Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система виявлення аномального трафіку на маршрутизаторі Mikrotik

Назва теми

КРКБ. 180129.18.01.06 ПЗ
Шифр

Галузь знань 12 – Інформаційні технології
Шифр, назва

Спеціальність 125 – Кібербезпека
Шифр, назва

Освітня програма Кібербезпека
Шифр, назва

Виконала студентка 4 курсу, група КБ-18-01 _____ А.О. Левандовський
Підпис, дата Ініціали, прізвище

Керівник _____ В.С. Орленко
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ С. В. Мостовий
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки _____ Ю. П. Кльоц
Підпис, дата Ініціали, прізвище

16 01 2022 р.

Хмельницький, 2022

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

1 03 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Левандовському Андрію Олександровичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Система виявлення аномального трафіку на маршрутизаторі Mikrotik

Керівник роботи кандидат технічних наук доцент Орленко Вікторія Сергіївна

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 01.03. 2022 р. № 18 додаток 10

2. Строк подання студентом проекту (роботи) на кафедру:

3. Вихідні дані до проекту (роботи) В кваліфікаційній роботі досліджується мережа підприємства, відбувається аналіз трафіку, в подальшому реалізовується програмний засіб для аналізу мережевого трафіку, контролю ходу пакетів в ньому, виявлення мережевих аномалій

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Дослідити предметну область, розробити фізичну та логічну схему мережі підприємства, розробити програмний продукт що відповідає меті кваліфікаційної роботи, реалізувати його роботу на підприємстві.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) «Алгоритм дії скрипта Base», «Алгоритм дії скрипта Analysis», «Логічна система мережі», «Фізична та інтегрована система мережі», «Зображення роботи AnomalyShield »

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормконтроль	Мостовий С. В., ст. викладач		
Антиплагіат	Мостовий С. В., ст. викладач		

7. Дата видачі завдання «30» січня 2022р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) Кваліфікаційної роботи	Термін виконання етапів роботи	Прим
1	Вибір та затвердження теми кваліфікаційної роботи	Січень	–
2	Отримання завдання на кваліфікаційну роботу	Січень	–
3	Аналіз об'єкта	Січень-лютий	–
4	Проектування логічних, фізичних систем мережі, підприємства	Лютий-березень	–
5	Програмна реалізація запропонованого рішення та тестування; аналіз результатів і оцінювання прийнятих рішень	Березень-квітень	–
6	Написання тексту пояснювальної записки та розробка графічних матеріалів	Травень	–
7	Остаточне коригування кваліфікаційної роботи з урахуванням зауважень керівника		–
8	Оформлення кваліфікаційної роботи як документа відповідно до вимог		–
9	Отримання супровідних документів. Нормконтроль	Червень	–
10	Підготовка до захисту та захист кваліфікаційної роботи		–

Студент _____ Підпис Левандовський А
Ініціали, прізвище

Керівник роботи _____ Підпис Орленко В.С.
Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система виявлення аномального трафіку на маршрутизаторі Mikrotik»

Автор роботи: Левандовський Андрій Олександрович

Керівник роботи: Орленко Вікторія Сергіївна

Пояснювальна записка: 62 с., 19 рис., 3 табл., 2 дод., 16 джерел.

Графічна частина: 5 плакатів.

СИСТЕМА ВИЯВЛЕННЯ АНОМАЛЬНОГО ТРАФІКУ НА МАРШРУТИЗАТОРІ MIKROTIK.

Метою кваліфікаційної роботи є аналіз трафіку у відділені «Укргазбанк» м.Хмельницький. Виявлення аномалій мережевого трафіку між банками для підтримки необхідного рівня сервісу й захисту мережевих ресурсів. Розроблення програмного забезпечення для виявлення аномального трафіку, побудова плану приміщення, логічної моделі мережі. Для виконання поставленої задачі було використане обладнання Mikrotik.

В результаті виконання кваліфікаційної роботи була реалізована система виявлення аномалій трафіку в мережі.

підпис студента

10.06.22

Дата

Формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
		Текстові документи			
А4	КРКБ.180129.18.01.06 ПЗ	Пояснювальна записка	62		
		Графічні матеріали			
А4	КРКБ.180129.18.01.06 Е8	Алгоритм “Analysis”	1		
А4	КРКБ.180129.18.01.06 Е8	Алгоритм “Base”	1		
А4	КРКБ.180129.18.01.06 Е8	Логічна система мережі	1		
А4	КРКБ.180129.18.01.06 Е8	Фізична та інтегрована схеми	1		
А4	КРКБ.180129.18.01.06 Е8	Зображення роботи AnomalyShield	1		

КРКБ.180129.18.01.01 ВП

Арк	№ док	Підпис	Дата
Зробив	Левандовський А.О.		13.06.22
Перевір.	Орленко В.С.		13.06.22
Н. контр.	Мостовий С.В.		15.06.22
В.	Кльоц Ю.П.		15.06.22

Система виявлення аномального трафіку на маршрутизаторі Mikrotik
Відомість роботи

Літера	Аркуш	Аркушів
У		1

ХНУ, КБ-18-1

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

IT	–	Інформаційні технології
IOT	–	Інтернет речей
NTA	–	Аналіз мережевого трафіку
TCP	–	Протокол керування передаванням
NIC	–	Мережева інтерфейсна карта
DTE	–	Кінцева обладнання даних
DCE	–	Кінцеве устаткування лінії зв’язку
HTTP	–	Протокол передачі даних
URI	–	Уніфікований ідентифікатор ресурсів
SMTP	–	Простий Протокол Пересилання Пошти

ВСТУП

Мережі різноманітних типів часто відчувають аномальну поведінку. Прикладами можуть бути атаки й передачі великого об’єму даних в IP-мережах, наявність зловмисників у розподілених системах відеоспостереження.

Аномалія мережі - це раптове й короткочасне відхилення від нормальної роботи мережі. Є аномалії що навмисно викликані задля нанесення шкоди для підприємства, наприклад атака на відмову в обслуговуванні в IP-мережі.

Різні аномалії проявляються в мережевій статистиці по-різному, тому розробка загальних моделей нормальної поведінки мережі та аномалій є важкою.

Поки що через складність проблеми складної системи аналізу, не вдалося розробити єдину модель, яка б врахувала всі особливості цих систем.

У цьому контексті системи тестуються з точки зору роботи в нормальних умовах. Було визначено основний стан системи. Аналізуючи можливі розбіжності, можна виявити атаки на IT, а також на мережі IoT та IoE.

Це стосується комп'ютерних систем, а також проміжних пристроїв, таких як комутатори, маршрутизатори та кінцеві пристрої включаючи датчики та інші активні елементи.

Існує очевидна відсутність моделей для аналізу процесів, які є актуальними, коли відбуваються такі події та явища, які їх супроводжують.

Розроблені на сьогодні підходи не вказують на конкретні аномальні дії користувачів. Це пояснюється тим, що поточний набір підходів, як правило, передбачає, що або навчальна інформація доступна для створення надійних класифікаторів, або що користувач здійснив велику кількість дій, які відхиляються від «нормальної» поведінки.

Метою кваліфікаційної роботи є виявлення аномального трафіку в мережі підприємства «Укргазбанк», використовуючи наявне устаткування компанії Mikrotik.

Завданням кваліфікаційної роботи є:

Розробка системи виявлення аномального трафіку, з виводом повідомлення адміністратору.

1 СИСТЕМИ ВИЯВЛЕННЯ АНОМАЛЬНОГО ТРАФІКУ

1.1 Аномальний трафік

Мережа — це просто будь-яка сукупність підключених апаратних частин або вузлів. Від найпростішого зв'язку між двома серверами до глобального Інтернету, весь цей спектр складається з мережевої активності.

Знання історії розвитку мереж спроможне допомогти краще зрозуміти те, як мережі виглядають зараз та як вони виглядали в минулому.

Перші комп'ютерні мережі були зв'язками між фізичними робочими станціями, персональними та настільними комп'ютерами, які були з'єднані кабелем Ethernet, або пізніше бездротовим способом. Кожен комп'ютер мав власний фізичний жорсткий диск, і жорсткі диски комп'ютерів часто були представлені різними літерами дисків на інтерфейсі операційної системи робочої станції та різними видами програмних додатків. [1]

Зловмисник може авторизуватись на фізичному комп'ютер із власним диском, після чого зловмисник витягнуте з комп'ютера диска або ввійде в мережеве програмне забезпечення, щоб отримати доступ до диска іншого комп'ютера в іншій частині кімнати або будівлі.

У цих ранніх установках, коли кінцеві користувачі часто вибирали доступ до мережевого диска зі спадного списку, інженери використовували конкретні топології мережі, щоб з'єднати ці компоненти робочої станції разом.

Топології концентратора, кільця, шини, зірки та дерева були одними із поширених мережевих структур, які використовувалися, щоб дозволити окремим комп'ютерам «взаємодіяти» один з одним та обмінюватися інформацією.

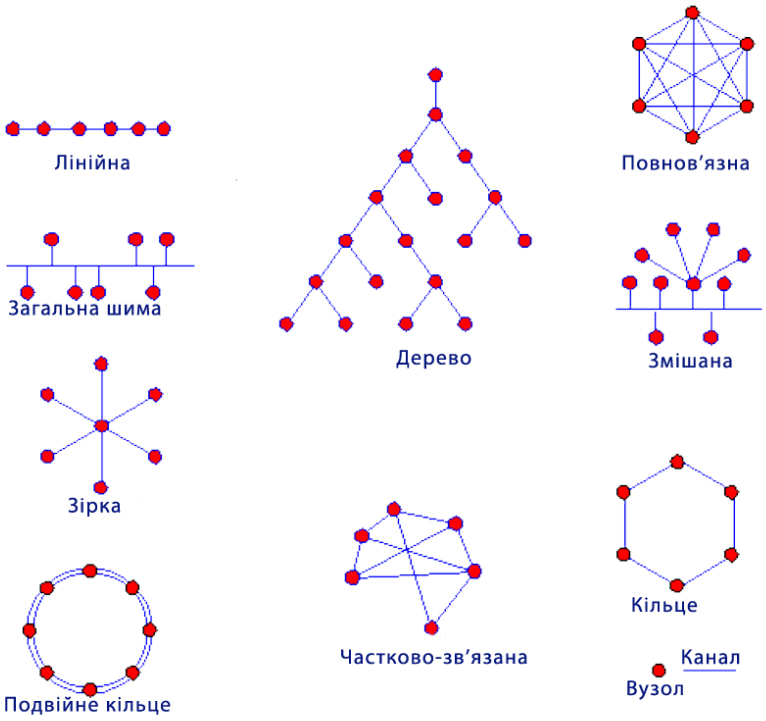


Рисунок 1.1 – Деякі типи топологій мережі.

Комп'ютери зазвичай розміщувалися в певній будівлі, але, можливо, були об'єднані в мережу в різних кімнатах або офісах.

Мережа — це сукупність комп'ютерів, серверів, мейнфреймів, мережевих пристроїв, периферійних або інших пристроїв, під'єднаних для обміну даними. Прикладом мережі є Інтернет, який об'єднує мільйони людей у всьому світі.

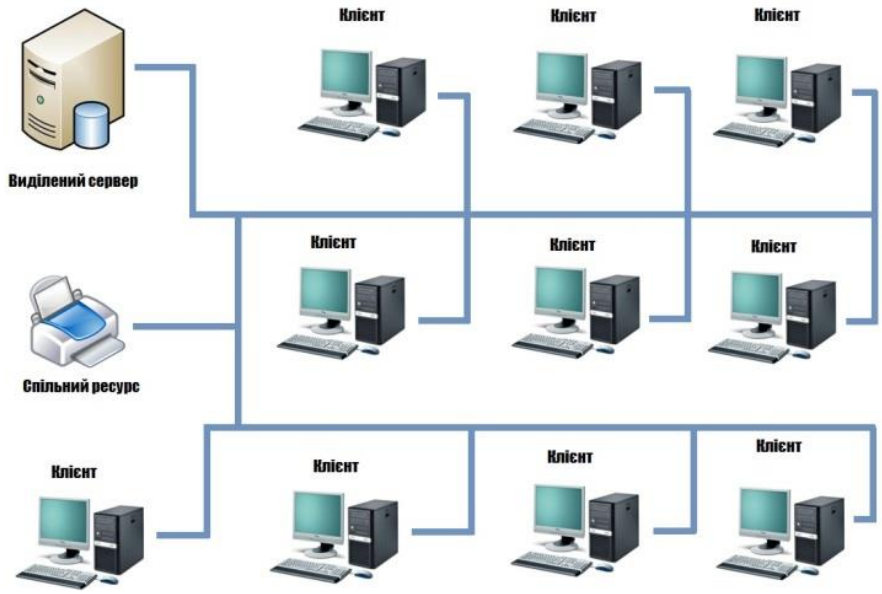


Рисунок 1.2 – Приклад локальної мережі

Переваги користування мережею.

У мережі більше переваг, ніж недоліків. Насправді, багато компаній сьогодні не існували б без доступу до якогось виду мережі. Нижче наведені переваги мережі:

- обмін даними з інформацією. Однією з найбільших переваг мережі є обмін даними та інформацією між кожним із пристроїв у ній. Крім того, мережі надають доступ до баз даних і допомагають у співпраці над більш складною роботою;
- зв’язок – мережа дає всім користувачам можливість швидко спілкуватися один з одним за допомогою чату, обміну миттєвими повідомленнями, електронної пошти та відеоконференцій;
- спільний доступ до обладнання – апаратні пристрої, підключені до мережі, можна спільно використовувати з усіма користувачами.

Нижче наведено кілька прикладів мережевого обладнання, яке можна спільно використовувати:

- NAS (сховище, підключене до мережі) може зберігати та отримувати доступ до величезної кількості інформації;
- Мережевий принтер дозволяє всім користувачам мережі друкувати на одному принтері;
- Потужніші комп’ютери, суперкомп’ютери та ферми візуалізації можуть виконувати складні завдання, для виконання яких звичайному одному комп’ютеру знадобиться більше часу;
- Спільне використання програмного забезпечення – за наявності відповідної ліцензії на програмне забезпечення також можна надати доступ до програмного забезпечення;
- Переказ грошей. Підключення до захищеної мережі дозволяє особі чи компанії здійснювати цифрові перекази грошей між банками та користувачами. Наприклад, мережа може дозволити компанії не тільки керувати нарахуванням заробітної плати працівників, а й перераховувати їх на банківський рахунок співробітника.

Недоліки мережі

Хоча мережа має багато переваг (згаданих вище), є й деякі недоліки. Нижче наведено недоліки мережі:

- Віруси та зловмисне програмне забезпечення. Мережі полегшують обмін інформацією між користувачами мережі. На жаль, це також означає, що віруси та шкідливі програми легше поширюються між комп’ютерами в мережі;
- Уразливості. Коли створюється мережа, вона вводить нові методи віддаленого доступу до комп’ютерів, особливо якщо вони підключені до Інтернету. Завдяки цим потенційним новим методам доступу до комп’ютера, він може створити нові вразливості для комп’ютерів, користувачів і даних у мережі;

- Складність – мережі складні, і для створення та керування мережею для бізнесу чи корпорації потрібен хтось із великим досвідом чи сертифікацією.

Мережевий трафік.

Мережевий трафік – це кількість даних, що переміщуються по комп'ютерній мережі в будь-який момент часу. Мережевий трафік, також званий трафіком даних, розбивається на пакети даних і надсилається по мережі, перш ніж знову збирається пристроєм або комп'ютером-отримувачем.[2]

Мережевий трафік можна розділити на такі категорії:

- Зайнятий/інтенсивний трафік – цей трафік споживає велику пропускну здатність;
- Трафік не в реальному часі - Споживання пропускної спроможності в робочий час;
- Інтерактивний трафік – є предметом конкуренції за пропускну здатність і може призвести до низького часу відповіді, якщо пріоритет додатків і трафіку не встановлено;
- Трафік, чутливий до затримок – є предметом конкуренції за пропускну здатність і може призвести до низького часу відповіді;

Мережевий трафік має два напрямки: північ-південь і схід-захід.

Трафік впливає на якість мережі, оскільки надзвичайно високий обсяг трафіку може означати низьку швидкість завантаження або неякісні підключення через Інтернет-протокол (VoIP). Трафік також пов'язаний з безпекою, оскільки надзвичайно велика кількість трафіку може бути ознакою атаки.

Пакети даних.

Коли дані передаються мережею або Інтернетом, їх спочатку потрібно розбити на менші пакети, щоб більші файли можна було ефективно передавати.

Мережа розбиває, організовує та об’єднує дані в пакети даних , щоб їх можна було надійно надіслати через мережу, а потім відкрити та прочитати іншим користувачем мережі. Кожен пакет використовує найкращий можливий маршрут для рівномірного розподілу мережевого трафіку.

Типи мережевого трафіку.

Щоб краще керувати пропускною здатністю, адміністратори мережі вирішують, як пакети будуть оброблятися мережевими пристроями, такими як маршрутизатори та комутатори. Існують дві загальні категорії мережевого трафіку: в режимі реального часу і не в реальному часі.

Трафік в режимі реального часу – трафік , який вважається важливим або критичним для бізнес-операцій, повинен доставлятися вчасно та з максимально високою якістю. Приклади мережевого трафіку в реальному часі включають VoIP, відеоконференції та перегляд веб-сторінок.

Трафік не в реальному часі, також відомий як трафік найкращих зусиль, це трафік, який адміністратори мережі вважають менш важливим, ніж трафік реального часу. Приклади включають протокол передачі файлів (FTP) для веб-публікації та електронних програм.

Аналіз мережевого трафіку – це метод, який використовується адміністраторами мережі для перевірки мережевої активності, керування доступністю та виявлення незвичайної активності. NTA також дозволяє адміністраторам визначати, чи існують якісь проблеми з безпекою чи операційними проблемами — чи можуть виникнути в подальшому — за поточних умов. Вирішення таких проблем у міру їх виникнення не тільки оптимізує ресурси організації, але й зменшує ймовірність атаки. Таким чином, NTA пов’язана з підвищеною безпекою. [3]

- Визначенням вузьких місць : вузькі місця можуть виникнути в результаті різкого зростання кількості користувачів в одному географічному місці;

- Усуненням проблем із пропускною здатністю : повільне з’єднання може бути пов’язано з тим, що мережа не призначена для збільшення кількості користувачів або активності;
- Покращенням видимість пристроїв у вашій мережі : Підвищена обізнаність про кінцеві точки може допомогти адміністраторам передбачити мережевий трафік і внести зміни, якщо це необхідно;
- Виявленням проблеми з безпекою та виправлення : NTA працює в режимі реального часу, сповіщаючи адміністраторів, коли є аномалія трафіку або можливе порушення.

Правильне програмне забезпечення для моніторингу мережі допомагає організаціям отримати доступ до всіх пристроїв і програм, що працюють у мережі. Важливо знати, які пристрої використовують найбільшу пропускну здатність, щоб за потреби переналаштувати мережу або внести зміни до типів вмісту, що фільтрується, щоб запобігти доступу до певних веб-сайтів або служб (наприклад, YouTube і Instagram).

Моніторинг інтернет-трафіку – це процес контролю всіх вхідних та вихідних даних з Інтернету на пристрій, мережу та середовище з метою адміністрування та/або виявлення будь-яких відхилень чи загроз

Моніторинг інтернет-трафіку в першу чергу здійснюється для оцінки будь-яких підозрілих або шкідливих вхідних або вихідних пакетів або активності. Як правило, це частина брандмауера та системи виявлення та запобігання вторгненням.

Моніторинг інтернет-трафіку можна виконувати вручну, переглядаючи пакети на предмет будь-якої активності, незвичної для користувача, мережі чи організації. Аналогічно, за допомогою таких автоматизованих інструментів, як брандмауери, невідповідні повідомлення та пакети автоматично відфільтровуються. Ці пакети можна видалити, заблокувати або надати лише обмежений доступ до мережі, Інтернету чи пристрою.

Це також використання засобу для огляду діяльності співробітників або окремих осіб в Інтернеті.

Правильний аналіз мережевого трафіку забезпечує організації наступні переваги:

- Виявлення вузьких місць мережі. Можуть існувати користувачі або програми, які споживають велику кількість пропускної здатності, таким чином складаючи основну частину мережевого трафіку. Для вирішення цих проблем можна застосувати різні рішення;
- Безпека мережі. Незвичайний обсяг трафіку в мережі є можливою ознакою атаки. Звіти про мережевий трафік надають цінну інформацію щодо запобігання таким атакам;
- Розробка мережі. Знання рівнів використання мережі дозволяє аналізувати майбутні вимоги..

Мережева аномалія

Проблеми в комп'ютерних мережах визначаються як аномалії трафіку, які вони викликають. Загалом, аномалія – це те, що суперечить очікуванням. Наприклад, пошкоджений комутатор може створити неочікуваний трафік в іншій частині мережі або нові коди помилок починають з’являтися, коли служба не працює. Усунення несправностей мережі засноване на аномаліях мережі.

Перший метод класифікації аномалій заснований на тому, чим вони відрізняються від звичайного стану. Аномалії можуть відрізнятися або за типом переданих даних (поведінкові), за кількістю переданих даних (за обсягом) або за обома критеріями. Інший спосіб класифікації аномалій за їх причиною:

- Технічна помилка - наприклад, несправність обладнання або перерва радіозв'язку через погоду;
- Людська помилка - наприклад, перебої в роботі мережі через неправильну конфігурацію або випадково від'єднаний мережевий кабель;

- Шкідлива людська діяльність – наприклад, інсайдерська атака, коли незадоволений співробітник компанії пошкоджує мережевий принтер, або зовнішня атака, коли супротивник намагається відключити мережу і завдати шкоди репутації.

1.2 Виявлення відомих аномалій трафіку

Є велика кільскість методів виявлення аномалій. Дивлячись на обставини кожна методика може бути краща ніж інша та індивідуально підходити для різних ситуацій або набору даних.

Інструменти виявлення перехоплюють дані трафіку, коли вони переміщуються по дротовій або бездротовій мережі, і копіюють їх у файл

Це називається захопленням пакетів . Хоча комп’ютери, як правило, створені так, щоб ігнорувати шум трафіку від інших комп’ютерів, засоби виявлення пакетів працюють навпаки.

Зазвичай коли встановлюється програмне забезпечення для виявлення пакетів, NIC (інтерфейс між комп’ютером і мережею) потрібно налаштувати на безладний режим. Це наказує комп’ютеру захоплювати й обробляти за допомогою засобу виявлення пакетів все, що потрапляє в мережу.

Елементи, які можна захопити, залежать від типу мережі . Для дротових мереж конфігурація мережевих комутаторів, що відповідають за централізацію зв'язку з кількох підключених пристроїв, визначає, чи може інструмент виявлення мережі бачити трафік у всій мережі або лише її частину.

У бездротових мережах інструменти захоплення пакетів зазвичай можуть захоплювати лише один канал за раз, якщо головний комп’ютер не має кілька бездротових інтерфейсів.

DDOS-атака

Як правило, зловмисники генерують великі обсяги пакетів або запитів, які в кінцевому підсумку перевантажують цільову систему.

Під час атаки розподіленої відмови в обслуговуванні (DDoS) зловмисник використовує кілька контрольованих або пошкоджених джерел, щоб продовжити.

DDoS-атаки є однією з найгрубіших форм кібератак, але вони також є однією з найпотужніших, і їх важко зупинити

Розподілена атака «Відмова в обслуговуванні» (DDoS-атака) передбачає, що зловмисник переповнює мережу або сервери жертви таким сплеском інтернет-трафіку, що їх інфраструктура переповнена кількістю запитів на доступ, сповільнюючи роботу служб або повністю відключаючи службу та запобігаючи законних користувачів від доступу до послуги.

Хоча DDoS-атака є однією з найменш складних категорій кібератак, вона також може бути однією з найбільш руйнівних і потужних, вибиваючи веб-сайти та цифрові служби в автономному режимі на значні періоди часу – від кількох секунд до кількох тижнів.

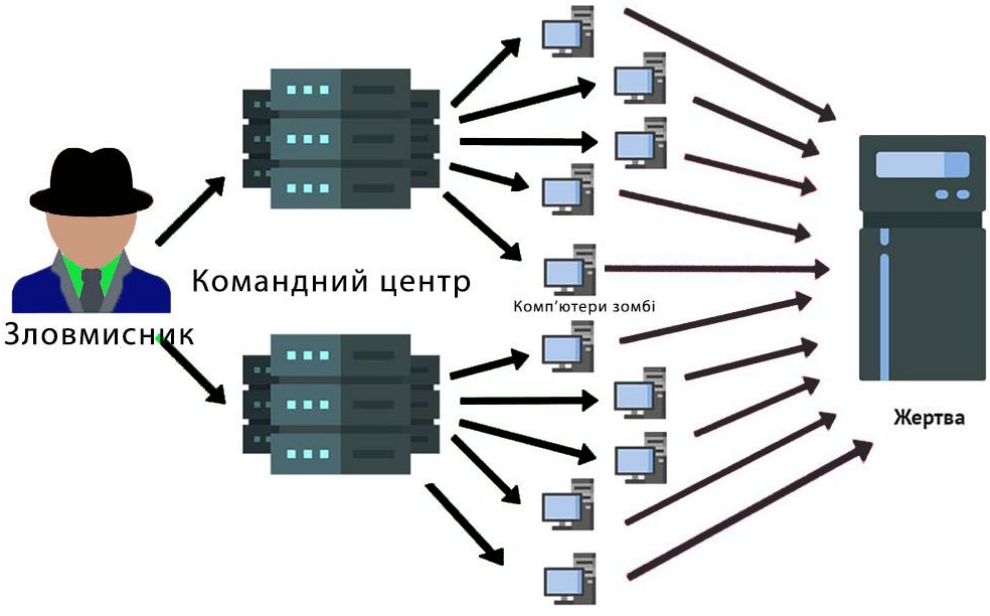


Рисунок 1.3 – Схема DDOS атаки

Методи захисту від DDoS.

Зменшена поверхня атаки.

Одним із перших методів пом’якшення DDoS-атак є мінімізація поверхні атаки, яка може бути націлена, тим самим обмежуючи можливості зловмисників і дозволяючи створювати захист в одному місці.

Зведення до мінімуму можливих точок атаки та надає зосередження на зусиллях із пом’якшення. У деяких випадках можна зробити це, розмістивши обчислювальні ресурси за мережами доставки вмісту (CDN) або балансувальниками навантаження і обмеження прямого інтернет-трафіку певними частинами інфраструктури, наприклад серверами баз даних. [4]

В інших випадках можна використовувати брандмауери або списки контролю доступу, щоб контролювати трафік, який надходить до програм.

Відстеження веб-трафіку та отримання чіткого уявлення про те, як виглядає звичайний трафік і що таке ненормальний трафік, також може відігравати важливу роль у захисті від DDoS-атак або виявленні їх.

Деякі експерти з комп’ютерної безпеки рекомендують налаштувати сповіщення, які повідомлятимуть вас, якщо кількість запитів перевищує певний поріг. Хоча це не обов’язково вказує на шкідливу активність, воно принаймні дає швидке попередження про те, що щось конкретне відбувається. [5]

Також корисно передбачити масштаби та стрибки веб-трафіку, з якими може допомогти постачальник хмарного хостингу.

Брандмауери та маршрутизатори можуть відігравати важливу роль у зменшенні потенційної шкоди від DDoS-атаки. Якщо налаштовано правильно, вони можуть перенаправляти фіктивний трафік, скануючи його як потенційно небезпечний і заблокувавши до його надходження. Однак важливо також зазначити, що для того, щоб це було ефективним, брандмауер і програмне забезпечення безпеки слід регулярно оновлювати, щоб залишатися максимально ефективними.

Використання служби захисту IP може бути ефективним способом перевірити власну пропускну здатність. Існують також постачальники послуг, які спеціалізуються на запобіганні DDoS, які можуть допомогти організаціям впоратися з раптовим сплеском веб-трафіку, допомагаючи запобігти збиткам від атак.

Двома ключовими міркуваннями для пом'якшення гіпермасштабних атак DDoS є пропускна здатність (або транзитна) пропускна здатність і потужність сервера для поглинання та пом'якшення атак.

Пропускна здатність потрібно переконатись, що хостинг-провайдер забезпечить достатню кількість резервного підключення до Інтернету, що дозволяє обробляти великі обсяги трафіку.

Оскільки кінцевою метою DDoS-атак є вплинути на доступність ресурсів/програм, потрібно знайти їх не лише поблизу ваших кінцевих користувачів, а й на важливих мережах Інтернету, що забезпечить користувачам легкий доступ навіть до вашої програми. з великими обсягами руху. Крім того, веб-додатки можуть зробити цей крок далі, використовуючи мережі доставки вмісту (CDN) та інтелектуальні послуги вирішення DNS. які забезпечують додатковий рівень мережевої інфраструктури для доставки вмісту та вирішення запитів DNS із місць, які часто знаходяться ближче до кінцевих користувачів.

Більшість атак DDoS — це масові атаки, які використовують багато ресурсів. Тому важливо швидко масштабувати обчислювальні ресурси. Можна зробити це, використовуючи великі обчислювальні ресурси або ресурси з такими функціями, як більш масштабовані мережеві інтерфейси або розширені мережі , які підтримують більші обсяги. Крім того, часто використовують балансувальники навантаження для постійного моніторингу та перемикання навантаження між ресурсами, щоб запобігти перевантаженню будь-яких ресурсів.

Що таке нормальний і ненормальний рух пакетів в мережі

Щоразу при виявленні високого рівня трафіку, що досягає хоста, основна вимога полягає в тому, щоб мати можливість приймати лише трафік, який наш хост може обробляти, не впливаючи на доступність. Ця концепція називається обмеженням швидкості. Більш просунуті методи захисту можуть піти далі й розумно приймати тільки легітимний трафік шляхом аналізу самих окремих пакетів. Для цього потрібно зрозуміти характеристики хорошого трафіку, який зазвичай отримує ціль, і вміти порівнювати кожен пакет із цим базовим рівнем.

Хорошою практикою є використання брандмауера веб-програм (WAF) проти таких атак, як ін'єкція SQL або підробка між сайтових запитів, які намагаються використати вразливість у самій програмі. Крім того, через унікальну природу цих атак, потрібно мати можливість легко створювати спеціальні засоби пом'якшення проти незаконних запитів, які можуть мати такі характеристики, як виглядати як хороший трафік або надходити з поганих API, неочікуваних регіонів тощо. Це іноді корисно для пом'якшення атак, оскільки вони вміють вивчати моделі трафіку та створювати спеціальні засоби захисту.

HTTP-flood атака — це тип об'ємної атаки розподіленої відмови в обслуговуванні, призначеної для насичення цільового сервера запитами HTTP . Після того, як ціль буде насичена запитами і не зможе відповідати на звичайний трафік, відмова в обслуговуванні відбудеться для додаткових запитів від існуючих користувачів.

HTTP-flood атаки є різновидом DDoS-атаки рівня 7. Рівень 7 є прикладним рівнем моделі OSI і відноситься до Інтернет-протоколів, таких як HTTP.

Щоб досягти максимальної ефективності, зловмисники зазвичай використовують або створюють ботнети , щоб максимізувати вплив своєї атаки. Використовуючи багато пристроїв, заражених зловмисним програмним

забезпеченням , зловмисник може примножити свої зусилля, запускаючи більший обсяг атаки.

Існує два різновиди HTTP-flood атак:

- HTTP GET атака . У цій формі атаки кілька комп'ютерів або інших пристроїв координуються для надсилання кількох запитів на зображення, файли чи інші елементи з цільового сервера. Коли ціль переповнена вхідними запитами та відповідями, відбувається відмова в обслуговуванні для додаткових запитів від законних джерел трафіку.
- HTTP POST атака . Зазвичай, коли форма надсилається на веб-сайті, сервер повинен обробити вхідний запит і перемістити дані в рівень збереження, найчастіше базу даних. Обробка даних форми та виконання необхідних команд бази даних є відносно інтенсивними в порівнянні з потужністю обробки та пропускною здатністю, необхідними для відправки запиту POST. Ця атака використовує нерівність у відносному споживанні ресурсів, надсилаючи численні запити POST безпосередньо на цільовий сервер, поки його потужність не буде насичена та не відбудеться відмова в обслуговуванні.

Захиститися від атаки HTTP-flood дуже важко, оскільки запити спочатку виглядають як звичайний трафік на веб-сайті. Зловмисне програмне забезпечення не надсилається на сервер і не робиться спроб використати будь-які вразливості безпеки. Натомість зловмисники наповнюють сервер авторизованими доступами. Оскільки це споживає набагато менше пропускної спроможності, ніж вторгнення в код сайту, атаки, як правило, спочатку не виявляються.

Як згадувалося раніше, пом'якшення атак рівня 7 є складним і часто багатогранним. Одне з можливих рішень – надіслати запит машині, яка запитує, щоб перевірити, чи є це бот , так само, як тест капчі, який зазвичай зустрічається під час створення облікового запису в Інтернеті.

Інші способи зупинити переповненість HTTP включають в себе використання брандмауера, веб-додатків, підтримку бази даних IP Reputation для відстеження та вибіркового блокування шкідливого трафіку й його аналіз.

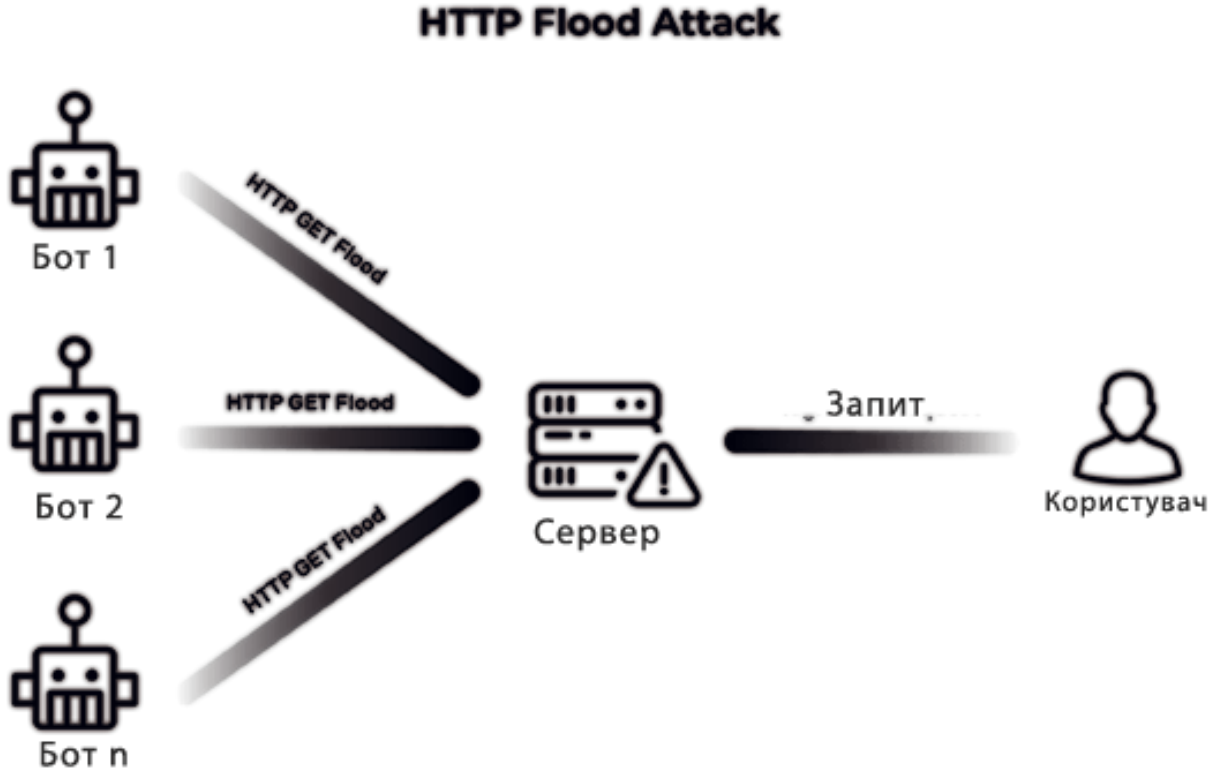


Рисунок 1.4 – Приклад HHTP GET Flood атаки.

1.3 Виявлення невідомих аномалій трафіку

Саме на підприємстві «Укргазбанк», на якому відбувалась переддипломна практика під час виконання кваліфікаційної роботи під визначення «аномалія трафіку» підлягає також і вхід на заборонені підприємством сайти.

Як тільки робітник банку намагається зайти на якийсь з заборонених ресурсів, сайт блокується, після чого адміністратор отримує інформацію про вхід на цей сайт.

Потреба в блокуванні небажаних сайтів була, й залишається однією з важливіших потреб для поліпшення безпеки мережі.

До прикладу одним з варіантів недозволених сайтів можуть бути різні соціальні мережі та месенджери, це можуть бути як заборонений в Україні сайт «Vkonakte.ru» , так і звичний всім користувачам інстаграм, та тим більше телеграм.

Саме блокування таких сайтів обумовлюється тим, що за допомогою них співробітники підприємства можуть поширювати внутрішню інформацію за межі компанії. Як інша причина, це може бути банальне сидіння в мережах гортаючи стрічку, замість виконання своїх прямих обов'язків, або під час роботи підвищуючи рівень появи помилок у роботі. Цілком виправдано буде одразу обмежити доступ на такі ресурси.

По тій самій причині одна з категорій сайтів що попадають під визначення «аномальні» для даної мережі також будуть різного виду відеохостинги, стрімингові платформи.

Також одна з варіацій можливої шкоди є використання соціальної інженерії на співробітниках компанії, що відвідують різного роду сайти з робочої мережі, так чином наражаючи мережу під небезпеку.

З іншої сторони деякі платформи, до прикладу «Facebook», в деяких випадках потрібні для ведення ділових перемовин, ще з близьких до цих потреб варіантів є «Skype» , та інші схожі засоби «зв'язку» між клієнтом та співробітником банку. В таких випадках сайт не можна охарактеризувати як заборонений, але й виключно дозволеним він не являється, розподілимо його в категорію «підозрілий».

Сайти з російськими та її країн доменами, також будуть заблокованими.

Рекомендованими до відвідування сайтами є: сайти фінансових установ, сайти по наданню державних послуг, та внутрішні сайти компанії.

1.4 Опис відомих систем виявлення аномального трафіку

Виявлення аномалій вимагає постійного моніторингу та аналізу вибраних мережевих показників. Система виявлення аномалій охоплює сценарій, коли виявляється щось несподіване, і аналіз оцінює це як аномалію, про це можна повідомити адміністратору мережі.

Існує дві основні категорії моніторингу мережі, які дозволяють виявляти аномалії:[6]

Пасивний моніторинг мережі

Комп'ютерна мережа включає зонди, які отримують дані з мережі та оцінюють їх. Ці дані можуть бути призначені безпосередньо для зондів (наприклад, події, надіслані через протокол SNMP), або вони можуть бути копією виробничого трафіку, який відбувається в мережі незалежно від того, підключено зонд чи ні.

Активний моніторинг мережі

Мережі також можуть містити зонди, як у пасивному моніторингу, але ці зонди генерують додатковий трафік, який вони надсилають через мережу. За допомогою цього трафіку можна регулярно визначати доступність або загальні параметри перевірених послуг, мережевих ліній і пристроїв.

Відмінності між активним і пасивним моніторингом мережі при виявленні аномалій мережі:

Може здатися, що активний моніторинг розширює можливості пасивного моніторингу, що робить його автоматично кращим варіантом. Проте проблема активного моніторингу полягає в тому, що він генерує додаткові дані в мережі.

Таким чином, при активному моніторингу пристрої моніторингу стають частиною виробничої мережі (що несе з собою, наприклад, ризики безпеки), і, отже, моніторинг не є повністю прозорим. Інша потенційна проблема полягає в тому, що дані моніторингу самі по собі можуть впливати на

функціональність мережі і, таким чином, бути джерелом проблем і аномалій (наприклад, це може збільшити навантаження на вже зайнятий сервер).

Методи виявлення аномалій

Підписи або на основі знань

Підпис точно описує, який тип даних шукає система. Прикладом підпису може бути пошук пакету, який має ту ж IP-адресу джерела, що й IP-адреса призначення, або пошук певного вмісту в пакеті.

Базові або статистичні

Базовий рівень описує кількість переданих даних, які мають певні спільні ознаки. Наприклад, це може бути кількість виявлених TCP-з'єднань за кожні 5 хвилин. Аномалія виникає, коли поточне значення (кількість запитів за останні 5 хвилин) значно відхиляється від засвоєного базового рівня; Іншим прикладом є пошук зміни розподілу пакетів відповідно до портів, до яких вони спрямовані

Реальність виявлення аномалій не така проста, як може здатися. Згодом виникне проблема, яка значно обмежить можливості виявлення аномалій. Далі буде описано дві найбільш критичні проблеми.

Хибнопозитивне виявлення

Відрізнити нормальну роботу від аномалій не завжди легко. Те, що вчора могло бути звичайним рухом, завтра може стати аномалією. Це відбувається тому, що передані дані змінюються незалежно від того, є в мережі проблема (аномалія) чи ні. Ось чому виявлення скоріше оперує оцінками ймовірності. Хоча кожна система або метод може використовувати його по-різному, основна ідея одна і та ж. Кожній виявленій події присвоюється оцінка, і якщо ця оцінка перевищує попередньо визначений поріг, вона позначається як аномалія.

Поріг для виявлення аномалій визначає чутливість виявлення. Якщо чутливість занадто висока, проблеми або аномалії будуть швидко виявлені,

але ціною збільшення кількості подій, які неправильно позначені як аномальні. Ці помилково позначені події називаються помилковими.

З іншого боку, якщо чутливість низька, зменшується кількість помилкових спрацьовувань, але також зменшується кількість правильно виявлених аномалій – аномалія деяких аномалій буде недостатньо високою, що дозволить їм залишитися без виявлення.

Прикладом хибнопозитивної події є ситуація, коли несподіване оновлення операційної системи передає великий обсяг даних, або коли несподівана обставина спонукає ненормальну кількість клієнтів одночасно підключитися до електронного магазину компанії.

Взагалі кажучи, неможливо гарантувати, що всі аномалії в мережі будуть виявлені і в той же час не буде помилкових спрацьовувань.

Причина, по якій помилкові позитивні події насправді є проблемою, полягає в тому, що під час автоматичної обробки подій легітимний трафік або послуга можуть бути ідентифіковані як проблематичні, а їхня діяльність буде обмежена. У той же час обробка та аналіз цих аномалій вручну вимагає величезної кількості часу та зусиль.

Моніторинг зашифрованого трафіку кидає виклик застарілим виявленням аномалій

З міркувань конфіденційності та безпеки в комп’ютерних мережах шифрування даних розширюється та вдосконалюється. Зашифрований зв’язок також впливає на виявлення аномалій, оскільки шифрування даних зменшує обсяг даних, з якими може працювати моніторинг та аналіз.

Наприклад, під час моніторингу зашифрованої електронної пошти адреси електронної пошти недоступні.

Важливо знати, на якому рівні відбувається шифрування. Більшість комунікацій шифрується лише на рівні програми, що означає, що все ще можна виконувати статистичний аналіз IP-адрес, портів призначення тощо.

Таким чином, шифрування не перешкоджає виявленню аномалій, але значно обмежує типи аномалій. виявлено.

Саме на підприємстві одним з варіантів аналізу аномального трафіку є Zeek, Першою що можна побачити в Zeek, є великий набір журналів, що описують мережеву активність. Сюди входять усі сеанси HTTP із запитаними URI, заголовками ключів, типами MIME та відповідями сервера; DNS запити з відповідями; SSL сертифікати; ключовий вміст сесій SMTP; та інше.[7]

На додаток до журналів, Zeek має вбудовану функціональність для цілого ряду завдань аналізу та виявлення, включаючи вилучення файлів із сеансів HTTP, виявлення шкідливого програмного забезпечення за допомогою взаємодії із зовнішніми реєстрами, звітування про вразливі версії програмного забезпечення, побаченого в мережі, виявлення популярних веб-сайтів. програми, виявлення грубого примусу SSH, перевірка ланцюжків сертифікатів SSL та багато іншого.

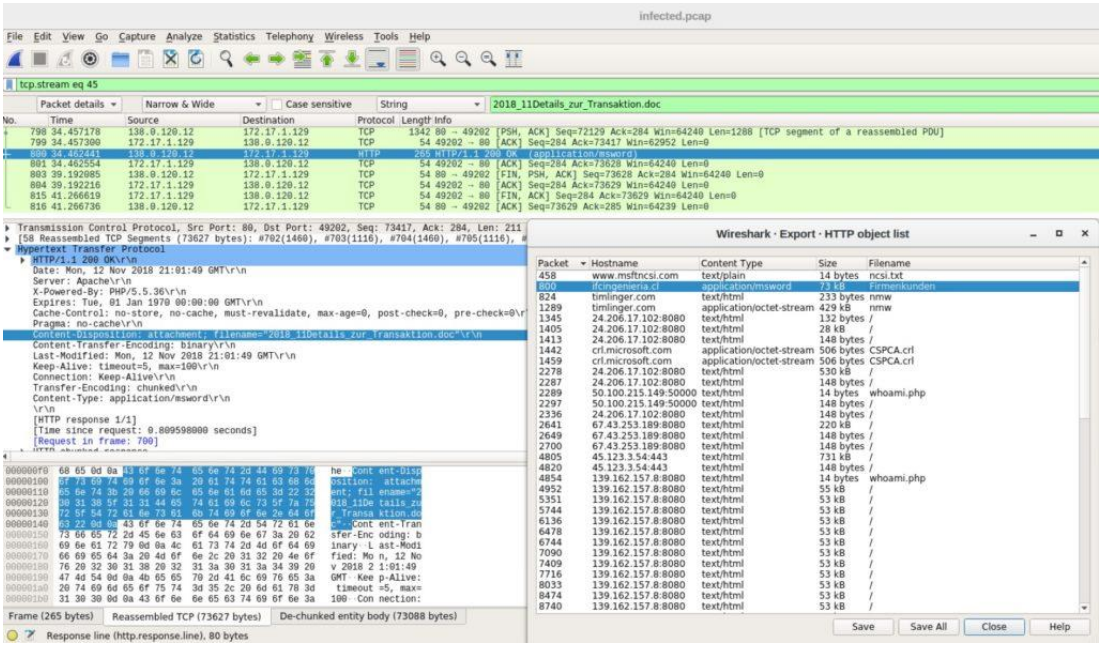


Рисунок 1.5 – Інтерфейс ПЗ Zeek

Якщо коротко, Zeek оптимізовано для інтерпретації мережевого трафіку та створення журналів на основі цього трафіку. Найбільша проблема з цим інструментом полягає в тому, що він має стрімку криву навчання,

підприємству, так як воно шукає підходи для виявлення підписів, краще спробувати системи виявлення вторгнень розроблену під час кваліфікаційної роботи.

Також не є аналізатором протоколів у сенсі Wireshark, який прагне відобразити кожен елемент мережевого трафіку на рівні кадру або системою для зберігання трафіку у формі захоплення пакетів (PCAP).

Під час кваліфікаційної роботи буде запропоновано інший програмний метод виявлення аномалій, а саме розроблений програмний засіб AnomalyShield, в якому буде деяка кількість схожих функцій з вищезгаданою програмою, також використаний програмний засіб буде більш оптимізований, візуально зрозумілим та легким для сприйняття інтерфейсом, з можливістю повідомлення адміністратора про виявлення аномалій в досліджуваній мережі.

2 ПОСТАНОВКА ЗАДАЧІ

Сьогодні на ринку програмного забезпечення винайдена велика кількість програмних продуктів як системного, так і прикладного призначення.

Саме з розвитком та розповсюдженням Інтернету досить часто стали використовуватися спеціальні програми для перехоплення й аналізу мережевого трафіку, але не всі вони є дієвими та актуальними.

Темою кваліфікаційної роботи є “система виявлення аномального трафіку на маршрутизаторі Mikrotik”

Завданням на дипломну роботу є виявлення аномального трафіку використовуючи маршрутизатор Mikrotik, та його можливості у відділені «Укргазбанк» м. Хмельницький де проходилась переддипломна практика.

Виявлення аномалій мережевого трафіку між банками для підтримки необхідного рівня сервісу й захисту мережевих ресурсів. При цьому враховується, що порушення цілісності інформації або перехоплення у мережі, у поточному контексті, є аномалією.

Аналіз мережевого трафіку допоможе у різних випадках використання, таких як виявлення шкідливого програмного забезпечення, виявлення використання вразливих протоколів і шифрів, усунення несправностей у повільній мережі, а також збір в реальному часі та архівних записів про те, що відбувається в мережі. Це покращує внутрішню видимість і усуває сліпі плями.

Розроблення програмного забезпечення для виявлення аномального трафіку, побудова плану приміщення, логічна та фізична моделі приміщень. Для виконання поставленої задачі було використане обладнання Mikrotik.

Mikrotik Router OS це досить потужний інструмент для створення мереж та їх управлінням, що включає в свій арсенал безліч функцій для роботи практично з усіма можливими мережевими протоколами.

Незважаючи на те, що сама операційна система побудована на ядрі linux, вона не є OpenSource проектом. Код Mikrotik Router OS не доступний громадськості і отримати доступ до командного рядка linux, неможливо. Також немає можливості створення власних пакетів програмного забезпечення. Всі зміни в самій Mikrotik Router OS та додавання функціоналу здійснюється виключно розробником.

Саме аналіз трафіку в мережі швидко поширився як варіант забезпечення безпечного та якісного безпровідного або провідного зв'язку. Це дозволяє організувати безпечну роботу , зменшити ресурсопотребність мережі, та підвищити її ефективність, хоча й аналіз трафіку мережі є ефективним, з іншої сторони потрібно підшукувати нові варіанти для аналізу мережі та їх моделювання в зв'язку з оновленням комп'ютерних мереж.

3 ВИЯВЛЕННЯ АНОМАЛЬНОГО ТРАФІКУ

3.1 Аналіз мережевого трафіку

Представлення даних

Метою мережі є передача інформації від одного комп'ютера до іншого. Для цього спочатку необхідно визначитися з типом кодування переданих даних, тобто їх комп'ютерного представлення. Це буде відрізнятися в залежності від типу даних, оскільки це може бути:

- Звукові дані
- Текстові дані
- Графічні дані
- Відео дані
- Інші

Представлення цих даних можна розділити на дві категорії:

- Цифрове представлення : кодування інформації в набір двійкових значень , тобто серії 0 і 1
- Аналогове представлення : в якому дані будуть представлені як зміна безперервної фізичної величини [8]

Носій передачі даних

Щоб налагодити передачу даних , між двома машинами має бути лінія передачі, яка також називається трактом або каналом передачі.

Ці шляхи передачі складаються з кількох секцій, що дають змогу передавати дані у вигляді електромагнітних, електричних, світлових або навіть акустичних хвиль. Отже, існує певне вібраційне явище, яке поширюється на фізичному середовищі.

Лінія передачі

Лінія передачі - це зв'язок між двома машинами. Термін відправник зазвичай позначає машину, яка надсилає дані, а одержувач – той, який їх отримує. Машини іноді можуть бути по черзі приймачами або передавачами (загалом це стосується комп’ютерів, під’єднаних мережею).

Лінія передачі, яку також іноді називають каналом передачі або каналом передачі , не обов'язково складається з одного фізичного середовища передачі, тому кінцеві машини (на відміну від проміжних машин), які називаються DTE кожен має обладнання, пов’язане з фізичним середовищем, до якого вони підключені, яке називається ETCD або DCE.

Передачі в мережі

Щоб передати двійкову інформацію в середовищі передачі, необхідно попередньо перетворити її в електричний сигнал, краще відповідний фізичним обмеженням системи передачі.

Комп’ютерні мережі зазвичай потребують дуже високої швидкості, кілька мегабіт в секунду.

У цьому контексті можливі дві методики передачі: так звана передача в режимі Bade, яка виконує лише просту трансформацію сигналу, і передача, яка виконує трансляцію спектру (модуляцію).

Передача основної смуги

Передача основної смуги, типова для більшості локальних мереж, складається з передачі цифрових сигналів безпосередньо через середовище передачі. На малюнку нижче узагальнено принцип передачі основної смуги.

Принцип передачі в основній смузі

Основне призначення кодера основної смуги полягає в тому, щоб:

- трансформувати цифровий сигнал в інший, щоб спектр нового сигналу був краще адаптований до характеристик середовища передачі (зокрема пропускної здатності)
- підтримувати синхронізацію між передавачем і приймачем.

Такий метод простий і недорогий, але вимагає високошвидкісного середовища передачі.

Пакет TCP/IP

У комп’ютерному словнику пакет є одиницею передачі мережевого рівня. Іншими словами, коли файл передається від однієї станції до іншої, він розбивається на певну кількість пакетів, які надсилаються один за іншим. Це називається комутацією пакетів . Крім того, що містять частину даних, пакети складаються із заголовка, в якому містяться характеристики відправлення (розмір файлу, адреса відправника та одержувача та технічна інформація).

Слово дейтаграма - це комп'ютерний термін, який використовується для опису передачі пакета без гарантії його отримання в місці призначення. Іноді він використовується для загального посилання на передані блоки даних.[10]

Мережевий протокол TCP зробив передачу пакетів більш надійною. Він виявляє збої передачі, які можуть виникнути, коли маршрутизатор перевантажений. Таким чином, коли передані пакети не досягають місця призначення, вони знищуються, а потім передаються повторно.

У IP-протоколі всі дані, що надсилаються через Інтернет, розбиваються на менші частини, які називаються пакетами .

Наприклад, коли веб-сторінка надсилається з веб-сервера на ноутбук користувача, дані, які утворюють веб-сторінку, передаються через Інтернет у вигляді серії пакетів.

Потім пакети знову збираються ноутбуком, щоб потім створити веб-сторінку на екрані. Щоб можна було встановити TCP-з'єднання, IP-пакет містить дані та інформацію.

Наприклад, IP-адреса джерела та призначення.

Ці дані зберігаються в заголовку IP-пакета

Середній IP-пакет має розмір 128 або 256 байт. З появою дуже високошвидкісних технологій банкоматів починають популяризуватися більші розміри близько 1500 байт.

Пакет є базовою одиницею для цифрового мережевого зв'язку. Пакет називають дейтаграмою, сегментом, блоком, коміркою або кадром, залежно від використовуваного протоколу передачі даних. Коли дані необхідно передати, перед передачею вони поділяються на подібні структури даних, які називаються пакетами, які знову збираються в вихідному блоці даних, як тільки вони досягають місця призначення.

Структура пакетів даних

Структура пакета залежить від типу пакета та протоколу.. Зазвичай пакет має заголовок і корисне навантаження.

Заголовок зберігає інформацію вище про пакет, послугу та інші дані, пов’язані з передачею. Наприклад, для передачі даних через Інтернет потрібно розбити дані на IP-пакети, які визначені в IP і IP-пакет включає:

IP-адреса джерела, яка є IP-адресою пристрою, який надсилає дані.

Цільова IP-адреса, яка є машиною або пристроєм, на який надсилаються дані.

Серійний номер пакетів, число, яке впорядковує пакети таким чином, щоб вони були зібрані таким чином, щоб отримати вихідні дані так само, як і перед передачею.

Як правило, заголовок має таку структуру:

Рисунок 3.1 – Структура заголовку ip-пакету

Поле «Номер версії» вказує версію протокола IP.

Поле «Довжина заголовку» вказує довжину, зазвичай вона рівна 20 байтам, але в деяких випадках довжина може бути збільшена.

Поле « Тип сервісу» вказує пріоритет пакету та його критерії пошуку маршруту.

Поле «Загальна довжина» вказує сумарну довжину пакету включно з заголовком й полем даних.

Поле «Ідентифікатор пакету» використовується для розпізнавання пакету.

Поле «Флаг» містить в собі ознаки пов’язані з фрагментацією.

Поле «Зміщення фрагменту» задає зміщення в байтах поля даних від початку спільного поля даних вихідного пакету.

Поле «Час життя» визначає граничний термін, протягом якого можливий рух пакету по мережі.

Поле «Протокол верхнього рівня» вказує якому протоколу належить інформація.

Поле «Вирівнювання» використовується для того щоб впевнитись що заголовок закінчується на 32-біт.

Корисне навантаження, яке представляє більшу частину пакета (всі розглядаються як накладні витрати) і фактично представляє дані, що передаються. [11]

Пакети відрізняються за структурою та функціональністю залежно від протоколів, які їх реалізують. VoIP використовує протокол IP і, отже, IP-пакети. У мережі Ethernet , наприклад, дані передаються в кадрах Ethernet

У моделі Інтернету , також званої моделлю TCP/IP, TCP стоїть вище IP. TCP/IP є однією з реалізацій «комутації пакетів» і становить основу нашого сучасного Інтернету .

Всупереч поширеній думці, TCP/IP — це не протокол, а набір протоколів. TCP вважається протоколом, орієнтованим на з'єднання, оскільки

він забезпечує доставку даних хосту-одержувачу без помилок. TCP використовує сегменти, щоб визначити, чи готова система-отримувач приймати дані.

Коли TCP хоста-відправника бажає встановити з'єднання, він посилає сегмент під назвою SYN на TCP хоста-отримувача. Приймаючий TCP повертає сегмент, який називається ACK , щоб підтвердити отримання сегмента.

TCP-відправник надсилає інший сегмент ACK, а потім ініціює надсилання даних. Такий обмін контрольною інформацією називається триетапним узгодженням . Модель TCP/IP - це 4-рівнева мережева архітектура, в якій протоколи TCP і IP відіграють переважну роль, оскільки вони є найпоширенішою реалізацією.

Модель TCP/IP - це 4-рівнева мережева архітектура:

У протоколі IP IP-пакети переміщуються через Інтернет через вузли, які є пристроями та маршрутизаторами (технічно називаються вузлами в цьому контексті), що знаходяться на шляху від джерела до місця призначення. Кожен пакет націлений на місце призначення на основі його адреси джерела та адреси призначення. На кожному вузлі маршрутизатор на основі розрахунків, які включають мережеву статистику та витрати, вирішує, якому сусідній вузол буде ефективніше надсилати пакет.

Цей вузол більш ефективний для відправки пакета. Це частина комутації пакетів , яка фактично очищає пакети в Інтернеті, і кожен з них знаходить свій шлях до місця призначення. Цей механізм безкоштовно використовує базову структуру Інтернету, що є основною причиною того, що дзвінки VoIP та Інтернет-дзвінки є найбільш безкоштовними або дуже дешевими.

На відміну від традиційної телефонії, де лінія або ланцюг між джерелом і призначенням повинні бути виділені та зарезервовані (так звана ком утація каналів), звідси висока вартість, комутація пакетів використовує існуючі мережі безкоштовно.

Іншим прикладом є TCP (Transmission Control Protocol), який працює з IP у тому, що ми називаємо пакетом TCP/IP. TCP відповідає за надійну передачу даних.

Щоб досягти цього, він перевіряє, чи прийшли пакети в порядку, чи відсутні пакети чи не дублюються, а також чи є затримка в передачі пакетів. Він контролює це, встановлюючи очікування та сповіщення, які називаються підтвердженнями.

Виявлення аномалій — це функція, актуальна для виявлення тенденцій трафіку, які не відповідають очікуванням. Це може бути пік або падіння трафіку, і ці варіації можуть бути з різних джерел:

- Рух роботів
- Технічний збій
- Охоплення ЗМІ
- Поточні події
- Публікація сторінки, статті чи вмісту

3.2 Апаратно-програмне забезпечення .

На підприємстві «Укргазбанк» знаходиться маршрутизатор моделі RB1100AHx2 компанії Mikrotik

Компанія була заснована для розробки маршрутизаторів і систем бездротового підключення для Інтернет-провайдерів.

Досвід Mikrotik у використанні стандартного обладнання для ПК та повних систем маршрутизації дозволив їм створити програмну систему RouterOS.

Ця система перетворює персональний комп’ютер на маршрутизатор (включаючи такі функції, як брандмауер , сервер і клієнт VPN), контролює трафік на основі про якість обслуговування (QOS), доступ до бездротової

мережі. Систему також можна використовувати для створення власного порталу.

Ця операційна система має багаторівневу ліцензію, причому кожен рівень пропонує більше функцій. Плата за ліцензію буде залежати від вибраного рівня. Для налаштування системи також доступний графічний інтерфейс під назвою Winbox. Нарешті, API дозволяє налаштувати систему та контролювати її

Доволі очікуємо, що маршрутизатор Mikrotik це чудовий вибір, оскільки у нього немає конкурентів за надійність. Дійсно його можна налаштувати 1 раз і при певних подіях та умовах доредаговувати певні налаштування.

Маршрутизатори Mikrotik довгий час залишалися пристроєм для професіоналів, однак із зростанням функціональності маршрутизатора веб-конфігуратор став більш зручним для користувачів.

Брандмауер – це інструмент, головна роль якого полягає в забезпеченні безпеки та захисту конфіденційних даних мережі. Він також захищає маршрутизатор і клієнтів від несанкціонованого доступу. Він складається з кількох елементів, таких як фільтр, списки доступу, mangle, Nat. Ця остання функція NAT є механізмом, який приховує приватні IP-адреси мережі за загальнодоступною адресою, щоб дозволити комп'ютерам мережі отримати доступ до Інтернету, зберігаючи таким чином публічні адреси.

Dynamic Host Configuration Protocol — це протокол для динамічного призначення адрес в IP-мережі на основі bootp. DHCP, що входить до складу Mikrotik, інтегрує клієнт і сервер. IP-адреси можна прив'язати до MAC-адрес за допомогою функції статичної оренди. DHCP-сервер прослуховує порт UDP 67, а клієнт - порт UDP 68.

У ході роботи використовувався маршрутизатор моделі RB1100AHx2 RB1100AHx2 — це гігабітний Ethernet-маршрутизатор розміром 1U для монтажу в стійку — з двоядерним процесором він може досягати мільйона пакетів в секунду та підтримує апаратне шифрування!

Продуктивний, стійковий маршрутизатор промислового класу, можливості якого збільшені майже вдвічі, завдяки новому процесору, і можуть легко покрити мережеві потреби середнього і навіть великого підприємства. Адже сумарна пропускна спроможність маршрутизатора RB 1100AHx2 перевищує 5Gbit. Можливо це завдяки новому потужному двоядерному мережному процесору PowerPC P2020 з тактовою частотою в 1066 МГц, який здатний обробляти понад один мільйон пакетів в секунду.

Як операційна система, в маршрутизаторі RB1100AHx2 використовується фірмова Mikrotik RouterOS найвищого рівня - Level6, що дозволяє без жодних обмежень використовувати всі як апаратні так і програмні можливості цього апаратно-програмного комплексу. Включаючи необмежену кількість тунельних з'єднань за протоколами PPPoE, PPTP, L2TP, OVPN та багатьма іншими.[12]

RB1100AHx2 поставляється в попередньо встановленому алюмінієвому корпусі висотою 1U для монтажу в стійку, блоку живлення та штепсельній вилці, зібраному та готовому до розгортання.

Рисунок 3.2 – Маршрутизатор RB1100AHx2

Таблиця 3.1 – Характеристики маршрутизатора RB1100AHx2

Код продукту	RB1100AHx2
Архітектура	КПП
ЦП	P202ASSE2KFB
Кількість ядер ЦП	2
Номінальна частота процесора	1066 МГц
Розміри	Корпус 1U: 44 x 176 x 442 мм, 1200 г. Тільки дошка: 365 г
Ліцензія RouterOS	6
Операційна система	RouterOS
Розмір оперативної пам'яті	2 ГБ
Розмір зберігання	128 МБ
Тип зберігання	NAND
MTBF	Приблизно 200 000 годин при 25°C
Перевірена температура навколишнього середовища	-35°C до 70°C
Апаратне прискорення IPsec	Так

Маршрутизатор поєднує модем з іншими пристроями, щоб забезпечити зв'язок між цими пристроями та Інтернетом. Більшість маршрутизаторів мають кілька мережевих портів, які дозволяють одночасно підключати кілька пристроїв до Інтернету.

Маршрутизатор аналізує IP-адресу призначення пакета даних , обчислює найкращий маршрут для досягнення його місця призначення та надсилає пакет даних.

Таблиця 3.2 – Живлення маршрутизатора RB1100AHx2

Кількість входів змінного струму	1
Діапазон входу змінного струму	100-240
Кількість входів постійного струму	2 (PoE-IN, 2-контактний термінал)
Вхідна напруга 2-контактної клеми	7-28 В
Максимальне споживання електроенергії	25 Вт
Тип охолодження	2
PoE в	Пасивний PoE
PoE у вхідній напрузі	10-28 Ст

Як правило, маршрутизатор фізично підключається до модему через мережевий кабель через Інтернет або порт WAN . Потім він також фізично підключається за допомогою кабелю до мережевої карти пристроїв, які потрібно підключити до Інтернету.

Більшість маршрутизаторів підключаються до інших мережевих пристроїв лише за допомогою кабелів і не вимагають, щоб драйвери працювали в Windows або інших операційних системах .

3.3 Логічна модель мережі

Побудова фізичної схеми та плану мережі приміщення банку буде першим пунктом в даній кваліфікаційній роботі.

Рисунок 3.3 – Фізичний план приміщення банку

На схемі зображено приміщення філії «Укргазбанку» з зображенням всіх комп’ютерів, інших приладів та робочих місць під’єднаних до однієї мережі. Приміщення розділене на декілька зон з різними призначеннями.

Кімнати облаштовані комп’ютерами та іншими пристроями (принтери, камери).

В центрі приміщення знаходиться зона очікування в якій розташований столик та дивани для відвідувачів.

Також є зона самообслуговування , зона обслуговування віп клієнтів, касові зони, та інші службові приміщення. В кімнаті адміністратора та касових відділах відсутні вікна, та до них йде лише один вхід через буферну зону.

Наступним завданням буде побудова інтегрованої фізичної моделі мережі

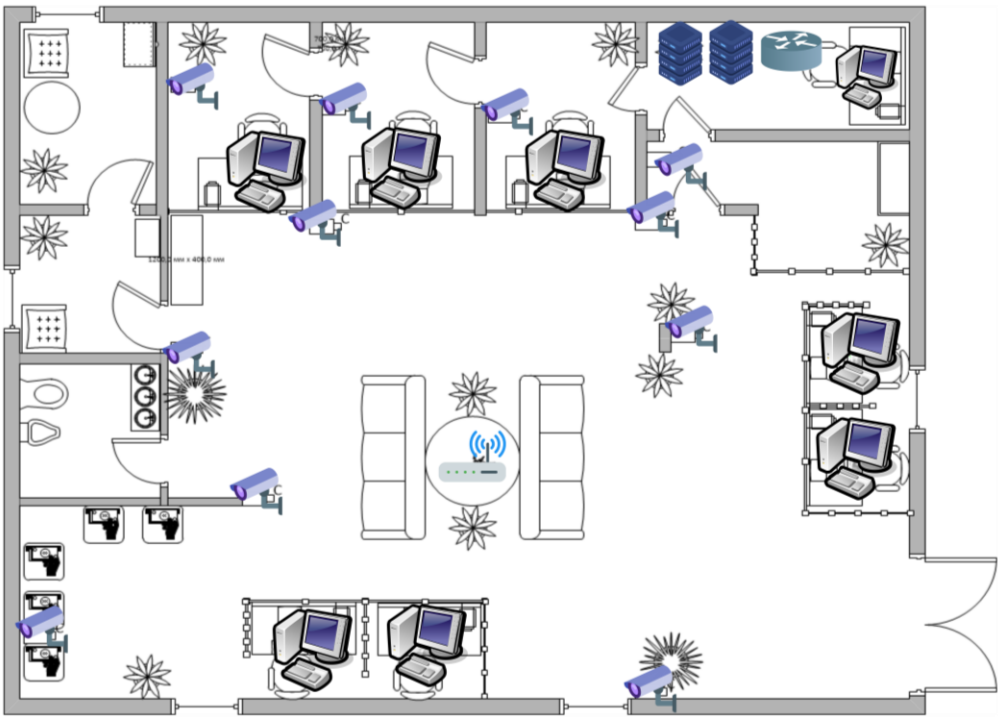


Рисунок 3.4 – Інтегрована фізична схема мережі філії «Укргазбанк»

Побудувавши інтегровану фізичну схему, наступним завданням буде побудова логічної схеми мережі, на рис. 2.5. зображена актуальна на час виконання кваліфікаційної роботи кількість приладів підключених до мережі, а саме:

Таблиця 3.3 – Список приладів на підприємстві в мережі

Вид приладу	Кількість
Службовий персональний комп’ютер	7
Персональний комп’ютер адміністратора	1
Камери відеоспостереження	11

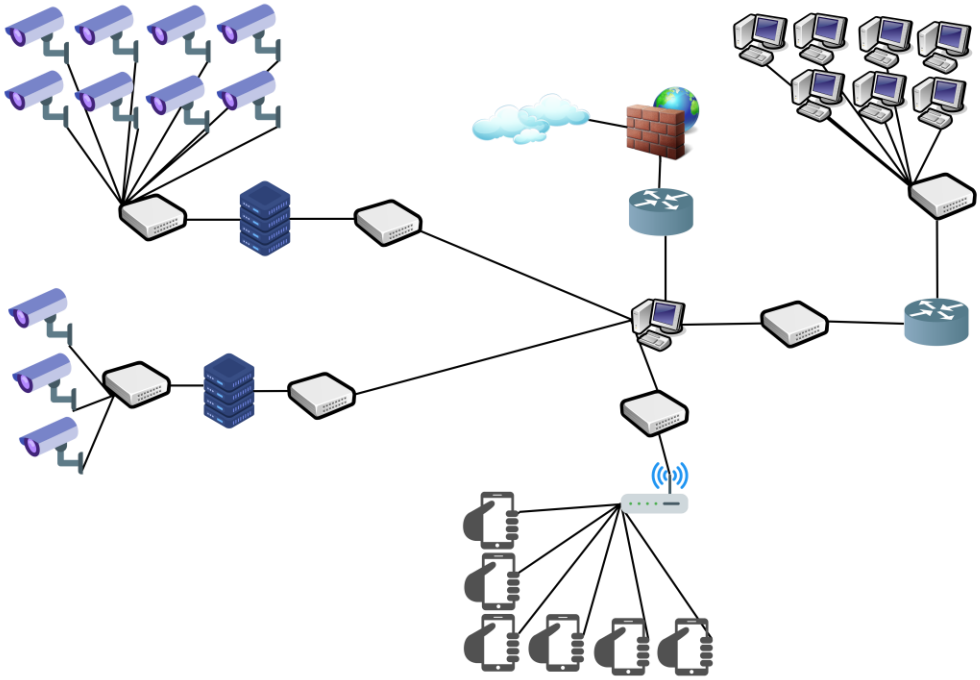


Рисунок 3.5 – Логічна система мережі

На малюнку вище зображена логічна система мережі з зображенням всіх пристроїв підключених до мережі.

3.4 Висновки

Отже обладнання що використовується під час виконання кваліфікаційної роботи належить компанії Mikrotik, а саме маршрутизатор RB1100AHx2.

В маршрутизаторі встановлена фірмова операційна система Mikrotik RouterOS найвищого рівня - Level6.

Був спроектований план приміщення використовуючи Microsoft Visio, після чого була побудована інтегрована фізична модель мережі , далі була сформована логічна система мережі, визначились в кількості пристроїв

підключених до однієї мережі та їх типі. Гостьова мережа Wi-Fi в філії відсутня.

Дізнався які засоби виявлення аномального трафіку вже присутні на підприємстві та визначились в якому напрямку будемо далі працювати.

4 ВИЯВЛЕННЯ АНОМАЛЬНОГО ТРАФІКУ

4.1 Алгоритм виявлення аномального трафіку.

Під час виконання кваліфікаційної роботи як аномальний трафік також ідентифікується і вхід на заборонені сайти працівників відділення, та різного види атаки на мережу банку.

Програмний засіб наділений можливістю блокування джерела атаки, призупиняючи можливу небезпеку

Найбільш ефективним блокування аномалій мережі буде в випадку, коли у базі є вже відомі або схожі , небезпеки.

В випадках коли адміністратор не має можливості відстежити й прийняти міри відносно аномального трафіку чудовим рішенням буде повідомлення про подію.

Адміністратору буде приходити сповіщення про зафіксований факт атаки , він матиме можливість швидко відреагувати на неї та виконати певні дії.

Аномальна поведінка є наслідком дій зловмисників. Спроба виявити аномальний трафік побудована на використані образу нормальної поведінки системи, при виявлені відходження від нормальної поведінки вона відразу буде класифікована як аномальна, а саме буде фіксуватися факт атаки або вторгнення.

Це може дозволити виявити вади у здійсненні керування безпекою, і виправити процедури керування

Буде набагато легше зробити висновки щодо частоти й типу атаки чи аномалій що дозволить вжити адекватних заходів безпеки

Але є й недоліки цього методу, а якщо більш детально, то це помилкові спрацьовування, таким чином не кожна аномалія може бути дійсно аномалією (атакою або загрозою), але система буде класифікувати її як загрозу.’

Рисунок 4.1 – Схема класифікацій мережевих аномалій

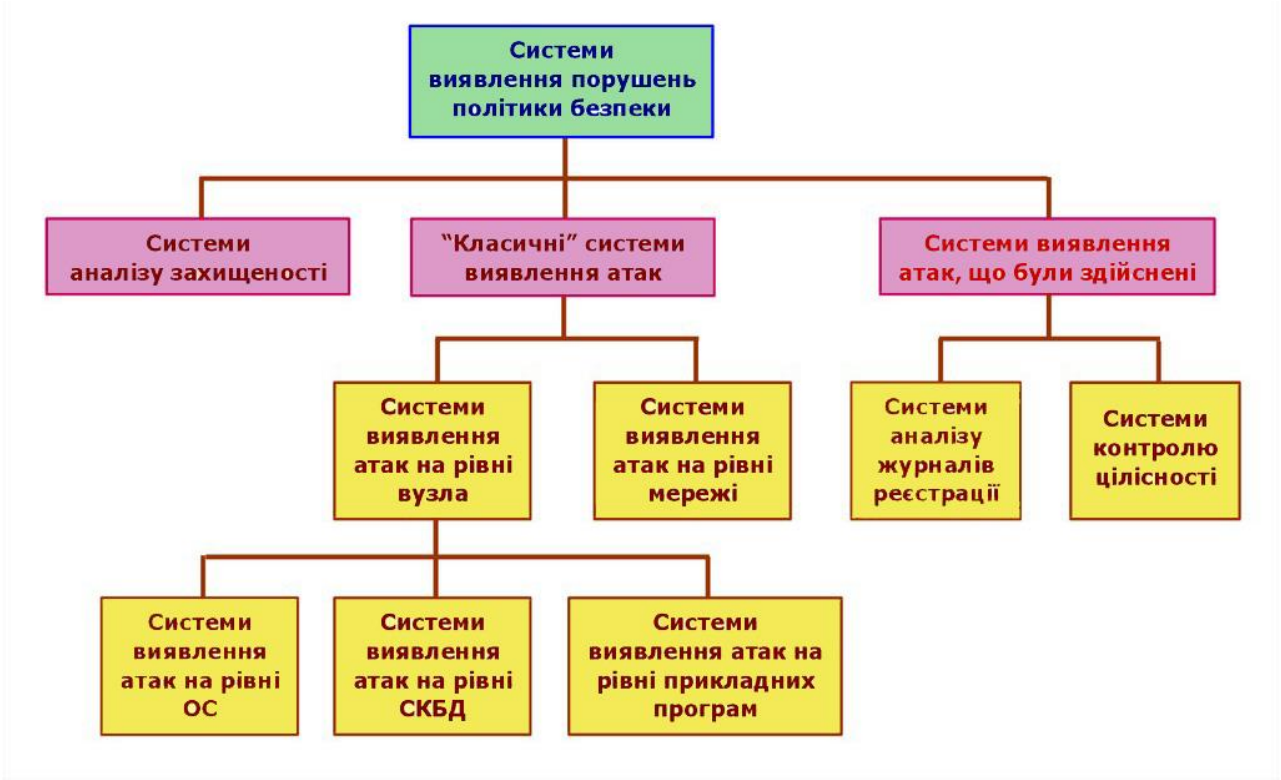


Рисунок 4.2 – Загальна класифікація систем виявлення аномалій

4.2 Структура та опис розробленого програмного забезпечення.

Виконання кваліфікаційної роботи продовжується написанням скрипта в середовищі RouterOS.

Хоч і можна писати скрипти в вікні "Source", але це зовсім не зручно. А зручно для редагування скриптів використати термінал. Для створення скрипта використовується така команда:

/system script add name=< 1>

Для його редагування потрібно використати таку команду:

/system script edit <1> source

Після виконання цієї команди в терміналі відкриється текстовий редактор, де з'явиться можливість написати власний скрипт. Наприклад:

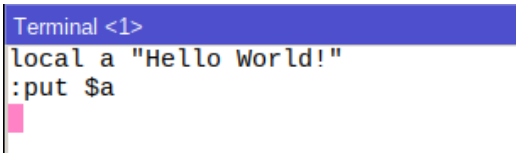


Рисунок 4.3 – Текстовий редактор

Саме скриптів для виявлення і обробки аномального трафіку буде кілька, зупинимось поки-що на першому з них, скрипт працює таким чином, що на початку роботи, а саме отриманні пакету даних відбувається перевірка на те чи є отримувач й/або джерело забороненими. Після перевірки при позитивному варіанті, якщо щось з вищеназваного є забороненим пакет блокується й цикл закінчується. Якщо ні, цикл продовжується та відбувається перевірка чи джерело та отримувач дозволені, якщо так, то пакет пропускається та цикл завершується , якщо ні, то дані записуються в базу даних з внесенням точного часу сигналу, отримувача, джерела, самого пакета. Після чого цикл завершується.

Кваліфікаційна робота виконана таким чином, що деяка частина поставлена в вигляді скриптів на офіційній операційній системі Mikrotik RouterOs, поєднаних з програмним кодом що в сумі дає вартий уваги результат.

Операційна система RouterOs надає можливість переглядати всі правила які були написані як власноруч, так і заготовлені. Щоб полегшити перегляд, також є ведення журналу з випадками підозри або виявлення аномалій мереж. В базу вноситься 4 категорії даних :

- Отримувач;
- Джерело;
- Пакет;
- Час.

За допомогою цих даних визначаються загрози, з’являється можливість зрозуміти ризики, усунути аномалії та оптимізувати роботу мережі. Дана система буде повідомляти адміністратора про деякі випадки підозр на аномальний трафік таким чином даючи адміністратору можливість вибору що далі робити з підозрілою активністю.

Оскільки до заборонених сайтів відноситься «WhatsApp» по тій причині що через даний ресурс можливий виток інформації на підприємстві , нижче буде наведений приклад скрипта написаний в середовищі MikroTik Script RouterOS, за допомогою якого буде відбуватись блокування даного ресурсу.

```
/ip firewall layer7-protocol add name=WhatsApp
regexp="^.+(whatsapp.com).*\$" /ip firewall filter add
action=drop chain=forward layer7-protocol=WhatsApp
```

Також реалізовано захист маршрутизатора від DDOS-атаки скриптом в середовищі Mikrotik Script RouterOS.

З’являється можливість передбачати, атаки DDOS, а саме обмеження кількості з’єднань в правилах брандмауера. Коли відбувається DDoS-атака, система виявляє, що кількість запитів на з’єднання перевищує вказаний ліміт.

```
/ip firewall filter
add chain=forward connection-state=new action=jump
jump-target=block-ddos
add chain=forward connection-state=new src-address-
list=ddoser dst-address-list=ddosed action=drop
add chain=block-ddos dst-limit=50,50,src-and-dst-
addresses/10s action=return
```

```
add chain=block-ddos action=add-dst-to-address-list
address-list=ddosed address-list-timeout=10m
add chain=block-ddos action=add-src-to-address-list
address-list=ddoser address-list-timeout=10m
```

Також задля зменшення помилок через неуважність, або з причини відволікання відбувається блокування різного виду сайтів відеохостингів які підвищують рівень помилок під час виконання службових зобов'язань на підприємстві. Як один з варіантів, це Youtube та Netflix»

```
/ip firewall layer7-protocol
add name=Netflix regexp="^.+(netflix.com).*\$"
/ip firewall filter
add action=drop chain=forward layer7-
protocol=Netflix
```

Вище наведений 1 з варіантів блокування Netflix.

Далі обмежимо доступ до відеохостингу Youtube.

```
/ip firewall layer7-protocol
add name=Youtube
regexp="^.+(youtube.com|googlevideo.com).*\$"
/ip firewall filter
add action=drop chain=forward layer7-
protocol=Youtube
```

Нище буде зображено кілька алгоритмів роботи даного програмного забезпечення.

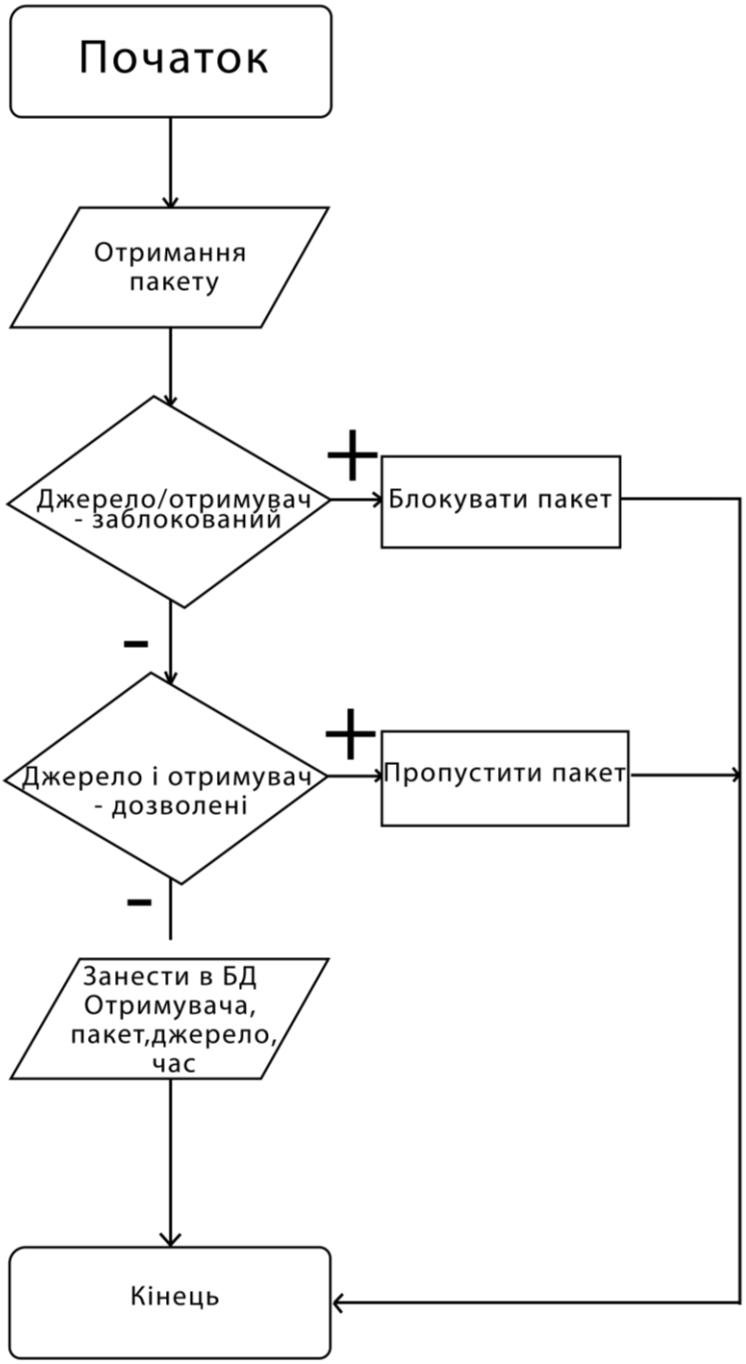


Рисунок 4.4 – Алгоритм дії скрипта Base.

Скрипт працює таким чином, що після початку роботи та відправлення пакету відбувається перевірка на дозволеність отримувача та самого джерела. В загальному існує три списка джерел, які поділяються на :

- Дозволені – Джерела що є дозволеними для користування в підприємстві,(попередньо визначені адміністратором). Це можуть бути офіційні сайти мереж банків, державних установ, та деякі джерела для проведення відеоконференцій. Можливі зміни методом переносу в «заблоковані», «підозрілі», або навпаки з них.
- Заборонені – Джерела, що є не дозволеними в мережі, також можливе редагування списку адміністратором, в цілому це деякі одиниці соц. мереж, стрімингові сайти, та сайти країни агресора.
- Підозрілі – Джерела що не підпадають ні в яку з вищезгаданих категорій, подальші дії над даними джерелами лягають на адміністратора мережі. Вони підлягають перевіркі, та в подальшому переносяться в одну з категорій.

Якщо скрипт розпізнає джерело або отримувача як забороненого подальший хід пакета даних блокується, та скрипт завершує свою роботу.

Якщо скрипт розпізнає джерело або отримувача як дозволеного, пакет проходить далі.

Якщо джерело розпізнається як підозріле, з’являється повідомлення та вирішується подальші дії з ним.

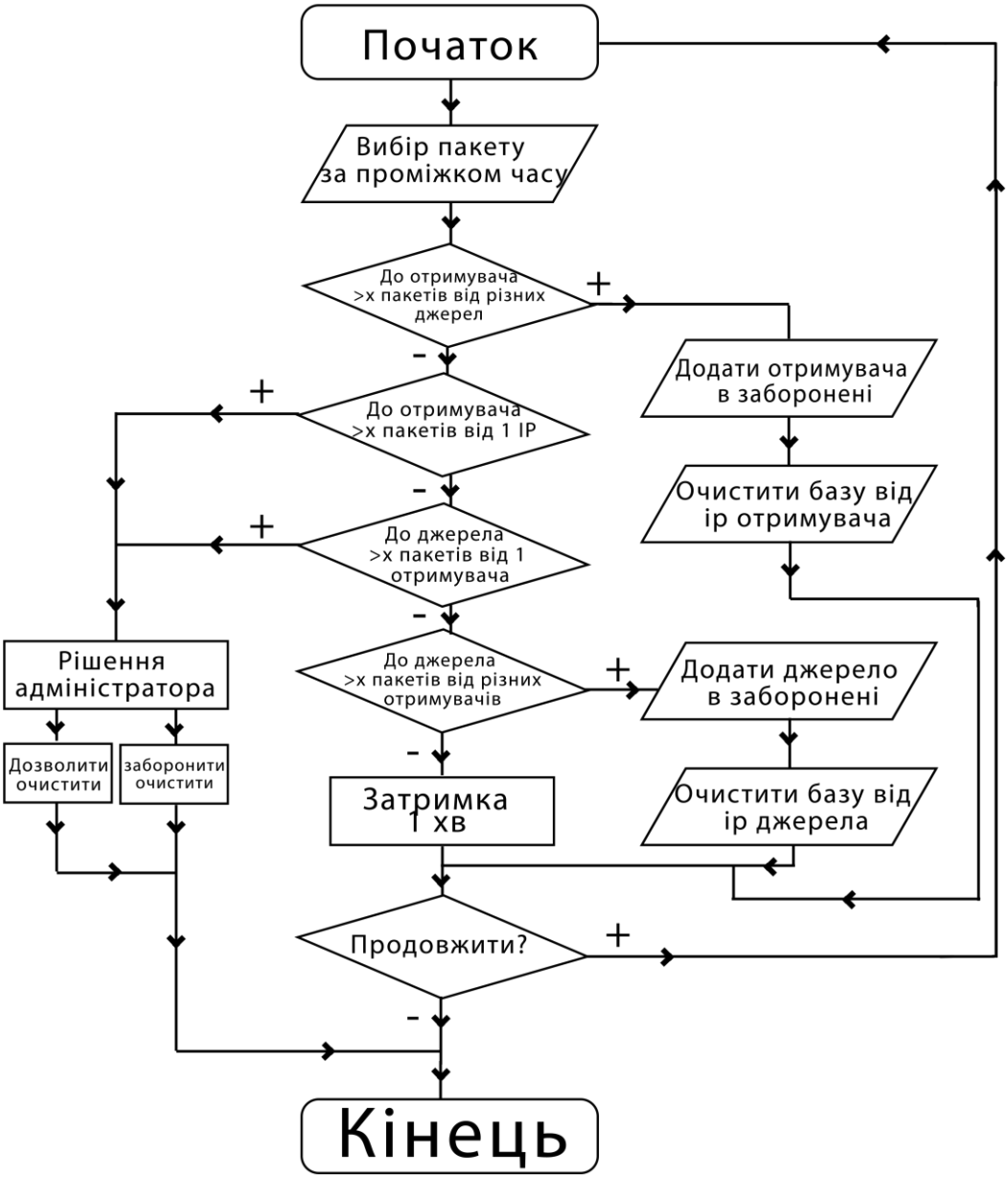


Рисунок 4.5 - Алгоритм дій скрипта Analysis

На малюнку вище зображений алгоритм дій наступного скрипта більш відкрито, відбувається відбір з бази даних за кількістю звернень схожих на аномальні явища пакетів, після чого відбувається перевірка в 4 кроки, під час якої джерело або отримувач може бути заблокований, або пропущений далі, при певних умовах з'являється повідомлення до адміністратора, який може або заблокувати пакет, або дозволити, тобто подальші дії з пакетом залежать від нього, можливо, також реалізована зміна статуса джерела й/або отримувача, якщо це буде потрібно на одну з 3 категорій, а саме: заборонений,

дозволений, підозрілий. Після чого скрипт перевіряє частоту пакетів, можлива повторна перевірка пакету, після чого відбувається закінчення циклу .

4.3 Тестування розробленого програмного забезпечення

На підприємстві були проведені налаштування маршрутизатора, введені в дію скрипти та реалізована інтуїтивно проста, та зручна візуальна оболонка, яка відкриває нові можливості та спрощує перегляд пакетів даних.

Програмний засіб отримав назву AnomalyShield. В майбутніх оновленнях додаток запрацює в більш широкому діапазоні з масштабнішими можливостями.

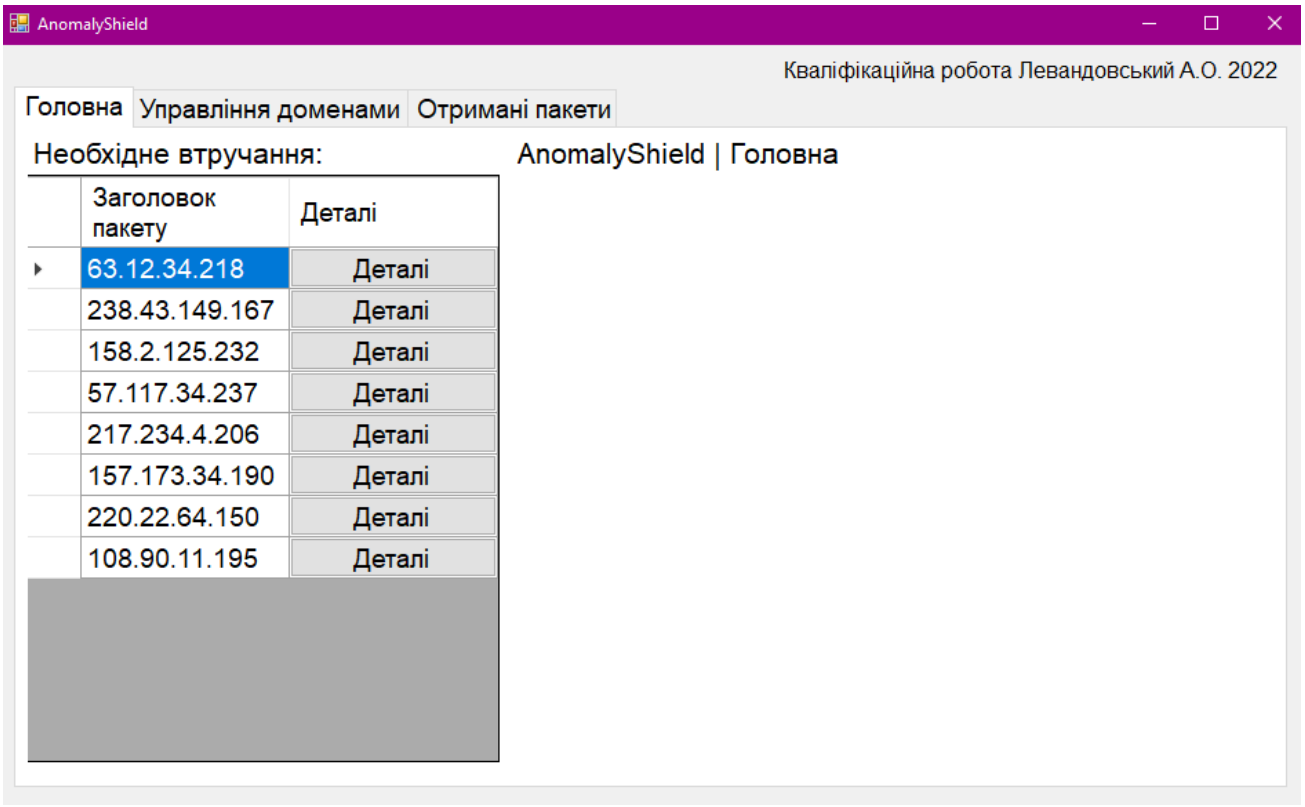


Рисунок 4.6 – Головне меню впровадженого продукту.

Відразу можна звернути увагу в верхній частині зображено 3 вкладки, розпочнемо з першої, а саме головної з них. Знову ж таки саме ця вкладка є найбільш важливою як і для адміністратора так і для мережі в цілому. Саме

сюди потрапляють пакети які частково пройшли перевірку та потребують перевірки адміністратором мережі. Пакети сортуються у вигляді списку в якому є всього 2 колонки. Після чого адміністратор який хоче зробити певну дію з пакетом, може ознайомитись з деталями, отримавши певну інформацію про пакет, та виконати подальші дії з ним.

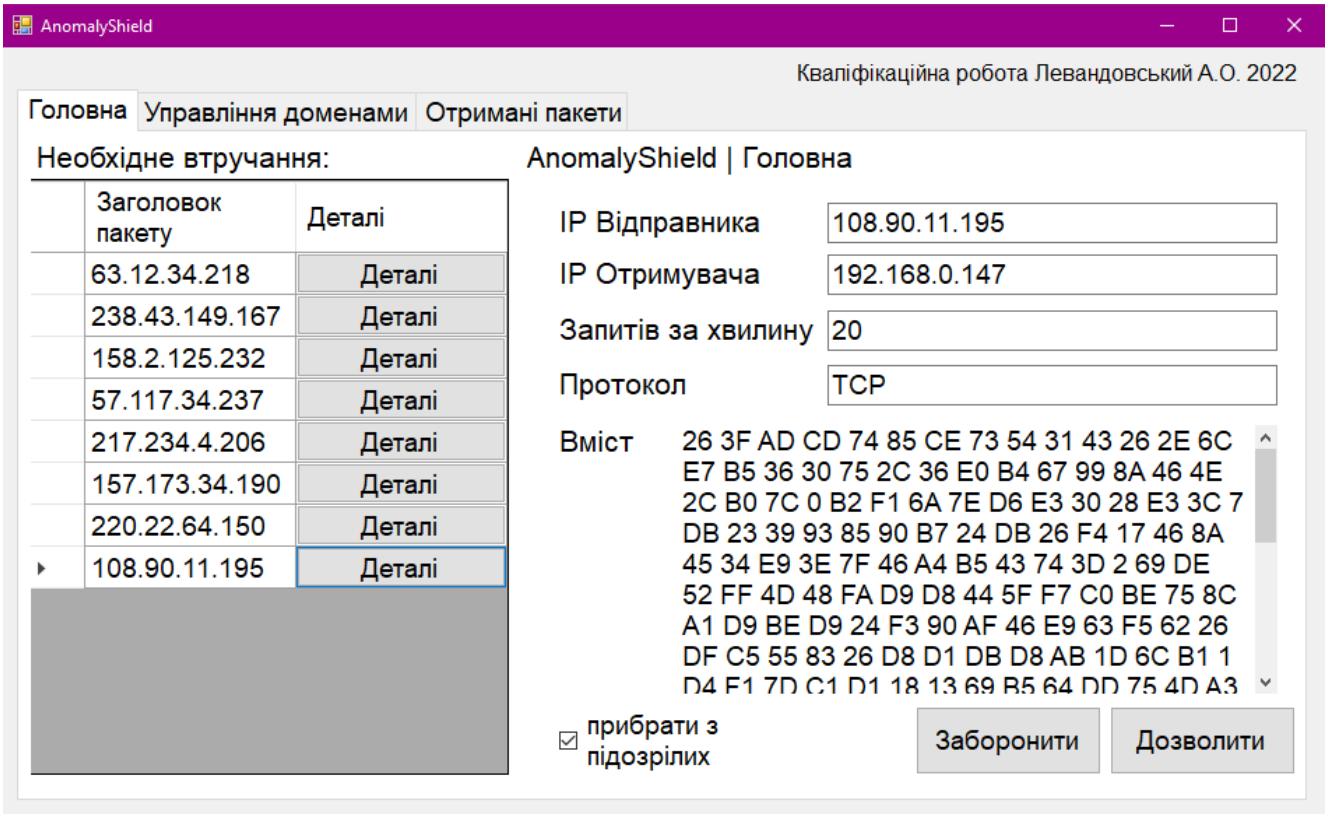


Рисунок 4.7 – Деталі підозрілого пакета даних.

Вище зображена та інформація, яку бачить адміністратор перед виконанням вердикту. А саме:

- Ip джерела
- Ip отримувача
- Кількість запитів на 1 хвилину часу
- Мережевий протокол
- Вміст пакету даних

Далі на розсуд адміністратора дається вибір дій з пакетом. Це може бути:

- Заборона з зміною категорії, в такому випадку пакет блокується та вноситься в список заборонених джерел.
- Заборона без зміни категорії, пакет блокується, але при наступному звернені знову потрапляє в категорію підозрілі
- Дозвіл з зміною категорії, пакет пропускається далі, та вноситься в список дозволених джерел.
- Дозвіл без зміни категорії, пакет пропускається 1 раз, після чого при наступному звернені він знову потрапляє в категорію підозрілі.

Після прийняття одного з рішень, пакет зникає з вкладки «необхідне втручання».

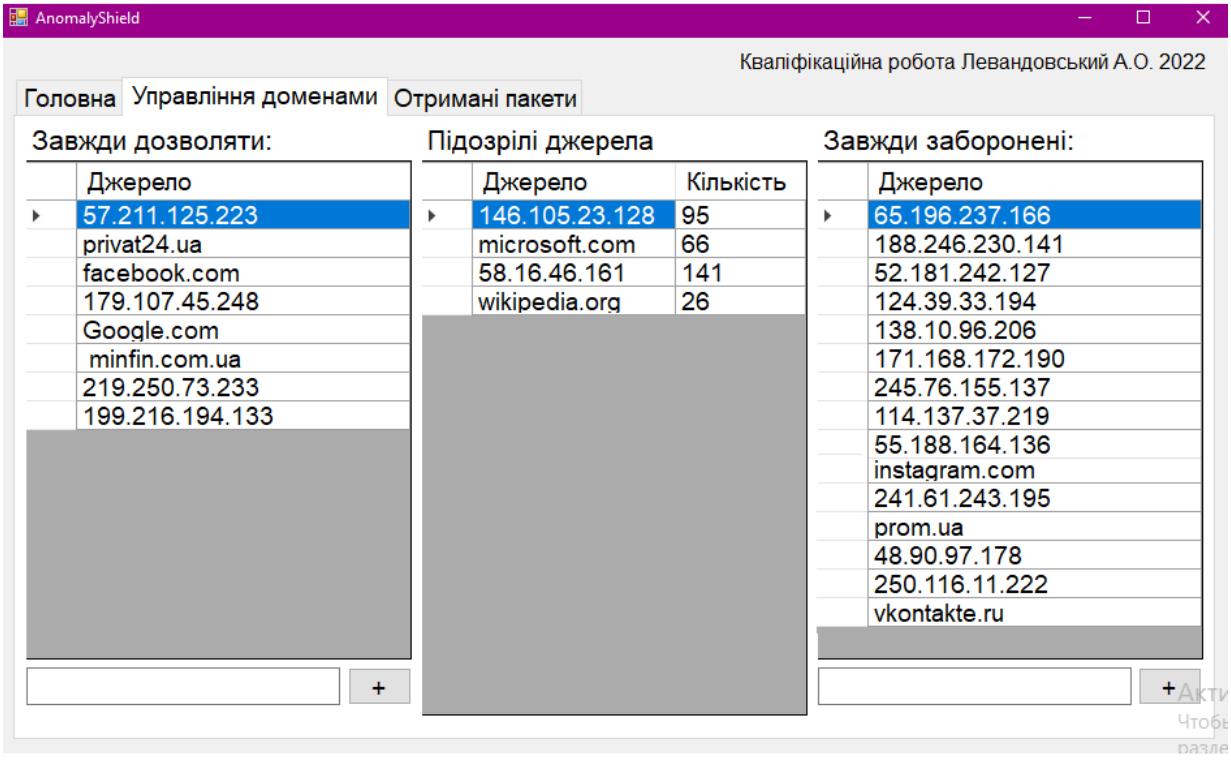
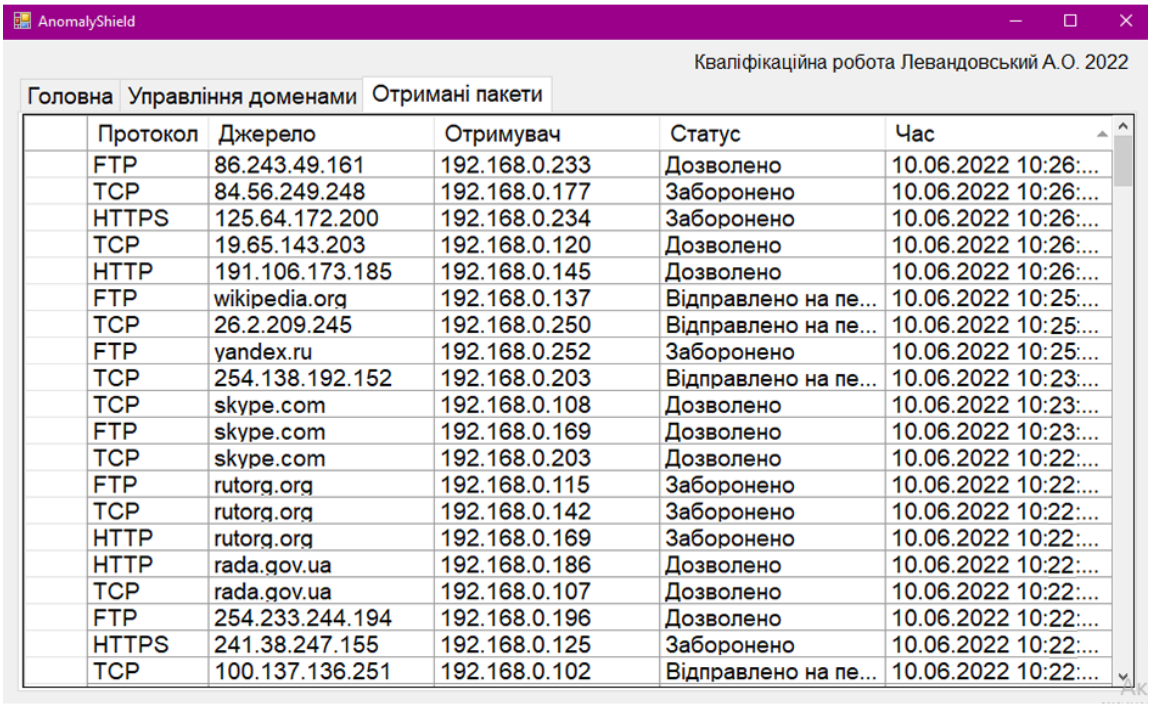


Рисунок 4.8 – Управління пакетами в AnomalyShield.

Є можливість перегляду списку заборонених дозволених та підозрілих джерел або отримувачів. Можливе видалення з підгрупи, або додавання вручну. Зміна списків відбувається в реальному часі, отже, якщо в вкладці «головна» з категорії «потребують втручання» буде обрана дія над пакетом пов’язана з зміною категорії, то зміна одразу відобразиться саме тут, в якомусь з списків. В категорії підозрілі джерела також зображена кількість звернень.

Реалізоване сортування, та в подальшому удосконаленню програмного засобу буде реалізований пошук в середині категорії, та показ більш детальної інформації відносно певних пакетів, а саме коли він був внесений в якийсь з списків, та по якій причині. Буде виконана робота над інтерфейсом, внесені зміни задля покращення зовнішнього вигляду, та кращої ергономічності.



Протокол	Джерело	Отримувач	Статус	Час
FTP	86.243.49.161	192.168.0.233	Дозволено	10.06.2022 10:26:...
TCP	84.56.249.248	192.168.0.177	Заборонено	10.06.2022 10:26:...
HTTPS	125.64.172.200	192.168.0.234	Заборонено	10.06.2022 10:26:...
TCP	19.65.143.203	192.168.0.120	Дозволено	10.06.2022 10:26:...
HTTP	191.106.173.185	192.168.0.145	Дозволено	10.06.2022 10:26:...
FTP	wikipedia.org	192.168.0.137	Відправлено на пе...	10.06.2022 10:25:...
TCP	26.2.209.245	192.168.0.250	Відправлено на пе...	10.06.2022 10:25:...
FTP	yandex.ru	192.168.0.252	Заборонено	10.06.2022 10:25:...
TCP	254.138.192.152	192.168.0.203	Відправлено на пе...	10.06.2022 10:23:...
TCP	skype.com	192.168.0.108	Дозволено	10.06.2022 10:23:...
FTP	skype.com	192.168.0.169	Дозволено	10.06.2022 10:23:...
TCP	skype.com	192.168.0.203	Дозволено	10.06.2022 10:22:...
FTP	rutorg.org	192.168.0.115	Заборонено	10.06.2022 10:22:...
TCP	rutorg.org	192.168.0.142	Заборонено	10.06.2022 10:22:...
HTTP	rutorg.org	192.168.0.169	Заборонено	10.06.2022 10:22:...
HTTP	rada.gov.ua	192.168.0.186	Дозволено	10.06.2022 10:22:...
TCP	rada.gov.ua	192.168.0.107	Дозволено	10.06.2022 10:22:...
FTP	254.233.244.194	192.168.0.196	Дозволено	10.06.2022 10:22:...
HTTPS	241.38.247.155	192.168.0.125	Заборонено	10.06.2022 10:22:...
TCP	100.137.136.251	192.168.0.102	Відправлено на пе...	10.06.2022 10:22:...

Рисунок 4.9 – Отримані пакети.

Вище зображено список пакетів, який оновлюється в реальному часі. На даному зображені з’являються всі вхідні пакети, з всіх категорій. Реалізоване сортування. Зображена деяка інформація про пакети, а саме:

- Мережевий протокол;
- Джерело;
- Отримувач в мережі;
- Статус пакета, дозволений заборонений чи підозрілий;
- Час отримання пакету;

4.4 Оцінка програмного продукту.

Програмний засіб AnomalyShield простий у використанні. Розроблений для контролю над мережею, дозволяє пропускати потрібні пакети, керувати ними у зручному інтерфейсі, без введення команд, та затрат часу, в режимі реального часу відображає потік даних з всією інформацією про них, включаючи одержувача та джерело.

Реалізований програмний засіб направлений на майбутнє вдосконалення, дозволяючи вводити новий функціонал в короткий термін.

Своєю простотою не навантажує сервера, аналізуючи вхідний та вихідний трафіки.

Розроблений програмний засіб успішно пройшов тестування в мережі підприємства та був оцінений як задовільний. Вхідний та вихідний трафік висліджувалися відмінно , пакети даних розподілялись по категоріях вірно, та в кожному випадку відбувались потрібні над ними дії.

Всі операції щодо перевірки пакетів на дозволеність джерел та отримувачів, кількість запитів, пройшли без помилок. Швидкодія програмного засобу також є задовільною.

4.5 Висновки

Завдання на кваліфікаційну роботу виконане успішно, реалізовані скрипти на базі маршрутизатора Mikrotik.

Скрипти реалізують перевірку пакетів за критеріями, блокують або дозволяють подальший рух пакетів по мережі. Вносять пакети в базу даних, дозволяють адміністратору взаємодіяти з ними. Зручно розподіляють пакети по категоріях.

Розроблено програмний засіб AnomalyShield. Програмний продукт дозволяє зручно керувати вхідними й вихідними пакетами. Програмний продукт потребує деякого графічного довершення для більш красивого подання інформації, але саме зручність користування знаходиться на високому рівні. Хід пакетів відбувається в реальному часі. Є можливість перегляду списку заборонених дозволених та підозрілих джерел або отримувачів. Можливий вивід детальнішої інформації про пакет при внесені вердикту адміністратора.

ВИСНОВКИ

У ході створення програмного забезпечення на тему кваліфікаційної роботи було проаналізовано та досліджено предметну область, і було розглянуто типи аномалій мережевого трафіку та види систем виявлення вторгнень виділено сутності предметної області, визначено актуальність розробки даного проекту, обґрунтовано корисність створення на підприємстві та проведено порівняльні роботи з іншими продуктами ідентичного напряму.

Завдання кваліфікаційної роботи було створення програмного засобу для аналізу мережевого трафіку на базі маршрутизатора Mikrotik, створити програмний засіб як візуальну оболонку виконуваних скриптів в операційній системі RouterOs.

Метою кваліфікаційної роботи була реалізація Системи виявлення аномального трафіку на маршрутизаторі Mikrotik.

Мета та завдання кваліфікаційної роботи були досягнуті в повному обсязі.

Під час тестування програмного продукту критичних помилок виявлено не було.

Проведені дослідження показали, що створена система має право на існування та здатна виявляти левову частку аномалій, але використовувати для кращого результату її слід у комбінації з іншими подібними системами.

Визначені сильніші та слабші сторони кожного з них. Даний програмний продукт має такі переваги:

- Зручний, зрозумілий дизайн;
- Сортування пакетів за часом, отримувачем;
- Система попередження адміністратора;
- Низькі системні вимоги:
- Якісне обладнання;

Також в ході роботи була побудована локальна та фізична моделі мереж.

Вивчено організаційну структуру підприємства й структуру інформаційних ресурсів компанії.

Програмний засіб AnomalyShield повністю готовий до використання, легкий для освоєння, та легкий для подальшого оновлення свого функціоналу, та зовнішнього вигляду.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. What is a network. *Techopedia.* URL: https://www.techopedia.com/definition/5537/network (дата звернення 14.03.2022)
2. What is Network Traffic. *Fortinet.* URL*:* https://www.fortinet.com/resources/cyberglossary/network-traffic (дата звернення 14.03.2022)
3. Network Traffic. *Techopedia.* URL: https://www.techopedia.com/definition/29917/network-traffic (дата звернення 14.03.2022)
4. QU'EST-CE QU'UNE ATTAQUE DDOS. *Aws.* URL: https://aws.amazon.com/fr/shield/ddos-attack-protection/ (дата звернення 17.04.2022)
5. Qu'est-ce qu'une attaque DDoS. *Zdnet.* URL: https://www.zdnet.fr/pratique/qu-est-ce-qu-une-attaque-ddos-tout-savoir-pour-les-reconna-tre-et-s-en-proteger-39911475.htm#comments (дата звернення 18.04.2022)
6. Science of Network Anomalies. *Flowmon.* URL: https://www.flowmon.com/en/blog/science-of-network-anomalies#what-is-network-anomaly (дата звернення 20.04.2022)
7. About Zeek. *Zeek.* URL: https://docs.zeek.org/en/current/about.html#what-is-zeek (дата звернення 20.04.2022)
8. Transmission de données. *maths.unsw.* URL: https://web.maths.unsw.edu.au/~lafaye/CCM/transmission/transintro.htm (дата звернення 12.05.2022)
9. Reseaux informatiques. *Apluseduc.* URL: https://apluseduc.com/387-techniques-de-transmission-de-donnees (дата звернення 12.05.2022)

10. Paquet : qu'est-ce que c'est. *Futura*. URL: https://www.futura-sciences.com/tech/definitions/informatique-paquet-18442 (дата звернення 15.05.2022)

11. Пакети данни. *Eyewated*. URL: https://bg.eyewated.com/%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B8-%D0%B4%D0%B0%D0%BD%D0%BD%D0%B8-%D0%B8%D0%B7%D0%B3%D1%80%D0%B0%D0%B6%D0%B4%D0%B0%D1%89%D0%B8%D1%82%D0%B5-%D0%B1%D0%BB%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5-%D0%BD%D0%B0/ (дата звернення 18.05.2022)

12. Techonologie Mikrotik: Le Wifi. *Memoireonline*. URL: https://www.memoireonline.com/08/13/7306/Techonologie-Mikrotik-Le-Wifi.html#_Toc295478443 (дата звернення 26.05.2022)

13. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ : ДП «УкрНДНЦ», 2016. – 26 с.

14. Система внутрішнього забезпечення якості освітньої діяльності : зб. нормат. док. / упоряд.: В. І. Бегняк, Г. В. Красильникова. – Хмельницький : ХНУ, 2015. – 445 с.

15. Текстові документи. Загальні вимоги. СОУ 207.01:2017 / Ю. Бойко, Г. Красильникова, Л. Першина, Т. Косянчук. – Хмельницький : ХНУ, 2017. – 45 с

16. СТУ 3582:2013. Інформація та документація. Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила. – На заміну ДСТУ 3582–97 ; чинний від 2013–08–22. – Київ : Мінекономрозвитку України, 2014. – 15 с

ДОДАТОК А

Лістинг програми

БЛОКУВАННЯ WhatsApp

```
/ip firewall layer7-protocol add name=WhatsApp
regexp="^.+(whatsapp.com).*\$" /ip firewall filter add
action=drop chain=forward layer7-protocol=WhatsApp
```

Захист маршрутизатора від DDOS-атак

```
/ip firewall filter
add chain=forward connection-state=new action=jump jump-
target=block-ddos
add chain=forward connection-state=new src-address-
list=ddoser dst-address-list=ddosed action=drop
add chain=block-ddos dst-limit=50,50,src-and-dst-
addresses/10s action=return
add chain=block-ddos action=add-dst-to-address-list address-
list=ddosed address-list-timeout=10m
add chain=block-ddos action=add-src-to-address-list address-
list=ddoser address-list-timeout=10m
```

Аналізатор

```
:local logBuffer "logParse"
```

Встановити ім'я сценарію синтаксичного аналізатора для запуску кожного запису журналу в буфері та внутрішня обробка

```
:local logParserScript "Log-Parser-Script"
:global logParseVar "" :local loglastparsetime :local
loglastparsemessage :local findindex :local property :local
value :local logEntryTopics :local logEntryTime :local
logEntryMessage :local curDate :local curMonth :local curDay
:local curYear :local clearedbuf :local lines
```

Отримання поточних налаштувань дати

```
:set curDate [/system clock get date] :set curMonth [:pick
[:tostr $curDate] 0 3] :set curDay [:pick [:tostr $curDate] 4
6] :set curYear [:pick [:tostr $curDate] 7 11] :set clearedbuf
0 :foreach rule in=[/log print as-value where
buffer=($logBuffer)] do={
```

Тепер усі дані збираються в пам'яті. Очистіть буфер журналу відразу, щоб надходили нові записи.

```
:if ($clearedbuf = 0) do={ /system logging action { :set lines
[get ($logBuffer) memory-lines] set ($logBuffer) memory-lines 1
set ($logBuffer) memory-lines $lines } :set clearedbuf 1 } #
```

Завершення очищення буфера журналу

```
:set logEntryTime "" :set logEntryTopics "" :set
logEntryMessage ""
```

Отримайте властивості кожного запису журналу

```
 :foreach item in=[:toarray $rule] do={ :set findindex [:find
[:tostr $item] "="] :set property [:tostr [:pick [:tostr $item]
0 $findindex]] :set value [:tostr [:pick [:tostr $item]
($findindex + 1) [:len [:tostr $item]]]] :if ([:tostr
$property] = "time") do={ :set logEntryTime $value } :if
([:tostr $property] = "topics") do={ :set logEntryTopics $value
} :if ([:tostr $property] = "message") do={ :set
logEntryMessage $value }
```

закінчення для кожного елемента

Установіть формат logEntryTime на повний формат (ммм/дд/рррр ГГ:ММ:СС)

```
:set findindex [:find [:tostr $logEntryTime] " "]
```

Якщо пробілів не знайдено, вказано лише час (ГГ:ММ:СС), вставте ммм/дд/рррр

```
:if ([:len $findindex] = 0) do={ :set logEntryTime ($curMonth .
"/" . $curDay . "/" . $curYear . " " . \ [:tostr
$logEntryTime]) }
```

Вказано лише (mmm/dd HH:MM:SS), вставте рік:

```
if ($findindex = 6) do={ :set logEntryTime ([:pick [:tostr
$logEntryTime] 0 $findindex] . "/" . $curYear . \ [:pick
```

```
[:tostr $logEntryTime] $findindex [:len [:tostr
$logEntryTime]]]) }
```

Дано лише (mmm HH:MM:SS), вставте день і рік

```
:if ($findindex = 3) do={ :set logEntryTime ([:pick [:tostr
$logEntryTime] 0 $findindex] . "/" . $curDay . "/" . $curYear .
\ [:pick [:tostr $logEntryTime] $findindex [:len [:tostr
$logEntryTime]]]) }
```

Кінець установити logEntryTime на повний формат

Пропустити, якщо logEntryTime і logEntryMessage збігаються з попереднім розібраним записом журналу

```
:if ($logEntryTime = $loglastparsetime && $logEntryMessage =
$loglastparsemessage) do={ } else={
```

Встановіть logParseVar, а потім запустіть скрипт аналізатора

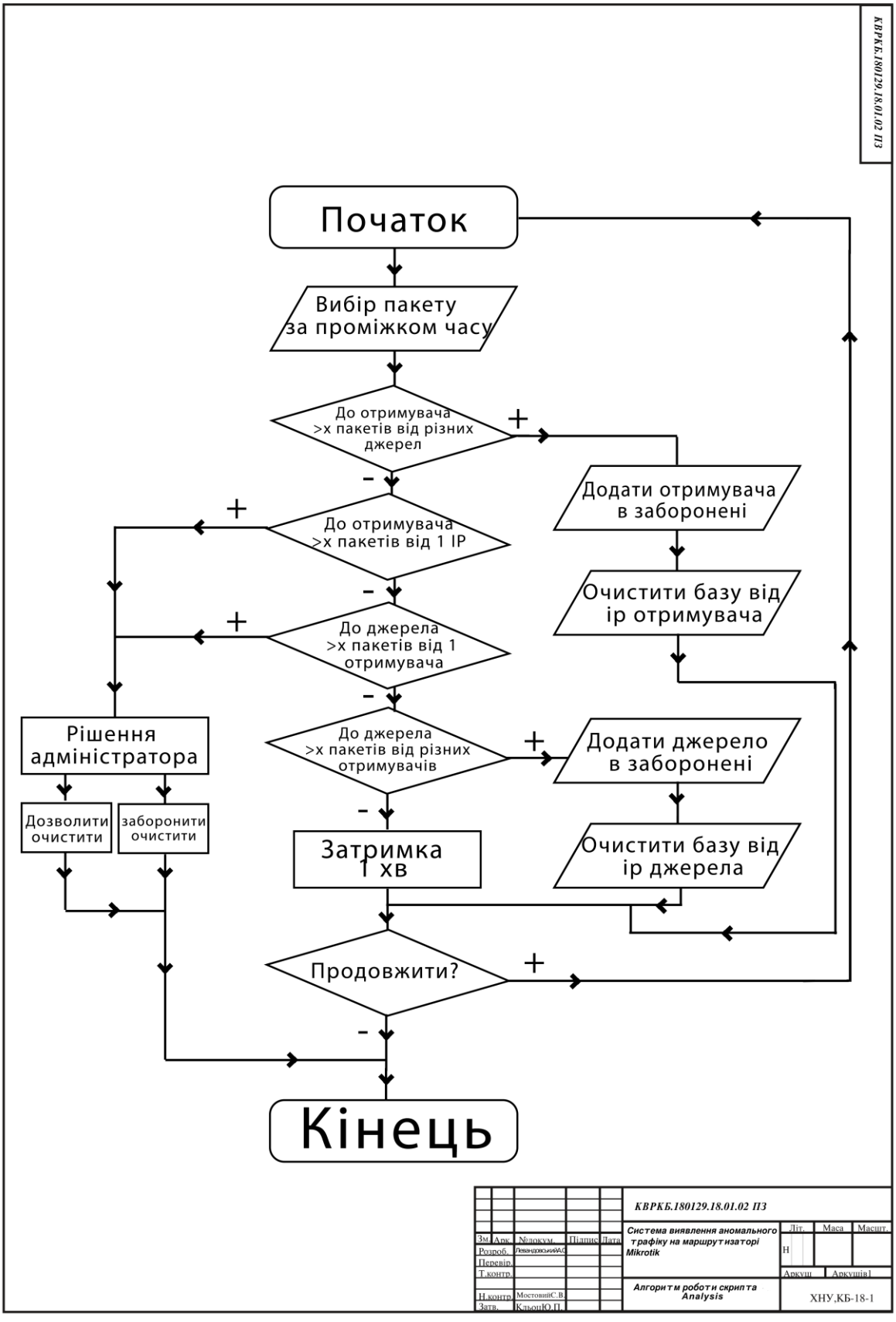
```
:set logParseVar ($logEntryTime . "," . $logEntryTopics . "," .
$logEntryMessage) /system script run ($logParserScript)
```

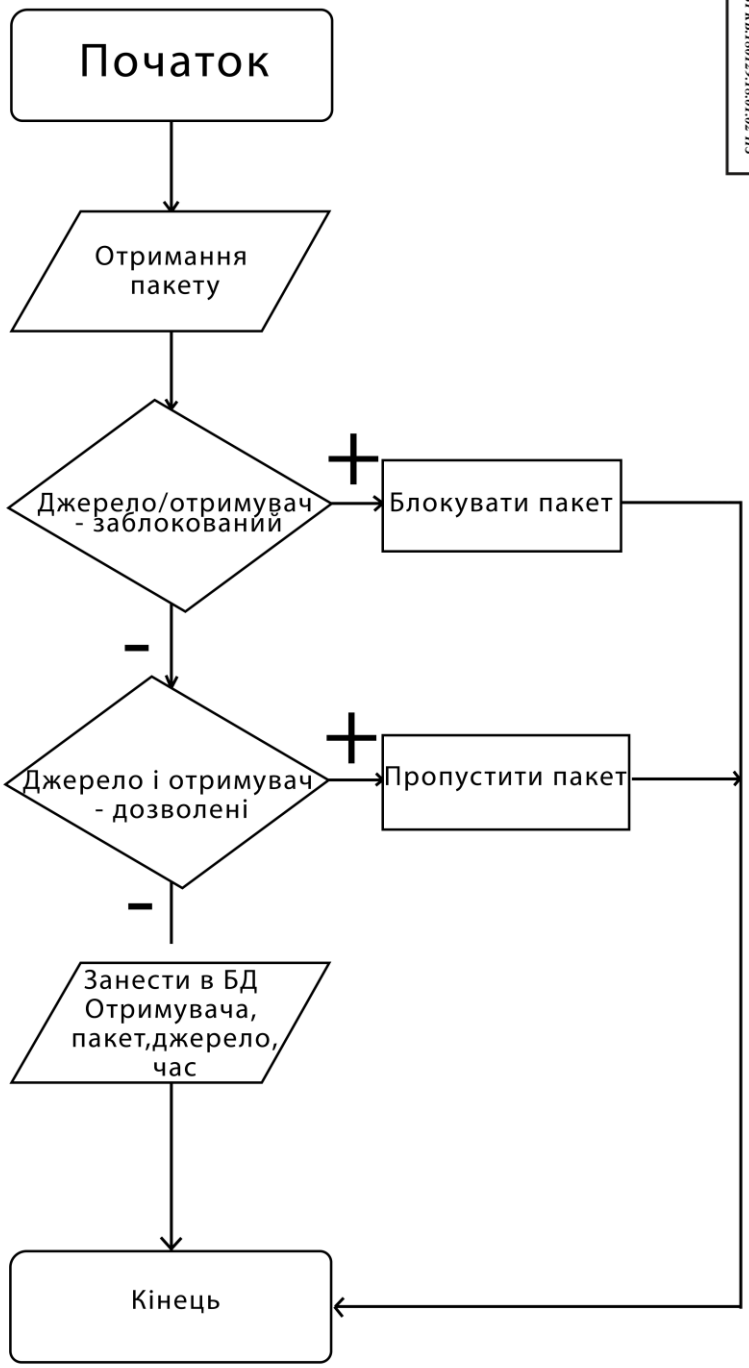
Оновити час останнього аналізу та останнє проаналізоване повідомлення

```
:set loglastparsetime $logEntryTime :set loglastparsemessage
$logEntryMessage }
```

кінець правила }

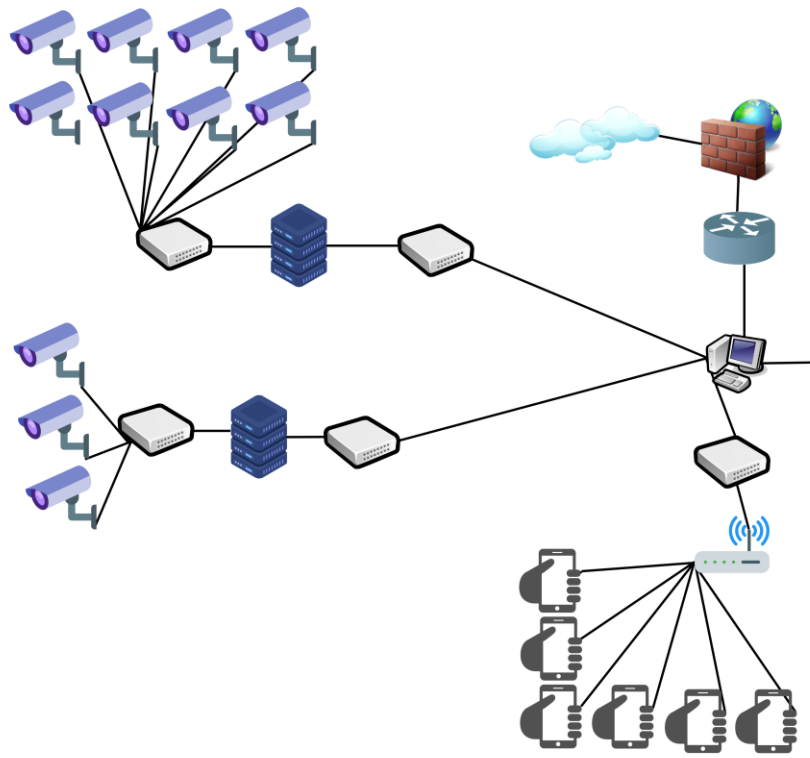
ДОДАТОК Б


КВРКБ.180129.18.01.02 ПЗ
Початок
Вибір пакету за проміжком часу
До отримувача >x пакетів від різних джерел
+
Додати отримувача в заборонені
-
До отримувача >x пакетів від 1 IP
+
Очистити базу від ір отримувача
-
До джерела >x пакетів від 1 отримувача
+
-
Рішення адміністратора
До джерела >x пакетів від різних отримувачів
+
Додати джерело в заборонені
Дозволити очистити
заборонити очистити
-
Затримка 1 хв
Очистити базу від ір джерела
Продовжити?
+
-
Кінець
КВРКБ.180129.18.01.02 ПЗ
Система виявлення аномального трафіку на маршрутизаторі Mikrotik
Літ.
Маса
Масшт.
Н
Аркуш
Аркушів 1
Алгоритм роботи скрипта Analysis
ХНУ,КБ-18-1
Зм. Арк. №докум. Підпис Дата
Розроб. ЛеванідовськийИ.О.
Перевір.
Т.контр.
Н.контр. МостовийС.В.
Затв. КльоцЮ.П.

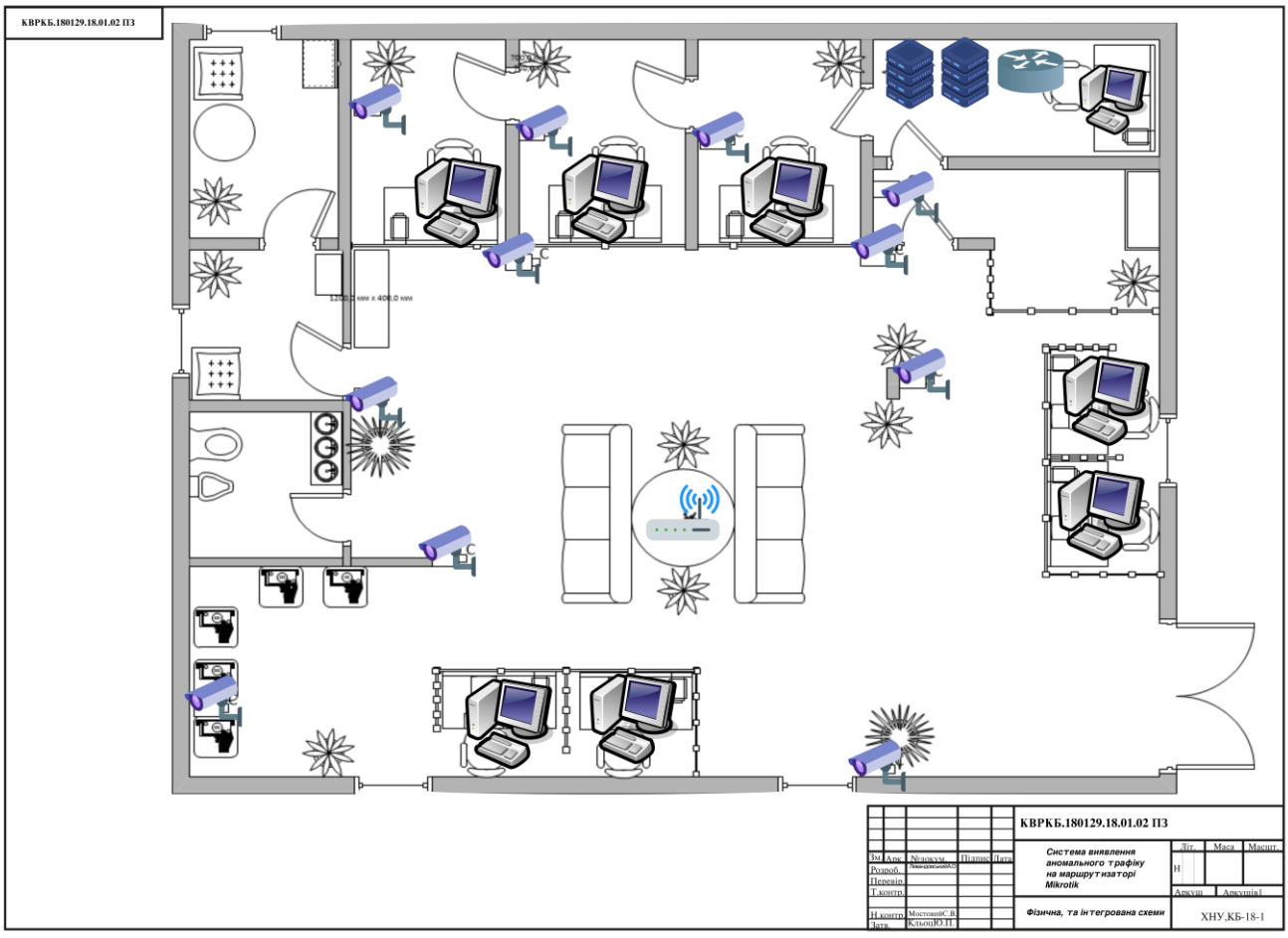


					КВРКБ.180129.18.01.02 ПЗ	
Зм.	Арк.	№докум.	Підпис	Дата	Система виявлення аномального трафіку на маршрутизаторі Mikrotik	Літ. / Маса / Масшт.
Розроб.		Левандовський А.С.				Н
Перевір.						Аркуш / Аркушів 1
Т.контр.					Алгоритм роботи скрипта Base	ХНУ,КБ-18-1
Н.контр.		Мостовий С.В.				
Затв.		Кльоц Ю.П.				

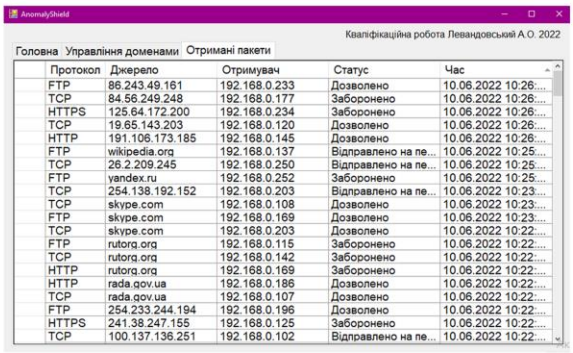
КВРКБ.180129.18.01.02 ПЗ

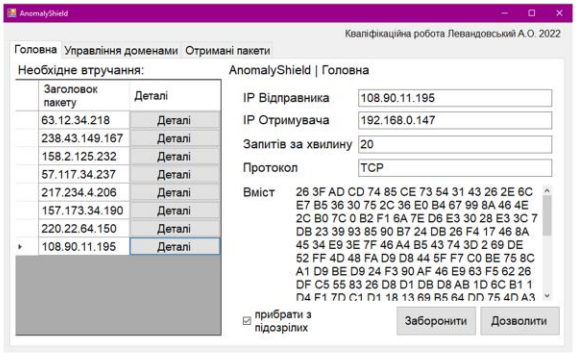


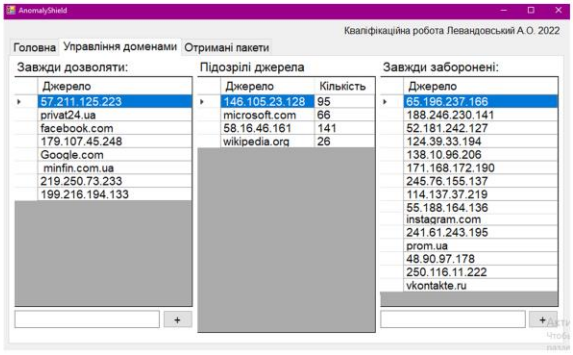
					КВРКБ.180129.18.01.02 ПЗ			
Змн.	Арк.	№докум.	Підпис	Дата	Система виявлення аномального трафіку на маршрутизаторі Mikrotik	Літ.	Маса	Масшт.
Розроб.		Лівандовський О.О.				Н		
Перевір.								
Т.контр.						Аркуш	Аркушів 1	
Н.контр.		Мостовий С.В.			Логічна система мережі	ХНУ,КБ-18-1		
Затв.		Кльоц Ю.Г.						

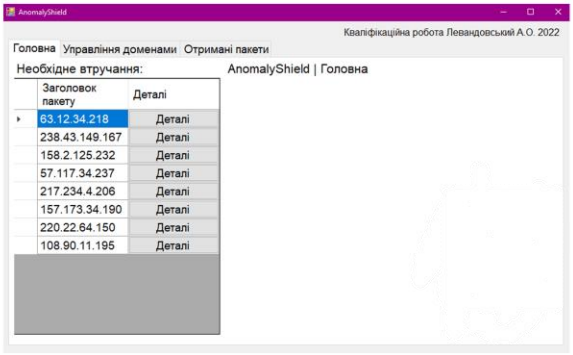

КВРКБ.180129.18.01.02 ПЗ
КВРКБ.180129.18.01.02 ПЗ
Система виявлення аномального трафіку на маршрутизаторі Mikrotik
Фізична, та інтегрована схеми
ХНУ,КБ-18-1

КВРКБ.180129.18.01.02 ПЗ









					КВРКБ.180129.18.01.02 ПЗ		
Зм.	Арк.	№докум.	Підпис	Дата	Система виявлення аномального трафіку на маршрутизаторі Mikrotik	Літ.	Маса	Масшт.
Розроб.		Левандовський О.О.				Н		
Перевір.						Аркуш	Аркушів 1	
Т.контр.					Зображення роботи AnomalyShield	ХНУ,КБ-18-1		
Н.контр.		МостовийС.В.						
Затв.		КльоцкоЮ.П.						

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Система виявлення аномального трафіку на маршрутизаторі Mikrotik

Автор: Левандовський Андрій Олександрович
Спеціальність: 125 – Кібербезпека
Освітня програма: освітньо-професійна
Науковий керівник: Орленко Вікторія Сергіївна, к.т.н, доцент
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 90,88%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про дотримання академічної доброчесності в Хмельницькому національному університеті (http://www.khnu.km.ua/root/files/01/10/03/0005.pdf) така авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту.

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1. Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 9,12%, з яких 4.1% є збігами з одним джерелом, зумовленими наявністю типових полів з стандартизованим текстом в рамках пояснювальної записки.
2. В тексті пояснювальної записки на 62 сторінки тексту виявлено лише 2 збіги у фрагментах речень довжиною до 10 слів, які утворюють загальновживані фрази.
3. Інші три збіги є збігами в назвах використаних друкованих видань, розміщених в переліку джерел посилань

Керівник роботи — Вікторія Орленко
Гарант ОП — Віктор Чещун
Завідувач кафедри КБ — Юрій Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Левандовський Андрій Олександрович

Тема *Система виявлення аномального трафіку на маршрутизаторі Mikrotik*

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 5; кількість сторінок записки 67.

1. Короткий зміст роботи та прийнятих рішень
в кваліфікаційній роботі досліджуються аномалії мережевого трафіку За результатами роботи створюється програмне забезпечення, відповідно до теоретичної основи, з можливістю використання на підприємстві .

2. Висновок про відповідність кваліфікаційної роботи завданню *Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині*

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: *У першому розділі було досліджено та проаналізовано суміжну предметну область, визначено основний напрям кваліфікаційної роботи, у другому розділі було обґрунтувано та визначено завдання на кваліфікаційну роботу, у третьому розділі було розроблено фізичну та логічні схеми мережі, ознайомлення з наявними методами виявлення аномалій мережі, у четвертому розділі було побудовано алгоритми, та реалізовано програмний продукт,*

4. Позитивні сторони роботи
В роботі запропоновано легкий до додавання нових функцій програмний продукт, оптимізований на швидку роботу, програмний засіб дає можливість швидко реагувати на загрози, та аномальний трафік в мережі, за допомогою реалізації контролю пакетів даних в режимі реального часу.

5. Негативні сторони роботи роботи
До запропонованого програмного продукту відсутній акт впровадження на підприємство, можливий більший функціонал

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В цілому кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження .

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «Добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Корецька Людмила Олександрівна – доцент кафедри АКІТ, ХНЕУ

«14» 06 2022. (підпис)

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Левандовського Андрія Олександровича
ПІБ здобувача вищої освіти

студента ФІТ, 4 курсу, групи КБ-18-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

14.06.2022
дата

підпис

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1011573160

Дата перевірки:
14.06.2022 11:18:38 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
14.06.2022 11:42:33 EEST

ID користувача:
100008300

Назва документа: **Антиплагіат Левандовський**

Кількість сторінок: **64** Кількість слів: **10104** Кількість символів: **76800** Розмір файлу: **8.00 MB** ID файлу: **1011443724**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

9.12%
Схожість

Найбільша схожість: **4.1%** з джерелом з Бібліотеки (ID файлу: **1011309101**)

3.45% Джерела з Інтернету	108	Сторінка 66
6.65% Джерела з Бібліотеки	135	Сторінка 67

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	2
Підозріле форматування	10 сторінок

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 12%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 105160 Название: Система виявлення аномального трафіку на маршрутизаторі Mikrotik Добавлено в БД: 2022-06-14 Авторы: Левандовський Андрій Олександрович Руководители: Муляр І.В, Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	65888	552	819 (1%)	13 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы