX auto-mac=no comment=Bridge
name=bridge1
/interface ethernet
    set [find default-name=ether1] name="1 UkrTelecom"
    set [find default-name=ether2] name="2 DU Network"
    set [find default-name=ether5] name="5 Satellite Net Service"
    set [find default-name=ether10] name="10 UkrTelecom Reserved"
    set [find default-name=sfp-sfpplus1] disabled=yes
/interface pppoe-client
    add allow=chap,mschap1,mschap2 disabled=no interface=
"5 Satellite Net Service" keepalive-timeout=60 max-mru=1480
max-mtu=1480 mrru=1600 name=sns user=XXXXXXXXXX
/ip firewall layer7-protocol
    add name=team regexp="^(post|get) /d(out|in).
aspx\\?.*client=dyngate"
    add name=team1 regexp="^\\x17"
    add name=Other regexp="^.+(anydesk|ammyy|aerodesk|teamviewe
r|relays.net.anydesk.com).*$"
/ip pool
    add name=" DU Pool" ranges=10.16.14.40-10.16.14.240
/ip dhcp-server
    add address-pool= DU Pool" interface=bridge1 name=" DU DHCP"
/routing bgp template
    set default as=65530 disabled=no name=default output.network
=bgp-networks
/routing ospf instance
    add name=default-v2
/routing ospf area
    add disabled=yes instance=default-v2 name=backbone-v2
/routing table
    add fib name=MarkVIP
    add fib name=MarkZAL
/user group
```

```

set full policy="local,telnet,ssh,ftp,reboot,read,write,
policy,test,winbox,pas\
sword,web,sniff,sensitive,api,romon,dude,tikapp,rest-api"
/interface bridge port
add bridge=bridge1 ingress-filtering=no interface="2 DU Network"
add bridge=bridge1 ingress-filtering=no interface=ether3
add bridge=bridge1 ingress-filtering=no interface=ether4
add bridge=bridge1 ingress-filtering=no interface=sfp-sfpplus1
/ip neighbor discovery-settings
set discover-interface-list=!dynamic
/ip settings
set max-neighbor-entries=8192
/ipv6 settings
set disable-ipv6=yes max-neighbor-entries=8192
/ip address
add address=10.16.14.1/23 interface=bridge1 network=10.16.14.0
add address=192.168.XXX.XXX2/30 interface="1 UkrTelecom"
network=192.168.XXX.XX0
add address=192.168.XXX.XXX8/30 interface="10 UkrTelecom
Reserved" network=192.168.XXX.XX6
/ip dhcp-server network
add address=10.16.14.0/23 dns-server=10.16.14.3,8.8.8.8 domain=
DU.Local gateway=10.16.14.1 netmask=23
/ip firewall filter
add action=accept chain=input comment="Allow Related
Connctions" connection-state=established,related
add action=drop chain=input comment="Drop all Invalid input"
connection-state=invalid
add action=accept chain=input comment="Allowed Input IP
list" src-address-list="Allowed Input"
add action=accept chain=input comment="Allow Ping Mikrotik"
protocol=icmp
add action=drop chain=input comment="Drop all other Input"
in-interface=!bridge1
add action=drop chain=forward comment="Block some user
by MAC" out-interface=\
"1 UkrTelecom" src-mac-address=D0:XX:XX:XX:A6
add action=drop chain=forward comment="Block some user
by IP" disabled=yes \
out-interface=sns src-address=10.16.14.XXX
add action=reject chain=forward comment=TeamViewer
disabled=yes \

```

```

layer7-protocol=team reject-with=icmp-network-unreachable
src-address=\
10.16.14.40-10.16.14.254
add action=reject chain=forward comment=TeamViewer
disabled=yes \
layer7-protocol=team1 reject-with=icmp-network-
unreachable src-address=\
10.16.14.40-10.16.14.254
add action=reject chain=forward comment=AllOtherRemote
disabled=yes \
layer7-protocol=Other reject-with=icmp-network-unreachable
src-address=\
10.16.14.40-10.16.14.254
add action=drop chain=forward comment=TeamViewer disabled=yes
dst-port=5938 \
protocol=tcp src-address=10.16.14.40-10.16.14.254
add action=drop chain=forward comment=TeamViewer disabled=yes
dst-port=5938 \
protocol=udp src-address=10.16.14.40-10.16.14.254
add action=accept chain=forward comment="Allow Ralated
Forward" connection-state=established,related
add action=drop chain=forward comment="Drop invalid
connections My Network" connection-state=invalid
add action=drop chain=forward comment="Drop all from WAN
not DSTNATed" connection-nat-state=!dstnat \
connection-state=new in-interface="1 UkrTelecom"
add action=drop chain=forward comment="Drop all from WAN not
DSTNATed" connection-nat-state=!dstnat connection-state=new
in-interface="10 UkrTelecom Reserved"
add action=drop chain=forward comment=" Drop all from
WAN not DSTNATed « connection-nat-state=!dstnat connection-
state=new in-interface=sns
add action=accept chain=forward comment="Allow DNS"
dst-port=53 in-interface=bridge1 protocol=udp
add action=accept chain=forward comment="GLOBAL Allow TCP"
dst-port=80,443,7680 in-interface=bridge1 protocol=tcp
add action=accept chain=forward comment="GLOBAL Allow UDP"
dst-port=123,443 in-interface=bridge1 protocol=udp
add action=accept chain=forward comment="Replication SPD
SRV-BASE" dst-port=21,25,110,5000,8090 in-interface=bridge1
protocol=tcp src-address=10.16.14.4
add action=accept chain=forward comment="Allow TCP MEDok
MAIL" dst-port=465,993 in-interface=bridge1 protocol=tcp
src-address=10.16.14.2

```

```

add action=accept chain=forward comment="ZOOM TCP"
dst-port=8801,8802 in-interface=bridge1 protocol=tcp
add action=accept chain=forward comment="ZOOM UDP"
dst-port=3478,3479,8801-8810 in-interface=bridge1 protocol=udp
add action=accept chain=forward comment="Allow TCP EasyCon"
dst-port=3478,5349,8443,8444,8958 in-interface=bridge1
out-interface="10 UkrTelecom Reserved" protocol=tcp
add action=accept chain=forward comment="Allow UDP
EasyCon" dst-port=3478,5349,31001-65535 in-interface=bridge1
out-interface="10 UkrTelecom Reserved" protocol=udp
add action=accept chain=forward comment="Allow TCP
EasyCon SNS" disabled=yes dst-port=3478,5349,8443,8444,8958
in-interface=bridge1 out-interface=sns protocol=tcp
add action=accept chain=forward comment="Allow UDP
EasyCon SNS" disabled=yes dst-port=3478,5349,31001-65535
in-interface=bridge1 out-interface=sns protocol=udp
add action=drop chain=forward in-interface=bridge1
out-interface="1 UkrTelecom"
add action=drop chain=forward in-interface=bridge1
out-interface="10 UkrTelecom Reserved"
add action=drop chain=forward in-interface=bridge1
out-interface="sns"

```

```

add action=accept chain=output comment="Google DNS ping
Allow" dst-address=8.8.4.4 out-interface="1 UkrTelecom"
protocol=icmp src-address=192.168.XXX.XX2
add action=drop chain=output comment="Google DNS ping Drop"
dst-address=8.8.4.4 out-interface=sns

```

/ip firewall mangle

```

add action=mark-routing chain=prerouting comment="VIP"
new-routing-mark=MarkVIP \
    passthrough=no src-address=10.16.14.30-10.16.14.39
add action=mark-routing chain=prerouting comment=DNS2
new-routing-mark=\
    MarkVIP passthrough=no src-address=10.16.14.10
add action=mark-routing chain=prerouting comment=RocketChat
new-routing-mark=\
    MarkVIP passthrough=no src-address=10.16.14.8
add action=mark-routing chain=prerouting comment=DNS1
new-routing-mark=\
    MarkVIP passthrough=no src-address=10.16.14.3
add action=mark-routing chain=prerouting comment="Zal OZ"
new-routing-mark=\

```

```

        MarkZAL                passthrough=yes                src-address=
        10.16.14.241-10.16.14.248
/ip firewall nat
add action=masquerade chain=srcnat out-interface="1 UkrTelecom"
add action=masquerade chain=srcnat out-interface=
"10 UkrTelecom Reserved"
add action=masquerade chain=srcnat out-interface=sns
add action=netmap chain=dstnat comment="RocketChat Server
SSH" disabled=yes \
    dst-port=22 in-interface=sns protocol=tcp
    to-addresses=10.16.14.8 to-ports=22
add action=netmap chain=dstnat comment="RocketChat HTTP"
dst-port=80 \
    in-interface=sns protocol=tcp to-addresses=
    10.16.14.8 to-ports=80
add action=netmap chain=dstnat comment="RocketChat SSL"
dst-port=443 \
    in-interface=sns protocol=tcp to-addresses=
    10.16.14.8 to-ports=443
add action=netmap chain=dstnat comment=RocketChat
dst-port=3000 in-interface=\
    sns protocol=tcp to-addresses=10.16.14.8 to-ports=3000
add action=netmap chain=dstnat dst-port=3389 in-interface=sns
protocol=tcp \
    src-address=XXX.XXX.XXX.XXX to-addresses=10.16.14.3
    to-ports=3389
/ip route
add disabled=no distance=3 dst-address=0.0.0.0/0 gateway=sns
routing-table=\
    MarkVIP suppress-hw-offload=no
add comment=Replication disabled=no dst-address=
10.1.10.0/24 gateway=\
    192.168.XXX.XX1 routing-table=MarkVIP suppress-hw-offload=no
add comment=ISP1 disabled=no distance=5 dst-address=
0.0.0.0/0 gateway=192.168.XXX.XX1
add comment=ISP2 disabled=yes distance=2 dst-address=
0.0.0.0/0 gateway=sns
add comment=GOOGLE disabled=no dst-address=8.8.4.4/32 gateway=
192.168.XXX.XX1
add comment=ukrposhta.ua disabled=yes dst-address=
91.209.214.17/32 gateway=sns
add comment=zakon.rada.gov.ua disabled=yes dst-address=
193.19.153.66/32 gateway=sns

```

```
add comment=EDR,MAIL disabled=no distance=1 dst-address=
212.90.190.0/24 \
    gateway=192.168.XXX.XX1 pref-src=0.0.0.0 routing-table=
    MarkVIP scope=30 \
        suppress-hw-offload=no target-scope=10
add comment=Reserv disabled=no distance=4 dst-address=
0.0.0.0/0 gateway=\
    192.168.XXX.XX7 routing-table=MarkZAL
```

/ip service

```
set telnet address=10.16.14.0/23 disabled=yes
set ftp address=10.16.14.0/23 disabled=yes
set www address=10.16.14.0/23
set ssh address=10.16.14.0/23 disabled=yes port=222
set www-ssl address=10.16.14.0/23
set api address=10.16.14.0/23
set winbox address=10.16.14.0/23
set api-ssl address=10.16.14.0/23
```

/system clock

```
set time-zone-autodetect=no time-zone-name=Europe/Kiev
```

/system identity

```
set name=GateWay
```

/tool netwatch

```
add down-script="/ip route enable [find comment=\"ISP2\"]"
host=8.8.4.4 \
    interval=30s up-script="/ip route disable [find comment=
    \"ISP2\"]"
```

Скрипт контролю авторизації користувачів

```
$user = $env:USERNAME;
$computer = $env:COMPUTERNAME;
$time = [datetime]::Now;
$string = "$computer at $time";
$Searcher = New-Object DirectoryServices.DirectorySearcher;
$Searcher.SearchRoot = "LDAP://DC= DU,DC=local";
$Searcher.SearchScope = 2;
$Searcher.Filter = "(&(objectCategory=person)(objectClass=user)
(SamAccountName=$user))";
$objUser = [adsisearcher]$Searcher.FindOne().Path;
$objUser.Put("Description",$string);
$objUser.SetInfo();

$string = "$user at $time";
$Searcher = New-Object DirectoryServices.DirectorySearcher;
$Searcher.SearchRoot = "LDAP://OU= Незадіяні,OU= DU,DC= DU,
DC=local";
$Searcher.SearchScope = 1;
$Searcher.Filter = "(&(objectCategory=computer)(name=$computer))";
$objComp = [adsisearcher]$Searcher.FindOne().Path;

if (-not ([string]::IsNullOrEmpty($objComp)))
{
    $objComp.Put("Description",$string);
    $objComp.SetInfo();
}
```

НОТАТКИ

Навчальне видання

СУБОТІН Олег Володимирович
РАЗЖИВІН Олексій Валерійович
КОЙФМАН Олексій Олександрович
АМЕЛІН Володимир Петрович

**ДОСЛІДЖЕННЯ І РОЗРОБКА
ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ
СИСТЕМИ УСТАНОВИ**

Навчальний посібник

Верстка	<i>Т. Клименко</i>
Обкладинка	<i>В. Савельєва</i>
Технічне редагування	<i>О. Гринюк</i>



Підписано до друку 25.09.2026 р.
Формат 60х84/16. Папір офсет.
Цифровий друк. Гарнітура Liberation.
Ум. друк. арк. 9,07. Наклад 300.
Замовлення № 0826-038.

Видавництво та друк: Олді+
65101, м. Одеса, вул. Інглезі, 6/1
тел.: +38 (095) 559-45-45, e-mail: office@oldiplus.ua
Свідоцтво ДК № 7642 від 29.07.2022 р.
Замовлення книг:
тел.: +38 (050) 915-34-54, +38 (068) 517-50-33
e-mail: book@oldiplus.ua

