ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки

Кваліфікаційна робота

Комп'ютерна система розпізнавання аномального трафіку з використанням машинного навчання

Виконала:
ст. гр. КІУКІ-21-2
Масленнікова К.Д.

Керівник:
ас. Романюк О.С.

Мета та завдання кваліфікаційної роботи

Метою кваліфікаційної роботи є розробка програмних засобів моніторингу передачі даних у корпоративній мережі.

Завдання:

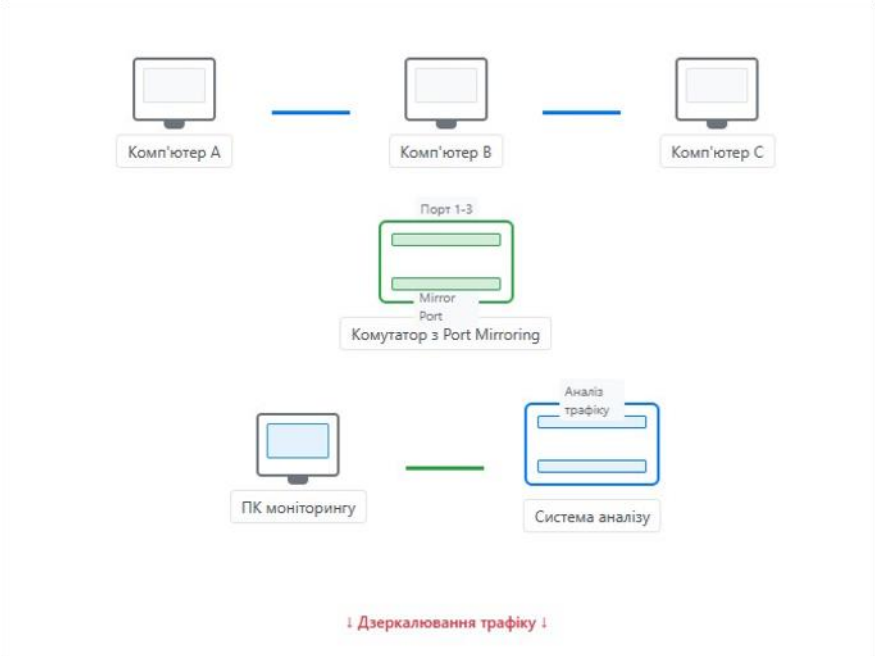
- провести аналіз існуючих методів моніторингу трафіку та виявлення аномалій у корпоративних мережах;
- проаналізувати сучасні алгоритми та підходи до класифікації та детектування мережевих аномалій, зокрема із використанням методів машинного навчання;
- обґрунтувати вибір моделі виявлення аномального трафіку, враховуючи специфіку корпоративного середовища;
- розробити архітектуру комп’ютерної системи моніторингу з урахуванням модулів збору, обробки, зберігання та візуалізації трафіку;
- спроєктувати та реалізувати модуль виявлення аномалій у трафіку з використанням машинного навчання.

3

Види моніторингу мережі

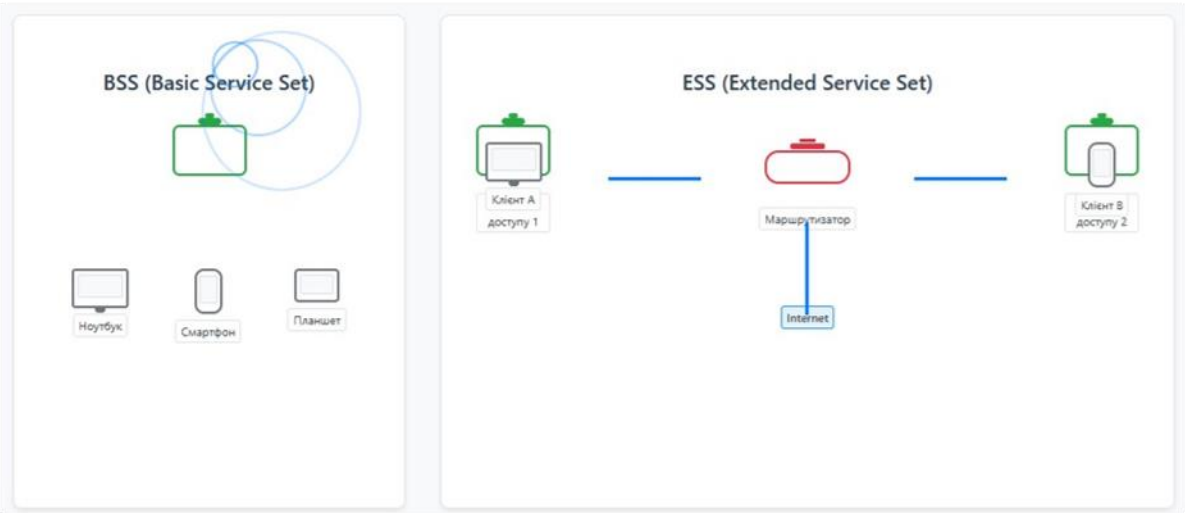
4

Моніторинг за допомогою комутаторів



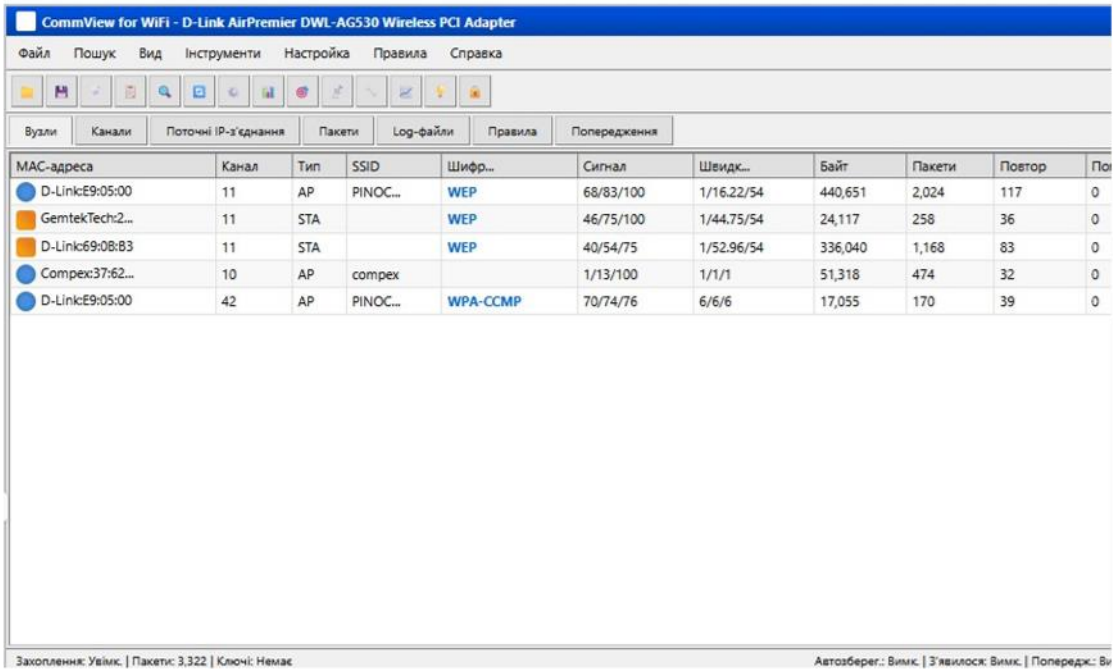
Мережі Wi-Fi

5

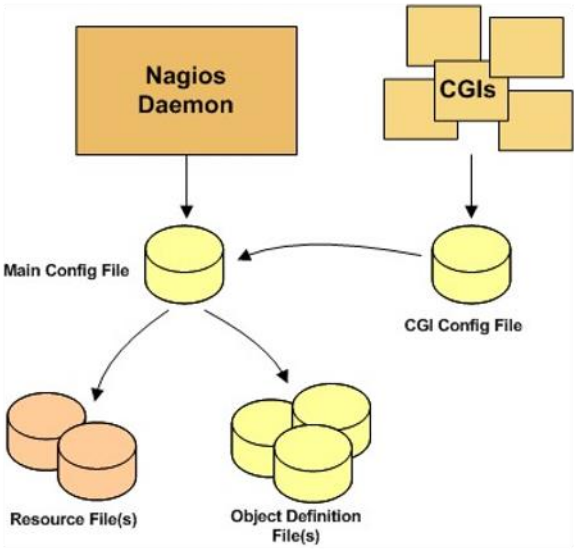


Типова картина вузлів бездротової мережі за допомогою мережевого аналізатора

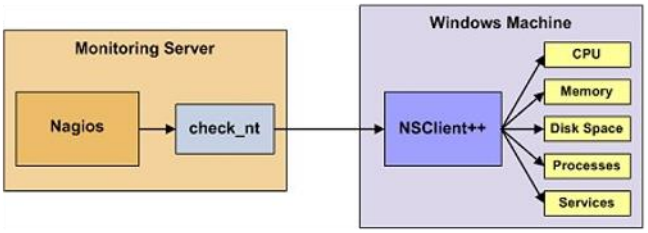
6

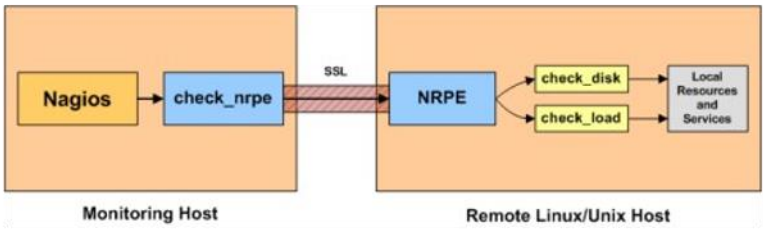


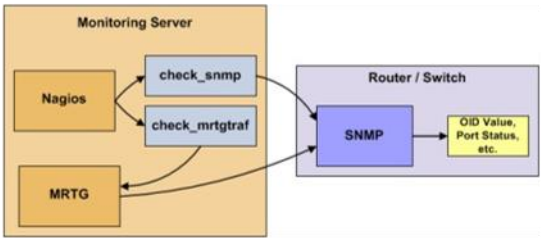
Вибір ядра системи моніторингу мережі 7



Схеми моніторингу хостів та завдяки SNMP 8

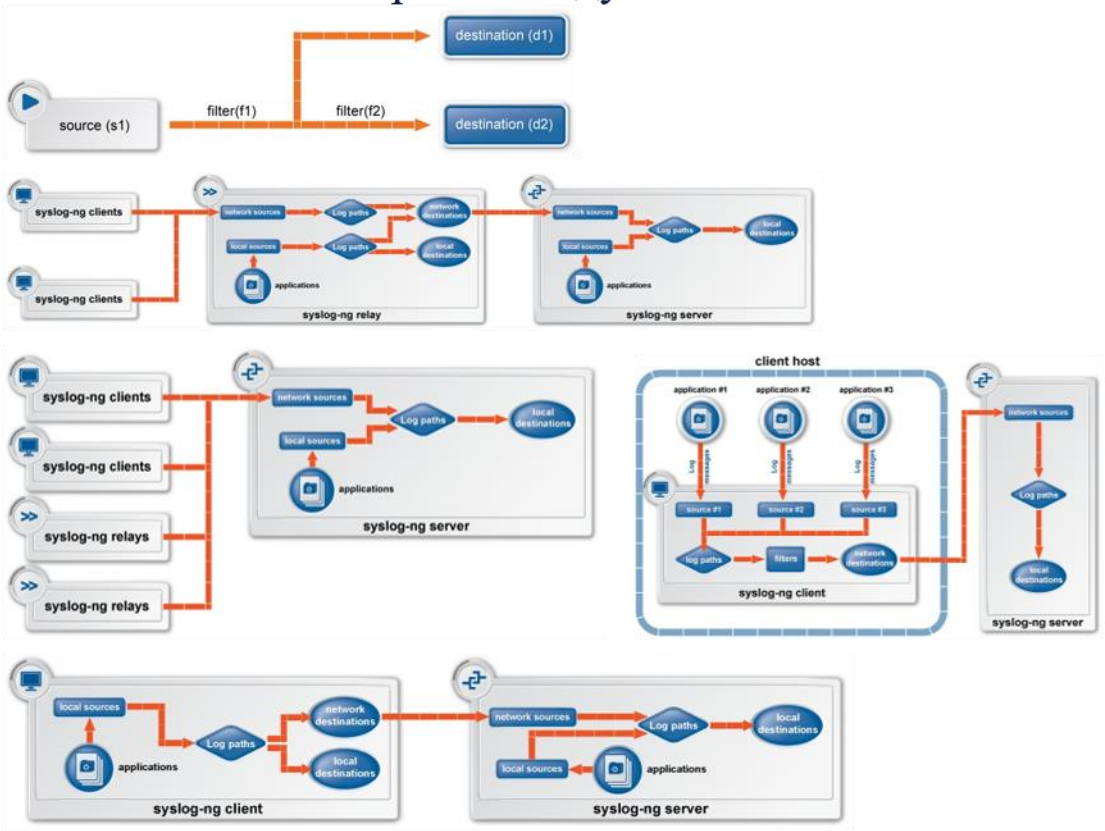






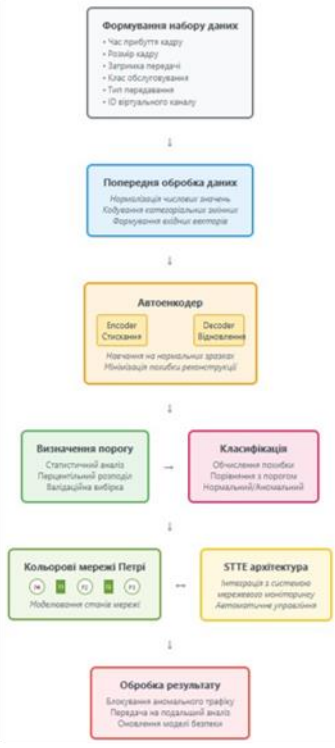
Розробка модулів системи

9



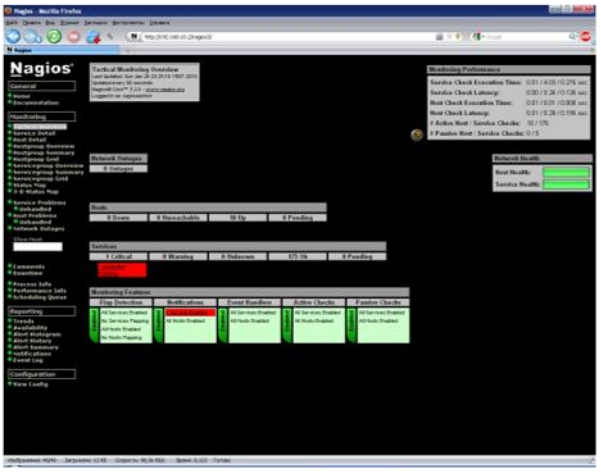
Модуль виявлення аномального трафіку з використанням машинного навчання

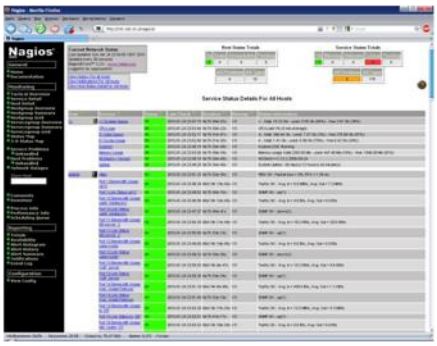
10



Web-інтерфейс комп’ютерної системи

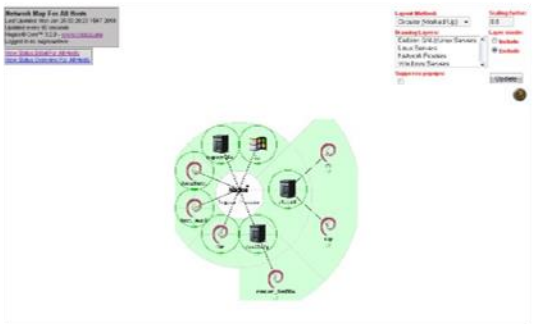
11

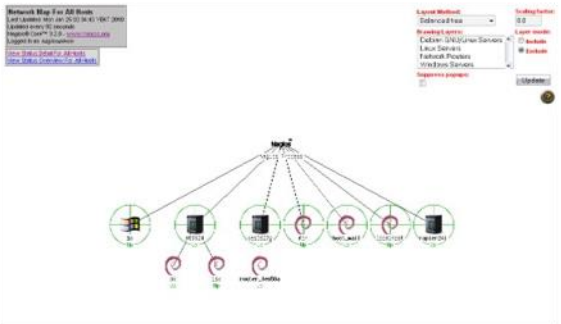


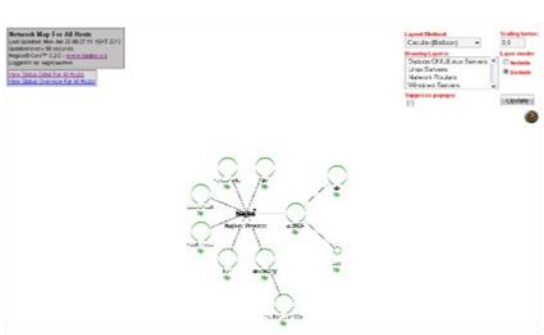


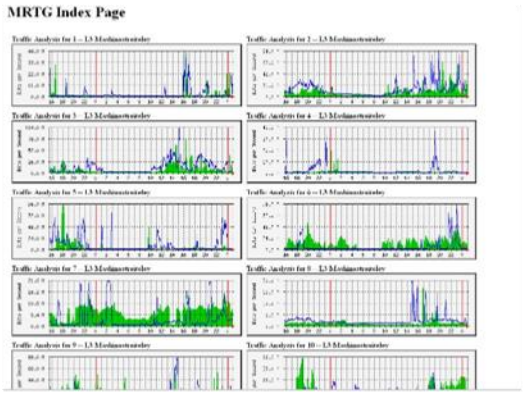
Інтерфейс комп’ютерної системи

12









Висновки

Розроблена комп'ютерна система розпізнавання аномального трафіку з використанням машинного навчання. Побудована модель дозволяє імітувати як регулярний, так і стохастичний трафік, що є важливим для дослідження реакції системи на змішані типи навантаження, а також виявляти аномальний трафік. Застосування генераторів трафіку з підтримкою QoS і використанням маркерів, які відповідають полям кадрів Ethernet, забезпечило можливість гнучкої перевірки системи на наявність ознак ненормованого або потенційно шкідливого трафіку. Це критично важливо при побудові засобів пасивного моніторингу та контролю в реальному часі. Структурне розділення функціональних блоків моделі: таких як класифікатор кадрів, планувальник передач, черги з пріоритетами та таймери перевірки доставки надало змогу не лише забезпечити ізоляцію ТТ-кадрів від ЕТ-трафіку, але й дозволило відслідковувати порушення режимів обслуговування, що часто є індикатором аномалій. Особливо це стосується кадрів, які порушують умови розкладу, дублюються або надходять у непризначений таймслот, що прямо вказує на несправність вузла або зловмисну активність.

Інтеграція автоенкодера в систему виявлення аномалій мережевого трафіку з використанням кольорових мереж Петрі представляє перспективний підхід до вирішення проблем сучасної мережевої безпеки. Поєднання адаптивних можливостей машинного навчання з математичною строгістю формальних методів моделювання створює основу для побудови ефективних систем автоматичного моніторингу та захисту мережевих інфраструктур.