Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки,
Факультет радіоелектроніки та телекомунікацій
(повне найменування інституту, факультету)

Кафедра інформаційних технологій електронних засобів
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
бакалавр
(ступінь вищої освіти)

на тему Розробка системи захисту інформації на підприємстві

Виконав: студент(ка) 4 курсу, групи РТ-618сп

Спеціальності 151 «Автоматизація та комп'ютерно–інтегровані технології»
(код і найменування спеціальності)

Освітня програма (спеціалізація)
«Автоматизація, мехатроніка та робототехніка»

Чумаченко.В.І.
(прізвище та ініціали)

Керівник Шило.Г.М
(прізвище та ініціали)

Рецензент Зеленьова Ірина Хівна
(прізвище та ініціали)

2021

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Інститут, факультет Інститут інформатики та радіоелектроніки,
Факультет радіоелектроніки та телекомунікацій
Кафедра інформаційних технологій електронних засобів
Ступінь вищої освіти бакалавр
Спеціальність 151 «Автоматизація та комп'ютерно-інтегровані технології»
(код і найменування)
Освітня програма (спеціалізація) Автоматизація, мехатроніка та робототехніка
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТЗ Огренич Є.С
к.т.н.
«31» 05 2021 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

Чумаченко Віталій Ігорович
(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) Розробка системи захисту інформації на підприємстві
керівник проєкту (роботи) Шило Галина Миколаївна, д.т.н. доцент кафедри ІТЕЗ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «26» квітня 2021 року №159
2. Строк подання студентом проєкту (роботи) 7 червня 2021 року
3. Вихідні дані до проєкту (роботи) інформаційна безпека на підприємстві
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Дослідження предметної області, аудит мережевої, технічної та програмної частини, аналіз здобутої інформації, інтеграція рішень, висновки, перелік посилань, додаток А.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
28 рисунків; 8 таблиць; 15 слайдів;

6. Консультанти розділів проєкту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 - 5	Шило.Г.М		
Нормоконтроль	Поспєєва.Г.Є.,ст викладач		

7. Дата видачі завдання «26» квітня 2021 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз та постановка технічного завдання	28.04.21	
2	Аудит мережевої, технічної та програмної частини	29.04.21	
3	Аналіз ризиків інформаційної безпеки підприємства	03.05.21	
4	Інтеграція рішень з мережевої, технічної та програмної частини	29.05.21	
5	Інтеграція рішень для забезпечення інформаційної безпеки підприємства	30.05.21	
6	Розробка моделі інформаційно захищеного підприємства та алгоритму забезпечення інформаційної безпеки підприємства	31.05.21	
8	Оформлення ПЗ та захист дипломного проекту	07.06.21	

Студент(ка) _____ Чумаченко.В.І.
(підпис) (прізвище та ініціали)

Керівник проєкту (роботи) _____ Шило.Г.М
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка до дипломного проекту : 60 с., 28 рис., 8 табл., 8 джерел.

Мета дипломної роботи – розробка моделі інформаційно захищеного підприємства та алгоритм забезпечення інформаційної безпеки підприємства.

У дипломному проекті реалізовано модель інформаційно захищеного підприємства та алгоритм забезпечення інформаційної безпеки підприємства, проведено аудити мережевої, технічної та програмної частини, інтегровано рішення з оптимізації мережевої, технічної та програмної частини, інтегровано правила для підвищення рівня інформаційної безпеки у відмовостійкому середовищі та реалізовано рішення для забезпечення інформаційної безпеки підприємства.

У результаті модель інформаційно захищеного підприємства та алгоритм з досягнення інформаційної безпеки підприємства.

Розроблені модель та алгоритм можуть використовуватись спеціалістами для досягнення аналогічного результату у рамках своїх підприємств.

RAID, FIREWALL, ACTIVE DIRECTORY, MIKROTIK, СЕРВЕР, СИСТЕМА, ІНФОРМАЦІЙНО ЗАХИЩЕНЕ ПІДПРИЄМСТВО, МОДЕЛЬ, АЛГОРИТМ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЕЦП – Електронний цифровий підпис

VPN – Virtual Private Network (віртуальна приватна мережа)

ПЗ – програмне забезпечення

ІБ – інформаційна безпека

IT – Information Technology (Інформаційні технології)

HP – Hewlett – Packard

SQL – Structured Query Language (мова структурованих запитів)

USA – United States of America

GSM – Groupe Spécial Mobile

DHCP – Dynamic Host Configuration Protocol (протокол динамічної конфігурації вузла)

ККД – Коефіцієнт корисної дії

ВСТУП

Комп'ютерні та інформаційні технології сьогодні охопили всі галузі економіки. Для будь–якої сучасної компанії інформація стає одним з головних ресурсів, її збереження і правильне використання має ключове значення для розвитку бізнесу і зниження рівня різноманітних ризиків. Актуальною проблемою для підприємства стає забезпечення інформаційної безпеки.

Інформаційна безпека підприємства – це набір засобів, методів і робіт, орієнтованих на захист інформаційної інфраструктури підприємства від будь–яких зовнішніх або внутрішніх загроз, які можуть призвести до крадіжки, псування, або несанкціонованого зміни даних на серверах або робочих станціях. Всі роботи, орієнтовані на побудову, підтримку і розвиток системи інформаційної безпеки мають основну мету – звести до мінімуму можливість заподіяння шкоди інформаційній інфраструктурі підприємства, а у разі форс–мажорних обставин, зведення до мінімуму такого збитку[1].

На рис.1 наведено принципи інформаційної безпеки.

Рисунок 1 – Принципи інформаційної безпеки

На сьогоднішній день нагальною постає проблема підвищення рівня інформаційної безпеки підприємства, яка значною мірою залежить від ступеня захищеності інформаційної сфери. Рівень інформаційної безпеки впливає на

розвиток та впровадження науково–технічних інновацій у процеси виробництва, збереження стабільності функціонування, забезпечення можливості економічного зростання.

Конфіденційна інформація представляє величезний інтерес для конкуруючих фірм. Саме вона стає причиною посягань з боку зловмисників. Багато проблем пов'язані з недооцінкою важливості загрози, у результаті чого для підприємства це може обернутися крахом і банкрутством. Навіть одиничний випадок недбалості робочого персоналу може принести компанії багатомільйонні збитки і втрату довіри клієнтів. Загрозу зазнають дані про склад, статус і діяльність компанії. Джерелами таких загроз є її конкуренти, корупціонери і злочинці. Особливу цінність для них представляє ознайомлення з захисною інформацією, а також її модифікація з метою заподіяння фінансового збитку. До такого результату може привести витік інформації навіть на 20%. Іноді втрата таємниць компанії може статися випадково, через недосвідченість персоналу або через відсутність систем захисту. Атмосфера ринкової економіки і високий рівень конкуренції змушують керівників компаній завжди бути напоготові і швидко реагувати на будь–які труднощі. Протягом останніх 20 років інформаційні технології змогли увійти в усі сфери розвитку, управління і ведення бізнесу.

З реального світу бізнес вже давно перетворився у віртуальний, досить згадати як стали популярні ЕЦП, у якого є свої закони. В даний час віртуальні загрози інформаційної безпеки підприємства можуть завдати йому величезної реальної шкоди. Недооцінюючи проблему, керівники ризикують своїм бізнесом, репутацією і авторитетом. Більшість підприємств регулярно зазнають збитків через витік даних. Захист інформації підприємства є пріоритетна задача у ході становлення бізнесу і його ведення. Забезпечення інформаційної безпеки – запорука успіху, прибутку і досягнення цілей підприємства [2].

Першим важливим фактором успіху в справі організації безпеки, є розуміння того, які активи і від яких загроз потрібно захистити. До впровадження системи організації інформаційної безпеки (СОІБ) необхідно провести ризик–

аналіз і вирішити, які ризики будуть оброблені системою, а які ми просто приймаємо. Цей етап дозволить заощадити гроші, і направити ресурси саме туди, де вони необхідні.

Зараз не тільки великі організації, а й середній і навіть малий бізнес починає усвідомлювати важливість даного напрямку, на жаль, більшість вже після того, як отримали пошкодження від витоків інформації, шифрування інформації, кібератак і внаслідок повного виведення з ладу обладнання та втрати прибутку. І все через нехтування і небажанням виділяти фінанси на захист і збереження власних ресурсів. Інша проблема полягає у фахівцях небажаючих навчатися і постійно розвивати інфраструктуру свого офісу / підприємства через низьке фінансування і відсутність прямих вказівок керівництва. Що працює як закономірність для обох сторін і як внаслідок рано чи пізно байдужість обох сторін призводить до пошуку винних і нездатності, а може навіть і неможливості, вжити заходів при появі інформаційної загрози.

Таким чином, метою дипломного проекту є розробка моделі та алгоритму створення інформаційно захищеного підприємств

1. АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Цінність даних

Поряд з класичними факторами виробництва, такими як праця, земля, капітал, інформація стає одним з основних ресурсів, що забезпечують діяльність компанії. Більш того, інформація, найчастіше, сама є вихідною сировиною або результатом виробництва – товаром, запропонованим кінцевому споживачу. З цієї точки зору інформація стає активом компанії, який потребує обліку та вираженні у загальноприйнятих кількісних показниках.

В незалежності від форм власності та виду діяльності установи, інформація є основою для прийняття найважливіших управлінських рішень, наприклад, визначення стратегії поведінки на ринку, планів подальшого розвитку, інвестування у проект, підписання угод. Одним з основних постачальників такої інформації для керівництва компанії є бухгалтерія. Головна проблема полягає в тому, що, як правило, в підсумковому балансі основна увага приділяється матеріальним складовим – майну, оборотним активам, зобов'язанням, дебіторської та кредиторської заборгованості, і мало уваги приділяється нематеріальним активам.

Більш складною і глобальною проблемою є визначення цінності інформаційного активу і об'єктивне вираження його в загальноприйнятому кількісному показнику – грошовому. Це завдання слабо формалізується, тому всі значення, отримані у результаті оцінки будуть наближеними. Тільки власник інформаційного активу або інша особа, яка отримує з його допомогою прибуток, може об'єктивно оголосити його грошову вартість. Для визначення вартості активу застосовуються різні методи. Найпростіший – це визначення вартості шляхом розрахунку трудовитрат на одиницю отриманої цінної інформації. Наприклад, середньогодинна ставка співробітника на витрачений їм час для отримання цих відомостей. Однак такий метод не дозволяє оцінювати вже наявні активи або активи, отримані іншим шляхом. Як визначилися вважати раніше,

інформаційний актив – це не просто цінні відомості, його потрібно розглядати як невід'ємну сукупність вищевказаних елементів. Тому, більш прогресивний підхід передбачає комбіновану оцінку вартості шляхом врахування багатьох чинників, серед яких, наприклад, вартість отримання інформації, її обробки і зберігання з використанням обчислювальної техніки, людські трудовитрати. Ще однією проблемою є те, що, в порівнянні іншими об'єктами, наприклад, основними засобами організації, інформаційні активи є дуже динамічною структурою, термін корисного використання яких, на увазі швидкої втрати актуальності інформації, вкрай невизначений і вартість яких також може значно змінюватися в дуже короткі проміжки часу. Це вимагає їх періодичної переоцінки. Причому оцінка за резервним значенням, яка формується на початок і кінець року, не відображає реальної картини. Ефективним варіантом визнаний метод оцінка виходячи з середнього значення за всі дні протягом звітного року.

Відповісти на питання де зазвичай зберігається найважливіша інформація не так просто, але безумовно один з варіантів це база даних підприємства. Значимість і цінність цієї інформації призводить до необхідності забезпечення захисту не тільки елементів інфраструктури, а й самих баз даних. Припустимо що конкурент отримав інформацію про всіх клієнтів з бази даних, або він зміг роздобути логістичні маршрути ваших вантажних автомобілів і завадив відвантаженню товару. Ці ситуації дорівнюють катастрофі. Щоб цього не сталося необхідно розмежовувати доступи і не давати одній людині абсолютну владу всередині бази даних, можливо навіть адміністратору.

Говорячи про документи це цілком можуть бути списки співробітників, чим конкурент може скористатися і переманювати працівників створюючи брак кадрів і проблеми підприємству.

І під кінець крадіжка і злом банківських даних, виведення фінансів підприємства або заморозку рахунків, що теж призведе якщо не до закриття, то до величезних проблем.

Діяльність будь–якої установи включає у себе отримання інформації, її обробку, прийняття рішень на основі аналізу інформації та передачу прийнятих

рішень по каналам зв'язку. Спотворення інформації, блокування її, отримання або впровадження неправдивої інформації сприяють прийняттю помилкових рішень.

Інформація – це специфічний продукт, тому необхідні чіткі межі, що визначають інформацію як об'єкт права, які дозволять застосовувати до неї законодавчі норми. Інформація залежно від категорії доступу до неї підрозділяється на загальнодоступну інформацію, а також на інформацію обмеженого доступу.

Публічна інформація – виходячи зі статті 1 Закону України «Про доступ до публічної інформації», це відображена та задокументована будь–якими засобами та на будь–яких носіях інформація, що була отримана або створена у процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом.

Інформація з обмеженим доступом — інформація, доступ до якої має лише обмежене коло осіб і оприлюднення якої заборонено розпорядником інформації відповідно до закону. Обмеження доступу до інформації здійснюється в інтересах національної безпеки або охорони законних прав фізичних та юридичних осіб. Обмежується доступ до інформації, а не до документу. Відповідно, якщо в одному документі міститься відкрита і закрита інформація, перша може бути надана на ознайомлення зацікавленій особі у вигляді окремого документу. До інформації з обмеженим доступом належить конфіденційна, службова та таємна інформація. Загалом, в Україні налічується близько 20 видів інформації з обмеженим доступом (банківська, лікарська, адвокатська таємниця, таємниця сповіді). Будь–яка інша інформація вважається відкритою і отримати доступ до неї мають право всі громадяни України, незалежно від того стосується їх ця інформація безпосередньо чи ні [3].

1.2 Аналіз ризиків

Ризик інформаційної безпеки – це ймовірність виникнення негативних подій, які завдають шкоди організації або фізичній особі.

Основними ризиками інформаційної безпеки є:

- ризик витоку конфіденційної інформації;
- ризик втрати або недоступності важливих даних;
- ризик використання неповної або спотвореної інформації;
- ризик поширення у зовнішньому середовищі інформації, що загрожує репутації організації.

На рис.1.1 наведено процентне відношення причасної вини до витоків інформації у організації.

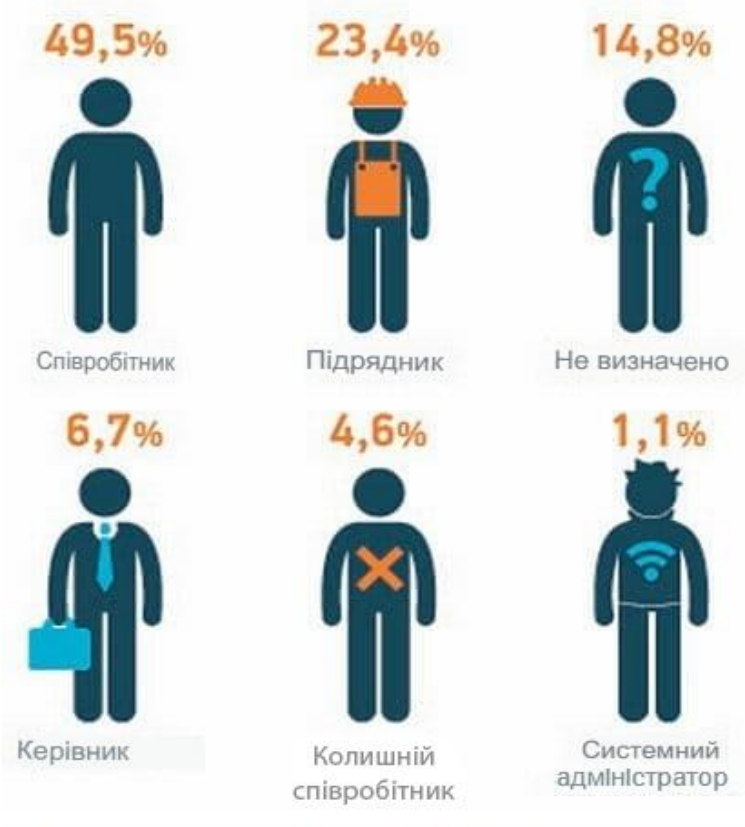

Рисунок 1.1 – Процентне відношення причасної вини до витоків інформації у організації

Втрата даних – пошкодження або втрата інформації в результаті впливу різних чинників, випадкових або навмисних дій. Втратити дані можна під час роботи з ними, а також при зберіганні інформації на комп'ютері, сервері або на масивах RAID. Втратити дані внаслідок ненавмисних причин, таких як стихійні лиха, катастрофи, нещасні випадки, збій ПЗ або устаткування, може будь–який користувач або компанія. Так само дані потрапляють під вплив чинників навколишнього середовища, наприклад пилу, вологи, тепла, під фізичні впливу.

Запобігти втраті даних можна прийнявши ряд заходів. Незалежно від джерела загрози основним захистом є резервне копіювання файлів. Важливо регулярно робити резервні копії і переконуватися, що копія повністю відповідає оригіналу.

На рис.1.2 наведено приклад втрати даних у зв’язку з пошкодженням секторів на жорсткому диску.

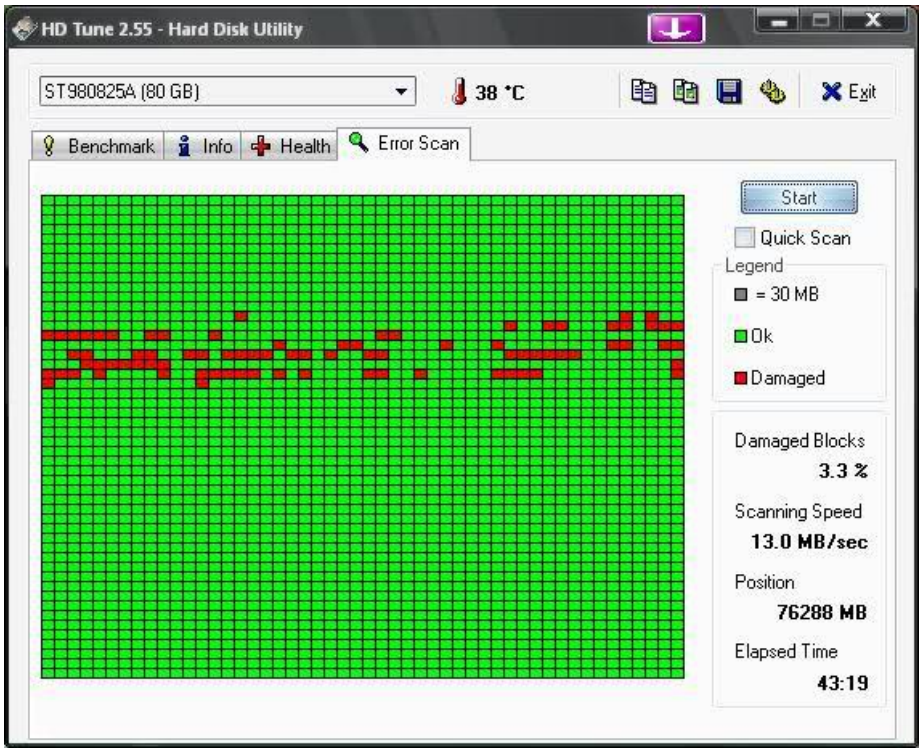

Рисунок 1.2 – Втрата даних у зв’язку з пошкодженням секторів на жорсткому диску

Чим більше недостовірна вхідна інформація, тим більш невизначеними будуть висновки, і, навпаки, при використанні достовірної інформації прийняте рішення буде оптимальним. Також може призвести до неправильного результату або до його відсутності зовсім, при цьому маючи затрати часу, фінансів, зусиль. Специфікою інформаційного забезпечення гірничодобувних галузей є висока частка витрат на отримання необхідної інформації (в основному геологічної) в собівартості видобутого мінерального сировини. Тому основним критерієм щодо оцінки достатності інформації є її сумарна вартість в порівнянні з очікуваними результатами використання інформаційних ресурсів. У більшості випадків пакети інформації, які використовуються при реалізації інноваційних проектів, є спочатку неповними.

Іноді ступінь неповноти може досягати критичних значень. Формування оптимального комплексу своєчасною, достовірною та достатньої інформації є предметом інженерних обґрунтувань і розрахунків. У процесі отримання, зберігання і використання інформація може бути загублена, забута, спотворена, скомпрометована або фальсифікована, у зв'язку з чим виникає необхідність врахування відповідних ризиків, які можуть позначитися на ефективності реалізації інноваційних проектів.

В ході виконання проектів з оцінки ризиків інформаційної безпеки необхідно враховувати, що ризики ІБ можуть мати різну ціну (викликати різний збиток). Наприклад, ступінь негативного впливу настання події ризику на репутацію постраждалої організації може змінюватися від дуже низької до високої. Події ризику мають різний вплив на репутацію постраждалої сторони, це представлено в рис. 1.3.

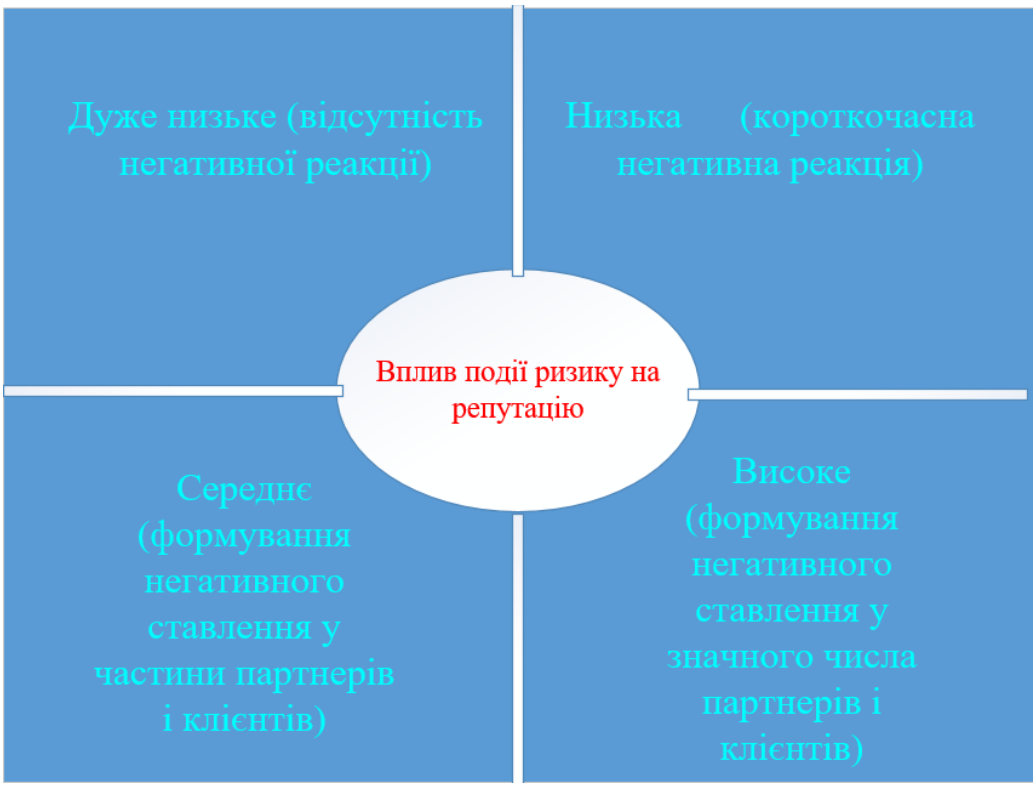

Рисунок 1.3 – Вплив події ризику на репутацію

1.3 Загрози інформаційної безпеки

Загрози інформаційної (комп'ютерної) безпеки – це різні дії, які можуть призвести до порушень стану захисту інформації. Іншими словами, це – потенційно можливі події, процеси або дії, які можуть завдати шкоди інформаційним і комп'ютерним системам [4].

Загрози ІБ можна розділити на два типи: природні і штучні. До природних відносяться природні явища, які не залежать від людини, наприклад урагани, повені, пожежі і таке інше. Штучні загрози залежать безпосередньо від людини і можуть бути навмисними і ненавмисними. Ненавмисні загрози виникають через необережність, неуважність і незнання.

На рис.1.4 наведено типи загроз ІБ.

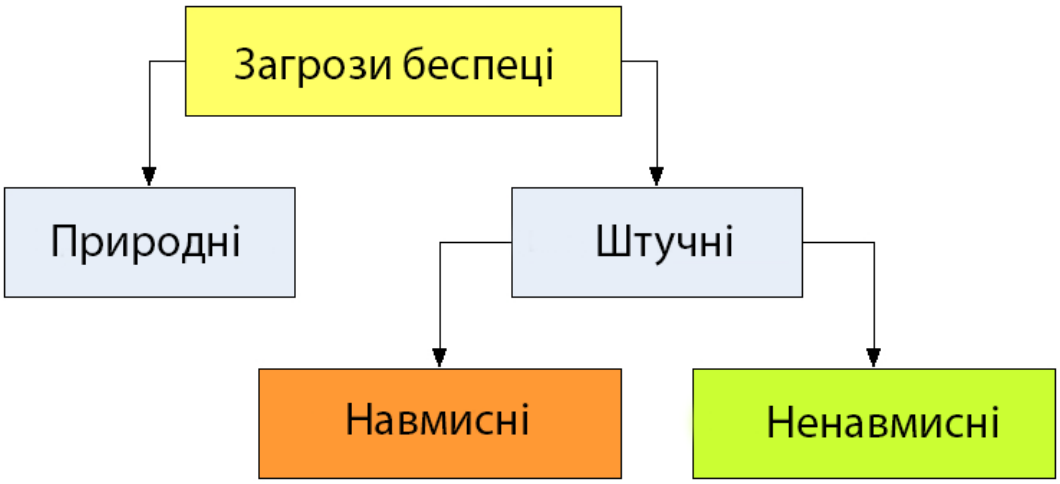

Рисунок 1.4 – Типи загроз ІБ

Небажаний контент – це не тільки шкідливий код, потенційно небезпечні програми і спам (тобто те, що безпосередньо створено для знищення або крадіжки інформації), але і сайти, заборонені законодавством, а також небажані ресурси з інформацією, що не відповідає віку споживача.

На рис.1.5 наведено найбільш небезпечні загрози інформаційною безпеки.

Рисунок 1.5 – Статистика найбільш небезпечних загроз інформаційній безпеки в світі

Спектр загроз інформаційних безпек, викликаних використанням шкідливого програмного забезпечення надзвичайно широкий. Ось деякі приклади таких загроз захисту інформації:

- впровадження вірусів та інших руйнівних програмних впливів;
- аналіз і модифікація / знищення встановленого програмного забезпечення;
- впровадження програм–шпигунів для аналізу мережевого трафіку і отримання даних про систему і стан мережевих з'єднань;
- використання вразливостей ПЗ для злому програмного захисту з метою отримання несанкціонованих прав читання, копіювання, модифікації або знищення інформаційних ресурсів, а також порушення їх доступності;
- розкриття, перехоплення і розкрадання секретних кодів і паролів;
- читання залишкової інформації в пам'яті комп'ютерів і на зовнішніх носіях;
- блокування роботи користувачів системи програмними засобами.

Більшість інцидентів інформаційної безпеки пов'язано з впливом внутрішніх загроз–витоку і крадіжки інформації, витоку комерційної таємниці і персональних даних клієнтів організації, збиток інформаційній системі пов'язані, як правило, з діями співробітників цієї організації. У класифікації внутрішніх загроз у першу чергу можна виділити дві великі групи: загрози, що здійснюються з корисливих або інших зловмисних міркувань; загрози, що здійснюються без злого умислу, з необережності або технічної некомпетентності.

Отже, злочини співробітників, здатних завдати шкоди збереженню інтелектуальної та комерційної власності організації (їх прийнято називати «інсайдерами») можна розділити на категорії зловмисного інсайду і ненавмисного інсайду.

Зловмисні інсайдери становлять певну небезпеку для інформаційної системи і конфіденційних даних, проте ймовірність зловмисних інцидентів мізерно мала в порівнянні з витоками інформації, що здійснюються з

необережності або внаслідок технічної безграмотності співробітників. Так, на жаль, більша частка всіх інцидентів інформаційної безпеки на об'єкті будь–якої складності є наслідком ненавмисних дій співробітників. Можливостей для таких витоків інформації безліч: від помилок введення даних при роботі з локальними мережами або Інтернетом до втрати носія інформації (ноутбук, USB–накопичувач, оптичний диск); від пересилання даних по незахищених каналах зв'язку до ненавмисного завантаження вірусів з розважальних веб–сайтів [5].

1.4 Наслідки та реакції в слід на атаку на інформаційну безпеку підприємства

Наслідки будь–яких атак і, відповідно, пріоритет при виділенні ресурсів на ті чи інші завдання забезпечення інформаційної безпеки значно різняться в залежності від галузі. Експерти виділяють найбільш актуальні види наслідків:

- штраф регуляторів,
- зупинка бізнес–процесів,
- крадіжка грошей,
- репутаційний збиток і ін.
- зниження продуктивності / непрацездатність.
- зараження користувачів вірусами – зламаний сервер може служити майданчиком для поширення шкідливого ПЗ / фішингу або інших;
- переправлення трафіку – користувачі зламаної системи можуть бути переправлені на інші сайти (зазвичай, казино, фінансові послуги і т.д.);
- приєднання до ботнету – обчислювальні потужності можуть використовуватися для спаму, атак на інші системи або для майнінгу;
- крадіжка даних і шпигунство – із зламаної системи можуть бути вкрадені дані і може бути встановлений бекдор, що дозволяє отримувати дані з системи і в подальшому;

- злом облікового запису – облікові записи можуть бути скомпрометовані як в атакованій системі, так і в інших системах – на жаль, у користувачів дуже часто однакові паролі для декількох різних систем;
- дефейс – на веб–сторінках може бути розміщена інформація, що завдає репутаційний збиток.

Наприклад, штрафу з боку регуляторів найбільше побоюються організації з жорстким регулюванням:

- державні компанії (62%);
- організації охорони здоров'я (62%);
- освітні (41%);
- фінансові організації (40%).

Багато галузей найбільш неприємним наслідком ІБ–загроз вважають зупинку бізнес–процесів. Важливим за значенням став репутаційний збиток:

- для транспортної галузі (81%);
- компаній ІТ і телекомунікацій (79%);
- освітніх організацій (65%);
- фінансового сектора (60%).

Банки та інші фінансові компанії відзначають підвищену заклопотаність наслідками, пов'язаними з крадіжкою грошових коштів.

Від коректності дій, що винують співробітники в разі виникнення інциденту загрози ІБ, буде залежати збиток – скільки грошей втратить компанія в результаті атаки [6].

Перевага на боці хакерів, вони не обмежені ні в часі, ні в методах, вони на крок попереду захисників. Універсального захисту від кіберзагроз поки що не існує, проте можна мінімізувати час виявлення та реагування на інциденти, якщо якісне спланувати і регламентувати порядок дій всіх залучених в цю діяльність співробітників.

На рис.1.6 наведено можливі реакції організацій на випадки кібератак.

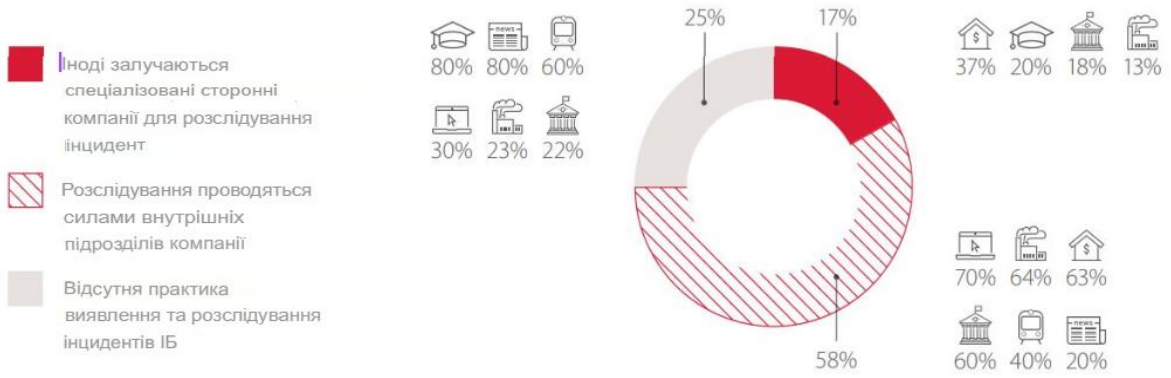

Рисунок 1.6 – Можливі реакції організацій на випадки кібератак

Технології привносять у бізнес не тільки нові можливості, але й нові ризики, якими необхідно ефективно управляти. На жаль, всього в 3% компаній задіяний комплексний підхід до захисту від кіберзагроз.

1.5 Постановка завдання

Мета дипломного проекту - розробити модель та алгоритм створення інформаційно захищеного підприємства на прикладі існуючого і функціонуючого підприємства.

Для досягнення поставленої мети необхідно:

- провести IT-аудит для визначення поточної ситуації в межах локально обчислювальної мережі та її ресурсів;
- провести аналіз і побачити проблеми продуктивності і відмовостійкості локальної обчислювальної мережі;
- підготувати вирішення проблем продуктивності і відмовостійкості мережевої інфраструктури;
- провести роботи з оптимізації та відмовостійкості мережевої інфраструктури;
- впровадження правил інформаційної безпеки в підготовлену інфраструктуру;
- розробка моделі інформаційно захищеного підприємства;
- розробка алгоритму забезпечення інформаційної безпеки підприємства.

2 АУДИТ МЕРЕЖЕВОЇ ТА КОМП'ЮТЕРНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

2.1 Мережева топологія підприємства

Перед початком аудиту необхідно провести аналіз технічної документації мережі та технічної документації стосовно доступів на мережеве обладнання, комп'ютерну техніку та сервера підприємства.

У всіх приміщеннях є розведення кабелів типу RJ45 поміщених у короба та протягнуті до відповідних розеток. Кабелі заведені в серверну кімнату в мережеву шафу, в мережевій шафі є комутаційна патч–панель, у яку скросовані всі дроти для подальшої зручності комутації з мережевим обладнанням і підключення через пасивне в активне обладнання. В даний час розширення або модифікації кабельної мережі не планується. Претензій до якості кабельної системи немає.

Головний маршрутизатор Mikrotik rb951g–2HnD виступає у ролі DHCP серверу, VPN серверу та firewall. До нього підключено комутатор HP ProCurve 2510G–24. До комутатору підключено шлюз IP телефонії, дві точки доступу та комп'ютери, що локально розміщено на території офісу. Через VPN-канал до Mikrotik rb951g–2HnD підключено RouteOS на HETZNER. Віддалені користувачі також підключаються до головного маршрутизатору Mikrotik rb951g–2HnD з використанням VPN.

На рисунку 2.1 наведено схему топології мережи.

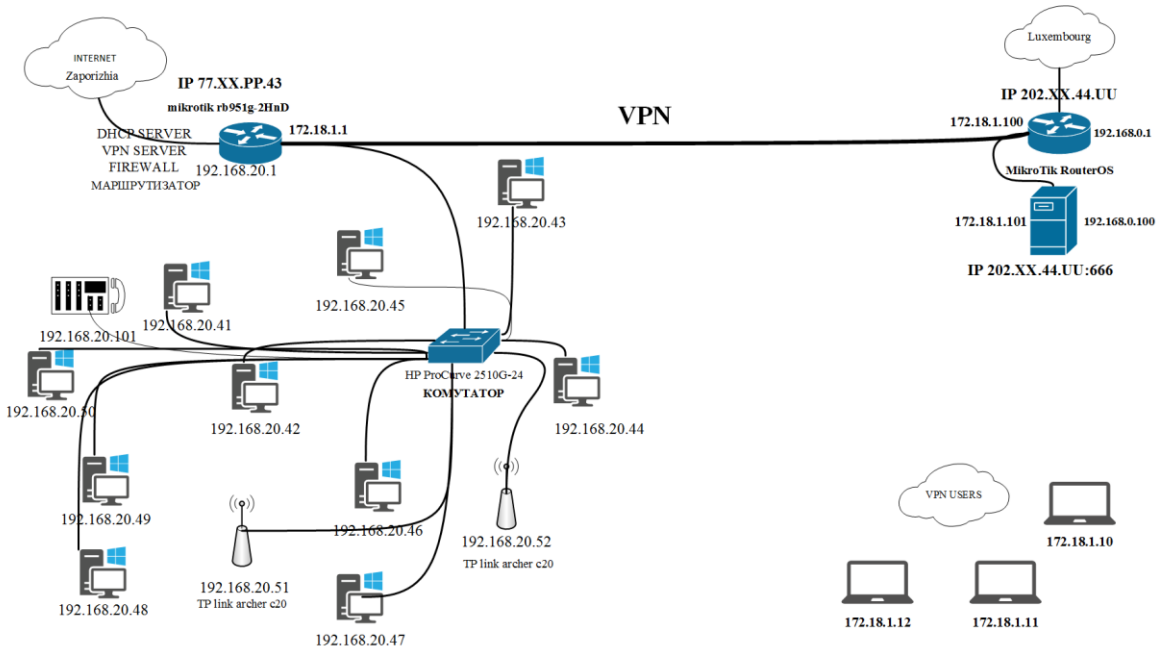

Рисунок 2.1 – Схема топології мережі

У компанії використовується різне мережеве обладнання. Повний перелік використовуваного обладнання наведено в таблиці 2.1

Мережева частина має ряд проблем:

- Головний маршрутизатор Mikrotik має завантаження процесора і оперативної пам'яті постійно на рівні 98–100% в більшості через firewall, але що одною причиною являється те що через карантин багато користувачів перейшли на віддалену роботу. Така загрузка для цього обладнання не є нормою і тягне за собою перебої в роботі інтернету та мережі, і передчасний вихід обладнання з ладу.
- Archer c20 працюють просто як точки доступу і користувачі, підключені до них, отримують адреси основної мережі маючи можливість підключатися до внутрішніх ресурсів мережі. Важливою особливістю є те що сигнал з них ловить поза зоною офісу організації.
- Доступ на сервера по RDP відкритий для всього інтернет порталу.

- Всі користувачі підключені по VPN мають доступ до локальної мережі підприємства.

Таблиця 2.1 – Мережеве обладнання

Приміщення	Обладнання	Призначення обладнання	IP адреса
Серверна	Маршрутизатор Mikrotik rb951g–2HnD	Підключення до Інтернет, VPN сервер та firewall	192.168.20.1 172.18.1.1
	Комутатор HP ProCurve 2510G–24	Підключення робочих місць користувачів	192.168.20.42
	GSM–шлюз Dinstar UC2000–VE–6G–B	Підключення провайдерів телефонії	192.168.20.101
Прийомна	Точка бездротового доступу (Wi–Fi) TP link archer c20	Для зручності користувачів використання телефонів	192.168.20.51
Основний зал	Точка бездротового доступу (Wi–Fi) TP link archer c20	Для зручності користувачів використання телефонів	192.168.20.52

2.2 Комп'ютерне та програмне забезпечення підприємства

Компанія закуповує б\у комп'ютерну і периферійну техніку з європейського корпоративного сегмента, комп'ютери йдуть разом з діючими ліцензіями на Windows 7 pro, більш докладна комп'ютерна комплектація в таблиці 2.2

Таблиця 2.2 – Комп'ютерна комплектація

Модель	процесор	пам'ять	Накопичувач	графіка	кількість
HP EliteDesk 800 G2 SFF	Intel Core i5–6500	16 GB DDR4	512 GB SSD	Intel HD Graphics 530	14
Acer Veriton N4640G	Intel Core i5–6400T	16 GB DDR4	128 GB SSD, 500 GB HDD	Intel HD Graphics 530	10
HP Slim Desktop PC 290–p0056	Intel Core i5–8400	8 GB DDR4	240 GB SSD	Integrated Intel UHD 630	10

Компанія орендує виділені потужності у хостингу Hetzner. Виділений сервер на якому розгорнут гіпервізор ESXI 6.0 і розміщені 6 серверів, список серверів представлений в таблиці 2.3

Програмна частина має ряд проблем:

- Не усі комп'ютери знаходяться у доменній групі, що дає користувачам можливість отримання неконтрольованого доступу.
- Операційні системи Windows 7 та Windows Server 2008 підтримку котрих Microsoft офіційно припинив, більше не отримують нових оновлень безпеки, не пишуть драйвера і програми. Данні операційні системи є ненадійними маючи уразливості, заходів щодо виправлення яких зроблено вже ніколи не буде.

Таблиця 2.3 – Перелік обладнання серверної групи

Найменування	ОС	Пам'ять (GB)	Накопичувач (TB)	Роль
Сервер активної директорії	Windows 2008 Server Enterprise	4	200GB	Управління користувачами і правами доступу.
Управлінський сервер	Windows 2008 Server Enterprise	64	2	Термінальний сервер
Бухгалтерський сервер	Windows 2008 Server Enterprise	48	2	Термінальний бухгалтерський сервер
Сервер ip телефонії	Centos 8	8	1	Сервер внутрішньої і зовнішньої ip телефонії
Сервер фінансового директора (FINDIR)	Windows 2012 Server Enterprise	16	1	Особистий віддалений робочий сервер
Файловий сервер	Windows 2008 Server Enterprise	8	4	Сервер зберігання робочих файлів

- Термінальний сервер бухгалтерії знаходиться не в доменній групі, деякі користувачі мають права адміністраторів, як наслідок повністю неконтрольована діяльність співробітників, що мають повний доступ до конфіденційної інформації.
- Всі бази даних 1с перебувають у файловому варіанті, роблячи бази абсолютно нічим не захищеними.

- Відсутній реплікатор контролера домену або його резервні копії. Відсутня можливість оперативного рішення, що призведе до простою роботи організації у разі несправності.
- Резервне копіювання інформації робиться не для всіх актуальних даних на сервері.
- Резервні копії зберігаються на цих же серверах.
- На сервері бухгалтерії головний бухгалтер використовує VPN сервіс з отриманням української адреси для входу у клієнт банк в зв’язку з підвищеною безпекою і необхідністю мати адресу своєї країни тим самим порушуючи роботу інших сервісів та співробітників на сервері.

3 ІНТЕГРАЦІЯ РІШЕНЬ ПО ОПТИМІЗАЦІЇ ТА ВІДМОВОСТІЙКОСТІ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

3.1 Міграція серверної групи

Серверна група потребує додаткових потужностей для додання двох серверів та збільшення потужності існуючих. Hetzner не дає можливості зміни конфігурації серверу, тому було прийнято рішення про міграцію серверної групи до України на своє обладнання. Це дає нам повний доступ і стовідсоткове управління серверним обладнанням, також підвищить швидкість передачі даних (у десять разів), тим самим роботи всієї інфраструктури, вирішить проблему з банками, і дасть можливість подальшого масштабування. З економічного боку приблизний термін окупності обладнання в порівнянні з щомісячною оплатою серверів Hetzner становить 1–2 роки.

3.1.1 Підбір серверного обладнання та його фізичне забезпечення

При підборі серверного обладнання треба було урахувати декілька основних моментів:

- Сервер має мати потужності, які серверна група займає зараз.
- Сервер має мати можливість бути доукомплектованим жорсткими дисками.
- Сервер має мати можливість бути доукомплектованим оперативною пам’яттю.
- Сервер має мати інтерфейс управління з веб-сторінки.
- Сервер має мати два блока живлення.
- Сервер має мати сучасне і високоякісне охолодження.

Під ці критерії було вибрано серверне обладнання HP ProLiant DL380p Gen8, яке ідеально підходить для потреб організації.

Технічні характеристики серверу наведено у табл.3.1.

Таблиця 3.1 – Технічні характеристики серверу

Тип процесора	2 x Intel Xeon E5–2680 v2(2.80 – 3.60 GHZ, ten core)
Кількість ядер	2 x 10
Кількість потоків	2 x 20
Обсяг пам'яті	256 GB 8*32
Максимальний обсяг пам'яті	768 GB
Кількість корзин	8
Кількість жорстких дисків	2 SSD по 1TB та 4 HDD 32TB
RAID–контролер	HP Smart Array P420i
Слоти для пам'яті	24
Блок живлення	2 x 750W
Управління інфраструктурою	Insight Control c ILO Advanced

Технічні особливості серверу:

- Функціональні можливості запобігають втраті даних, скорочують простої, спрощують обслуговування і включають у себе HP SmartDrives, HP Smart Socket Guide, набір напрямних "Snap and Go" і можливість доступу до компонентів без спеціальних інструментів.
- Технологія Integrated Lifecucle Automation забезпечує інтуїтивне управління системою С спрощеним виділенням ресурсів, ефективним

управлінням станом і оповіщенням, автоматичним обслуговуванням мікропрограм і ПЗ.

- Технологія Dynamic Workload Acceleration об'єднує системи зберігання даних, обчислювальні ресурси і процеси введення–виведення, забезпечуючи високу продуктивність і відмовостійкість.
- Технологія Automated Епегду Optimization економить місце, скорочує енергоспоживання і ресурси охолодження, необхідні при інтенсивному навантаженні, розширюючи простір центру обробки даних.
- Послуги HP Proactive Support забезпечують кращі в галузі показники швидкодії. HP iLO Management Engine включає HP iLO, HP Agentless Management, HP Active Health System, HP Intelligent Provisioning і вбудоване рішення віддаленої підтримки від HP.
- HP iLO Management Engine включає HP iLO, HP Agentless Management, HP Active Health System, HP Intelligent Provisioning і вбудоване рішення віддаленої підтримки від HP.
- HP Insight Online і HP Insight Remote Support забезпечують цілодобовий віддалений моніторинг, персональний доступ до вашої IT–інфраструктури і підтримку її стану в будь–який час.
- HP SmartUpdate прискорює розгортання і спрощує оновлення шляхом систематичного оновлення інфраструктури серверів в центрі обробки даних.
- HP Insight Control надає широкі можливості управління в рамках життєвого циклу інфраструктури вашого сервера HP ProLiant. Технологія HP iLO Advanced забезпечує розширені функції віддаленого сервера, зниження витрат на IT–відрядження і прискорення вирішення проблем.
- HP SmartMemory запобігає втраті даних і час простоїв з допомогою поліпшених засобів обробки помилок.

- Нова технологія HP SmartDrive підвищує зручність обслуговування і запобігає втраті даних завдяки таким функціям, як значок стану і індикатор "Не извлекать".
- Сімейство процесорів Intel Xeon E5 – 2600 забезпечує максимальну продуктивність, пам'ять, можливість підключення і пропускну здатність на кожен слот введення/виведення для ресурсоємних процесів.
- Вперше експлуатуються в тій галузі температурні ZD–датчики для точного управління вентиляторами серверів і його прямого охолодження, а також скоротившись непотрібних витрат на живлення вентиляторів і охолодження.
- Відповідають стандарту 80 + блоки живлення HP с загальним слотом забезпечують до 94% ефективності (Platinum) і підтримують послуги HP Power Discovery[7].
- Конфігурації серверів, що відповідають стандарту ENERGY STAR.

На рис.3.1 –рис.3.5 наведено зовнішній вигляд обладнання серверу.

Рисунок 3.1 – Передня панель з корзинами серверу hp proliant dl380p gen8

Рисунок 3.2 –Роз’єми серверу hp proliant dl380p gen8

Рисунок 3.3 – Комплектація серверу hp proliant dl380p gen8

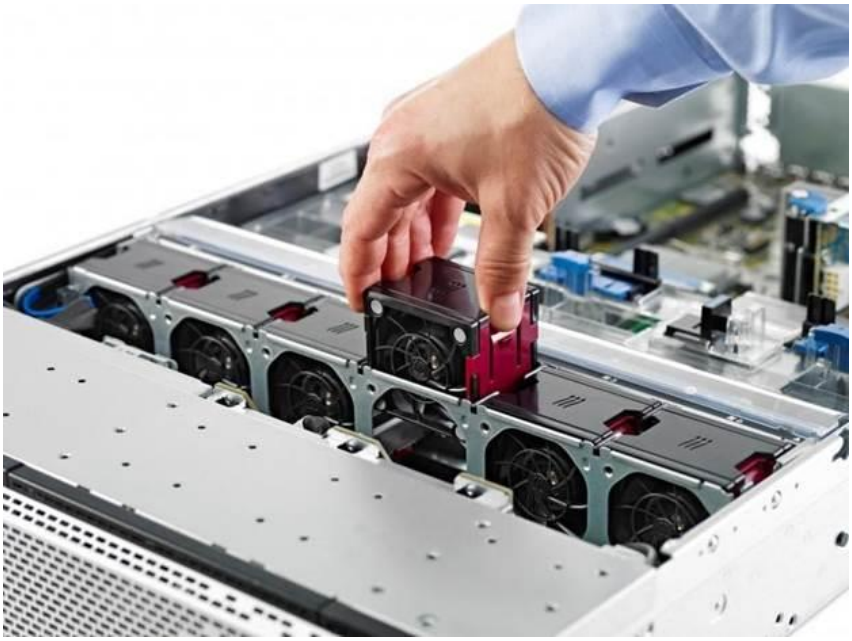

Рисунок 3.4 – Комплектація кулерів серверу HP proliant dl380p gen8

Під даний сервер було підібрано джерело безперебійного живлення Eaton 9SX.

Рисунок 3.5 – Джерело безперебійного живлення Eaton 9130 5000ВА

Таблиця 3.2 – Технічні характеристики джерела безперебійного живлення Eaton 9130 5000ВА

Виробник	USA
Тип архітектури	Безперервної дії (On–line)
Технологія	подвійне перетворення напруги з системою корекції коефіцієнта потужності (PFC)
Номінальна напруга	200/208/220/230/240 В
Діапазон вхідної напруги	176–276 В без зниження номінальної потужності
Вихідна напруга / THDU	200/208/220/230/240 в + / – 1%; THDU <2%
ККД	До 94% в режимі онлайн, 98% в режимі високої продуктивності
Допустиме перевантаження	102–110%: 120с, 110–125%: 60с, 125–150%: 10С, >150%: 500мс

Особливості Eaton 9130:

- ККД 9130 в режимі подвійного перетворення напруги досягає 95%, а в режимі високої ефективності–98%, що дозволяє скорочувати витрати на електроенергію;

- забезпечує велику потужність, займаючи при цьому менше місця, має коефіцієнт потужності 0,9, який дозволяє захищати велике навантаження, економлячи простір для установки іншого обладнання;
- графічний РК–дисплей з підтримкою російської мови допомагає легко робити настройки і забезпечує швидкий доступ до даних про статус ДБЖ;
- унікальна технологія АВМ продовжує термін служби батарей і оптимізує час їх підзарядки;
- має можливість підключатися до комп'ютерного обладнання та слідкувати за ним, може правильно виключати сервер при низькому заряді батареї.

До джерела безперебійного живлення підключено сервер, маршрутизатор, комутатор та GSM-шлюз. Це дає можливість безперебійної роботи при відключені світла та навіть інтернету, користувачі можуть і не здогадуватися відсутність цих факторів. Джерело безперебійного живлення налаштовано так, якщо ємність акумулятора батареї падає нижче 50 відсотків відправляє користувачам повідомлення про екстрене завершення роботи і зберігання своїх даних.

Вимоги до забезпечення фізичної безпеки серверного обладнання:

- доступ до зон, де обробляється або зберігається важлива інформація, повинен управлятися і бути обмежений тільки повноважними особами;
- засоби управління автентифікацією, наприклад, картка управління доступом плюс персональний ідентифікаційний номер [PIN], повинні використовуватися, щоб дозволяти і підтверджувати будь–який доступ;
- контрольний журнал всього доступу повинен міститися в надійному місці;
- персоналу допоміжних служб третьої сторони повинен бути наданий обмежений доступ в зони безпеки або до засобів обробки важливої інформації тільки тоді, коли потрібно;

- цей доступ повинен бути дозволений і повинен постійно контролюватися;
- права доступу в зони безпеки повинні регулярно аналізуватися і оновлюватися, і скасовуватися, якщо необхідно;
- повинні бути враховані відповідні норми і стандарти з техніки безпеки та охорони праці;
- ключові засоби повинні бути розташовані так, щоб уникнути доступу до них широкої публіки;
- там, де це може бути застосовано, будівлі та кімнати повинні бути скромними і повинні давати мінімальне вказівку на їх мету, без яскравих написів, зовні будівлі або всередині нього, що вказують на наявність видів діяльності з обробки інформації;
- покажчики та внутрішні телефонні книги, що вказують на місця розташування засобів обробки важливої інформації, не повинні бути легко доступні широкій публіці.

3.1.2 Перевірка серверних операційних систем на наявність проблем

Користувачи були позбавлені повного доступу на серверах, з серверів було видалено все програмне забезпечення, яке не стосується роботи. Також у цілях безпеки було використано Dr.Web CureIt. Це відмінний безкоштовний антивірус, котрий знаходить те, що інші антивіруси не бачать завдяки своєї актуальної бази вірусів, яка обновляється кожну годину. Ефективно лікує системи так само після зараження шкідливими вірусами. За цих причинах було вибрано це програмне забезпечення для перевірки серверної групи на віруси. Приклад перевірки на віруси утилітою від Dr.WEB curelt наведено на рисунку 3.6

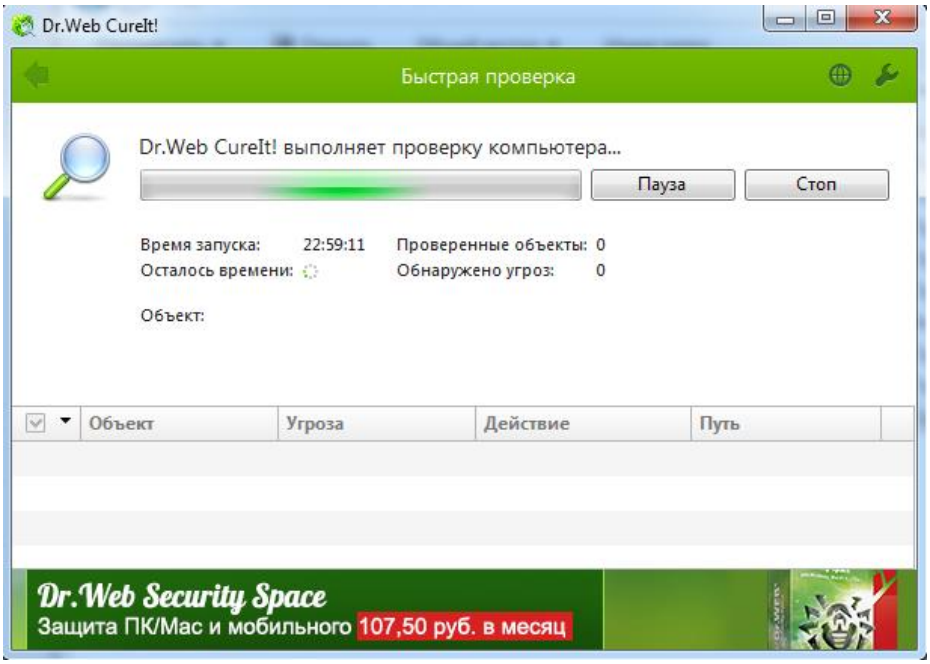

Рисунок 3.6 – Перевірка на віруси утилітою від Dr.WEB curelt.

3.1.3 Міграція серверної групи

На робочий комп’ютер було встановлено програмне забезпечення Veeam Backup & Replication та встановлено підключення до хостів VMWARE ESXI. Завантаження усієї серверної групи зайняло 2 дні.

На рис.3.7 наведено структуру виконання міграції.

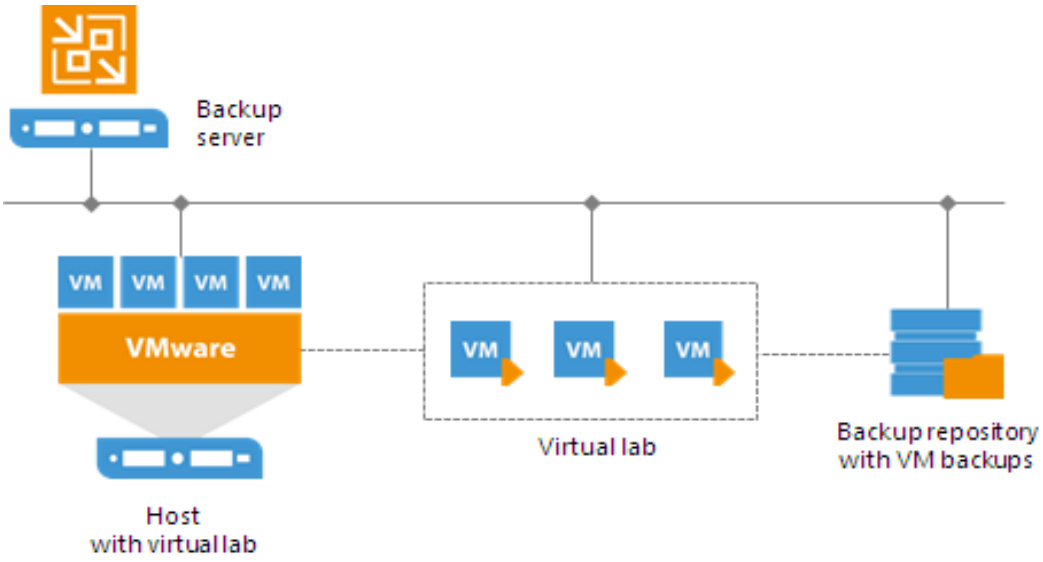

Рисунок 3.7 – Структура виконання міграції

3.1.4 Налаштування серверу HP ProLiant DL380p Gen8

Для серверу був обраний RAID 10, він виконує постійне дублювання даних з можливістю заміни накопичувача на гарячу і забезпечує швидке читання і запис даних.

На рис.3.8 наведено RAID 10.

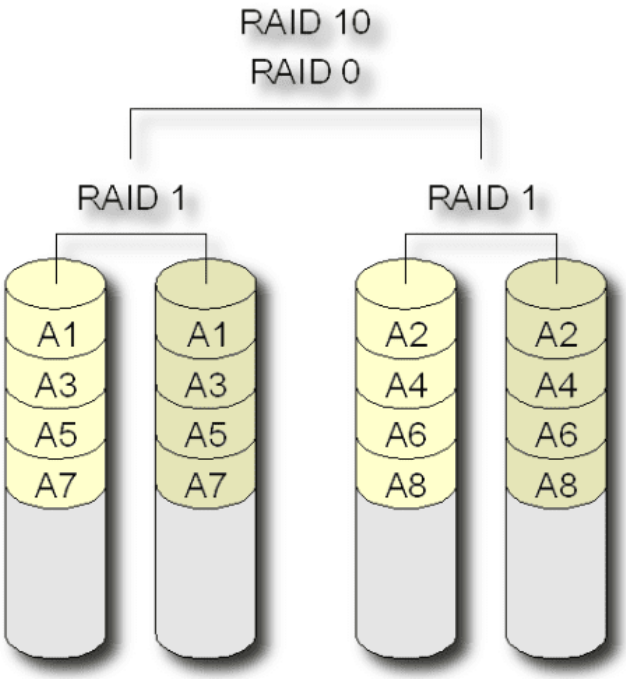

Рисунок 3.8 – RAID 10

На сервер було встановлено гіпервізор нової версії ESXI 6.5 і розгорнуто усю серверну групу.

3.2 Інтеграція рішень з вирішування мережевих проблем локально обчислювальної мережі

Зміна центрального маршрутизатора на модель Mikrotik RB4011iGS+RM. Це дозволить зняти навантаження з мережі і вирішить проблему з відключеннями користувачів по VPN. Ця модель має 4 ядра замість одного і 1 гігабайт оперативної пам'яті замість 250 мегабайт, він з легкістю витримає атаки на firewall, підключення користувачів і при цьому буде здатний масштабувати мережу виступаючи DHCP і VPN сервером для інших філіалів в майбутньому. Конфігуруємо мережу таким чином, дозволяючи отримання адресації тільки для певних мак адресів у мережі, у firewall маршрутизатора Mikrotik, залишаймо

можливість підключатися тільки з певних адрес і обмежуємо кількість спроб введення даних для VPN підключень до двох з наслідком блокування адреси на 72 години захищаючи так себе від перебору паролів.

На рис.3.9 наведено завантаженість нового маршрутизатора.

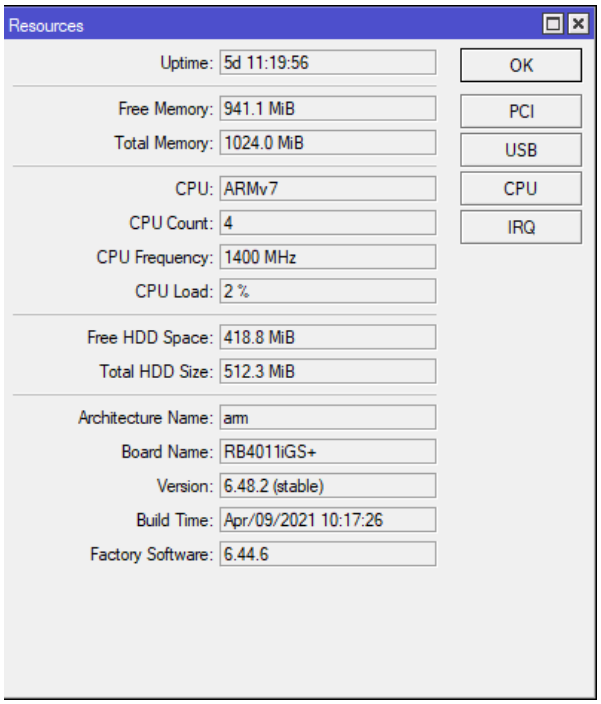

Рисунок 3.9 – Завантаженість нового маршрутизатора Mikrotik RB4011iGS+RM

Дві точки доступу archer c20 скинуті до заводських налаштувань, кабелі інтернету були перетknуті з порту LAN у порт WAN і налаштовані як гостьові мережі.

Головний маршрутизатор Mikrotik RB4011iGS+RM виступає у ролі DHCP серверу, VPN серверу та firewall. До нього на пряму підключено комутатор HP ProCurve 2510G–24 до якого підключено сервер, шлюз IP телефонії, дві точки доступу та комп’ютери локально розміщені на території офісу.. Віддалені користувачі також підключаються до головного маршрутизатору Mikrotik RB4011iGS+RM по VPN.

На рис.3.10 наведено оновлену схему топології мережи.

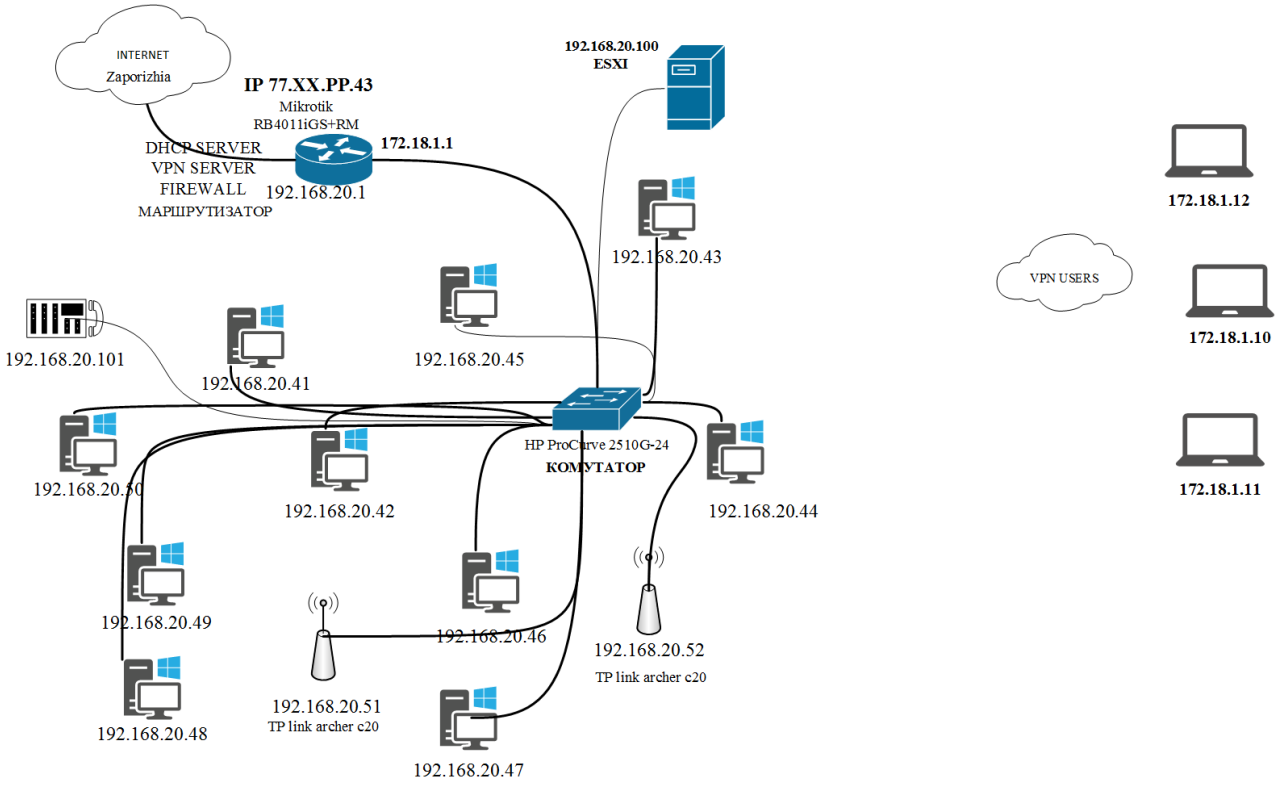

Рисунок 3.10 – Оновлена схема топології мережі

4 ІНТЕГРАЦІЯ РІШЕНЬ ДЛЯ ЗБІЛЬШЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1 Оптимізація операційних систем в домені

На один з комп’ютерів було встановлено систему Windows 10 pro, з використанням ключей ліцензій, встановлено стандартний набір програм і останнє оновлення 21H1, після чого зроблена резервна копія системи і розповсюджена на інші комп’ютери організації. Також було додано усі комп’ютери до доменної групи (рис.4.1).

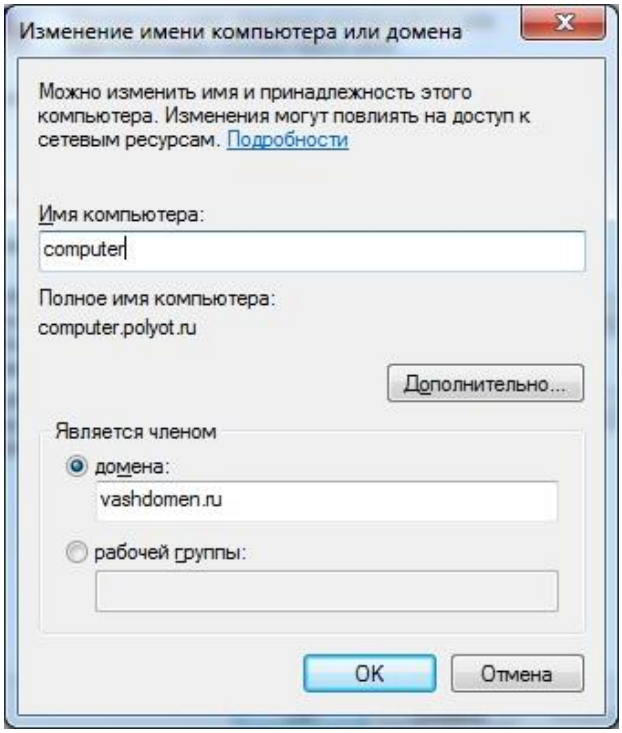

Рисунок 4.1 – Додання комп’ютеру в домен

Наступним кроком було оновлення серверних операційних систем до Windows server 2016 R2 Datacenter (рис.4.2, рис.4.3).

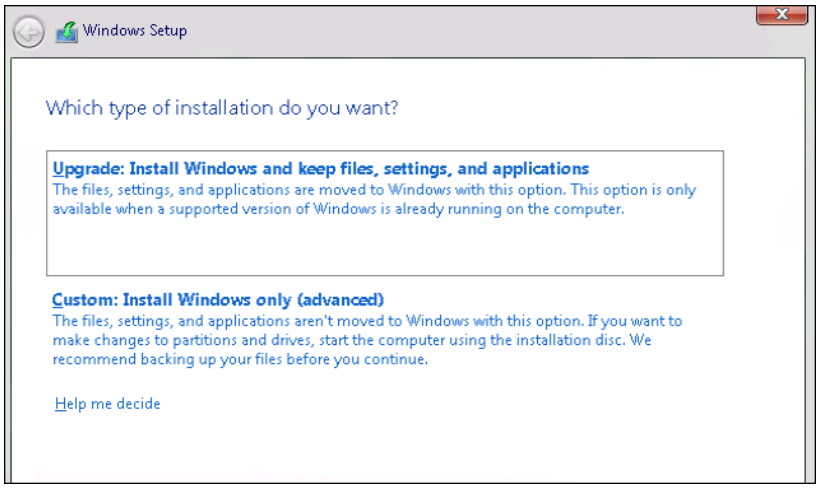

Рисунок 4.2 – Вибір оновлення серверної операційної системи

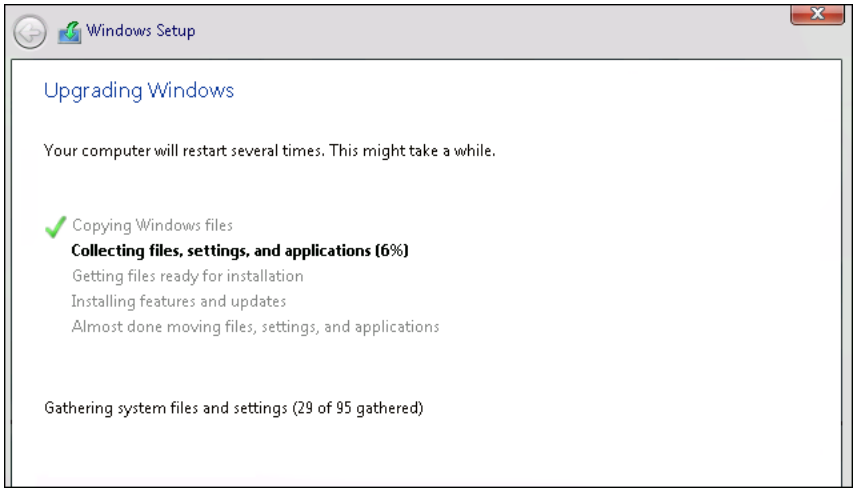

Рисунок 4.3 – Процес оновлення серверної операційної системи

4.2 Додання серверу баз даних до серверної групи

На операційній системі Windows 2016 Server Enterprise був розгорнутий сервер і на ньому підняті ролі 1с серверу та SQL Серверу. У SQL були додані усі бази даних підприємства натомість звичайного файлового варіанту.

На рис.4.4 наведено приклад реалізації клієнт–серверної архітектури

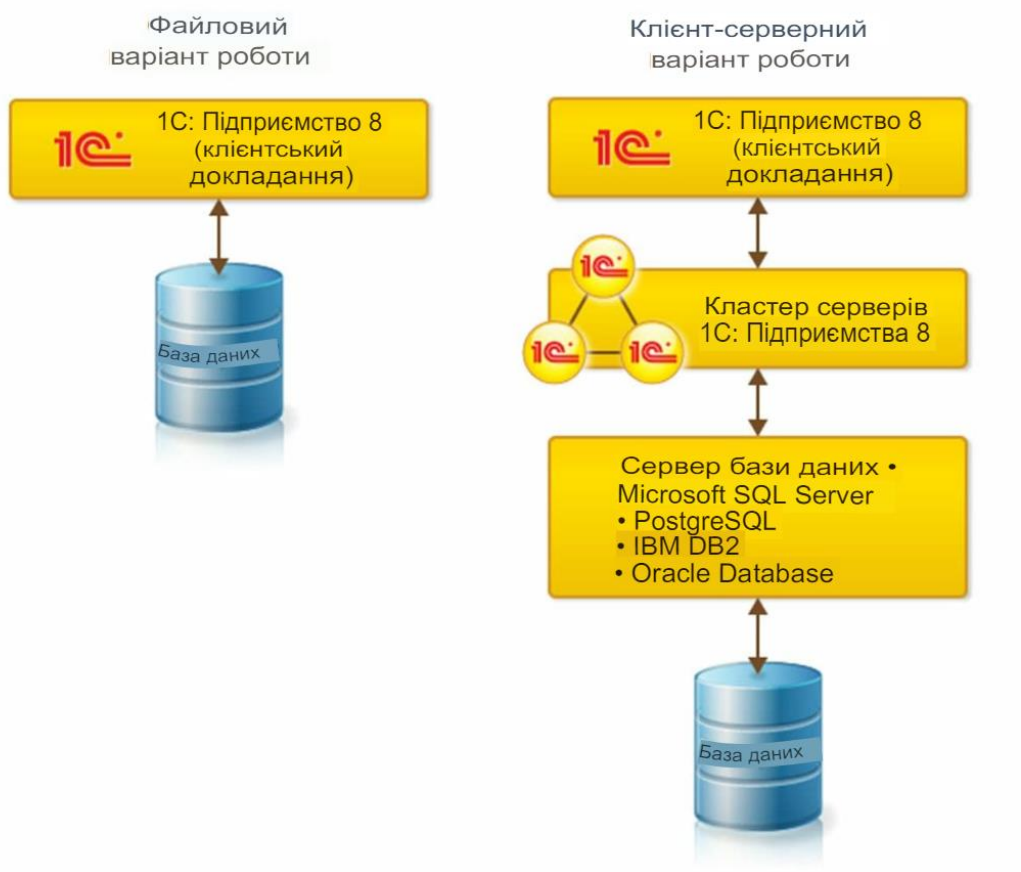

Рисунок 4.4 – Приклад реалізації клієнт–серверної архітектури

Базовий принцип захисту даних в клієнт–серверному варіанті полягає в тому, що користувачі не мають прямого доступу до файлів інформаційної бази. «Посередником» між клієнтами 1С: Підприємства 8.1 і сервером СУБД є робочий процес rphost, який звертається із запитом до СУБД від імені свого облікового запису. Потім отриманий результат повертає клієнту.

Комплексне поняття безпеки системи складається на основі її захищеності на різних ділянках. Можна виділити три основні ділянки захисту даних:

- Клієнт–кластер 1С: Підприємства
- Кластер 1С: Підприємства – СУБД
- Користувач системи

У табл.4.1 наведено алгоритм аудиту безпеки бази даних

Таблиця 4.1 – Алгоритм аудиту безпеки бази даних

Ймовірна загроза безпеці	Ділянка	Ймовірність	Наслідки	Ймовірний зловмисник	Трудомісткість
1	2	3	4	5	6
1. Доступ користувачів до адміністративних дій конфігуратора	клієнт	Висока	Копіювання всієї інформації	Програміст, просунутий користувач	Середня
2. Відсутність розмежувань доступу в режимі 1С: Підприємство"	клієнт	Середня	Копіювання ключової інформації	Програміст, просунутий користувач	Висока
3.Несанкціонований доступ до даних сервера СУБД	СУБД	Середня	Псування інформації, копіювання інформації	Адміністратор	Середня
4. Використання старих логінів	Клієнт, Кластер, СУБД	Низька	Наслідки залежать від прав облікового запису	Звільнений співробітник	Низька
5.Несанкціонований доступ до файлів кластера серверів	Кластер	Низька	Псування інформації, можливість створення нових баз	Адміністратор, програміст	Низька
6. Наявність вразливостей операційної системи, СУБД	Клієнт, Кластер, СУБД	Низька	Підвищення прав за допомогою ломалок, опублікованих в Інтернеті, можливе повне копіювання інформації	Адміністратор, просунутий користувач	Низька

Продовження таблиці 4.1 – Алгоритм аудиту безпеки бази даних

1	2	3	4	5	6
7. Віруси, трояни, логери	Клієнт, Кластер, СУБД	Низька	Псування інформації, отримання даних, розкриття паролів користувачів	Адміністратор, просунутий користувач	Низька
8. Паролі на моніторах, слабкі паролі	Клієнт	Середня	Несанкціонований доступ до облікових записів користувачів з подальшим доступом до даних	Просунутий користувач, звільнений співробітник	Низька
9. Перехоплення інформації	Клієнт–Кластер, Кластер–СУБД	Мінімальний	Перехоплення паролів з подальшим доступом до даних	Високо кваліфікований системний програміст, мережевий фахівець	Висока

Основні привила роботи з СУБД базами 1С:

- Облікові дані для підключення до СУБД не повинні мати адміністративних прав;
- Необхідно розмежовувати права доступу до баз СУБД, наприклад, створювати для кожної інформаційної бази свій обліковий запис, що дозволить мінімізувати втрату даних при зломі одного з облікових записів;
- Рекомендується обмежити фізичний і віддалений доступ до серверів баз даних і 1С Підприємства;
- Рекомендується використовувати шифрування для баз даних, це дозволить зберегти конфіденційні дані, навіть якщо зловмисник отримає фізичний доступ до файлів СУБД;
- Також одним з важливих рішень є шифрування або установка пароля на резервні копії даних;

- Обов'язковим є створення адміністраторів кластера 1С, а також сервера 1С, так як за замовчуванням якщо не створені користувачі, повний доступ до інформаційних баз отримують абсолютно всі користувачі системи.

4.3 Додання серверу резервних копій та оновлення серверної групи

Перелік обладнання серверної групи наведено у табл.4.2.

Таблиця 4.2 – Оновлена серверна група

Найменування	ОС	Процесор Intel Xeon E5–2680 v2	Пам’ять (GB)	Накопичувач (TB)	Роль
1	2	3	4	5	6
Сервер активної директорії	Windows 2016 Server Enterprise	2	4	200GB	Управління користувачами і правами доступу.
Управлінський сервер	Windows 2016 Server Enterprise	8	64	3	Термінальний сервер
Бухгалтерський сервер	Windows 2016 Server Enterprise	8	64	4	Термінальний бухгалтерський сервер

Продовження таблиці 4.2 – Алгоритм аудиту безпеки бази даних

1	2	3	4	5	6
Сервер ip телефонії	Centos 8	2	8	1	Сервер внутрішньої і зовнішньої ip телефонії
Сервер фінансового директора (FINDIR)	Windows 2016 Server Enterprise	4	16	1	Особистий віддалений робочий сервер
Файловий сервер	Windows 2016 Server Enterprise	2	8	4	Сервер зберігання робочих файлів
SQL сервер	Windows 2016 Server Enterprise	8	64	4	Сервер баз даних
Сервер резервних копій	Windows 2016 Server Enterprise	4	16	32	Сервер зберігання резервних копій

На сервері резервних копій було створено план резервних копій за допомогою програмного забезпечення Acronis True Image, детально вказаний в таблиці 4.3

Таблиця 4.3 – План резервного копіювання

Назва серверу	Тип копіювання	Час початку	Стиснення
Управлінський	Повний та інкрементний	Повна копія серверу в понеділок, середу, суботу в 19:00 та інкрементні копії кожен день	максимальне
Бухгалтерський	Повний та інкрементний	Повна копія в вівторок, четвер, неділю в 19:00 та інкрементні копії кожен день	максимальне
Файловий	Повний та інкрементний	Повна копія в п’ятницю в 20:00 та інкрементні копії кожен день	максимальне
Контролер домену	Повний	Повна копія кожну суботу в 23:00	максимальне
Сервер ір телефонії	повний	Кожну п’ятницю в 21:00	максимальне
Сервер фінансового директору	Повний та інкрементний	Повна копія кожну п’ятницю в 23:00 та інкрементні копії кожен день	максимальне
SQL	Повний	Повна копія серверу кожний день в 01:00	максимальне

Резервне копіювання серверів цілком обрано і зроблено для можливості швидкого розгорнення останньої актуальної копії у коротші часи. Перезапис резервних копій відбуваються кожні три копії.

4.4 Додаткові рішення для збільшення рівня інформаційної безпеки

Інтегруємо правила для усіх комп’ютерів в домені :

1) All Removable Storage Classes: Deny All Access (Знімні носії всіх класів: Заборонити будь доступ) – дозволяє повністю заблокувати доступ з комп'ютера до будь–яких типів зовнішніх пристроїв зберігання. Щоб увімкнути цю політику, відкрийте її та переведіть у стан Enable, наведено на рис.4.5

Зроблено для запобігання копіювання інформації на з ' ємні носії.

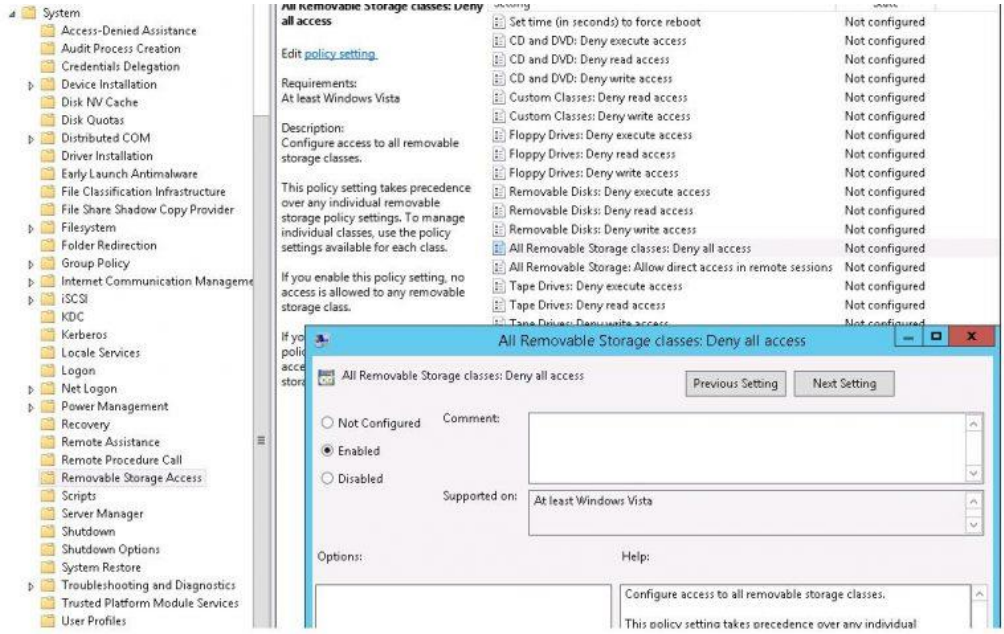

Рисунок 4.5 – Групова політика блокуюча з'ємні носії

2) Відключити буфер обміну у RDP сесіях на серверах. Do not allow Clipboard redirection (Clipboard redirection використовується для копіювання тексту і файлів через буфер обміну в RDP) , наведено на рис.4.6

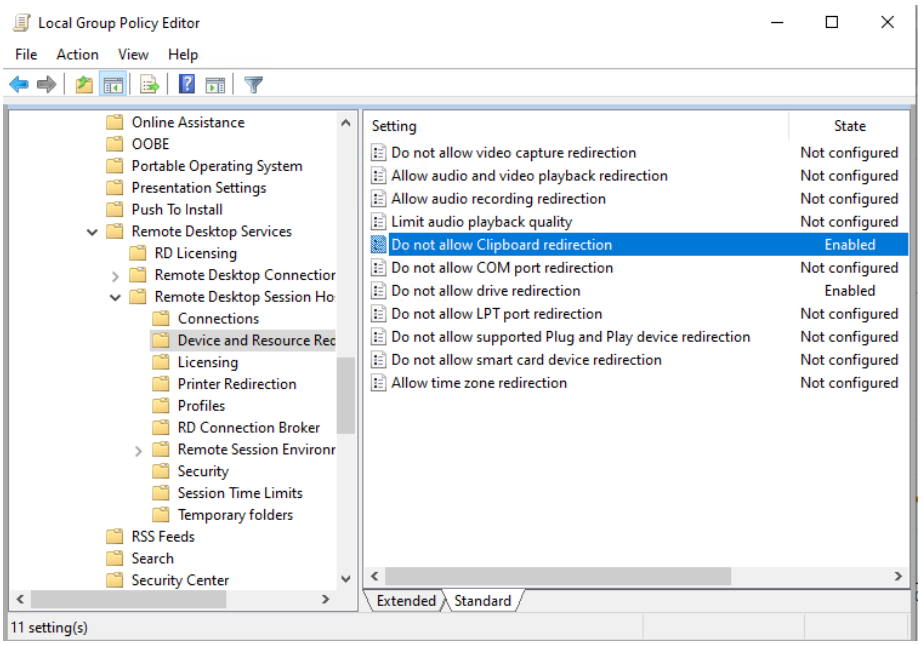

Рисунок 4.6 – Групова політика блокуюча буфер обміну

3) Включити правила політики паролів у домені:

- Вести журнал паролів (Enforce password history) – визначає кількість старих паролів, які зберігаються в AD, забороняючи користувачеві повторно використовувати старий пароль (однак адміністратор домену або користувач, якому делеговані права на скидання пароля в AD, може вручну задати для аккаунта старий пароль). Включити запам’ятовування останніх 24 паролів.
- Максимальний термін дії пароля (Maximum password age) – визначає термін дії пароля в днях. Після закінчення терміну дії пароля Windows зажадає у користувача змінити пароль. Забезпечує регулярність зміни пароля користувачами. Срок дії пароля – 42 дні.
- Мінімальна довжина пароля – Minimum password length) – не рекомендується робити пароль коротше, ніж 8 символів. Мінімальна довжина пароля – 7 символів.
- Пароль повинен відповідати вимогам складності (Password must meet complexity requirements) – при включенні цієї Політики користувачеві заборонено використовувати ім'я свого облікового запису в паролі (не більше ніж

два символи поспіль з username або Firstname), також в паролі повинні використовуватися 3 типи символів з наступного списку: цифри (0 – 9), Символи у верхньому регістрі, символи в нижньому регістрі, спец символи ($,#, % і т.д.). Крім того, для виключення використання простих паролів (зі словника популярних паролів) рекомендується періодично виконувати аудит паролів облікових записів домену, наведено на рис.4.7

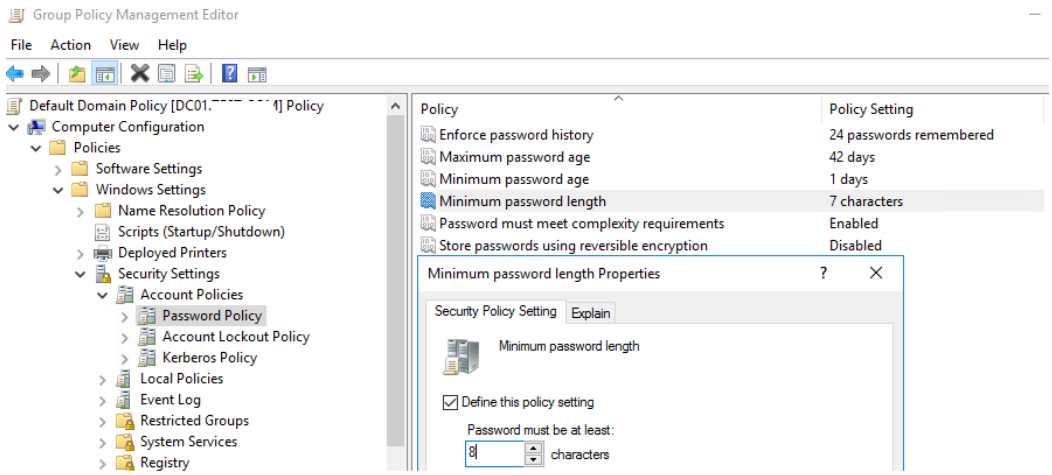

Рисунок 4.7 – групова політика паролів

4) Чітке розмежування доступів до робочої інформації.

5) Купівля та реєстрація свого почтового домену організації, зобов’язуючи співробітників користуватися саме цими почтовими скриньками для можливості контролю їх роботи.

6) За вимогою керівництва для деяких користувачів включити записи дзвінків.

7) Провести обучаючий курс для співробітників по основам інформаційної безпеки і донести важливість цього заходу.

На рис.4.9 наведено схему результатів виконаних робіт.

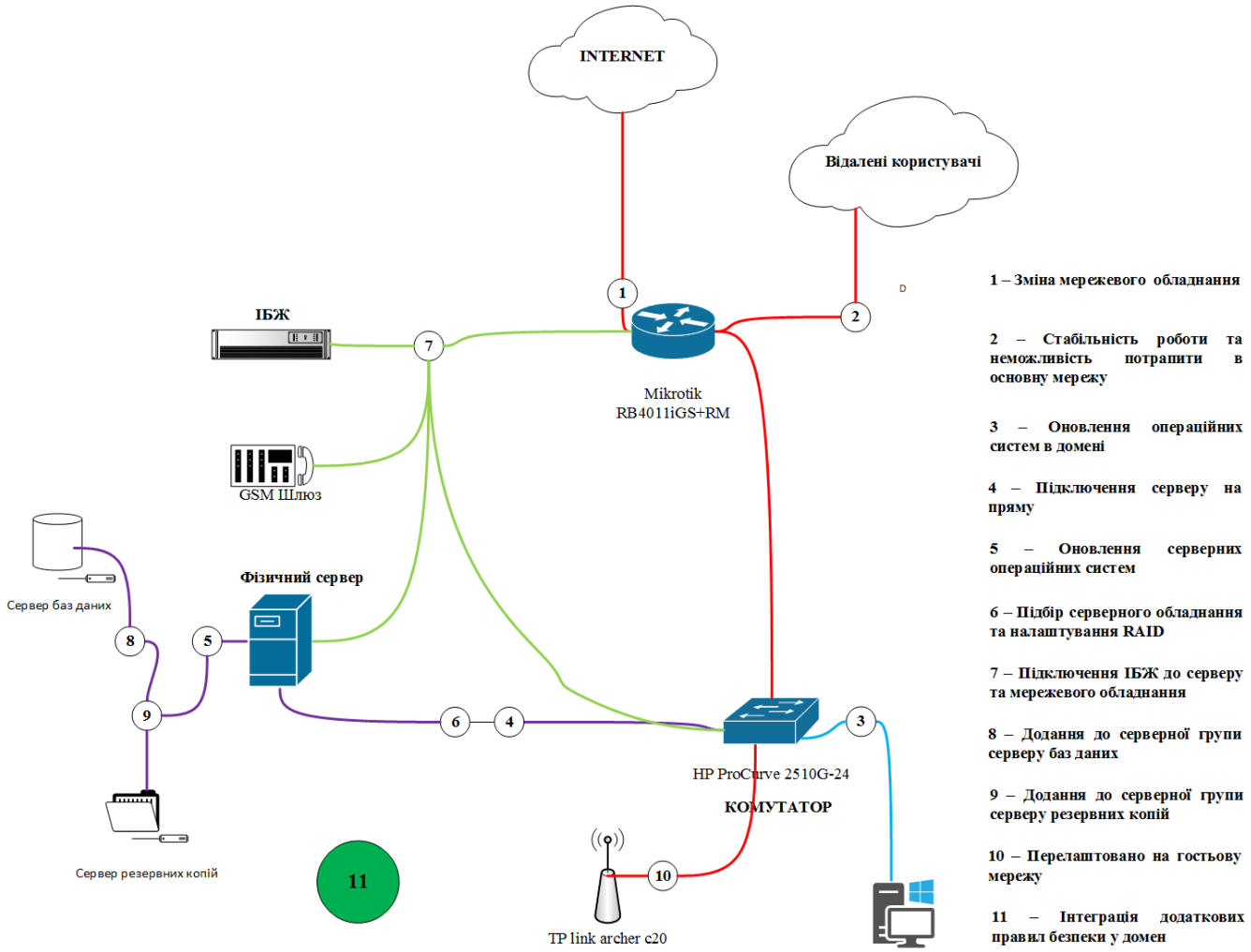

Рисунок 4.9 – схема результатів виконаних робіт

5. АЛГОРИТМ ТА МОДЕЛЬ ІНФОРМАЦІЙНО ЗАХИЩЕНОГО ПІДПРИЄМСТВА

Спочатку здобувається вся технічна документація побудови мережі та доступи до усього обладнання яке обслуговує спеціаліст. Інформація перевіряється на актуальність методом аудиту технічної, програмної та мережевої частини підприємства. Проводиться аналіз результатів аудиту технічної, програмної, мережевої частин та їх праця в комплексі, в ході якого виявляється список проблем та підготовлюється план з інтеграції рішень для їх вирішення. План узгоджується та проводяться підготовчі роботи, після цього проводяться роботи по інтеграції рішень технічної, програмної, мережевої частин стосовно оптимізації роботи підприємства. Перевіряються результати проведених робіт та вже у відмовостійке середовище інтегруються правила стосовно збільшення рівня інформаційної безпеки.

Алгоритм створення інформаційно безпечного підприємства наведено на рис.5.1

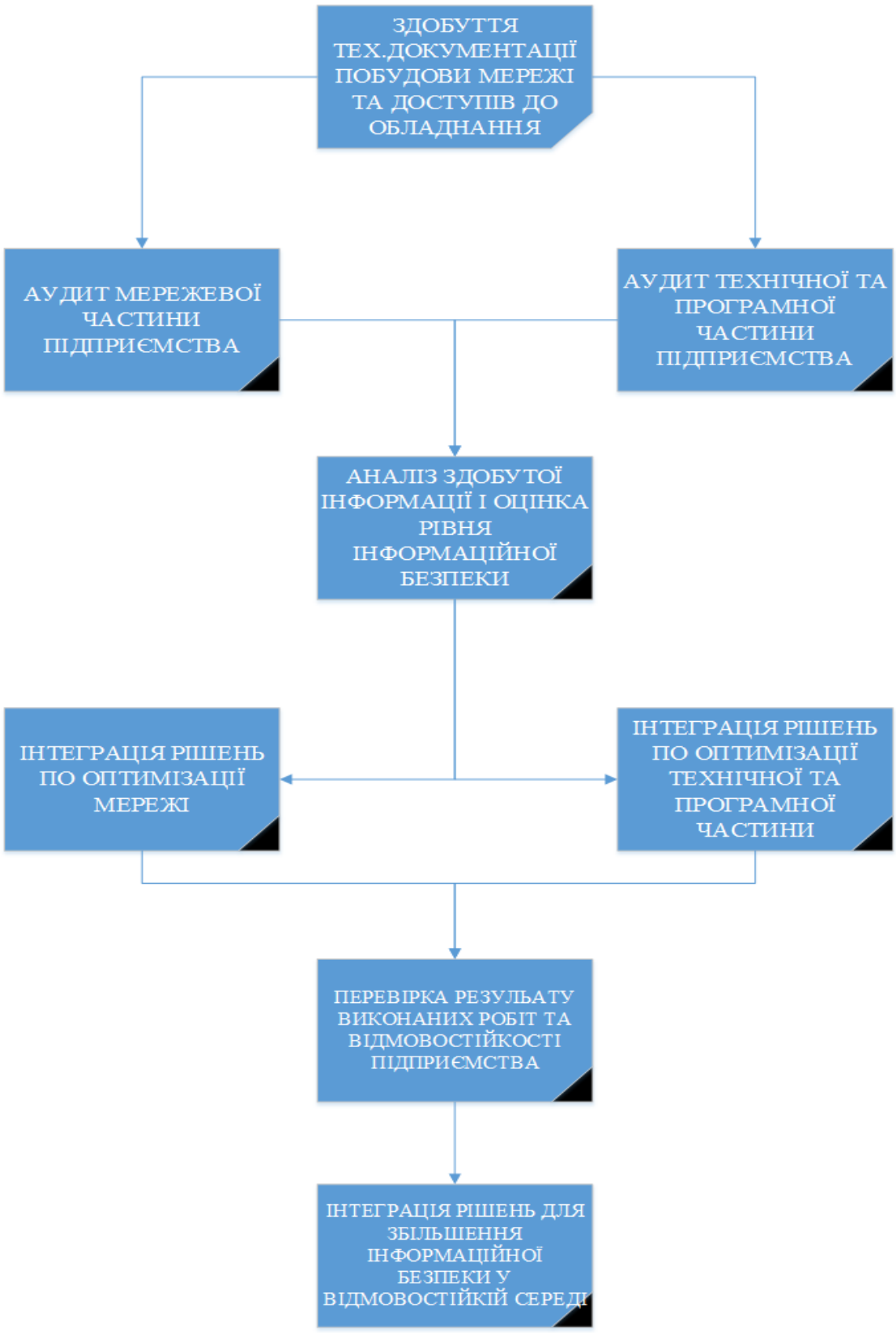

Рисунок 5.1 – Алгоритм створення інформаційно безпечного підприємства

Модель інформаційно захищеного підприємства втілює у собі оптимізовану та відмовостійку до усіх основних ризиків мережеву інфраструктуру підприємства. Захищену від зовнішніх спроб здобуття доступу до мережі та захищена з середини чітко прописаними правами користувачів на різних рівнях авторизації. Відмовостійку до втрати електронапруги та інтернету. Маючи декілька рівнів резервного копіювання даних та відмовостійку до відказу операційної системи чи фізичних носіїв.

Модель інформаційно захищеного підприємства наведено на рис.5.2

Рисунок 5.2 – Модель інформаційно захищеного підприємства

Модель інформаційно захищеного підприємства втілює у собі оптимізовану та відмовостійку до усіх основних ризиків мережеву інфраструктуру підприємства. Захищену від зовнішніх спроб здобуття доступу до мережі та захищена з середини чітко прописаними правами користувачів на різних рівнях авторизації. Відмовостійку до втрати електронапруги та інтернету.

Маючи декілька рівнів резервного копіювання даних та відмовостійку до відказу операційної системи чи фізичних носіїв.

ВИСНОВКИ

Рівень розвитку інформаційних неминуче веде за собою і збільшення загроз, збільшуючи необхідність в засобах інформаційної безпеки все більш широкому колу користувачів.

В результаті дипломного проектування розроблено модель інформаційно захищеного підприємства та алгоритм забезпечення інформаційної безпеки підприємства, що дозволяє спеціалістам, які працюють у організаціях, що потребують оптимізації та збільшення рівня інформаційної безпеки керуючись моделлю та алгоритмом досягти необхідного рівня інформаційної безпеки на своєму підприємстві. Керуючись моделлю та алгоритмом з'являється можливість значно заощадити час, який раніше люди витрачали на вирішення питань, пов'язаних з інформаційною безпекою, але так її і не досягали.

Модель та алгоритм створено у результаті пророблено роботи на реальному підприємстві, завдяки чому підкреслено практичну значимість отриманних результатів для організації будь якого рівня та масштабу.

Модель та алгоритм мають просту структуру, що враховує особливості сприйняття і переробки інформації, а також аспекти роботи спеціаліста з інформаційною безпекою. Це зменшує час освоєння моделі та алгоритму і підвищує загальну продуктивність роботи спеціалісту.

Загалом у кваліфікаційній роботі бакалавра:

– проведено аудит мережевої, технічної та програмної частини підприємства;

– проведено аналіз здобутої інформації стосовно мережевої, технічної та програмної частини підприємства;

– інтегровані рішення по оптимізації та збільшенню відмовостійкості мережевої інфраструктури підприємства;

– інтегровані рішення безпеки збільшуючи рівень інформаційної безпеки на підприємстві;

– проведена розробка моделі інформаційно захищеного підприємства та алгоритму з досягнення інформаційної безпеки підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Информационная безопасность [Електронний ресурс]. — Режим доступу: https://bcs.kiev.ua/infosecurity

2. Информационная безопасность на предприятии [Електронний ресурс]. — Режим доступу: https://tvoi.biz/biznes/informatsionnaya–bezopasnost/informatsionnaya–bezopasnost–na–pred.html

3. Информация как объект правовых отношений [Електронний ресурс]. — Режим доступу: http://www.consultant.ru/document/cons_doc_LAW_61798/c3b53a3601408c50895476568264472cfd0a83bc/

4. Угрозы информационной безопасности [Електронний ресурс]. — Режим доступу: https://www.anti–malware.ru/threats/information–security–threats

5. Комплексная защита информации на предприятии [Електронний ресурс]. — Режим доступу: http://rus.safensoft.com/security.phtml?c=791

6. Сколько стоит информационная безопасность [Електронний ресурс]. — Режим доступу: https://www.ptsecurity.com/ru–ru/research/analytics/is–cost–2017/

7. Сервер HP ProLiant DL380p Gen8 [Електронний ресурс]. — Режим доступу: https://servak.com.ua/servers/server–hp–proliant–dl380p–g8–sff–25–bays.html

8. Вопросы безопасности информационных систем на платформе 1С:Предприятие 8.1 [Електронний ресурс]. — Режим доступу: https://its.1c.ru/db/metod8dev/content/5816/hdoc