Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістр

студента *Петраш Євгеній Ігорович*

академічної групи *125м-22-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Аналіз та підвищення рівня захищеності інтернет-зв'язку підприємства «FixUp»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ас. Рибальченко Ю.П.			
економічний	к.е.н., доц. Пілова Д.П.	90	відмінно	

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.
«_____» _____ 2023 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістр

студенту *Петрашу Євгенію Ігоровичу* **академічної групи** *125м-22-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації[1] _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Аналіз та підвищення рівня захищеності інтернет-зв'язку ПІДПРИЄМСТВА «FixUp»*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.2023 №1227-с

Розділ	Зміст	Термін виконання
Розділ 1	СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ. Аналіз поточного рівня захищеності мережі та розгляд методів підвищення рівня захищеності мережі	27.09.2023 – 06.10.2023
Розділ 2	СПЕЦІАЛЬНА ЧАСТИНА. Оновлення мережевого обладнання та впровадження системи запобігання вторгнень	07.10.2023 – 15.11.2023
Розділ 3	ЕКОНОМІЧНИЙ РОЗДІЛ. Визначення та аналіз економічної ефективності системи захисту інтернет-мережі	16.11.2023 – 24.11.2023

Завдання видано _____ Тетяна КАГАДІЙ
(підпис керівника) (ім'я, призвище)

Дата видачі завдання: 21.09.2023 р.

Дата подання до екзаменаційної комісії: 30.11.2023 р.

Прийнято до виконання _____ Євгеній ПЕТРАШ
(підпис студента) (ім'я, призвище)

РЕФЕРАТ

Пояснювальна записка: 96 с., 22 рис., 15 табл., 4 додатки, 22 джерел.

Об`єкт дослідження: мережа інтернет-зв'язку підприємства «FixUp».

Мета роботи: підвищення рівня захисту інтернет-зв'язку в інформаційно-комунікаційній системі підприємства «FixUp».

Методи розробки: спостереження, порівняння, аналіз, опис.

У першому розділі проводиться аналіз сучасного стану кіберзахищеності об'єктів інформатизації та визначено стратегічний напрямок підвищення рівня безпеки в умовах постійно зростаючих загроз кібербезпеки. Проаналізована нормативно-правова база, що регулює сферу захисту інформації, з метою визначення ключових вимог та стандартів, які будуть визначати стратегічний курс у забезпеченні інформаційної безпеки.

У спеціальній частині було проведено дослідження переваг використання більш професійного мережевого обладнання з функцією системи запобігання вторгненням, яке показало, що нове запропоноване обладнання демонструє високий рівень захищеності мережі та відмовостійкості.

В економічному розділі наведені розрахунки та обґрунтування всіх заходів, спрямованих на вдосконалення та аналіз економічної ефективності захищеності інтернет-мережі.

Практичне значення роботи полягає у підвищенні рівня захищеності інтернет-зв'язку в інформаційно-комунікаційній системі підприємства «FixUp».

ІНФОРМАЦІЙНА БЕЗПЕКА, ІДЕНТИФІКАЦІЯ, ІНФОРМАЦІЙНИЙ АКТИВ, КІБЕРБЕЗПЕКА, РЕЄСТР ІНФОРМАЦІЙНИХ АКТИВІВ.

ABSTRACT

Explanatory note: 96 p., 22 fig., 15 tab., 4 appendices, 22 sources.

The object of the work: Internet communication network of enterprise «FixUp».

The purpose of the work: increasing the level of Internet communication protection in the information and telecommunication system of «FixUp» enterprise.

Development methods: observation, comparison, analysis, description.

In the first section, the current state of cyber security of informatization objects is analyzed and the strategic direction of increasing the level of security in the conditions of constantly growing cyber security threats is determined. The legal framework governing the field of information protection was analyzed in order to determine the key requirements and standards that will determine the strategic course in ensuring information security.

In a special part, a study of the advantages of using more professional network equipment with the function of an intrusion prevention system was carried out, which showed that the new proposed equipment demonstrates a high level of network security and fault tolerance.

The economic section provides calculations and justification of all measures aimed at improving and analyzing the economic effectiveness of Internet network security.

The practical significance of the work consists in increasing the level of security of Internet communication in the information and communication system of the enterprise "FixUp".

INFORMATION SECURITY, IDENTIFICATION, INFORMATION ASSET, CYBERSECURITY, INFORMATION ASSET REGISTER.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ – державний стандарт України;

КЗ – контрольована зона;

КС – комп'ютерна система;

НД ТЗІ – нормативний документ в галузі технічного захисту інформації;

ОІД – об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ІЗоД – інформація з обмеженим доступом;

ІТС – інформаційно-комунікаційна система;

DoS – Denial-Of-Service Attack (атака на відмову в обслуговуванні);

DDoS – Distributed Denial-Of-Service Attack (розподілена атака на відмову в обслуговуванні);

FTP – File Transfer Protocol (протокол передавання файлів);

HTTP – HyperText Transfer Protocol (протокол передачі гіпертекстових документів);

HTTPS – HyperText Transfer Protocol Secure (захищений протокол передачі гіпертекстових документів);

IDS – Intrusion Detection System (система виявлення вторгнень);

IPS – Intrusion Prevention System (система запобігання вторгнень);

LAN – Local Area Network (локальна мережа);

PoE – Power-over-Ethernet (живлення по мережі Ethernet);

SIEM – Security information and event management;

TFTP – Trivial File Transfer Protocol (тривіальний протокол передачі файлів);

VPN – Virtual Private Network (віртуальна приватна мережа);

WAN – Wide Area Network (глобальна мережа);

WPS – Wi-Fi Protected Setup (захищене налаштування Wi-Fi);

ЗМІСТ

ВСТУП

В епоху високих технологій і швидкого розвитку інтернет-зв'язку, питання кібербезпеки стає надзвичайно актуальним і стратегічно важливим для різноманітних сфер діяльності, включаючи обслуговування електроніки та роздрібну торгівлю аксесуарами. Однією з організацій, яка надає послуги ремонту телефонів і планшетів, а також торгівлі чохлами, є підприємство «FixUp». Збільшення обсягів обробки конфіденційної інформації клієнтів та інтенсивність ведення бізнес-спілкування через інтернет робить їхню корпоративну мережу особливо вразливою до кіберзагроз.

У світлі непередбачуваних та високотехнологічних кіберзагроз, які можуть призвести до втрати конфіденційної інформації, порушення послуг та інших серйозних наслідків, питання захищеності інтернет-зв'язку стає невідкладним завданням. Наявність цифрових даних, що стосуються клієнтів і підприємницької діяльності, підвищує значущість вивчення та вдосконалення методів захисту, щоб уникнути потенційних загроз та залишитися невразливими перед високотехнологічними атаками.

Задачами дослідження є ретельний аналіз поточного стану захищеності інтернет-зв'язку підприємства «FixUp», визначення загроз та атак, які можуть бути спрямовані на корпоративну мережу, розгляд засобів моніторингу та відстеження безпеки для своєчасного виявлення можливих загроз, аналіз і визначення поточних заходів та їх ефективність у захисті мережі та класифікація і оцінка засобів забезпечення безпеки для подальшого використання.

Це дослідження є важливим не лише для безпеки інтернет-зв'язку підприємства «FixUp», але й для підприємств подібного профілю. Отримані результати стануть основою для вдосконалення стратегій безпеки та захисту інформації в умовах постійної кіберзагрози.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Вступ

Сучасний бізнес, особливо інформаційно-технічні сервісні центри, повинен управлятися не лише складністю власних операцій, але й високими ризиками, пов'язаними із кіберзагрозами. У даному контексті, підприємство «FixUp» виступає ключовим гравцем у галузі ремонту та обслуговування комп'ютерної та мобільної техніки. Забезпечення безпеки інформації та засобів обробки даних стає стратегічним завданням для збереження стабільності підприємства та надійності в очах клієнтів.

Підприємство «FixUp» спеціалізується на наданні послуг ремонту та обслуговування технічних пристроїв. Ця компанія функціонує у двох ключових напрямах: ремонт та технічне обслуговування комп'ютерів і мобільних пристроїв, а також інтернет-магазин, що спеціалізується на продажу запчастин та аксесуарів для ремонту техніки. Це важливо враховувати при розгляді системи кіберзахисту, оскільки обидва напрями взаємодіють у сфері обробки конфіденційної інформації.

З кожним роком загрози кібербезпеки стають більш складними та винахідливими. Для компаній, таких як підприємство «FixUp», які зберігають конфіденційні дані про клієнтів, проводять фінансові операції та управляють внутрішніми процесами, розробка ефективної стратегії кіберзахисту стає необхідністю. З урахуванням стрімкого розвитку цифрових технологій та збільшення кількості кібератак, необхідно систематично оновлювати та удосконалювати заходи безпеки.

Згідно аналітичного звіту Держспецзв'язку України за І півріччя 2023 року, упродовж січня-червня 2023 року кількість кібератак проти України зросла до 762 зареєстрованих інцидентів, що більше ніж удвічі за показники ІІ половини минулого року. Водночас кількість критичних кібератак за цей період зменшилася на 81% – до 27 критичних інцидентів, що свідчить про покращення захисту.

Обрана тема дослідження виникла з потреби докладного аналізу та вдосконалення системи кіберзахисту ІТС підприємства «FixUp». Необхідно переоцінити існуючі заходи безпеки, визначити потенційні ризики та розробити

нові стратегії для підвищення рівня безпеки. З розвитком кіберзагроз та з'явою нових векторів атак, актуалізація цього завдання стає необхідною умовою для збереження стабільності бізнесу.

Основною метою даного дослідження є ретельний аналіз поточного стану кіберзахищеності ІТС підприємства «FixUp» та розробка ефективних заходів для підвищення рівня безпеки. Завдання включають в себе вивчення існуючих технічних та організаційних заходів, їх аналіз ефективності конкретних рекомендацій для подальшого удосконалення системи кіберзахисту.

1.1.1. Аналіз сучасного стану кіберзахищеності ІТС

Однією з ключових загроз є можливість несанкціонованого доступу до інформації. Зловмисники можуть спробувати використати слабкі місця в мережі або вразливості програмного забезпечення для незаконного отримання конфіденційних даних. Для протидії цій загрозі необхідно здійснювати регулярний моніторинг мережі, оновлювати програмне забезпечення та використовувати механізми автентифікації.

Було детально розглянуто, яка інформація циркулює в ІТС підприємства «FixUp»:

- Організаційно-розпорядча інформація:

Зберігання та обробка: Організаційно-розпорядча інформація, яка включає в себе документацію та дані про організаційну структуру та управління, зберігається на комп'ютерах менеджера (ПК-1) та бухгалтера (ПК-4). Ця інформація може бути редагована за потреби менеджером та бухгалтером.

Доступ та поширення: За потреби організаційно-розпорядча інформація може поширюватися серед майстрів з ремонту через локальну мережу або корпоративну електронну пошту. Контрольований доступ та визначення рівнів прав доступу гарантують, що інформація надається тільки уповноваженим особам.

Види зберігання: Організаційно-розпорядча інформація зберігається в двох форматах: паперовому та електронному. Електронний формат забезпечує зручний

доступ та редагування, тоді як паперовий формат може використовуватися як резервне копіювання.

- Бухгалтерська звітність:

Зберігання та обробка: Бухгалтерська звітність обробляється та зберігається на комп'ютері бухгалтера (ПК-4). Це включає в себе дані про фінансовий стан компанії та бухгалтерські документи.

Доступ та поширення: Для забезпечення обмеженого, але необхідного доступу, бухгалтерська інформація може поширюватися до комп'ютера менеджера (ПК-1) через локальну мережу чи корпоративну електронну пошту. Доступ контролюється за допомогою відповідних прав.

Види зберігання: Інформація бухгалтерської звітності зберігається в паперовому та електронному форматах, надаючи гнучкість у виборі джерела під час роботи чи аудиту.

- Фінансова звітність:

Зберігання та обробка: Інформація фінансової звітності обробляється та зберігається на комп'ютері бухгалтера (ПК-4) та включає дані про прибутки, витрати та інші фінансові аспекти діяльності.

Доступ та поширення: Для потреб менеджера (ПК-1) інформація може бути поширена через локальну мережу або електронну пошту. Контроль доступу має важливе значення для забезпечення конфіденційності.

Види зберігання: Фінансова інформація зберігається в паперовому та електронному форматах, забезпечуючи надійність та доступність.

- Інформація про співробітників:

Зберігання та обробка: Дані про співробітників зберігаються на комп'ютері бухгалтера (ПК-4) та включають в себе особисті та кадрові дані.

Доступ та поширення: Інформація може поширюватися за потреби через локальну мережу чи електронну пошту. Контроль доступу важливий для збереження конфіденційності.

Види зберігання: Інформація про співробітників зберігається в обох форматах – паперовому та електронному.

- Інформація про клієнтів:

Зберігання та обробка: Інформація про клієнтів обробляється та зберігається на комп'ютері менеджера (ПК-1). Ця інформація може включати особисті дані та історію обслуговування.

Доступ та поширення: За потреби інформація може бути поширена до бухгалтера (ПК-4) через локальну мережу або електронну пошту.

Види зберігання: Інформація про клієнтів зберігається в паперовому та електронному форматах для забезпечення зручного доступу та редагування.

- Інформація про вартість послуг та товарів:

Зберігання та обробка: Інформація про вартість послуг та товарів обробляється та зберігається на комп'ютері менеджера (ПК-1).

Доступ та поширення: Інформація може поширюватися до бухгалтера (ПК-4) за потреби через локальну мережу або електронну пошту.

Види зберігання: Інформація про вартість послуг та товарів зберігається виключно в електронному форматі для забезпечення швидкого та зручного доступу.

- Інформація про ремонтні роботи:

Зберігання та обробка: Інформація про ремонтні роботи зберігається та редагується на комп'ютері менеджера (ПК-1) і поширюється до комп'ютерів майстрів з ремонту (ПК-2 та ПК-3) через локальну мережу.

Доступ та поширення: Дані можуть поширюватися серед майстрів для координації та узгодження робіт.

Види зберігання: Інформація про ремонтні роботи зберігається виключно в електронному форматі для забезпечення ефективного керування та зручного доступу.

Ця ретельна категоризація дозволяє легше розуміти, як інформація обробляється та розповсюджується в межах ІТС підприємства «FixUp».

Умовні позначення:

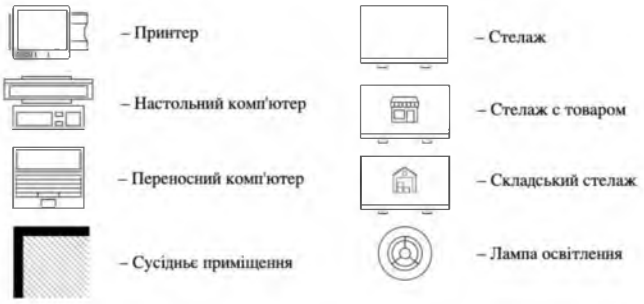


Рисунок 1.1 – Генеральний план. Загальний

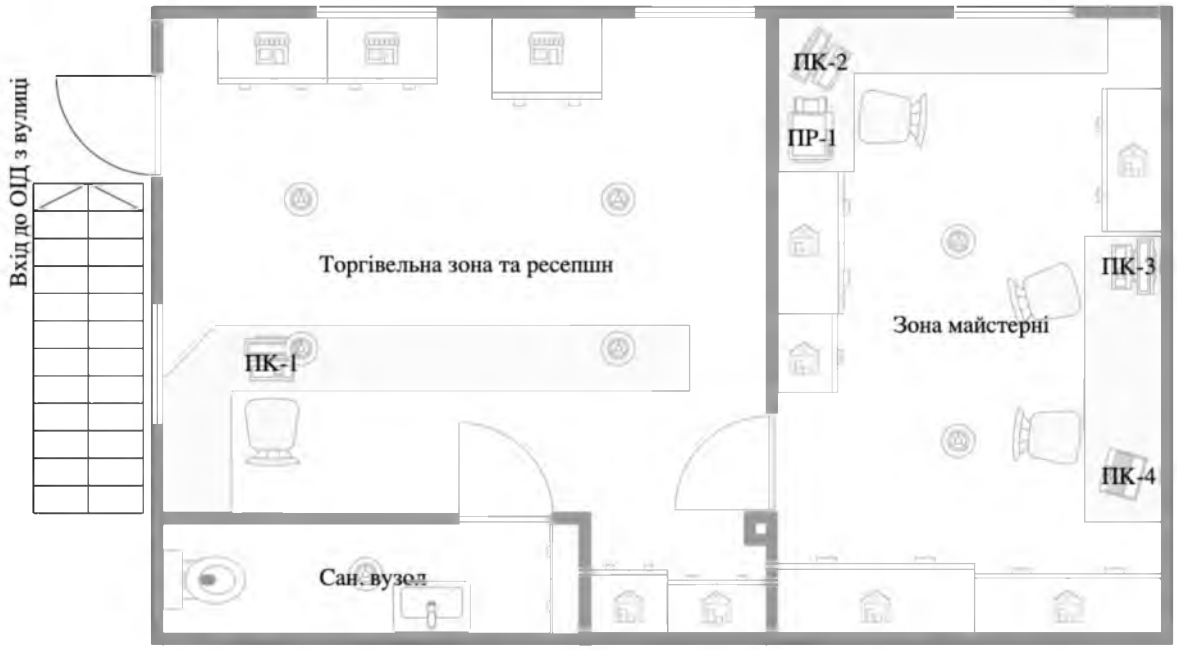


Рисунок 1.2 – Генеральний план. Опис приміщень

Для оцінки рівня кожної із розглянутих загроз в контексті цілісності, доступності та конфіденційності інформації для кожного конкретного випадку, проведено аналіз порушень цих властивостей. Цей аналіз дозволить визначити найбільш критичні вразливості в системі. Результати аналізу відображено у таблиці 1.1, де К відповідає конфіденційності, Ц - цілісності, Д - доступності.

Таблиця 1.1 – Результати аналізу рівня загроз

Вразливість	Наслідок	Порушення
Виток конфіденційної інформації	З урахуванням того, що конфіденційна інформація (організаційно-розпорядча, бухгалтерська, фінансова, дані про співробітників, клієнтів, тощо) зберігається на комп'ютерах, існує загроза витоку цієї інформації через несанкціонований доступ або атаки на систему. Це може призвести до непередбачуваних наслідків, таких як втрата довіри клієнтів або витрати на відновлення репутації	К
Атаки на електронні засоби зберігання	Враховуючи, що інформація зберігається в електронному форматі, існує загроза атак на системи зберігання даних, такі як віруси, шкідливі програми або кібератаки. Це може призвести до пошкодження або втрати інформації	Ц, Д
Неавторизований доступ до інформації	Наявність локальної мережі може стати об'єктом для несанкціонованого доступу до даних. Якщо недостатньо захищена, локальна мережа може стати	К, Ц

Продовження таблиці 1.1 – Результати аналізу рівня загроз

Вразливість	Наслідок	Порушення
	вразливою до атак, що може призвести до доступу до конфіденційної інформації	
Атаки на службу Wi-Fi	Застосування бездротового підключення до ІТС може призводити до загроз атак на службу Wi-Fi. Якщо не застосовані належні заходи безпеки, атаки на мережу можуть призвести до незаконного доступу та витоку інформації	Д
Втрата електронних документів	Зберігання документації в електронному форматі ставить перед загрозою можливу втрату даних внаслідок технічних збоїв, непередбачених обставин чи атак на систему	Ц, Д
Несанкціоновані зміни в інформаційній системі	Атаки на інформаційну систему можуть спрямовуватися на зміну, видалення або руйнування даних. Це може призвести до втрати чи викривлення інформації, що має стратегічне значення для підприємства	К, Ц
Соціальна інженерія	Атаки можуть бути спрямовані на співробітників, з метою отримання конфіденційної інформації через соціальне впливання. Недостатня свідомість персоналу може стати фактором ризику	К

Продовження таблиці 1.1 – Результати аналізу рівня загроз

Вразливість	Наслідок	Порушення
Несправність систем резервного копіювання	В разі відсутності чи несправності системи резервного копіювання може виникнути загроза втрати даних внаслідок технічних проблем чи випадкового видалення	Ц

Отже, проведений аналіз визначає широкий спектр загроз, які вимагають комплексного підходу до кіберзахисту для забезпечення надійності та конфіденційності інформації в ІТС підприємства «FixUp».

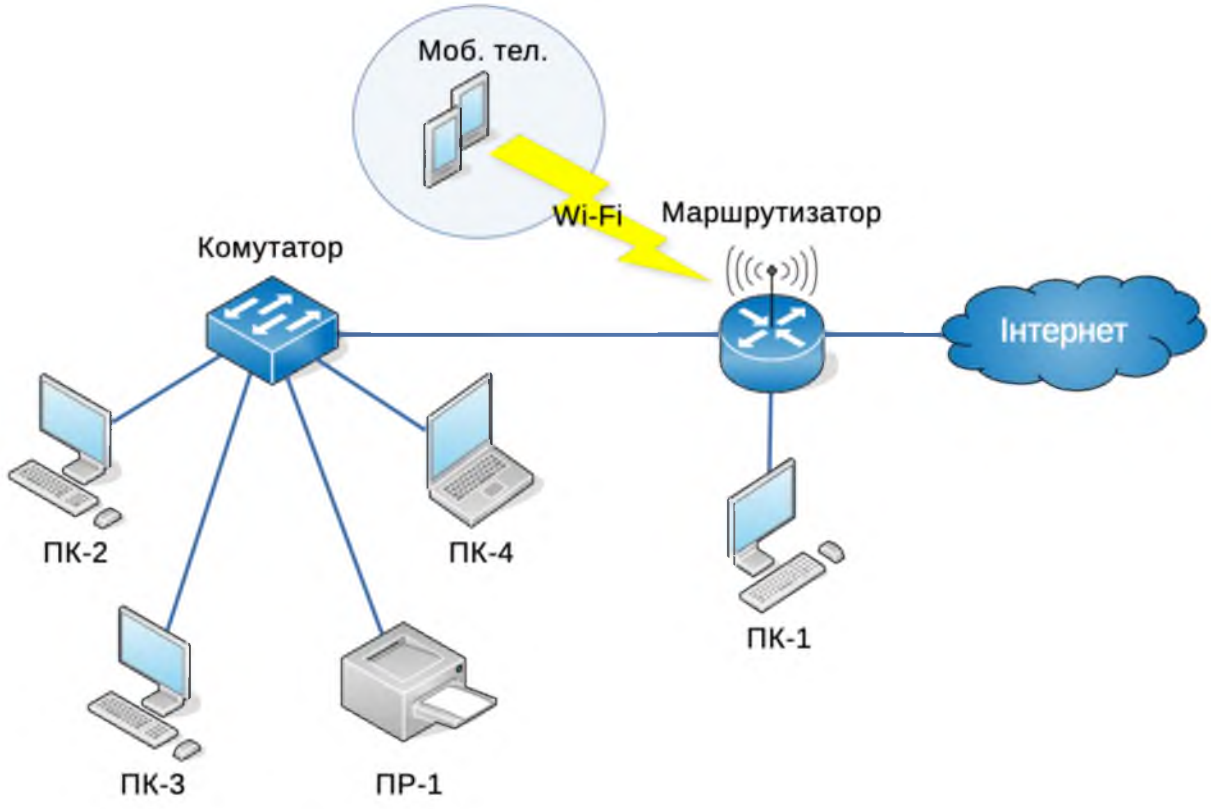


Рисунок 1.3 – Схема поточного стану ІТС

ІТС ОІД реалізується у формі "зірки", що включає один маршрутизатор із опцією Wi-Fi та один комутатор. Цей конфігураційний комплекс виступає як розгалужена мережева структура, спроєктована для множинного користування та

здатна обробляти як конфіденційну інформацію з обмеженим доступом, так і відкриту інформацію. Крім того, система має необмежений доступ до мережі Інтернет, наданий Інтернет-провайдером "DTS". Класифікація ІТС відповідає третьому класу автоматизованих систем.

В обчислювальну систему входять чотири персональні комп'ютери, з яких три – стаціонарні, один – портативний, а також один принтер, об'єднаний в собі функції принтера, ксерокса і сканера. Структурна схема ІТС представлена на рисунку 1.3.

Таблиця 1.2 містить перелік обладнання ІТС, де вказано використане мережеве обладнання. Зокрема, в мережі використовується маршрутизатор TP-LINK Archer A8 із чотирма портами LAN, функцією Wi-Fi та пропускною здатністю 1.9 Гбіт/с. Крім того, для об'єднання пристроїв у локальній мережі використовується комутатор TP-LINK TL-SG108-M2 із восьми портами LAN і пропускною здатністю 2.5 Гбіт/с.

Таблиця 1.2 – Мережеве обладнання

№	Назва	Модель	Специфікація
1	2	3	4
1	Маршрутизатор	TP-LINK Archer A8	4 порти LAN; Wi-Fi-; 1 .9Гбіт/с
2	Комутатор	TP-LINK TL-SG 108-M2	8 портів LAN; 2.5Гбіт/с

Інформація щодо основних та додаткових технічних засобів, які використовуються на ОІД, подається у таблицях 1.3 та 1.4. У вказаних таблицях відображена детальна інвентаризація технічного обладнання, надаючи повний огляд основних та додаткових засобів, які забезпечують функціональність та безпеку системи.

Таблиця 1.3 – Основні технічні засоби

Ім’я	Ім’я в ІС	Специфікація	Серійний номер	Користувач
ПК-1	Manager1-PC	Монітор ASUS VA24EHE, на столі, 1.5м до границі КЗ	41NP030691	Менеджер
		Клавіатура Defender HM-710, на столі, 1.5м до границі КЗ	KB0942665-34	
		Миша Genius NS-120, на столі, 1.5м до границі КЗ	12964WA5442SE	
		Системный блок ASUS D500MAES, під столом, 1.5м до границі КЗ	X550CC-X0420H	
ПК-2	Master1-PC	Монітор Samsung SyncMaster 2343BW, на столі, менше 1м до границі КЗ	GR356FE360844FE	Майстер з ремонту
		Монітор Samsung SyncMaster 940N, на столі, менше 1м до границі КЗ	GT18H4UR300158E	
		Клавіатура A4Tech KV-300H, на столі, менше 1м до границі КЗ	RM1702K300H0	
		Миша A4Tech G9-500FS, на столі, менше 1м до границі КЗ	UE1812012407	
		Системний блок іншої конфігурації, під столом, менше 1м до границі КЗ	–	
ПК-3	Master2-PC	Монітор Samsung SyncMaster 2343BW, на столі, менше 1м до границі КЗ	GR238FG547224FD	

Продовження таблиці 1.3 – Основні технічні засоби

Ім’я	Ім’я в ІС	Специфікація	Серійний номер	Користувач
		Монітор Samsung SyncMaster 940N, на столі, менше 1м до границі КЗ	GT22H4UD605352E	
		Клавіатура Logitech G213 Prodigy, на	1841SCK08A18	
		столі, менше 1м до границі КЗ		
		Миша Logitech M170, на столі	1738LZX30UWA8	
		Системний блок іншої конфігурації, під столом, менше 1м до границі КЗ	–	
ПК-4	Buhgalter 1-PC	Ноутбук Lenovo ThinkPad E14, на столі, менше 1м до границі КЗ	PF-0QQJQM	Бухгалтер
ПР-1	HP-M428dw	МФУ HP LaserJet Pro M428dw, на столі, 2м до границі КЗ	VNB4F85NF2	–
Маршрутизатор	TL-ArcherA8	4 порти LAN; Wi-Fi-; 1.9Гбіт/с, закріплений на стіні, 1м до границі КЗ	2167481000585V1.0	–
Комутатор	TL-SG108	8 портів LAN; 2.5Гбіт/с, закріплений на стіні, менше 1м до границі КЗ	5467351000234A	–

Таблиця 1.4 – Допоміжні технічні засоби

Ім’я	Специфікація	Серійний номер	Користувач
Світлоідодна лампа 1-7 (7 шт.)	VIS-30-E27, в стелі	–	–
IP-відеокамера спостереження з Wi-Fi 1-3 (3 шт.)	TP-LINK Tapco C200, на стіні, 1.5м до границі КЗ (1), менше 1м до границі КЗ (2-3)	NSC20KH2-K25, NSC20HS-FK3, NS7D4KHF-3F5	–
Настільні лампи 1-7 (7 шт.)	На столі	–	–
Інфрачервона паяльна станція	ACHI IR6500, на столі, менше 1м до границі КЗ	ND3894YF762K	Майстер з ремонту
Термо-воздушна паяльна станція 1	Lukey 852D, на столі, менше 1м до границі КЗ	84ND9B3534	Майстер з ремонту
Термо-воздушна паяльна станція 2	Lukey 852D, на столі, 1м до границі КЗ	34NV9FG432	Майстер з ремонту
Лабораторний блок живлення 1	Zhaoxin RXN 305D, на столі, менше 1м до границі КЗ	ENK23KR3-30V	Майстер з ремонту
Лабораторний блок живлення 2	Zhaoxin RXN 305D, на столі, 1м до границі КЗ	EDK42KR3-30V	Майстер з ремонту
Лабораторний блок живлення 3	Zhaoxin RXN 305D, на столі, 1.5м до границі КЗ	EBK212R3-30V	Майстер з ремонту
Осцилограф	Hantek DSO5102P, на столі, менше 1м до границі КЗ	JF2387F3F	Майстер з ремонту
Мультиметр 1-4 (4 шт.)	UNI-T UT33C, в столі, менше 1м до границі КЗ	MUT33432LF, MUT3343245,	Майстер з ремонту

Продовження таблиці 1.4 – Допоміжні технічні засоби

Ім’я	Специфікація	Серійний номер	Користувач
		MUT33432N4, MUT33432B1	
Програматор мікросхем	TL866 Universal programmer, в столі, 1.5м до границі КЗ	F312MR-866	Майстер з ремонту
Тачскрин-дисплей сепаратор	RUNTOP, на столі, менше 1м до границі КЗ	–	Майстер з ремонту
RLC-тестер	В столі, менше 1м до границі КЗ	–	Майстер з ремонту
Ультразвукова ванна	В стелажі, 2м до границі КЗ	–	Майстер з ремонту
Принтер-тестер для картриджів 1	Samsung ML-1660, на столі, менше 1м до границі КЗ	SML12FJ4G4	Майстер з ремонту
Принтер-тестер для картриджів	Samsung CJX-1000, в стелажі, 2м до границі КЗ	SCJXS892KG6	Майстер з ремонту
Програматор мультиконтролерів	В столі, менше 1м до границі КЗ	–	Майстер з ремонту
Мікроскоп	МБС-10, на столі, менше 1м до границі КЗ	–	Майстер з ремонту
Програматор мобільних телефонів	OCTOPLUS, Medusa PRO, в стелажі, 3м до границі КЗ	–	Майстер з ремонту
Програматор флеш-пам’яті	TNM5000, в стелажі, 2м до границі КЗ	JFK32MRF453	Майстер з ремонту

Таблиця 1.5 – Характеристика комп'ютерів

Ім'я	Ім'я в ІС	Характеристики
ПК-1	Manager1-PC	Процесор: Intel Pentium G4620
		Оперативна пам'ять: DDR3 4 ГБ
		Накопичувач: HDD 1 ТБ
		Відео карта: Інтегроване відео
		Материнська плата: H270
ПК-2	Master1-PC	Процесор: AMD Ryzen 7
		Оперативна пам'ять: DDR3 8 ГБ
		Накопичувач: SSD 250 ГБ, HDD 1 ТБ
		Відео карта: Nvidia GTX 650
		Материнська плата: Gigabyte G1 Sniper Z-97
ПК-3	Master2-PC	Процесор: AMD Ryzen 7
		Оперативна пам'ять: DDR3 16 ГБ
		Накопичувач: SSD 250 ГБ, HDD 2 ТБ
		Відео карта: Nvidia GTX 650
		Материнська плата: Gigabyte G1 Sniper Z-97
ПК-4	Buhgalter1-PC	Процесор: Intel Core i5-10210U
		Оперативна пам'ять: DDR4 8 ГБ
		Накопичувач: M.2 SSD 120 ГБ, HDD 500 ГБ
		Відео карта: Інтегроване відео
		Материнська плата: Lenovo

Таблиця 1.6 – Програмне забезпечення

Ім'я	Тип ПЗ	Встановлено	Тип ліцензії	Термін дії ліцензії
Windows 10 Home	Системне	ПК-1, ПК-4	Корпоративна	Необмежений
Ubuntu 21.04 LTC	Системне	ПК-2	Free	–

Продовження таблиці 1.6 – Програмне забезпечення

Ім’я	Тип ПЗ	Встановлено	Тип ліцензії	Термін дії ліцензії
Windows 10 Pro	Системне	ПК-3	Корпоративна	Необмежений
Windows 7 Ultimate	Системне	ПК-3	Корпоративна	Необмежений
Драйвери	Системне	ПК-1 – ПК-4	–	–
CRM	Прикладне	ПК-1 – ПК-4	Корпоративна	1 рік (підписка)
ERP	Прикладне	ПК-1 – ПК-4	Корпоративна	1 рік (підписка)
M.E. Doc	Прикладне	ПК-4	Корпоративна	1 рік (підписка)
1С: Каса	Прикладне	ПК-1, ПК-4	Корпоративна	Необмежений
1С: Бухгалтерія	Прикладне	ПК-4	Корпоративна	Необмежений
Google Chrome	Прикладне	ПК-1 – ПК-4	Free	–
Пакет програм MS Office (Word, Excel, Outlook)	Прикладне	ПК-1 – ПК-4	Корпоративна	1 рік (підписка)
7-Zip	Прикладне	ПК-1 – ПК-4	GNU	–
TeamViewer	Прикладне	ПК-2, ПК-3	Пропрієтарна	Необмежений
Notepad++	Прикладне	ПК-2, ПК-3	Volume license	–
Proteus	Прикладне	ПК-2, ПК-3	Пропрієтарна	Необмежений
Visual Analyser	Прикладне	ПК-2, ПК-3	Free	–
Sprint-Layout	Прикладне	ПК-2, ПК-3	Пропрієтарна	Необмежений
SP Flash Tool	Прикладне	ПК-2, ПК-3	Free	–

Продовження таблиці 1.6 – Програмне забезпечення

Ім’я	Тип ПЗ	Встановлено	Тип ліцензії	Термін дії ліцензії
QFIL	Прикладне	ПК-2, ПК-3	Free	–
Odin	Прикладне	ПК-2, ПК-3	GNU	–
ASUS Flash Tool	Прикладне	ПК-2, ПК-3	Free	–
XiaoMiFlash	Прикладне	ПК-2, ПК-3	GNU	–
Aida 64	Прикладне	ПК-2, ПК-3	GNU	–
Memtest	Прикладне	ПК-2, ПК-3	Free	–
Recuva	Прикладне	ПК-2, ПК-3	Пропрієтарна	Необмежений
Victoria	Прикладне	ПК-2, ПК-3	Free	–
Driver Pack	Прикладне	ПК-2, ПК-3	Пропрієтарна	Необмежений
3uTools	Прикладне	ПК-2, ПК-3	GNU	–
iTunes	Прикладне	ПК-2, ПК-3	GNU	–

Всі пристрої ІТС встановлюють взаємозв'язок за допомогою крученої пари, яка подається з першого поверху до ОІД і подальше підключається до маршрутизатора. Далі, з маршрутизатора відбувається з'єднання з комп'ютером ПК-1 та комутатором. Функцією комутатора є забезпечення підключення комп'ютерів ПК-2, ПК-3, ПК-4 та принтера ПР-1. Можливість друку на принтері ПР-1 реалізується через локальну мережу, при цьому всі комп'ютери в локальній мережі мають безперешкодний доступ до цього принтера. Така структура взаємозв'язку пристроїв ІТС дозволяє забезпечити ефективний обмін даними та спільне використання ресурсів у межах інформаційної системи.

1.1.2. Обґрунтування важливості підвищення рівня безпеки в контексті росту загроз кібербезпеки

Обґрунтування важливості підвищення рівня безпеки в контексті росту загроз кібербезпеки базується на наступних аспектах:

- Загроза несанкціонованого доступу:

Однією з ключових загроз є можливість несанкціонованого доступу до інформації, яка включає конфіденційні дані. Зловмисники можуть використовувати слабкі місця в мережі або вразливості програмного забезпечення для незаконного отримання цих даних. Підвищення рівня безпеки необхідно для ефективного контролю за доступом та моніторингу мережі, а також для вчасного оновлення програмного забезпечення та впровадження надійних механізмів аутентифікації.

- Організаційно-розпорядча інформація:

Зберігання та обробка конфіденційної інформації про організаційну структуру та управління вимагає високого рівня безпеки. Забезпечений контрольований доступ та визначення рівнів прав доступу гарантують, що ця інформація надається тільки уповноваженим особам, а оновлення та редагування відбувається відповідно до політик компанії.

- Бухгалтерська, фінансова та клієнтська інформація:

Інформація про бухгалтерські та фінансові показники, а також особисті дані клієнтів, представляє значущий об'єм конфіденційної інформації. Забезпечений обмежений, але необхідний доступ до цих даних через локальну мережу вимагає ретельного контролю, щоб уникнути неправомірного використання або розголошення.

- Інформація про співробітників та ремонтні роботи:

Забезпечення конфіденційності особистих та кадрових даних співробітників є важливим для управління персоналом. Інформація про ремонтні роботи також має свою конфіденційність, і контрольований доступ до цих даних через локальну мережу є ключовим для ефективного керування та безпеки.

- Збереження у різних форматах:

Інформація зберігається в паперовому та електронному форматах, і обидва ці варіанти потребують високого рівня захисту. Ефективне управління цією різноманітністю форматів вимагає системного підходу до кіберзахисту.

Враховуючи вищезазначені аспекти, підвищення рівня безпеки стає невід'ємною частиною стратегічного управління та планування бізнесу, оскільки воно спрямоване на захист інформації, стабільність бізнес-процесів та дотримання законодавчих вимог.

1.1.3. Аналіз нормативно-правової бази у сфері захисту інформації

Основи нормативно-правового забезпечення в сфері інформаційної безпеки визначаються через формування та підтримку його нормативно-правової бази, розгляданої як юридичний механізм досягнення системної упорядкованості в сфері інформаційної безпеки. Нормативна база представляє собою організаційно-функціональний образ системи інформаційної безпеки, виражений юридичною мовою, який відповідає її цільовому призначенню.

Правові норми в даному контексті виконують подвійну функцію: забезпечують моделювання як самої системи національної безпеки, так і її підсистем, а також визначають та формалізують їх функціональні, організаційні та інформаційні структури. Вони слугують не лише засобом нормування, але і інформаційною функцією, сприяючи впорядкуванню та підтримці системи інформаційної безпеки.

Нормативно-правове забезпечення інформаційної безпеки визначається як процес, що включає в себе створення та підтримку необхідних конструктивних організаційно-функціональних характеристик системи інформаційної безпеки за допомогою нормативно-правового впливу.

Система нормативно-правового забезпечення інформаційної безпеки складається з сукупності законів та підзаконних нормативних актів. Ці документи формують нормативно-правове поле для оптимального функціонування системи національної безпеки та виконання нею свого призначення.

При розробці рекомендацій з підвищення рівня інформаційної безпеки важливо опиратися на наступні нормативні документи:

- Закон Україні «Про інформацію»
- Закон Україні «Про захист інформації»

- Закон Україні «Про захист інформації в інформаційно-комунікаційних системах»
- НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»
- НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»
- НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»
- НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»
- НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»
- НД ТЗІ 3.6-001-2000 «Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.»
- ДСТУ 3396.1-96 «Захист інформації. Технічний захист. інформації. Порядок проведення робіт»

1.2. Вибір методу дослідження та проєктування

На даному етапі проведено відбір та конкретизація методологічних підходів та інструментів, які зазначаються для використання в ході проведення комплексного дослідження та етапу проєктування інформаційної системи. Великою вагою наділяється саме процес обрання оптимального методу, який відповідає конкретним вимогам та сприяє досягненню чітко визначених цілей проєкту.

Рішення, обрані на цьому етапі, визначають подальший успіх реалізації інформаційної системи та досягнення максимально ефективних результатів відповідно до запланованих цілей.

1.2.1. Розгляд методів та підходів до підвищення кіберзахищеності ІТС

Було проаналізовано методи та стратегії, які можуть бути використані для ефективного підвищення рівня кіберзахисту ІТС підприємства «FixUp». З огляду на зростання загроз у кіберпросторі, важливість розробки та застосування найсучасніших заходів безпеки надто актуальна.

Далі зазначено методи та підходи, які будуть використовуватись в даному контексті:

- Оновлення мережевого обладнання: Здійснення переходу до сучасного та вдосконаленого мережевого обладнання, включаючи маршрутизатор та комутатор, з метою покращення надійності та забезпечення вищого рівня захисту мережі. Це включає у себе встановлення нового обладнання, яке враховує останні технологічні стандарти та має розширені можливості у сфері кібербезпеки.
- Встановлення системи виявлення та запобігання вторгнень: Впровадження системи виявлення та запобігання вторгнень дозволить вчасно розпізнавати незвичайну активність або потенційні загрози в мережі. Ця система надасть можливість реагувати на можливі атаки та вчасно ізолювати їх.

Серед вказаних методів та підходів, які були розглянуті, було визначено що оновлення мережевого обладнання та встановлення системи виявлення та запобігання вторгнень стане ключовим елементом стратегії підвищення кіберзахищеності в ІТС підприємства «FixUp».

Далі було детально проаналізовано обрані методи, визначено їх переваги та визначено необхідні заходи для успішного впровадження. У рамках цього аналізу було детально розглянуто, як кожен метод може сприяти підвищенню рівня кіберзахищеності ІТС підприємства «FixUp», а також визначено конкретні етапи та вимоги для їх ефективного використання.

1.3. Оновлення мережевого обладнання

На даний момент використовується бездротовий маршрутизатор TP-LINK Archer A8. TP-Link Archer A8 – це універсальний бездротовий маршрутизатор, який використовується для організації мережі вдома або в невеликому офісі. Маршрутизатор підтримує стандарт 802.11ac і здатний працювати в двох частотних діапазонах 2,4 і 5 ГГц. При цьому, максимально підтримувана швидкість з'єднання в TP-Link Archer A8 становить 600 і 1300 Мбіт/с відповідно. Передача даних в три потоки завдяки 3x3 MIMO дозволяє досягти максимуму можливостей для максимальної ефективності. Технологія MU-MIMO забезпечує комфортну роботу великої кількості підключених пристроїв. Для дротового доступу в TP-Link Archer A8 передбачено чотири гігабітних порти Ethernet.

Варто відзначити, що цей маршрутизатор, по-перше розроблений для домашнього використання та не має належного рівня кіберзахисту для застосування в системах, де вимагається принаймні базовий рівень захисту від кіберзагроз.

Рисунок 1.4 – Зовнішній вигляд маршрутизатора

На рисунку 1.4 зображено зовнішній вигляд маршрутизатора TP-LINK Archer A8.

Важливим недоліком цього конкретного маршрутизатора в нашому випадку є існування виявленої вразливості CVE-2019-7405. Ця конкретна вразливість створює серйозний ризик, оскільки дозволяє віддаленому несанкціонованому користувачеві заволодіти контролем над налаштуваннями маршрутизатора за допомогою протоколу Telnet у локальній мережі (LAN).

Особливо важливо відзначити, що цей потенційний нападник може також використовувати цю вразливість для з'єднання з сервером протоколу передачі файлів (FTP) як через локальну, так і через глобальну мережу WAN.

Вразливість було виявлено експертом з безпеки «X-Force Red».

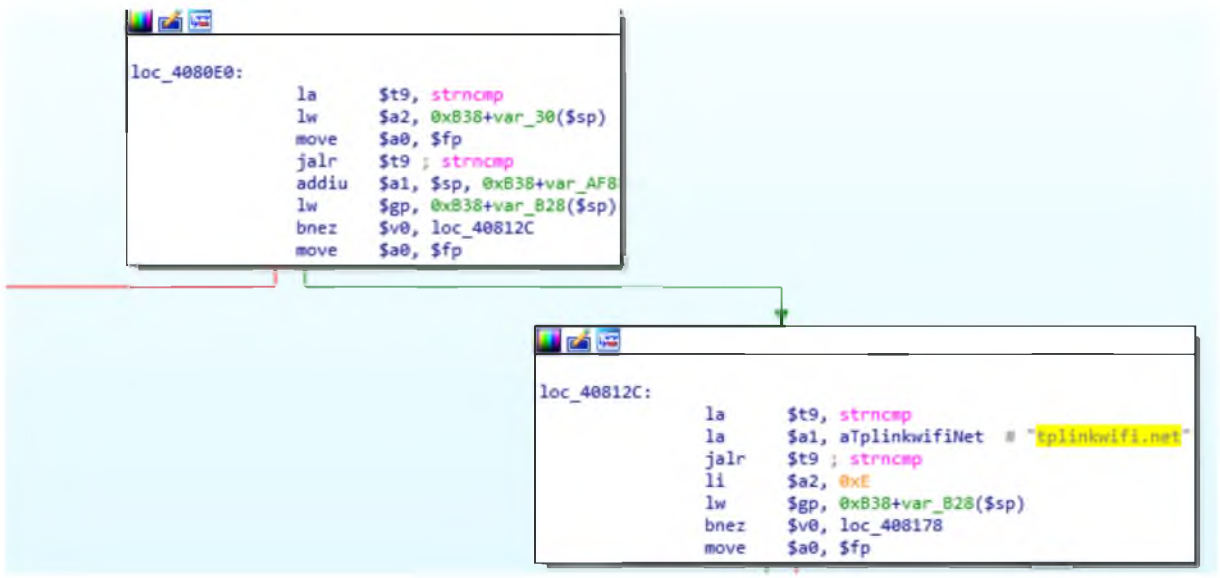


Рисунок 1.5 – Частина коду ПЗ маршрутизатора

Порушник міг відправити HTTP-запит із символьним рядком, довжина якого перевищує допустиму кількість байт. У результаті цього пароль користувача анулюється і замінюється порожнім значенням. Важливо зазначити, що перевірялись лише HTTP-заголовки реферера, що дозволяло порушнику обходити службу httpd пристрою за допомогою жорстко закодованого значення `tplinkwifi.net`, яке відображено в частині коду ПЗ маршрутизатора на рисунку 1.5.

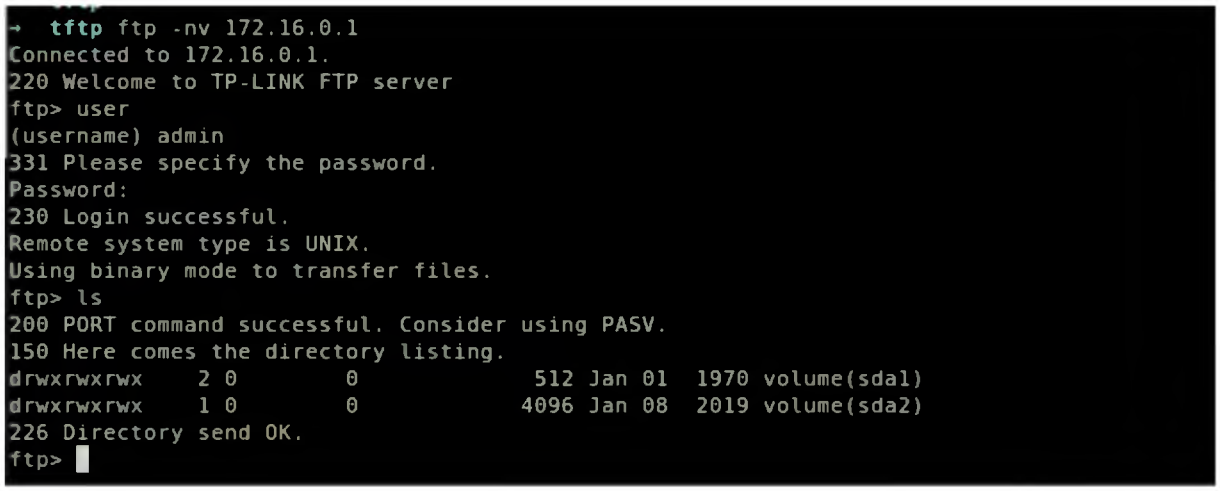


Рисунок 1.6 – Успішне підключення до зламаного маршрутизатору

На рисунку 1.6 продемонстровано успішне підключення порушника до FTP-серверу через протокол TFTP. Командою `tftp` встановлюється з'єднання з FTP-сервером, розташованим за IP-адресою 172.16.0.1. Сервер вітає порушника. Порушник вводить ім'я `admin`, сервер відповідає, що необхідно вказати пароль. Після введення пустого паролю відбувається успішний вхід (230 Login successful).

Порушник вводить команду `ls` для виведення списку файлів на сервері. Сервер вказує, що команда PORT виконана успішно, і рекомендує розглянути використання PASV. Потім відбувається передача інформації про каталог, і його вміст виводиться користувачу.

Єдиним видом користувачів на зазначеному маршрутизаторі є адміністратори, які мають повноваження кореневого користувача (root-права). Це означає, що після успішної атаки зловмисник автоматично отримує повноваження адміністратора, завершуючи атаку. Покрім того, легітимний користувач може втратити доступ до пристрою, оскільки пристрій перестає приймати введені паролі. Це може стати причиною того, що легітимні користувачі втрачають можливість користуватися пристроєм, якщо їхні паролі втрачають актуальність або стають непридатними.

Крім того, важливо зазначити, що маршрутизатор TP-LINK Archer A8, окрім виявленої вразливості, обмежений обсягом доступних портів для підключення пристроїв по крученій парі — усього чотири порти LAN та один WAN. Це

обмеження в кількості портів стає фактором, що ускладнює підключення більшого числа пристроїв без додаткового використання комутатора.

Рисунок 1.7 – Задня панель маршрутизатора TP-LINK Archer A8

На Рисунку 1.7 представлено задню панель маршрутизатора, де видно, що маршрутизатор оснащений чотирма портами LAN (помаранчеві) та одним портом WAN (синій). Також на задній панелі розташовані перемикач ввімкнення, кнопка RESET, кнопка WPS та роз'єм для живлення.

Ця обмежена кількість портів призводить до необхідності використання додаткового комутатора для розширення можливостей підключення пристроїв. Враховуючи потреби в сучасних робочих мережах, це обмеження стає перешкодою для зручного та ефективного використання мережевих ресурсів.

Для вирішення проблеми обмеженості кількості портів у комутатора, наразі використовується настільний 8-портовий комутатор TP-LINK TL-SG108-M2, який має пропускну здатність 2500 Мбіт/с.

TP-LINK TL-SG108-M2 - це неуправляючий комутатор, спроєктований для ефективного керування мережевим трафіком. Завдяки комутаційній матриці з потужністю 40 Гбіт/с та швидкістю пересилання пакетів 29.8 Mpps, цей комутатор забезпечує стабільну та надійну роботу мережі. Таблиця MAC-адресів розміром на 16 тисяч адрес дозволяє ефективно керувати адресами пристроїв у мережі.

Рисунок 1.8 – Зовнішній вигляд комутатора TP-LINK TL-SG108-M2

Завдяки восьми гігабітним портам Ethernet, включаючи восьмий порт із швидкістю 2.5G Ethernet, цей комутатор забезпечує швидку передачу даних та підтримує високі швидкості з'єднання. Можливість роботи з Jumbo-фреймами розміром 10240 байт дозволяє оптимізувати передачу великого обсягу даних.

На рисунку 1.8 зображено зовнішній вигляд комутатора TP-LINK TL-SG108-M2.

1.4. Система виявлення та запобігання вторгнень

Системи виявлення вторгнень (IDS) та запобігання вторгненням (IPS) представляють собою програмні або апаратні комплекси, призначені для забезпечення безпеки мережі та комп'ютерів. Системи виявлення вторгнень є пасивною системою виявлення, яка у режимі реального часу проводить аналіз всього трафіку і, за потреби, повідомляє про виявлені загрози. Ця система не вносить зміни до мережевих пакетів і не впливає на функціонування мережевої інфраструктури. У той час система запобігання вторгненням може активно перешкоджати доставці пакетів, аналогічно до брандмауера, спрямовуючи або блокуючи їх з метою запобігання потенційним загрозам.

В поточній конфігурації ІТС система виявлення та запобігання вторгнень взагалі не використовується взагалі, що призводить до серйозної вразливості мережі перед потенційними кіберзагрозами та атаками. Система виявлення та запобігання вторгнень є важливим елементом в інфраструктурі кібербезпеки,

оскільки вона відповідає за реагування на невизначені або аномальні активності в мережі, які можуть бути ознакою можливого вторгнення.

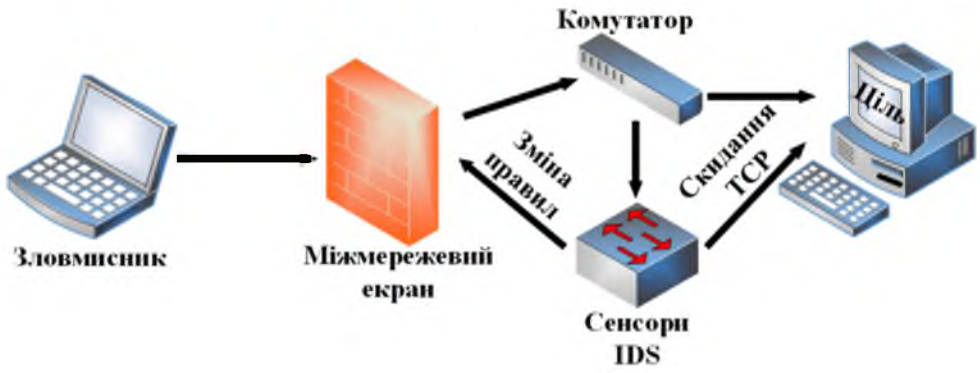


Рисунок 1.9 – Система виявлення вторгнень

Система виявлення вторгнень, будучи програмним або апаратним рішенням, має призначення виявляти несанкціонований доступ до комп'ютерних систем чи мережі та неправомірне управління ними, зазвичай через мережу Інтернет. Про будь-яку активність шкідливого ПЗ або про порушення типової роботи централізовано збирається інформація SIEM-системою. SIEM-система обробляє дані отримані від багатьох джерел і використовує методи фільтрування тривог для розрізнення несанкціонованої активності від хибного спрацювання тривоги. Про що оповіщається або адміністратор або операційний центр безпеки. Система виявлення вторгнень встановлюють паралельно з мережевими потоками, і ця система обробляє копію проходячого трафіку. Архітектура системи виявлення вторгнень зображена на рисунку 1.9.

Рисунок 1.10 – Система запобігання вторгнень

Деякі системи виявлення вторгнень можуть виявляти початкові етапи атак на мережу, включаючи раніше невідомі загрози. Такі рішення відомі як системи запобігання вторгненням (IPS). IPS виходять за межі простого оповіщення та вживають різні заходи для блокування атак, такі як розірвання з'єднань або виконання зазначених адміністратором дій. Зазвичай вони поєднують у собі функції обох типів систем та називаються системами виявлення і запобігання вторгненням (IDPS). Архітектура системи запобігання вторгнень зображена на рисунку 1.10.

Рисунок 1.11 – Схема роботи мережевого екрану

Хоча й IDS, і мережевий екран відносяться до засобів забезпечення інформаційної безпеки, мережевий екран відрізняється тим, що обмежує надходження на хост або підмережу певних видів трафіку для запобігання вторгнень і не відслідковує вторгнення, які відбуваються всередині мережі. IDS, навпаки, пропускає трафік, аналізуючи його і сигналізуючи при виявленні підозрілої активності. Виявлення порушення безпеки проводиться звичайно з використанням евристичних правил та аналізу сигнатур відомих комп'ютерних атак. Система яка розриває з'єднання називається системою запобігання вторгненням і є однією з видів мережевого екрану на рівні застосунку. Схема роботи мережевого екрану зображена на рисунку 1.10.

Існують різні типи систем виявлення вторгнень, розміри яких варіюють від індивідуальних комп'ютерів до великих мереж. Серед найпоширеніших класифікацій виділяють системи виявлення вторгнень у мережу (англ. Network Intrusion Detection Systems, NIDS), що аналізують вхідний мережевий трафік, та системи виявлення вторгнень на основі аналізу хостів (англ. Host-Based Intrusion Detection Systems, HIDS), що відслідковують важливі файли операційних систем. Систему виявлення вторгнень також можна класифікувати за методами виявлення загроз, такими як розпізнавання сигнатур (виявлення відомих патернів, таких як шкідливе ПЗ) та виявлення аномалій (розпізнавання відхилень від нормального трафіку, часто за допомогою машинного навчання).

Основне розрізнення полягає у тому, як обидва рішення реагують на інциденти. Система виявлення вторгнень фактично є інструментом моніторингу. Він розпізнає потенційно небезпечну активність і попереджує про неї. Система запобігання вторгнень може не лише виявити проблему, але й вжити заходів, спрямованих на боротьбу з загрозою – перервати з'єднання або заблокувати IP-адресу, з якого відбуваються підозрілі дії.

Також відрізнення у способі інтеграції в інфраструктуру та взаємодії з мережевим трафіком, де система виявлення вторгнень встановлюють паралельно з мережевими потоками, і ця система обробляє копію проходячого трафіку, а систему запобігання вторгнень вбудовують у мережу, дозволяючи трафіку проходити через себе. У цьому випадку система виявлення вторгнень виглядає більш перевагою, оскільки при вичерпанні обсягів, відведених захисному рішенню на обробку трафіку, система виявлення вторгнень не впливатиме на мережеву активність. У той час як система запобігання вторгнень може стати «вузьким місцем» в захисній системі, додатково навантажуючи обладнання брандмауера.

Як вже зазначалося, система виявлення вторгнень відстежує трафік. Під час спостереження він порівнює мережеву активність із власною базою даних мережевих загроз. За допомогою такого підходу рішення вивчило виявляти:

- Мережеві атаки;
- Спроби доступу до даних;
- Активність шкідливих програм;
- Спроби сканування портів;
- Аномальну активність;
- Використання бот-мереж та майнінг-пулів;
- Порушення політик безпеки.

Системи IDS поділяють на дві категорії згідно з принципом дії:

- Сигнатурні: Їхній принцип роботи схожий на активність антивірусного програмного забезпечення. Ці IDS аналізують сигнатури за допомогою постійно оновлюваної бази. Якщо немає доступу до бази або вона застаріла, ефективність сигнатурного рішення зменшується. Існує ризик і некоректного визначення нової атаки з невідомою сигнатурою. Сигнатурні IDS відстежують стан системи, а не події.
- Основані на аномаліях: Це рішення використовує технології машинного навчання. Для його правильної роботи на об'єкті потрібно провести попереднє навчання. Тривалість навчання залежить від складності IT-інфраструктури компанії. Принцип роботи такий: система вивчає роботу мережі за поточний період часу і порівнює з аналогічним періодом у пошуку аномалій трьох типів — статистичних, аномалій протоколів і трафіку. Такі системи захисту є ефективними, але складними.

1.4.1. Типи систем виявлення вторгнень за місцем встановлення

Два найпоширеніших види систем виявлення вторгнень за місцем встановлення:

- Система виявлення вторгнень в мережі (NIDS);
- Система виявлення вторгнень на рівні хоста (HIDS).

Перша працює на рівні мережі, в той час як друга – лише на рівні окремого хоста.

Мережеві системи виявлення вторгнень (NIDS)

Технологія NIDS дозволяє розмістити систему в стратегічно важливих точках мережі і аналізувати вхідний/вихідний трафік всіх пристроїв у мережі. NIDS аналізують трафік на глибокому рівні, "заглядаючи" в кожний пакет від канального рівня до рівня додатків.

NIDS відрізняється від мережевого екрана, або файервола. Файервол фіксує лише атаки, що надходять ззовні мережі, у той час як NIDS може виявити і внутрішню загрозу.

Мережеві системи виявлення вторгнень контролюють всю мережу, що дозволяє уникнути витрат на додаткові рішення. Проте є недолік: NIDS відстежує весь мережевий трафік, споживаючи велику кількість ресурсів. Чим більше обсяг трафіку, тим вище потреба в ресурсах процесора і оперативної пам'яті. Це призводить до помітних затримок обміну даними і зниження швидкості роботи мережі. Великий обсяг інформації також може «перегрузити» NIDS, змушуючи систему пропускати деякі пакети, що робить мережу вразливою.

Хостова система виявлення вторгнень (HIDS)

Альтернативою мережевим системам є хостові. Такі системи встановлюються на один хост всередині мережі і захищають лише його. HIDS також аналізують всі вхідні та вихідні пакети, але лише для одного пристрою. Система HIDS працює за принципом створення снапшотів файлів: вона робить знімок поточної версії та порівнює його з попереднім, тим самим виявляючи можливі загрози. HIDS найкраще встановлювати на критично важливі машини в мережі, які рідко змінюють конфігурацію.

1.4.2. Системи виявлення вторгнень на основі сигнатур

Системи виявлення вторгнень цього типу працюють за подібним до антивірусного програмного забезпечення принципом. Вони аналізують сигнатури

і порівнюють їх із базою, яка повинна постійно оновлюватися для забезпечення коректної роботи. Відповідно, основним недоліком сигнатурних систем виявлення вторгнень є те, що якщо, з якихось причин, база недоступна, мережа стає уразливою. Також, якщо атака є новою і її сигнатура невідома, існує ризик того, що загроза не буде виявлена.

Сигнатурні системи виявлення вторгнень можуть відстежувати шаблони або стани. Шаблони – це сигнатури, які зберігаються в постійно оновлюваній базі, а стани – це будь-які дії всередині системи.

Початковий стан системи – це нормальна робота, відсутність атаки. Після успішної атаки система переходить в скомпрометований стан, тобто зараження пройшло успішно. Кожна дія (наприклад, встановлення з'єднання за протоколом, що не відповідає політиці безпеки компанії, активація ПЗ і таке інше) може змінити стан. Таким чином, сигнатурні системи виявлення вторгнень відстежують не дії, а стани системи. Як можна зрозуміти з опису вище, NIDS частіше відстежують шаблони, тоді як HIDS переважно фокусуються на станах.

1.4.3. Системи виявлення вторгнень засновані на аномаліях

Цей тип систем виявлення вторгнень, за принципом роботи, в певному відношенні схожий на відстеження станів, але має більший охоплення.

Системи виявлення вторгнень засновані на аномаліях, використовують технології машинного навчання. Для правильної роботи таких систем виявлення загроз необхідний період навчання. Рекомендується адміністраторам протягом перших кількох місяців повністю вимкнути сигнали тривоги, щоб система могла навчатися. Після тестового періоду вона готова до роботи. Система аналізує роботу мережі в поточний момент, порівнює її з аналогічним періодом і виявляє аномалії.

Аномалії поділяються на три категорії:

- статистичні;
- аномалії протоколів;
- аномалії трафіку;

Статистичні аномалії виявляються, коли система виявлення вторгнень складає профіль стандартної активності (обсяг вхідного/вихідного трафіку, запускаємі додатки і тому інше) і порівнює його з поточним профілем. Наприклад, для компанії характерний зріст трафіку в будні дні на 90%. Якщо трафік раптово збільшиться не на 90%, а на 900%, система сповістить про загрозу.

Для виявлення аномалій протоколів система виявлення вторгнень аналізує комунікаційні протоколи, їх зв'язки з користувачами, додатками і створює профілі. Наприклад, веб-сервер повинен працювати на порту 80 для HTTP і 443 для HTTPS. Якщо інший порт буде використовуватися для передачі інформації по HTTP або HTTPS, система виявлення вторгнень відправе сповіщення.

Також IDS можуть виявляти аномалії, будь-яку небезпечну або навіть загрозливу активність у мережевому трафіку. Наприклад, при розгляді атаки DoS. Якщо спробувати провести таку атаку «в лоб», її розпізнає і зупинить навіть файервол. Творчі злочинці можуть випускати пакети з різних адрес (DDoS), що вже складніше виявити. Технології системи виявлення вторгнень аналізують мережевий трафік і завчасно запобігають подібним атакам.

1.5. Визначення конкретних практичних результатів, які буде досягнуто з впровадженням нової конфігурації

Одним з ключових аспектів визначення результатів є оптимізація продуктивності ІТС, що передбачає підвищення ефективності виявлення та блокування шкідливого коду, а також зниження часу відновлення після інцидентів. Це спрямовано на забезпечення неперервності бізнес-процесів та зниження впливу інцидентів на роботу ІТС.

Досягнення оптимізації продуктивності передбачає вдосконалення алгоритмів виявлення вторгнень та оптимізацію реакційних заходів. Це включає в себе розробку ефективних сигнатур для виявлення нових типів загроз, покращення механізмів аналізу аномалій та впровадження сучасних методів машинного навчання для прогнозування та усунення загроз.

Додатковим результатом буде забезпечення високої ступені впевненості в безпеці ІТС, що визначатиметься низьким рівнем вразливостей та високою надійністю захисту. Оцінювання цього результату включатиме аналіз кількості та типів виявлених загроз, а також ефективність застосованих заходів протидії.

Додатково, важливо буде впровадження системи виявлення вторгнень (IDS) для ефективного виявлення та реагування на події, що порушують безпеку мережі. Це допоможе у недопущенні несанкціонованого доступу та запобіганні подальшим інцидентам кібербезпеки.

Крім того, передбачається виправлення вразливостей, зокрема у бездротовому маршрутизаторі TP-LINK Archer A8, для запобігання можливим атакам та забезпечення надійного рівня кіберзахисту в мережі. Вирішення виявленої вразливості CVE-2019-7405 та інших потенційних ризиків є важливим кроком для підвищення загальної стійкості та безпеки ІТС.

Узагальнюючи, успішне впровадження нової конфігурації передбачає покращення ефективності, забезпечення високого рівня безпеки та надійності мережевої інфраструктури, а також реагування на потенційні кіберзагрози та виявлення вторгнень.

1.6. Постановка задачі

Для реалізації визначеної стратегії та досягнення визначених практичних результатів, передбачається проведення комплексного впровадження конкретних заходів з урахуванням вищезазначених методів та підходів, які були ретельно розглянуті в попередньому розділі. Кожен із цих заходів націлений на покращення кіберзахищеності та оптимізацію роботи ІТС підприємства «FixUp». Зокрема:

Оновлення мережевого обладнання: Заміна бездротового маршрутизатора TP-LINK Archer A8 на більш сучасну модель з підвищеним рівнем кіберзахисту, підтримкою сучасних шифрувань та виправленням виявленої вразливості. Розширення кількості портів для підключення пристроїв без необхідності використання додаткового комутатора.

Реалізація Системи Виявлення Вторгнення: Розробка та впровадження спеціалізованої системи виявлення вторгнень для ефективного моніторингу мережі

та реагування на потенційні загрози. Це включає в себе встановлення програмного та апаратного забезпечення, розробку сигнатур та алгоритмів аналізу для виявлення вразливостей та непередбачуваної активності.

Кожен із цих елементів є важливим етапом в реалізації стратегії безпеки та спрямований на досягнення конкретних цілей. Впровадження цих заходів передбачає комплексний підхід до удосконалення кіберзахищеності ІТС підприємства «FixUp» та забезпечення її оптимальної функціональності в умовах сучасних кіберзагроз.

1.7. Висновки

У даному розділі було здійснено аналіз сучасного стану кіберзахищеності об'єктів інформатизації та визначено стратегічний напрямок підвищення рівня безпеки в умовах постійно зростаючих загроз кібербезпеки. Проаналізована нормативно-правова база, що регулює сферу захисту інформації, з метою визначення ключових вимог та стандартів, які будуть визначати стратегічний курс у забезпеченні інформаційної безпеки. Особлива увага приділена вибору ефективного методу підвищення кіберзахищеності ІТС, визначеного як метод дослідження та проєктування, що передбачає глибокий аналіз і розробку нової конфігурації, відповідної сучасним вимогам кіберзахисту.

Конкретні практичні результати, що очікуються від впровадження нової конфігурації, визначені врахуванням виявлених вразливостей та врахуванням несприятливих тенденцій. Сформульовані завдання націлені на досягнення стратегічної мети з підвищення рівня інформаційної безпеки ІТС підприємства «FixUp» за допомогою інноваційних заходів та передових технологій в галузі кіберзахисту. У результаті проведеного аналізу та визначення конкретних заходів, робочий план розвитку кіберзахисту готовий до впровадження з метою оптимізації захисту інформації та підвищення стійкості до потенційних кіберзагроз.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1. Загальні відомості про ОІД

Підприємство «FixUp» виступає як високотехнологічний сервісний центр, який спеціалізується на виконанні ремонтних та технічних обслуговуваних процедур для комп'ютерної та мобільної техніки. Компанія розпочала свою діяльність у 2016 році та швидко визначилася на ринку як надійний партнер у сфері ремонтних послуг. Головним напрямком діяльності підприємства «FixUp» є високоякісний ремонт та технічне обслуговування електронної та мобільної техніки з використанням передових технологій та кваліфікованим персоналом.

Додатковим стратегічним напрямком діяльності є власний Інтернет-магазин, який пропонує широкий асортимент запчастин для ремонту комп'ютерів та мобільних пристроїв, а також аксесуарів для різноманітних мобільних пристроїв, включаючи планшети та телефони. Цей додатковий напрямок дозволяє компанії комплексно задовольняти потреби клієнтів, надаючи не лише послуги ремонту, але й можливість самостійного удосконалення та модернізації їхніх технічних пристроїв.

2.2. Обстеження ОІД

2.2.1. Обстеження фізичного середовища

Офісне приміщення компанії знаходиться за адресою проспект Дмитра Яворницького, 111, Дніпро, Дніпропетровська область, 49000. Графік роботи офісу з 10:00 до 18:00, з понеділка по суботу, неділя вихідний.

ОІД розташований на другому поверсі офісної будівлі, яка обладнана всього двома поверхами. До ОІД примикають сусідні офісні приміщення, які знаходяться на першому поверсі та за західною і південною внутрішньою стіною приміщення ОІД, інші стіни – зовнішні та ні до чого не примикають.

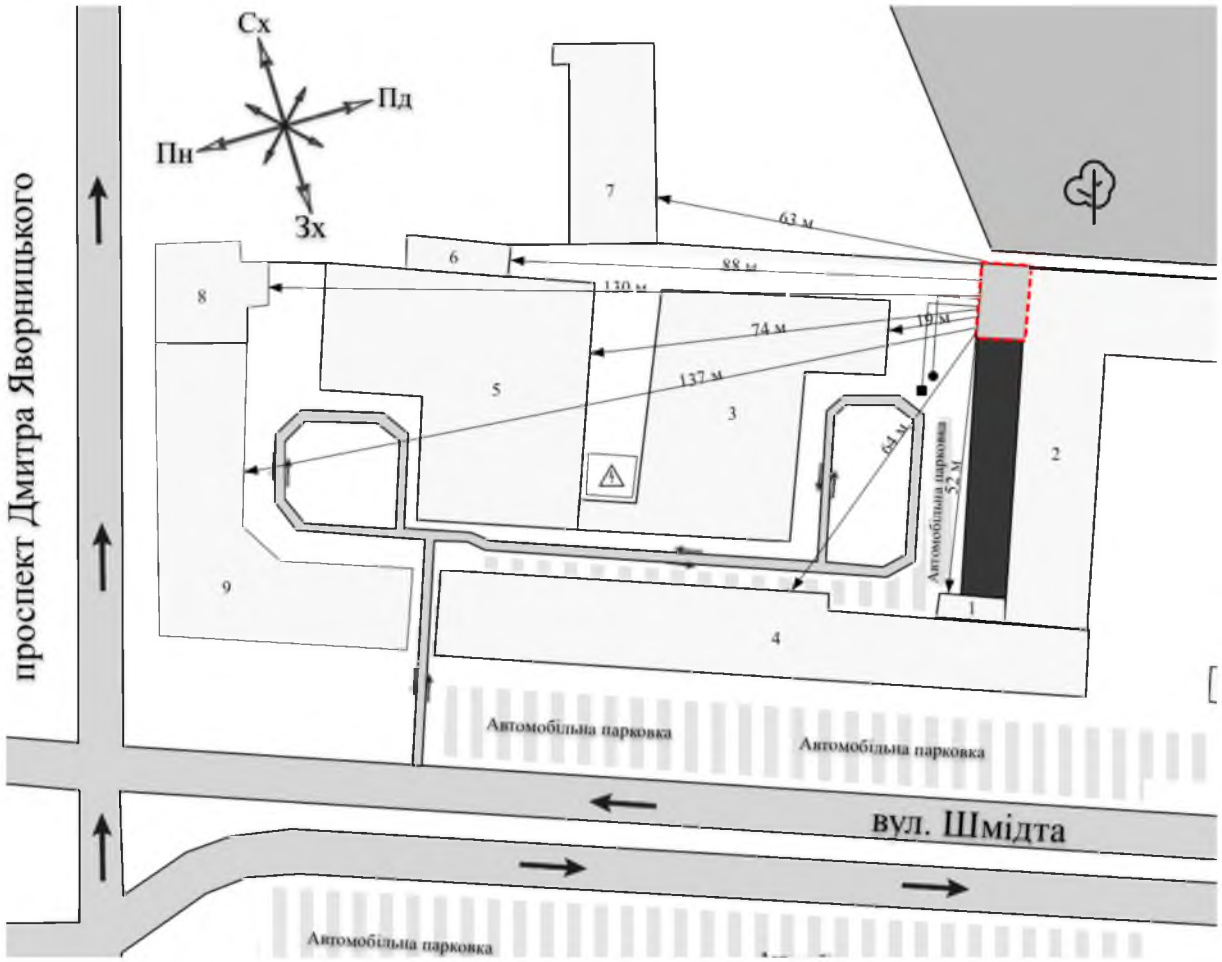
Вхід до ОІД можливий лише з вулиці, використовуючи сходи, які прямують безпосередньо на другий поверх будівлі до вхідних дверей ОІД. Межі контрольованої зони визначені стінами приміщення, де розташований ОІД.

Приміщення ОІД має чотири вікна: перше вікно розташоване з північної сторони, а три інші – зі східної сторони, обладнані залізними гратами зовнішньої сторони приміщення. Розмір осередку грат складає 15 см на 30 см, а діаметр арматури - 15 мм.

Охорону об'єкта забезпечує охоронна служба «Гуард». Охоронця на об’єкті немає. Деталі розташування ОІД на місцевості відображено ситуаційному плані, який зображено на рисунку 2.1, та в таблиці 2.1.

Таблиця 2.1 – Характеристика будівель та споруд

№	Найменування	Адреса	Кількість поверхів	Відстань до ОІД, м
1	Нежила технічна будівля	проспект Дмитра Яворницького, 111	1	52
2	Малі торгівельні приміщення	Шмідта, 2Б	1	–
3	Офісні приміщення	проспект Дмитра Яворницького, 111	1	19
4	Нежилий будинок з магазинами	Шмідта, 3	3	64
5	Торгівельний центр «Berlin»	проспект Дмитра Яворницького, 111	4	74
6	Господарський корпус	–	1	88
7	Багатоквартирний житловий будинок	проспект Дмитра Яворницького, 109	5	63
8	Нежилий будинок з магазинами	проспект Дмитра Яворницького, 109а	3	130
9	Нежилий будинок з магазинами	проспект Дмитра Яворницького, 111а	3	137



Умовні позначення:

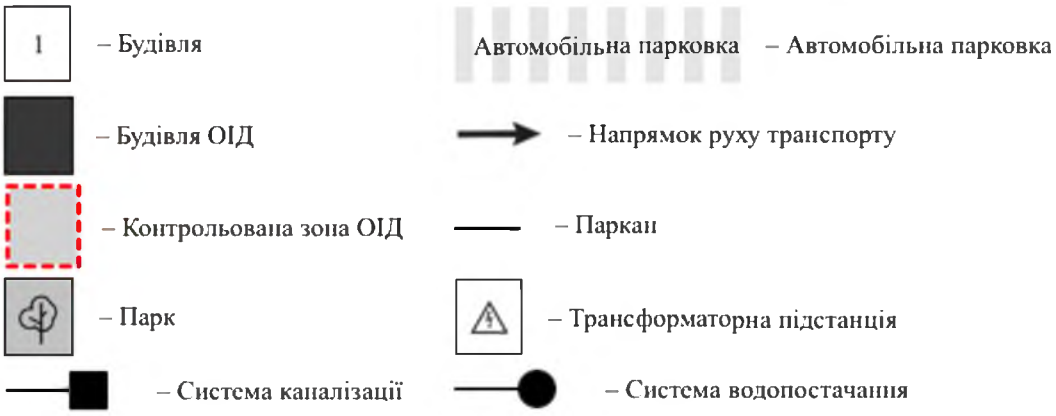


Рисунок 2.1 – Ситуаційний план

Системи забезпечення опалення, водопостачання та каналізації є централізованими та мають підключення через підвальне приміщення будівлі. Основні інженерні комунікації впритул входять в будівлю через це підвальне приміщення. Система електропостачання також централізована, проте трансформаторна підстанція розташована на відстані 75 метрів від будівлі ОІД.

Постачання електроенергії здійснюється підземними комунікаціями, які вводяться в підвальне приміщення.

Рисунок 2.2 – Генеральний план. Загальний

Мережа Інтернет-провайдера «DTS» також централізована і постачається до офісу з розподільного щитка, розташованого на першому поверсі будівлі. Кабельна лінія прокладена від розподільного щитка до ОІД.

Площа всіх приміщень ОІД становить 53,94 м² з розмірами 9,30 м на 5,80 м. Висота стелі складає 3 м, при цьому конструкція виконана із залізобетонних плит.

Товщина несучих стін становить 50 см і виготовлена із шлакоблоків, тоді як перегородки мають товщину 20 см і складаються із цегли. Підлога виготовлена з залізобетонних плит і має товщину 30 см.

Рисунок 2.3 – Генеральний план. Опис приміщень

Вхідні двері розміром 110 см на 210 см виконані з металу, мають товщину 90 мм і оснащені врізаним замком під ключ.

Міжкімнатні двері мають розміри 90 см на 210 см і виготовлені з ДСП, товщина дверей становить 60 мм, також вони обладнані врізаним замком під ключ.

Чотири вікна відчиняються всередину приміщення та виготовлені із ПВХ, оснащені однокамерним склопакетом (два скла). Розміри кожного вікна – 110 см на 140 см.

Сектор видимості вікон охоплює будівлі №3 та №5 з північної сторони та парк зі східної сторони.

На вікні з північної сторони встановлені горизонтальні жалюзі, які частіше залишаються у відкритому положенні для забезпечення природного освітлення.

Схема генерального плану ОІД наведена на рисунку 2.2 та 2.3.

У наступних підрозділах були вжиті всі необхідні заходи для підвищення рівня кіберзахисту, а також проведено докладне дослідження, спрямоване на вивчення впливу цих заходів.

2.3. Оновлення мережевого обладнання

У першому розділі аналізу було виявлено низку недоліків у поточному мережевому обладнанні, представленому у вигляді маршрутизатора та комутатора. Виявлені проблеми включають невідповідність вимогам мережі, недостатній рівень кіберзахисту та наявність вразливостей у системі безпеки.

На даний момент використовується бездротовий маршрутизатор TP-LINK Archer A8, який, хоча і є універсальним і придатним для використання в домашніх умовах чи невеликих офісах, має обмежені можливості щодо кількості портів та рівня кіберзахисту. Маршрутизатор, на жаль, має існуючі вразливості, такі як CVE-2019-7405, що створює серйозний ризик.

Наявність вразливостей, зокрема CVE-2019-7405, дозволяє несанкціонованому користувачеві отримати доступ до налаштувань маршрутизатора через протокол Telnet. Це може призвести до невпізнання автентифікації та до втрати контролю над пристроєм. Зловмисники можуть також використовувати цю вразливість для підключення до FTP-серверу, що становить потенційну загрозу для даних у локальній та глобальній мережі.

У зазначеному маршрутизаторі обмежена кількість доступних портів, що ускладнює підключення більшої кількості пристроїв. Для подолання цього обмеження використовується додатковий комутатор TP-LINK TL-SG108-M2 з високою пропускною здатністю та підтримкою восьми гігабітних портів Ethernet, включаючи один порт із швидкістю 2.5G Ethernet.

У зв'язку з виявленими проблемами, пропонується замінити поточний маршрутизатор та комутатор на більш безпечне та продуктивне обладнання –

маршрутизатор Cisco 891W-AGN-A-K9. Використання нового маршрутизатора вирішить проблему нестачі портів та значно підвищить рівень кіберзахисту мережі. Заміна обладнання дозволить не лише розширити можливості підключення пристроїв, але й забезпечить високий рівень кіберзахисту, враховуючи важливість цього аспекту у сучасних умовах використання мережевих ресурсів.

Рисунок 2.4 – Зовнішній вигляд маршрутизатора Cisco 891W-AGN-A-K9

Маршрутизатори Cisco серії 890 із вбудованими сервісами (ISR) поєднують в собі доступ до Інтернету, комплексний захист і бездротові сервіси в єдиному високопродуктивному пристрої, який легко розгортати та керувати. Вони ідеально підходять для використання як обладнання для обслуговування клієнта (CPE) в невеликих філіалах підприємства та в середовищах, де надаються управляючі послуги провайдерів.

Це потужні пристрої з фіксованою конфігурацією, які призначені для забезпечення безпечного та широкосмугового доступу, включаючи Metro Ethernet і бездротове підключення до локальної мережі (WLAN). Вони призначені для

використання в невеликих офісах та малих підприємствах для об'єднання в корпоративні мережі.

Cisco 891W-AGN-A-K9 (рисунок 2.4) – маршрутизатор компанії Cisco. Маршрутизатор представляє серію маршрутизаторів Cisco 891. Всі маршрутизатори цієї серії мають два інтерфейси WAN RJ-45 (для зв'язку з глобальною мережею передачі даних). Один з цих інтерфейсів працює за технологією Fast Ethernet (пропускна здатність підключеної лінії зв'язку становить 100 Мбіт/с), а інший – Gigabit Ethernet (пропускна здатність підключеної лінії зв'язку становить 1 Гбіт/с).

Крім того, всі маршрутизатори Cisco 891, поряд з маршрутизатором Cisco 891W-AGN-A-K9, мають 8 локальних портів RJ-45 з підтримкою Fast Ethernet, USB, AUX і консольний порт (консольний порт і запасний порт управління входять до складу маршрутизатора Cisco 891W-AGN-A-K9 одноразово, в той час, як порт USB 2.0 – дворазово).

Єдиною відмінністю від серії маршрутизаторів Cisco 892 є наявність запасного порту V.92 (у серії маршрутизаторів Cisco 892 замість нього є ISDN BRI). Порт V.92 маршрутизатора Cisco 891W-AGN-A-K9 служить для модемного з'єднання з глобальною мережею передачі даних (якщо по інших портах зв'язок встановити не вдається або неможливо). Протокол V.92 у маршрутизаторі Cisco 891W-AGN-A-K9 нині використовується дуже рідко, оскільки його максимальна швидкість прийому даних становить 56 кбіт/с, а передачі – 48 кбіт/с.

Маршрутизатор включає в себе вбудовану бездротову точку доступу для надання дво-смугового бездротового зв'язку за технологією Wi-Fi стандартів 802.11a/b/g/n. Функція PoE використовується для живлення IP-телефонів та інших пристроїв.

Рисунок 2.5 – Задня панель маршрутизатора Cisco 891W-AGN-A-K9

Характеристики маршрутизаторів Cisco 890 Series включають інтерфейси, такі як WAN порти, LAN порти з підтримкою PoE, USB 2.0 порт, підтримку 802.11a/g/n, консольний і допоміжний порт. Програмне забезпечення Cisco IOS забезпечує розширений набір функцій IP. Маршрутизатори мають пам'ять DRAM та Flash для ефективного виконання завдань.

На рисунку 2.7 представлено задню панель маршрутизатора, на якій відображені порти та роз'єми, включаючи резервний порт WAN (FE WAN), SDN, основний порт WAN (GE WAN), SFP, порт USB, V.92 backup, 8 портів 10/100/1000 Ethernet з 4 портами PoE, консоль/допоміжний порт, роз'єм живлення, перемикач увімк./вимк., кнопку скидання, заземлення та слот безпеки Kensington.

Таблиця 2.2 – Порівняльна характеристика обладнання

Характеристика	Cisco 891W-AGN-A-K9	TP-LINK Archer A8	TP-LINK TL-SG 108-M2
Стандарти WLAN	Точка доступу на основі стандартів IEEE 802.11n draft	IEEE 802.11ac/n/a 5 ГГц; IEEE 802.11n/b/g 2,4 ГГц	–

Продовження таблиці 2.2 – Порівняльна характеристика обладнання

Характеристика	Cisco 891W-AGN-A-K9	TP-LINK Archer A8	TP-LINK TL-SG 108-M2
	v2.0 із сумісністю 802.11 a/g; Автоматичний вибір швидкості для 802.11a/g/n; 2,4 ГГц, 5 ГГц		
Стандарти шифрування WLAN	WEP; WPA; AES (WPA2); WPA/WPA2-Enterprise; PSK; TKIP/SSN; EAP	WEP; WPA; WPA2; WPA/WPA2-Enterprise	–
Інтерфейси	Керовані 8 x LAN 10/100 Мбіт/с порти RJ45; 1 x WAN 10/100/1000 Мбіт/с і 1 x WAN Fast Ethernet порти RJ45; Автоматичний MDI/MDIX, BASE-T	4 x LAN 10/100/1000 Мбіт/с порти RJ45; 1 x WAN 10/100/1000 Мбіт/с порт RJ45	Не керовані 8 x 10/100/1000 Мбіт/с порти RJ45; Автоматичний MDI/MDIX
Швидкість передачі пакетів, Mpps	11.9	11.9	11.9
Сертифікація		FCC, RoHS	CE, FCC, RoHS

Продовження таблиці 2.2 – Порівняльна характеристика обладнання

Характеристика	Cisco 891W-AGN-A-K9	TP-LINK Archer A8	TP-LINK TL-SG 108-M2
Споживання електроенергії, Ватт/год	До 80 (220 В/50 Гц)	До 18 (220 В/50 Гц)	До 3,75 (220 В/50 Гц)

На таблиці 2.2 наведена порівняльна характеристика обладнання. На основі представленої інформації можна зробити висновок, що переваги використання залишаються саме за маршрутизатором Cisco 891W-AGN-A-K9. Його характеристики, такі як стандарти WLAN, стандарти шифрування WLAN, інтерфейси та сертифікація, роблять його більш ефективним і надійним рішенням порівняно з конкурентами.

Маршрутизатор Cisco 891W-AGN-A-K9 встановлено замість існуючого маршрутизатора, і в зв'язку з цим не буде потрібен додатковий комутатор, який використовувався раніше для розширення можливостей підключення пристроїв

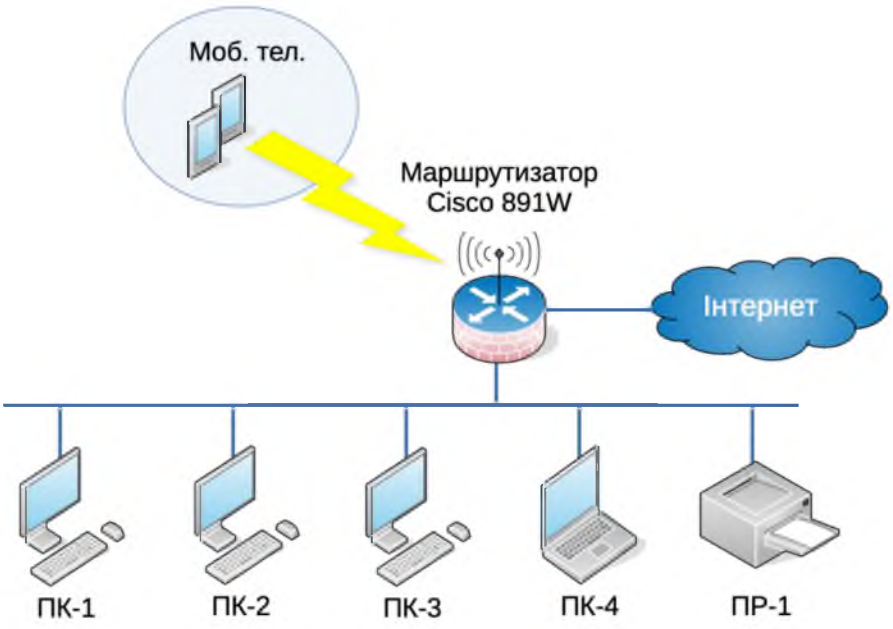


Рисунок 2.6 – Схема ІТС після проєктування

На рисунку 2.6 відображена нова схема ІТС після проєктування, де використовується маршрутизатор Cisco 891W-AGN-A-K9. Після підключення маршрутизатора треба провести базове налаштування.

Вмикаємо шифрування паролей, використовуєм нову модель AAA та локальну базу користувачів. Створюємо користувача з максимальними правами:

```
> service password-encryption
> aaa new-model
> aaa authentication login default local
> username admin privilege 15 secret PASSWORD
```

Даємо ім’я хосту в мережі:

```
> hostname router
> ip domain-name router.domain
```

Генеруємо ключ для авторизації та налаштуємо SSH:

```
> crypto key generate rsa modulus 1024
> ip ssh time-out 60
> ip ssh authentication-retries 2
> ip ssh version 2
```

Вмикаємо прискорену комутацію пакетів:

```
> ip cef
```

Налаштовуємо час на зону GMT+2 та оновлюємо системний годинник через NTP:

```
> clock timezone Ukraine 2
> clock summer-time Ukraine recurring last Sun Mar 2:00 last Sun Oct 2:00
> ntp update-calendar
```

Налаштовуємо DNS увімкнувши простір імен, внутрішній DNS сервер, та публічний DNS сервер:

```
> ip domain-lookup
> ip dns server
> ip name-server 4.2.2.2
> ip name-server 208.67.222.222
> ip name-server 208.67.220.220
```

Налаштуємо локальну мережу та ввімкнемо підрахунок пакетів, що передаються клієнтами, щоб зручно переглядати хто більше використовує трафіку:

```
> interface Vlan1
  description === LAN ===
  ip address 192.168.1.1
> ip accounting output-packets
! подивитися статистику можна командою:
> show ip accounting
! очистити:
> clear ip accounting
```

Налаштування сервера DHCP

```
! виключаємо деякі адреси з пулу
> ip dhcp excluded-address 192.168.1.1 192.168.1.99
! і налаштовуємо пул адрес
> ip dhcp pool LAN
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.1
  dns-server 192.168.1.1
```

Налаштуємо Інтернет та Firewall:

```
! налаштовуємо фільтр вхідного трафіку (за замовчуванням все заборонено)
> ip access-list extended FIREWALL
  permit tcp any any eq 22

! включаємо інспектування трафіку між локальною мережею та Інтернетом
> ip inspect name INSPECT_OUT dns
```

```
> ip inspect name INSPECT_OUT icmp
> ip inspect name INSPECT_OUT ntp
> ip inspect name INSPECT_OUT tcp router-traffic
> ip inspect name INSPECT_OUT udp router-traffic
> ip inspect name INSPECT_OUT icmp router-traffic

! налаштовуємо порт в Інтернет і вішаємо на нього певний захист
> interface FastEthernet0/0
  description === Internet ===
  ip address 192.168.1.1 255.255.255.0
  ip virtual-reassembly
  ip verify unicast reverse-path
  no ip redirects
  no ip directed-broadcast
  no ip proxy-arp
  no cdp enable
  ip inspect INSPECT_OUT out
  ip access-group FIREWALL in

! ну і насамкінець шлюз за замовчуванням
> ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Після успішного виконання основних операцій з налаштування маршрутизатора та підключення клієнтських пристроїв переходимо до аналізу та оцінки впливу оновленого мережевого обладнання на ефективність ІТС.

2.4. Дослідження результатів ефективності мережі ІТС після оновлення мережевого обладнання

У цьому етапі зроблено акцент на дослідженні отриманих результатів, спрямованих на виявлення покращень у функціонуванні та продуктивності інформаційно-комунікаційної системи. Ретельно проаналізовано вплив оновлених

параметрів мережі на продуктивність, надійність та загальну ефективність ІТС з метою забезпечення його оптимального функціонування.

Шляхом аналізу лог-файлів пристроїв TP-Link Archer A8 та Cisco 891W-AGN-A-K9, ми здобули можливість ретельно дослідити і кількісно оцінити випадки відмов у роботі маршрутизаторів протягом 30-денного періоду. Отримані дані ілюструють відмінності в стабільності між обома пристроями.

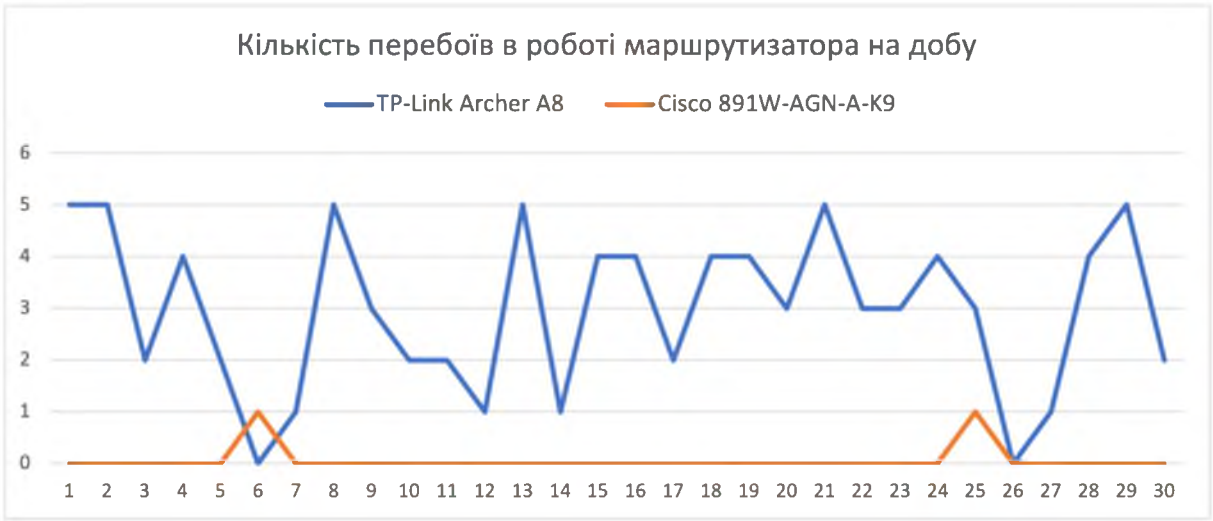


Рисунок 2.7 – Кількість перебоїв в роботі маршрутизатора на добу

Аналіз (рисунок 2.7) вказує на те, що перший маршрутизатор (TP-Link Archer A8) проявляє підвищену частоту відмов, викликаючи збої в роботі приблизно 2-4 разів на добу, а в загальній кількості це 86 збоїв за 30 діб. У той час як другий маршрутизатор (Cisco 891W-AGN-A-K9) виявив лише 2 випадки відмов за весь аналізований період, відзначаючись значною стабільністю в порівнянні з першим.

Для розрахунку відсоткового поліпшення в ситуації, де кількість відмов зменшилась з 86 до 2, використаємо наступну формулу:

$$\text{Поліпшення} = \left(\frac{\text{Початкова кількість} - \text{Кінцева кількість}}{\text{Початкова кількість}}\right) \cdot 100 \qquad (2.1)$$

В нашому випадку рішення буде таким:

$$\text{Поліпшення} = \left(\frac{86-2}{86}\right) \cdot 100 \approx 97.67 \qquad (2.2)$$

Отже, ситуація поліпшилась на 97.67%, що є дуже значним покращенням в стабільності всієї мережі.

Щодо відновлення роботи, наявність лог-файлів також дозволяє нам провести детальний аналіз часу, витраченого на відновлення функціональності в разі кожного випадку збою.

Це включає в себе не лише загальний час відмови, але і час, що витрачений на виявлення, локалізацію та усунення причин виникнення збою. З отриманих даних ми можемо докладно визначити, скільки часу було затрачено на кожному етапі відновлення роботи мережевого обладнання, що надасть нам цінний інсайт у ефективність вжитих заходів та розроблених процедур. Детально по-добово час на відновлення відображено на рисунках 2.10 та 2.11.

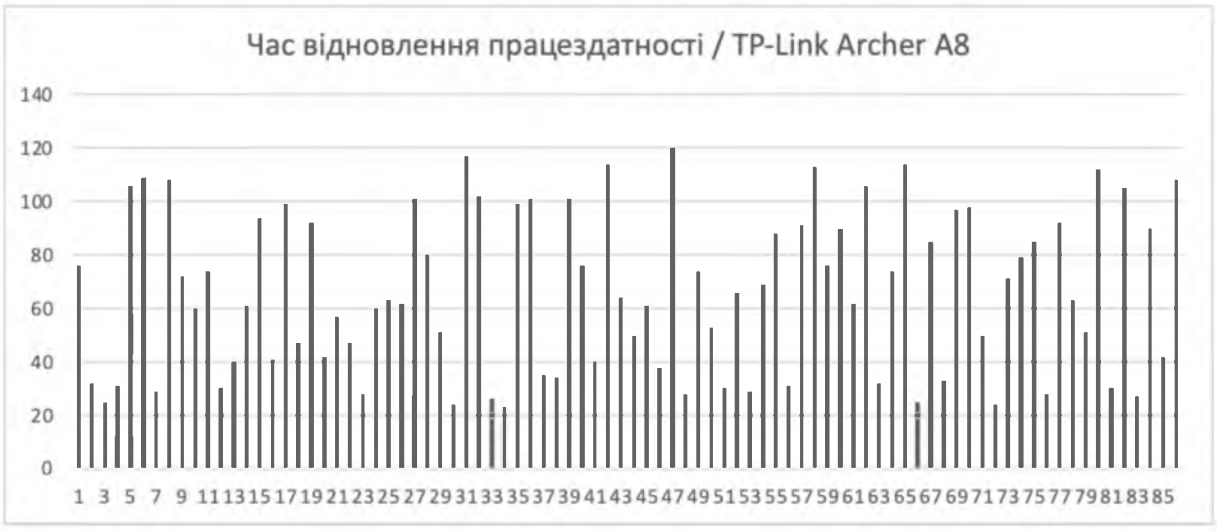


Рисунок 2.8 – Час відновлення працездатності першого маршрутизатора

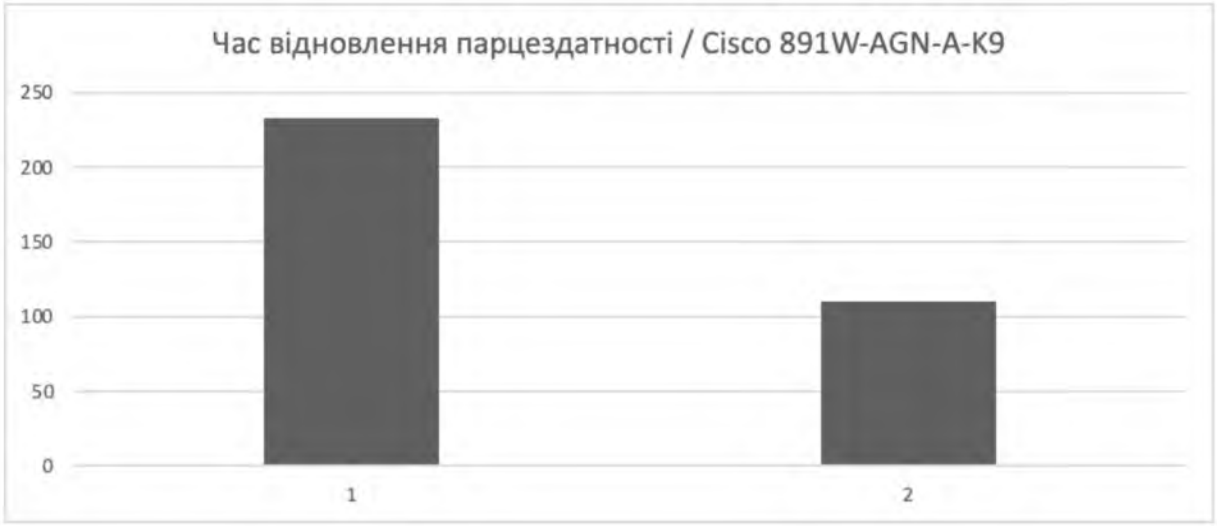


Рисунок 2.9 – Час відновлення працездатності другого маршрутизатора

Аналізуючи представлені графіки (рисунок 2.8 та 2.9), ми можемо зробити висновок, що середній час, необхідний для відновлення роботи першого маршрутизатора, складає 66 секунд для кожного конкретного випадку, при цьому зафіксовано 86 випадків загальною тривалістю в 5663 секунд, що становить майже 95 хвилин непрацездатного часу. Щодо другого маршрутизатора, середній час відновлення становить 170 секунд на випадок, і це враховуючи лише 2 випадки з загальною тривалістю в 343 секунди.

Ці дані надають можливість провести більш детальний аналіз ефективності відновлення кожного маршрутизатора окремо та в порівнянні між собою.

Для розрахунку відсоткового поліпшення в ситуації, де кількість відмов зменшилась з 86 до 2, використаємо формулу, яку ми використовували раніше:
В нашому випадку поліпшення складатиме:

$$\text{Поліпшення} = \left(\frac{5663 - 343}{5663}\right) \cdot 100 \approx 93.94 \qquad (2.3)$$

В цьому випадку ситуація також поліпшилась, поліпшилась на 93.94%. Ці висновки свідчать про різницю в надійності та стабільності мережевих пристроїв,

яка безпосередньо впливає на продуктивність та доступність мережі для користувачів.

Зазначимо також, що в новому маршрутизаторі вбудовано величезну кількість технологічних рішень, призначених для забезпечення високого рівня безпеки та захисту. Ці технології охоплюють широкий спектр заходів, спрямованих на усунення можливих загроз та вразливостей, що можуть виникнути в процесі експлуатації мережевого обладнання. Нова модель маршрутизатора володіє передовими засобами ідентифікації, контролю доступу та захисту від різноманітних кіберзагроз, надаючи комплексний підхід до забезпечення безпеки мережі. Порівняння наведено у таблиці 2.3:

Таблиця 2.3 – Порівняльна характеристика (безпека мережі)

Cisco 891W-AGN-A-K9	TP-Link Archer A8
• SSL VPN для безпечного віддаленого доступу • Апаратно-прискоренений DES, 3DES, AES 128, AES 192 та AES 256 • Підтримка інфраструктури з відкритим ключем (PKI) • 50 тунелів IPsec • Клієнт та сервер Cisco Easy VPN • Прозорість NAT • DMVPN • VPN з шифруванням транспорту для груп без тунелів • IPsec з можливістю станового аварійного відновлення • IPsec, що свідомий VRF	• Міжмережевий екран SPI • Управління доступом • Прив'язка IP- та MAC-адрес • Шлюз прикладного рівня

Продовження таблиці 2.3 – Порівняльна характеристика (безпека мережі)

Cisco 891W-AGN-A-K9	TP-Link Archer A8
• IPsec через IPv6 • Адаптивна технологія управління • Шлюз застосункового рівня протоколу ініціювання сеансу (SIP) • Брандмауер Cisco IOS: ○ Брандмауер політики на основі зон ○ Брандмауер зі свідомим інспекційним маршрутизаційним брандмауером ○ Брандмауер прозорий інспекції зі свідомим станом ○ Розширений контроль та управління застосунками ○ Проксі-аутентифікація HTTPS, FTP та Telnet ○ Динамічна та статична безпека порту ○ Брандмауер із свідомим аварійним відновленням ○ Брандмауер, свідомий VRF • Фільтрація вмісту: ○ Підписна фільтрація вмісту за допомогою Trend Micro ○ Підтримка Websense та SmartFilter ○ Чорні та білі списки програмного забезпечення Cisco IOS • Інтегрований контроль загроз:	

Продовження таблиці 2.3 – Порівняльна характеристика (безпека мережі)

Cisco 891W-AGN-A-K9	TP-Link Archer A8
○ Система запобігання вторгнень (IPS) ○ Керування пакетами керування ○ Гнучке пакетне відповідання Захист мережевого фундаменту	

Також важливо відзначити, що в новому маршрутизаторі впроваджено значну кількість технологічних рішень, які спрямовані на забезпечення високого рівня безпеки та захисту бездротових мереж (WLAN). Порівняння наведено у таблиці 2.4:

Таблиця 2.4 – Порівняльна характеристика (безпека бездротової мережі)

Cisco 891W-AGN-A-K9	TP-Link Archer A8
• Стандарт 802.11i • WPA та AES (WPA2) • Аутентифікація EAP: ○ Cisco LEAP, PEAP, ○ Протокол автентифікації на транспортному рівні (EAP TLS), ○ Гнучкий протокол автентифікації через безпечний тунель (EAP-FAST), ○ Протокол автентифікації на тунельному рівні (EAP-TTLS), ○ Протокол автентифікації-Модуль інформації про абонента (EAP-SIM),	• WEP • WPA • WPA2 • WPA/WPA2-Enterprise (802.1x) • WPA3

Продовження таблиці 2.4 – Порівняльна характеристика (безпека бездротової мережі)

Cisco 891W-AGN-A-K9	TP-Link Archer A8
○ Протокол автентифікації-Повідомлення з хешуванням (EAP-MD5), ○ Протокол автентифікації-Тунельний TLS (EAP-TTLS) • Статичне та динамічне шифрування Wired Equivalent Privacy (WEP) • Шифрування протоколу TKIP/SSN (Temporal Key Integrity Protocol/Simple Security Network) • Аутентифікація та фільтрація за MAC-адресою • База даних користувачів для забезпечення виживання місцевої аутентифікації за допомогою LEAP та EAP-FAST • Налаштований обмежений ліміт кількості бездротових клієнтів • Налаштований облік RADIUS для бездротових клієнтів Передвизначені ключі (PSKs) (WPA-Small Office or Home Office [WPA-SOHO])	

2.5. Система виявлення та запобігання вторгнень

Системи виявлення вторгнень стають все більш необхідним доповненням інфраструктури мережевої безпеки. На відміну від мережевих екранів, які працюють на основі політики безпеки, системи виявлення вторгнень виступають як засоби моніторингу та спостереження за підозрілою активністю. Вони можуть виявляти атаки, які ухилилися від мережевих екранів, та повідомляти про це адміністратору, який, в свою чергу, приймає подальші заходи щодо запобігання атаки. Використання технологій виявлення вторгнень не робить систему абсолютно безпечною. Використання системи виявлення вторгнень допоможе досягти декількох цілей:

- Виявлення вторгнень або мережевих атак.
- Прогнозування можливих майбутніх атак та виявлення вразливостей для запобігання їх подальшому розвитку. Зазвичай зловмисник виконує ряд попередніх дій, таких як, наприклад, сканування мережі або інше тестування для виявлення вразливостей цільової системи.
- Провести документування існуючих загроз;
- Забезпечити контроль якості адміністрування з точки зору безпеки, особливо великих і складних мережах;
- Отримати корисну інформацію про вторгнення, які відбулися, для відновлення та коригування факторів, що спричинили вторгнення;
- Визначити місце розташування джерела атаки відносно локальної мережі (зовнішні або внутрішні атаки), що є важливим при прийнятті рішень щодо розміщення ресурсів в мережі.

В новому маршрутизаторі Cisco 891W-AGN-A-K9 вже вбудований функціонал системи запобігання вторгнень, що знімає необхідність встановлювати додаткове обладнання для цієї мети. Як зазначалось вище, система запобігання вторгнень являє собою програмну або апаратну систему мережевої та комп'ютерної

безпеки, яка виявляє вторгнення або порушення безпеки та автоматично захищає від них.

Системи запобігання вторгнень можна розглядати як розширення систем виявлення вторгнень (IDS), так як завдання відстеження атак залишається однаковою. Однак, вони відрізняються в тому, що система виявлення вторгнень повинна відслідковувати активність в реальному часі і швидко реалізовувати дії щодо запобігання атак.

2.5.1. Методи реагування на атаки. Після початку атаки

Методи реалізуються вже після того, як була виявлена інформаційна атака. Це означає, що навіть у разі успішного виконання системі, що захищається може бути завдано шкоди.

– Блокування з'єднання:

Якщо для атаки використовується TCP-з'єднання, то реалізується його закриття за допомогою посилки кожному або одному з учасників TCP-пакета з встановленим прапором RST. У результаті зловмисник позбавляється можливості продовжувати атаку, використовуючи мережеве з'єднання. Даний метод найчастіше реалізується з допомогою наявних мережевих датчиків.

Метод характеризується двома основними недоліками:

- Не підтримує протоколи, відмінні від TCP, для яких не вимагається попереднього встановлення з'єднання (наприклад, UDP і ICMP);
- Метод може бути використаний тільки після того, як зловмисник вже отримав несанкціоноване з'єднання.

– Блокування записів користувачів:

Якщо кілька облікових записів користувачів були скомпрометовані в результаті атаки або виявилися їх джерелами, то здійснюється їх блокування хостовими

датчиками системи. Для блокування датчики повинні бути запущені від імені облікового запису, який має права адміністратора.

Також блокування може відбуватися на заданий строк, який визначається налаштуваннями Системи запобігання вторгнень.

– Блокування хоста комп'ютерної мережі:

Якщо з одного з хостів була зафіксована атака, то може бути проведене його блокування хостовими датчиками або блокування мережевих інтерфейсів або на нього, або на маршрутизаторі або комутаторі, за допомогою яких хост підключений до мережі. Розблокування може відбуватися через заданий проміжок часу або за допомогою активації адміністратора безпеки. Блокування не скасовується після перезапуску або відключення від мережі хоста. Так само для нейтралізації атаки можна блокувати ціль атаки, хост комп'ютерної мережі.

– Блокування атаки за допомогою мережевого екрану:

Система запобігання вторгнень формує і надсилає нові конфігурації в мережевий екран, за якими екран буде фільтрувати трафік від порушника. Така реконфігурація може відбуватися в автоматичному режимі з допомогою стандартів OPSEC (наприклад SAMP, CPMI).

Для мережевих екранів, які не підтримують протоколи OPSEC, для взаємодії із Системою запобігання вторгнення може бути використаний модуль-адаптер:

- На який будуть надходити команди про зміну конфігурації мережевого екрану;
- Який буде редагувати конфігурації мережевого екрану для модифікації його параметрів.

– Зміна конфігурації комунікаційного обладнання:

Для протоколу SNMP (англ. Simple Network Management Protocol — простий протокол керування мережею), система запобігання вторгнень аналізує і змінює параметри з бази даних MIB (такі як таблиць маршрутизації, налаштування портів)

з допомогою агента пристрою, щоб блокувати атаку. Також можуть бути використані протоколи TFTP, Telnet та інші.

– Активне придушення джерела атаки:

Метод теоретично може бути використаний, якщо інші методи виявляться марними. Система запобігання вторгнень виявляє і блокує пакети порушника, та здійснює атаку на його сайт, за умови, що його адресу однозначно визначено і в результаті таких дій не буде завдано шкоди іншим легальним вузлам. Такий метод реалізовано в декількох некомерційних ПО:

- NetBuster – запобігає проникненню в комп'ютер «Троянського коня». Він може також використовуватися як засіб «fool-the-one-trying to NetBus-you» («обдури того, хто намагається проникнути до тебе на «Троянському коні»). У цьому випадку він розшукує шкідливу програму і визначає комп'ютер який запустив її, а потім повертає цю програму адресанту.
- Tambu UDP Scrambler – працює з портами UDP. Продукт діє не тільки як фіктивний UDP-порт, він може використовуватися для «паралізації» апаратури хакерів за допомогою невеликої програмки UDP flooder.

Так як гарантувати виконання всіх умов неможливо, широке застосування методу на практиці поки що неможливо.

2.5.2. Методи реагування на атаки. На початку атаки

Методи реалізують заходи, які запобігають виявлені атаки до того, як вони досягають мети.

– З допомогою мережевих датчиків:

Мережеві датчики встановлюються в розрив каналу зв'язку так, щоб аналізувати всі пакети які проходять. Для цього вони оснащуються двома мережевими адаптерами, які функціонують у «змішаному режимі», на прийом і на передачу, записуючи всі пакети в буферну пам'ять, звідки вони зчитуються

модулем виявлення атак системи запобігання вторгнень. У разі виявлення атаки ці пакети можуть бути видалені. Аналіз пакетів проводиться на основі сигнатурного або поведінкового методів.

– За допомогою датчиків хостових:

Віддалені атаки, які реалізуються відправкою від зловмисника серією пакетів. Захист реалізується з допомогою системи виявлення вторгнень за аналогією з мережевими датчиками, але на відміну від останніх мережева компонента перехоплює і аналізує пакети на різних рівнях взаємодії, що дає запобігати атакам по криптозахищеним IPseci (скорочення від IP Security) SSL/TLS з'єднанням.

Та локальні атаки при несанкціонованому запуску зловмисником програм або інших діях, що порушують інформаційну безпеку. Перехоплюючи системні виклики всіх додатків і аналізуючи їх, датчики блокують ті виклики, які становлять небезпеку.

2.6. Дослідження переваг використання системи виявлення та запобігання вторгнень

Використовуване мережеве обладнання, а саме маршрутизатор TP-Link Archer A8 мав на борту тільки мережевий екран без особливих функцій. Зараз же, після оновлення мережевого обладнання нам доступні мережевий екран та всі переваги і особливості системи виявлення та запобігання вторгнень, яка вбудована в новий маршрутизатор Cisco 891W-AGN-A-K9 та називається Cisco IPS. Ця інтегрована система надає нам додаткові рівні безпеки та ефективні інструменти для виявлення та протидії потенційним загрозам у мережі.

Таким чином, враховуючи інформацію, подану у попередніх підпунктах, можна зробити наступні висновки:

Атаки та загрози, від яких мережевий екран при правильній конфігурації має можливість захищати наведено в таблиці 2.5.

Таблиця 2.5 – Види загроз, від яких захищає мережевий екран

Загроза	Опис загрози
Бекдор доступу	Це атаки з використанням вразливостей у встановленому на ПК програмному забезпеченні: операційній системі, утилітах, прикладних додатках. Такі проломи можуть бути скрізь, включаючи Windows, вони дозволяють хакеру отримати доступ до пристрою, надсилати і приймати з нього з трафік. Мережевий екран блокує такі дії
Фішинг	Шахрайська схема, в ході якої користувач потрапляє на фальшивий (фішинговий) сайт, один в один відомий веб-ресурс, що копіює. Наприклад, повторює сторінки входу до соціальної мережі чи оплати через онлайн-банкінг. Людина вводить особисті дані і вони потрапляють до рук зловмисника. Мережевий екран забороняє підключення до підозрілих сайтів
Злам віддаленого доступу	За допомогою віддаленого робочого столу користувач може керувати комп'ютером через інтернет, тобто дистанційно. Хакери можуть перехопити цей доступ та вкрасти важливі дані. До завдань брандмауера входить заборона на передачу такого трафіку

Продовження таблиці 2.5 – Види загроз, від яких захищає мережевий екран

Загроза	Опис загрози
Переадресація маршруту	Пакети даних передаються по мережі певними маршрутами, а цей вид атак передбачає заміну шляху проходження інформації таким чином, щоб кінцевий пристрій нічого не «підозрював»
DDoS-атаки	Оскільки головне завдання брандмауера це фільтрація, він допомагає впоратися з напливом величезних обсягів трафіку. Блокування працює як на вхідні, так і на вихідні пакети, якщо ваш пристрій спробують використовувати як атакуючий

Отримуємо результат, що мережевий екран може захистити від 5 типів загроз, серед яких бекдор доступу, фішинг, злам віддаленого доступу, переадресація маршруту та DDoS-атаки.

Мережевий екран встановлює правила для обмеження або дозволу трафіку на основі портів та протоколів. Однак існує потенціал для зловмисників використовувати легітимні порти для відправлення трафіку, який не є законним. У контексті цього сценарію система виявлення та запобігання вторгнень відіграє важливу роль, адже вона не лише аналізує вміст пакетів, але й може використовувати кореляцію в часі для виявлення можливих атак.

Робота системи виявлення та запобігання вторгнень полягає в тому, щоб прослідковувати і аналізувати зміст пакетів, а також встановлювати зв'язки в часі для виявлення атак, які можуть бути непростими для виявлення іншими засобами безпеки. Система виявлення та запобігання вторгнень і мережевий екран

взаємодіють, спільно переконуючись, що трафік, дозволений мережевим екраном, відповідає вимогам легітимності і не приховує потенційних загроз. Такий підхід гарантує комплексний захист мережі, унеможливлюючи зловмисникам використовувати лазівки у вигляді легітимного трафіку для впровадження атак.

Однією з ключових особливостей є виявлення аномалій. Хоча глибока інспекція пакетів може визначити нелегітимний трафік для кожного окремого пакета, важливо підкреслити, що ця специфікація обмежена рівнем аналізу окремих пакетів. У випадку, коли інфікована система активно сканує інші хости, використовуючи, наприклад, сканування ICMP або TCP SYN, система виявлення та запобігання вторгнень може ефективно виявити цю діяльність, що стає можливим завдяки його здатності аналізувати широкий спектр пакетів та взаємодії.

Механізми фільтрації мережевого екрана базуються на правилах портів та протоколах, що робить його обмеженим у виявленні такого роду сканування. Мережевий екран може пропустити ігнорувати таку діяльність, оскільки його основний фокус – на рівні окремих пакетів, а не на поведінці великої кількості пакетів, що може вказувати на систематичні аномалії чи атаки.

Рисунок 2.10 – Найпоширеніші методи кібератак за 2022-2023 роки

Опираючись на статистику найпоширеніших методів кібератак за 2022-2023 роки (рисунок 2.10), можемо зробити висновок, що використання системи запобігання вторгнень стане дуже важливим та необхідним рішенням, щоб надійно

захистити мережу від таких поширених атак як: фішинг, трояни, бекдор доступу, шкідливий програмний код, DDoS атаки та інше.

Система запобігання вторгнень має в своєму арсеналі здатність виявляти та протиставлятися багатій кількості різноманітних типів атак і потенційних загроз інформаційній безпеці, зокрема такі як приведено в таблиці 2.6.

Таблиця 2.6 – Види загроз, від яких захищає система запобігання вторгнень

Загроза	Опис загрози
Бекдор доступу	Це атаки з використанням вразливостей у встановленому на ПК програмному забезпеченні: операційній системі, утилітах, прикладних додатках. Такі проломи можуть бути скрізь, включаючи Windows, вони дозволяють хакеру отримати доступ до пристрою, надсилати і приймати з нього з трафік. Мережевий екран блокує такі дії
Фішинг	Шахрайська схема, в ході якої користувач потрапляє на фальшивий (фішинговий) сайт, один в один відомий веб-ресурс, що копіює. Наприклад, повторює сторінки входу до соціальної мережі чи оплати через онлайн-банкінг. Людина вводить особисті дані і вони потрапляють до рук зловмисника. Мережевий екран забороняє підключення до підозрілих сайтів

Продовження таблиці 2.6 – Види загроз, від яких захищає система запобігання вторгнень

Загроза	Опис загрози
Злам віддаленого доступу	За допомогою віддаленого робочого столу користувач може керувати комп'ютером через інтернет, тобто дистанційно. Хакери можуть перехопити цей доступ та вкрасти важливі дані. До завдань брандмауера входить заборона на передачу такого трафіку
Переадресація маршруту	Пакети даних передаються по мережі певними маршрутами, а цей вид атак передбачає заміну шляху проходження інформації таким чином, щоб кінцевий пристрій нічого не «підозрював»
DDoS-атаки	Оскільки головне завдання брандмауера це фільтрація, він допомагає впоратися з напливом величезних обсягів трафіку. Блокування працює як на вхідні, так і на вихідні пакети, якщо ваш пристрій спробують використовувати як атакуючий
Неавторизований доступ	Перехоплення та усунення спроб отримання несанкціонованого доступу до систем та ресурсів
Підвищення привілеїв користувача	Виявлення та заборона спроб отримання несанкціонованих привілеїв

Продовження таблиці 2.6 – Види загроз, від яких захищає система запобігання вторгнень

Загроза	Опис загрози
Використання вразливостей та шкідливого ПЗ	Боротьба з експлуатацією вразливостей та поширенням шкідливого програмного забезпечення

Крім того, система також гарантує захист від:

- Змін, заражень та перехоплення контролю ресурсами компанії;
- Цілеспрямованих атак з метою крадіжки даних чи засобів;
- Проблем із доступом до сайту та сервісів компанії;
- Проникнення у внутрішню мережу компанії;

Рисунок 2.11 – Кількість унікальних фішингових сайтів, зафіксованих з 2013 по 2022 роки

Як ми бачимо на рисунку 2.11, щорічно спостерігається динаміка зміни кількості унікальних фішингових веб-сайтів, яка то менше, то більше, із виявленою тенденцією зростання від 2020 року. У період до 2020 року фіксувалася певна коливання, проте з вступом у 2020 рік спостерігається збільшення кількості фішингових сайтів, що підкреслює актуальність поглибленого аналізу та заходів безпеки для виявлення та запобігання фішинговим атакам, враховуючи зростаючу кількість унікальних фішингових сайтів та загрози, пов'язані із сучасними методами атак, наразі вкрай важливо вжити заходів для ефективного захисту.

Проведене дослідження показало, що оновлення мережевого обладнання та впровадження системи запобігання вторгнень має великий потенціал для суттєвого покращення загального рівня безпеки інформаційно-комунікаційної системи підприємства «FixUp».

Цей перехід передбачає переоснащення мережевого обладнання від «домашнього» до професійного рівня, що забезпечить доступ до розширеного спектру інструментів для забезпечення безпеки інформації. Така стратегія призначена для вдосконалення системи обробки даних та мережевих з'єднань і зробить компанію менш вразливою перед сучасними загрозами кібербезпеки.

2.7. Висновки

Після проведення процесу оновлення мережевого обладнання вдалося досягти не тільки суттєвого підвищення рівня захищеності, але й усунути вразливість, що стосувалася попередньої версії обладнання, а саме CVE-2019-7405. Це оновлення виявилося вкрай корисним, покращуючи не лише загальний стан безпеки, але й неймовірно сприятливо позначилося на важливих аспектах захисту мережевого середовища. Також, слід зазначити, що значно поліпшилась ситуація стосовно надійності мережевого обладнання, кількість відмов мережевого обладнання зменшилась з 86 до 2 відмов на місяць (на 97,67%), а загальний час на відновлення працездатності мережі зменшився з 5663 секунд до 343 секунд на місяць (на 93,94%).

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Обрана тема кваліфікаційної роботи пов'язана з проблемою забезпечення інформаційної безпеки в сучасних умовах, де висока залежність від інформаційних технологій супроводжується зростаючими загрозами та ризиками кібербезпеки. Проблема полягає у необхідності вдосконалення технічних засобів для захисту інформації в організації від сучасних кіберзагроз.

Актуальність вирішення цієї проблеми пояснюється тим, що інформаційні системи стають об'єктом постійного впливу кібератак, а їх захист є критично важливим для забезпечення діяльності підприємства. Запровадження нових програмних та технічних рішень у сфері інформаційної безпеки є головним завданням для підвищення стійкості та захищеності інформаційних ресурсів.

Аналіз очікуваних результатів передбачає отримання покращень у функціонуванні, стабільності та захищеності ІТС підприємства «FixUp». Очікується підвищення рівня безпеки, виявлення та запобігання кіберзагрозам, а також оптимізація ефективності заходів інформаційного захисту.

У кваліфікаційній роботі запропонований метод вирішення проблеми базується на впровадженні стратегії провести комплекс заходів, який включає в собі оновлення мережевого обладнання (заміну бездротового маршрутизатора та розширення портів), а також реалізацію Системи Запобігання Вторгнень (IPS) для моніторингу та реагування на потенційні загрози.

Ці методи передбачають впровадження нових технологій та алгоритмів, спрямованих на забезпечення повного спектру захисту від кіберзагроз. Техніко-економічне обґрунтування проєкту включає визначення чинників економічної ефективності, які будуть враховані при оцінці результативності вирішення поставленої проблеми.

3.1. Розрахунок (фіксованих) капітальних та поточних витрат

До капітальних витрат належать витрати на розробку заходів із забезпечення інформаційної безпеки, а також витрати на придбання матеріальних та нематеріальних активів.

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

3.1.1. Визначення трудомісткості розробки засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації.

Трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні:

$t_{тз}$ – тривалість складання технічного завдання на розробку засобів захисту інформації в гетерогенних мережах, $t_{тз} = 12$;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в = 30$;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а = 24$;

$t_р$ – тривалість розробки засобів захисту інформації в гетерогенних мережах, $t_м = 22$;

$t_д$ – тривалість підготовки технічної документації, $t_д = 6$;

Отже,

$$t = t_{тз} + t_в + t_а + t_р + t_д = 12 + 30 + 24 + 22 + 6 = 94 \text{ години} \quad (3.1)$$

3.1.2. Розрахунок витрат на підвищення рівня захищеності інформації в ІТС

Витрати на розробку заходів підвищення рівня захищеності інформації $К_{пз}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу $З_{мч}$:

$$З_{зп} = t \cdot З_{пр} = 94 \cdot 170 = 15980 \text{ грн.} \quad (3.2)$$

$$К_{пз} = З_{зп} + З_{мч} = 15980 + 740{,}08 = 15820{,}08 \text{ грн.} \quad (3.3)$$

де :

t – загальна тривалість операцій, годин;

$З_{пр}$ – средньогодинна заробітна плата спеціаліста с інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = \mathbf{t} * С_{мч} = \mathbf{94 \cdot 12{,}11 = 1138{,}08} \text{ грн} \quad (3.4)$$

де:

t – трудомісткість операцій із побудови ефективної системи доступу персоналу, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \cdot t_{нал} \cdot С_{е} + \frac{Ф_{зал} \cdot Н_{а}}{F_{р}} + \frac{К_{лпз} \cdot Н_{апз}}{F_{р}} \text{ грн.} \quad (3.5)$$

де:

Р – встановлена потужність ПК, кВт;

$С_{е}$ – тариф на електричну енергію, грн/кВт*година

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_{а}$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_{р}$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_{р} = 1920$).

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$С_{мч} = 0,7 \cdot 5 \cdot 2,64 + \frac{6600 \cdot 0,6}{1920} + \frac{5150 \cdot 0,3}{1920} = 12,11 \text{ грн.} \quad (3.6)$$

Відповідно до поставлених задач в контексті підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації необхідне придбання наступних матеріальних активів:

Таблиця 3.1 – Вартість матеріальних активів

Матеріальний актив	Кількість	Ціна, грн.	Вартість, грн.
Cisco 891W-AGN-A-K9	1	21700	21700
Разом:			21700

Заплановані витрати на налагодження системи інформаційної безпеки в розмірі 7500 грн. ($К_н = 7500$ грн.)

Капітальні (фіксовані) витрати на проєктування та впровадження проєктного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_н \quad (3.7)$$

де:

$К_{пр}$ – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу;

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

Отже, капітальні (фіксовані) витрати на розробку засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі складуть:

$$К = 15820{,}08 + 21700 + 7500 = 45020{,}08 \text{ грн} \quad (3.8)$$

3.2. Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак} \text{ грн.} \quad (3.9)$$

де:

$С_в$ – вартість відновлення й модернізації системи;

$С_к$ – витрати на керування системою в цілому;

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки).

$С_а$ – Річний фонд амортизаційних відрахувань, визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ).

При розробці засобів захисту інформації в гетерогенних мережах для підвищення рівня інформаційної безпеки в інформаційно-комунікаційній системі організації витрати на відновлення й модернізації системи не матимуть місце.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос} \text{ (грн.)} \quad (3.10)$$

Таблиця 3.2. Групи основних засобів та інших необоротних активів і мінімально допустимі строки їх амортизації

Групи	Мінімально допустимі строки корисного використання років
Група 4 – машини та обладнання З них: Електронно-обчислювальні машини, інші машини для автоматичного оброблення інформації, пов'язані з ними засоби зчитування або друку інформації, пов'язані з ними комп'ютерні програми (крім програм, витрати на придбання яких визнаються роялті, та/або програм, які визнаються нематеріальним активом), інші інформаційні системи, комутатори, маршрутизатори, модулі, модеми, джерела безперебійного живлення, та засоби їх підключення до комунікаційних мереж, телефони (в тому числі стільникові), мікрофони і рації, вартість яких перевищує 2500 гривень.	5 2

Таблиця 3.3. Строки амортизації нематеріальних активів

Групи	Строк дії права користування
Група 5 – авторське право та суміжні з ним права (право на комп'ютерні програми, програми для електронно-обчислювальних машин, компіляції даних (бази даних)), крім тих, витрати на придбання яких визнаються роялті;	Відповідно до правовстановлюючого документа, але не менш ніж 2 роки

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}\ (грн.) \quad (3.11)$$

Річні амортизаційні відрахування матеріальних активів, які відповідно до чинного законодавства України підлягають амортизації, визначатимуться, виходячи зі строку корисного використання 5 років. Сума амортизаційних відрахувань визначається за прямолінійним методом нарахування амортизації. Таким чином, річні амортизаційні відрахування складуть:

$$С_а = 4608\ грн \quad (3.12)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати. Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 15980 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо реалізації засобів захисту інформації в гетерогенних мережах потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (15980 \cdot 12 + 15980 \cdot 12 \cdot 0{,}1) \cdot 0{,}25 = 52734\ грн. \quad (3.13)$$

Ставка ЄСВ для всіх категорій платників з 01.04.2023 р. складає 22%. (мінімальний ЄСВ 1562,00 грн.)

$$С_{єв} = 52734 \cdot 0{,}22 = 11601{,}48\ грн. \quad (3.14)$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е\ (грн.) \quad (3.15)$$

де:

Р – встановлена потужність апаратури інформаційної безпеки, ($Р = 0{,}5$ кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е = 2{,}64$ грн. кВт/год).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 0{,}5 \cdot 1920 \cdot 2{,}64 = 2534{,}40 \text{ грн} \quad (3.16)$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2%:

$$С_{тос} = 45020{,}08 \cdot 0{,}02 = 900{,}40 \text{ грн} \quad (3.17)$$

Таким чином, витрати на керування системою інформаційної безпеки ($С_к$) становлять:

$$С_к = 4608 + 52734 + 11601{,}48 + 2534{,}40 + 900{,}40 = 72378{,}28 \text{ грн.} \quad (3.18)$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) не виникають.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 72378{,}28 \text{ грн.} \quad (3.19)$$

3.2. Оцінка можливого збитку

3.2.1. Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 20000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 10000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 3 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 760 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 3;

N – середнє число атак на рік, 8.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \quad (3.20)$$

де:

$П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum З_с}{F} \cdot t_п = \frac{10000 \cdot 6}{176} \cdot 4 = 1363.64 \text{ грн.} \quad (3.21)$$

де:

F – місячний фонд робочого часу (при 40-а годинному робочоіму тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.22)$$

де:

$П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} * t_{ви} = \frac{10000 \cdot 6}{176} \cdot 6 = 2045{,}45 \text{ грн.} \quad (3.23)$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о}{F} * t_в = \frac{20000 \cdot 2}{176} \cdot 2 = 454{,}55 \text{ грн.} \quad (3.24)$$

Витрати на заміни встаткування або запасних частин можуть скласти 3400 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 2045{,}45 + 454{,}55 + 3400 = 5900 \text{ грн.} \quad (3.25)$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньо-годинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) \quad (3.26)$$

$$V = \frac{580000}{2080} \cdot (4 + 2 + 6) = 3346{,}15 \text{ грн.} \quad (3.27)$$

де:

$F_г$ – річний фонд часу роботи (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 454{,}55 + 5900 + 3346{,}15 = 9700{,}70 \text{ грн.} \quad (3.28)$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \Sigma_I \, \Sigma_N \, U = \Sigma_3 \, \Sigma_7 \, 9700{,}70 = 203714{,}70 \text{ грн.} \quad (3.29)$$

3.2.2. Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ (грн.)} \quad (3.30)$$

де:

B – загальний збиток від атаки у разі перехоплення інформації, 203714,70 грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки за становитиме:

$$E = 203714{,}70 \cdot 0{,}4 - 72378{,}28 = 9107{,}6 \text{ грн} \quad (3.31)$$

3.3. Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

За методикою сукупної вартості володіння (ТСО) визначають такі показники економічної ефективності системи інформаційної безпеки як Коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o). Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$\text{ROSI} = \frac{E}{K} \text{ (частки одиниці)} \quad (3.32)$$

де:

E – загальний ефект від впровадження системи інформаційної безпеки грн.;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI складе:

$$\text{ROSI} = \frac{9107{,}6}{45020{,}08} = 0{,}20 \text{ (частки одиниці)} \quad (3.33)$$

Проєкт визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (N_{\text{деп}} - N_{\text{інф}})/100 \quad (3.34)$$

де:

$N_{деп}$ – річна депозитна ставка, (18%);

$N_{інф}$ – річний рівень інфляції, (11%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0{,}20 > (11 - 18)/100 = 0{,}20 > 0{,}07 \quad (3.35)$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки. Відповідно термін окупності розробки засобів підвищення ефективності системи захисту інформації складе:

$$T_o = \frac{К}{E} = \frac{1}{ROSI} = \frac{1}{0{,}20} = 5 \text{ років} \quad (3.36)$$

3.4. Висновки

Запропонований метод вирішення проблеми, базований на впровадженні стратегії провести комплекс заходів, який включає в собі оновлення мережевого обладнання (заміну бездротового маршрутизатора та розширення портів), а також реалізацію Системи Запобігання Вторгнень (IPS) для моніторингу та реагування на потенційні загрози можна вважати економічно доцільними, оскільки значення коефіцієнту повернення інвестицій ROSI, що складає 0,20 при величині економічного ефекту 9107,60 грн. Отримане значення коефіцієнта ROSI перевищує дохідність альтернативного вкладення коштів. Термін окупності при цьому складатиме 5 років. Капітальні витрати на засоби захисту інформації складуть в 45020,08 грн., а щорічні експлуатаційні витрати складатимуть 72378,28 грн.

ВИСНОВКИ

У ході виконання роботи було проведено аналіз поточного стану кіберзахищеності об'єктів інформаційних технологій та визначено стратегічний напрямок для підвищення рівня безпеки в умовах постійно зростаючих загроз у сфері кібербезпеки. Було проведено дослідження можливих опцій використання засобів захисту інформації в комп'ютерній мережі підприємства «FixUp». На основі цього аналізу були ідентифіковані найбільш ефективні засоби захисту, розглянуто їхні механізми функціонування та запропоновані конкретні заходи для покращення безпеки інтернет-мережі.

У практичній частині проекту, після впровадження процесу оновлення мережевого обладнання, було досягнуто не лише значного підвищення рівня захисту, але й усунення вразливостей, які виникали у попередньому обладнанні і стосувалися, зокрема, CVE-2019-7405. Це оновлення виявилося дуже ефективним, покращуючи не тільки загальний рівень безпеки, але й відзначаючи позитивний вплив на ключові аспекти захисту мережевого середовища, а також слід відзначити, що ситуація з надійністю мережевого обладнання значно поліпшилась, а кількість відмов знизилась майже на 95%.

У економічному розділі був здійснений розрахунок економічного ефекту від впровадження та налагодження розроблених засобів захищеності інтернет-мережі, які зменшать збитки від атак на мережу. За результатами розрахунків, коефіцієнт повернення інвестицій (ROSI) складає 0,20 грн./грн., а термін окупності капітальних інвестицій становить до 5 років. Це дає змогу зробити висновок, що впровадження системи захисту, яка містить запропоновані удосконалення для комп'ютерної мережі підприємства «FixUp», є економічно доцільним рішенням.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кваліфікаційна робота магістра. Методичні рекомендації до виконання для студентів спеціальності 125 Кібербезпека (освітньо-професійна програма «Кібербезпека») / Упоряд.: О.Ю. Гусев, В.І. Корнієнко, В.І. Магро, Д.С. Тимофеєв – Дніпро: НТУ «ДП» 2022.
2. Методичні рекомендації до економічної частини дипломного проєкту зі спеціальності 125 кібербезпека / Упоряд.: Д.П. Пілова – Дніпро: НТУ «ДП» 2019.
3. Закон Україні «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України-1992-No48. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12
4. Закон Україні «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 No80-VI // Відомості Верховної Ради України-1994-No80. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-вр
5. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999] – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)
6. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999] – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)
7. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. [Чинний від 04.12.2000] – К.: ДСТСЗІ СБУ, 2000-No53 (Нормативний документ системи технічного захисту інформації)
8. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. [Чинний від

28.04.1999] – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)

9. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. [Чинний від 28.04.1999] – К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації)
10. НД ТЗІ 3.6-001-2000 Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. [Чинний від 20.12.2000] – К.: ДСТСЗІ СБУ, 2000-No60 (Нормативний документ системи технічного захисту інформації)
11. ДСТУ 3396.1-96 Захист інформації. Технічний захист. інформації. Порядок проведення робіт
12. ДСТСЗІ СБ України. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» – 2003. – 16 с.
13. М. В. Грайворонський, О. М. Новіков. Безпека інформаційно-комунікаційних систем – 2009. – 608 с.
14. В. І. Мєшков, В. О. Віролайнен. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах – 2012. – 4 с.
15. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – Питер, 2012. — 960 с.
16. А.Г. Микитишин, М.М. Митник, П.Д Стухляк. Телекомунікаційні системи та мережі: навчальний посібник для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» (українська) – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя. 131 с.
17. А.Г. Микитишин, М.М. Митник, П.Д Стухляк. Комп'ютерні мережі: [навчальний посібник] – Львів: «Магнолія 2006», 2013. — 256 с.

18. Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. – Львів: «Магнолія 2006», 2010. – 262 с.
19. A fuzzy Intrusion Detection System based on categorization of attacks [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://www.semanticscholar.org/paper/A-fuzzy-Intrusion-Detection-System-basedon-of-Varshovi-Rostamipour/8dc771ce3584a6daafeb2023b752b2e99e03f5d8.
20. Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://www.amazon.com/Intrusion-Detection-Introduction-SurveillanceCorrelation/dp/0966670078.
21. А. Корченко, «Модель базових компонент для виявлення кібератак на ресурси інформаційних систем», Актуальні проблеми управління інформаційною безпекою держави: VI наук.-практ. конф., Київ, 2015, С. 274-275.
22. С. Казмірчук, А. Корченко, Т. Паращук, «Аналіз систем виявлення вторгнень», Захист інформації, Т.20, №4, С. 259-276, 2018.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	1	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	34	
6	А4	Спеціальна частина	33	
7	А4	Економічний розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1. ПетрашЄІ_125м_22_1_ПЗ.docx
2. ПетрашЄІ_125м_22_1_ПЗ.pdf
3. ПетрашЄІ_125м_22_1_Презентація.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («Дев'яносто»).

Керівник розділу _____ к.е.н., доц. Пілова Д.П.
(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу

студента групи 125м-22-1 Петраша Євгенія Ігоровича

на тему: «Аналіз та підвищення рівня захищеності інтернет-зв'язку підприємства "FixUp"»

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 96 сторінках та містить 22 рисунки, 15 таблиць, 22 джерела та 4 додатків.

У вступній частині роботи автор приділяє увагу аналізу та дослідженню існуючої інформаційної безпеки при роботі в інтернет-мережах на підприємстві «FixUp».

У спеціальному розділі кваліфікаційної роботи приведено комплекс організаційних заходів забезпечення інформаційної безпеки та захисту інформації підприємства, оновлення мережевого обладнання, впровадження системи запобігання вторгнень. Наведені результати щодо ефективності використання системи в конкретних умовах та рекомендації щодо вибору та впровадження систем забезпечення інформаційної безпеки для підприємства.

В економічному розділі розрахована вартість та рентабельність впровадження щодо підвищення рівня захищеності інтернет-мережі «FixUp» та капітальні витрати.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам "Положення про систему виявлення та запобігання плагіату".

Як зауваження необхідно відзначити деякі стилістичні неточності та недостатню проробку окремих питань.

В цілому кваліфікаційна робота заслуговує оцінки «_____», а її автор присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Керівник спец. розділу	_____ (підпис)	Ю.П. Рибальченко (ініціали, прізвище)
Керівник кваліфікаційної роботи	_____ (підпис)	Т.С. Кагадій (ініціали, прізвище)