Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**ОТЧЕТ О ВЫПОЛНЕНИИ ЛАБОРАТОРНОЙ РАБОТЫ №3**

**по дисциплине**  
 **«Технологии проектирования программного обеспечения»**

Работу выполнил студент группы 35/2 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Т. Э. Айрапетов

Направление подготовки: 02.03.03 Математическое обеспечение и администрирование информационных систем

Отчет принял   
доц. каф. ИТ            А. Н. Полетайкин

Тема: Техническое задание на создание программного продукта.

Цель: Освоение методики предварительного анализа разрабатываемой программы; освоение задач формулирования функциональных и нефункциональных требований к программной реализации отдельных задач и к программе в целом; выработка навыков разработки технического задания.

Задание:

1. Установить назначение и общую цель создания программы.
2. Определить структуру программы и состав функциональных задач.
3. Разработать функциональные требования к программе:

* требования к входным и выходным данным;
* требования к программной реализации задач;
* специальные требования к математическому обеспечению программной реализации задач;

1. Разработать модель требований в нотации UML
2. Разработать требования к информационному обеспечению (к базе данных).
3. Разработать требования к инструментальному программному обеспечению (к системе управления базой данных (СУБД), к средству разработки программ (IDE), средствам автоматизированного проектирования ПО)
4. Установить нефункциональные требования к программе. Дать не менее 5 наиболее очевидных для данной системы требований из перечня:

* требования к надежности;
* требования к эффективности;
* требования к безопасности;
* требования к эргономичности и удобству использования;
* требования к численности и квалификации персонала и режиму работы;
* требования к переносимости;
* требования к сопровождаемости;
* требования к особенностям поставки;
* требования к защите информации от несанкционированного доступа;
* требования по сохранению информации при авариях;
* требования к соответствию стандартам качества.

Индивидуальная тема: ПС обнаружения вторжений в компьютерной сети.

**1. Назначение и цель.** Назначение – анализ трафика сети для выявления угроз информационной безопасности. Цель создания программы – повышение эффективности обнаружения угроз компьютерной сети и улучшение автоматизации работы аналитиков информационной безопасности.

**2. Структура программы и перечень задач.** ПС обнаружения вторжений должна решать такие задачи:

* анализ трафика сети;
* классификация вторжений и выявление угроз;
* сохранение обнаруженных вторжений в базу данных.

**3. Функциональные требования к задачам.**

3.1 Требования к задаче анализа трафика сети. Трафик сети должен быть представлен в виде данных формата PCAP для дальнейшего анализа. Формат PCAP (Packet Capture) представляет собой стандартный способ хранения данных, касающихся сетевого трафика. Этот формат широко используется в инструментах для анализа и мониторинга сетевого взаимодействия. Пример данных формата PCAP можно увидеть на рисунке 1.

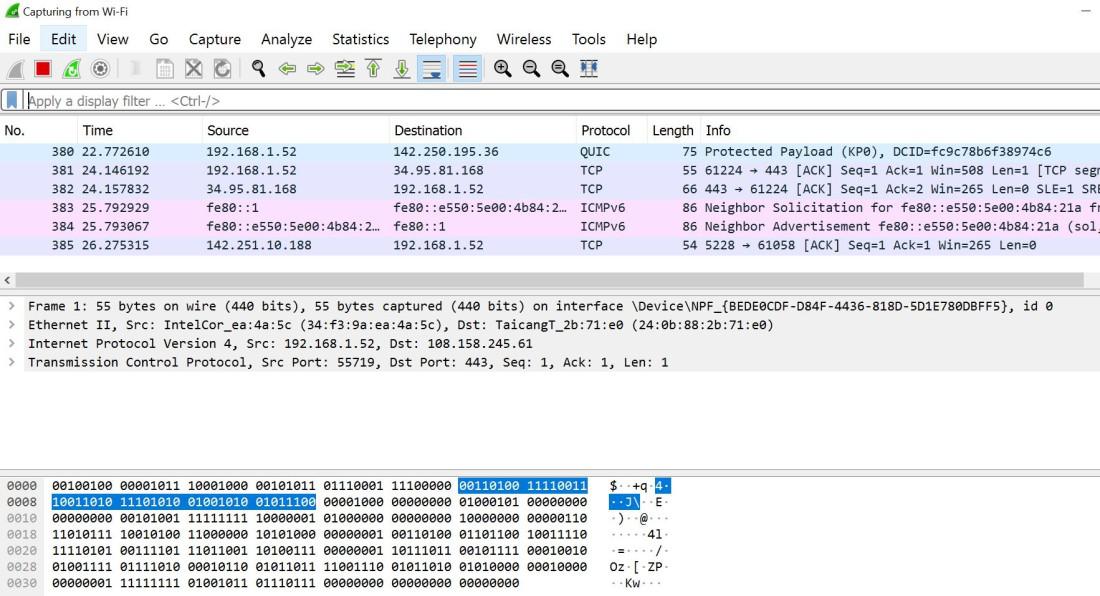


Рисунок 1 – Пример захвата сетевого трафика в утилите Wireshark

Трафик может приходить с довольно большой скоростью (до 1 Гб/сек), в связи с чем, ПС должна быть способна обрабатывать такой объем данных.

Анализ трафика должен быть реализован на основе моделей машинного обучения, настроенных на классификацию вредоносного и обычного трафика. Для обучения модели машинного обучения используются наборы данных. Различные наборы данных предоставляют разное количество признаков – от основных характеристик, таких как временные метки, источники и цели сетевого взаимодействия, до более специфичных параметров, таких как коды ошибок, заголовки протоколов, и объемы передаваемых данных. Вариативность признаков в разных наборах данных играет ключевую роль в формировании обучающих выборок, требуя тщательного анализа и адаптации методов анализа данных в соответствии с особенностями каждого конкретного набора.

3.2 Требования к задаче классификации и выявлению угроз. Классификация угроз должна происходить с высокой точностью, причем важно, чтобы ПС замечала также и неизвестные ранее атаки. При выявлении угрозы аналитик должен получать уведомление.

3.3 Требования к задаче сохранения обнаруженных вторжений в базу данных. При выявлении угрозы ПС должна сохранять данные о ней в формате PCAP-файлов захвата, а в базе данных идентификатор вторжения.

**4. Модель требований в нотации UML.**

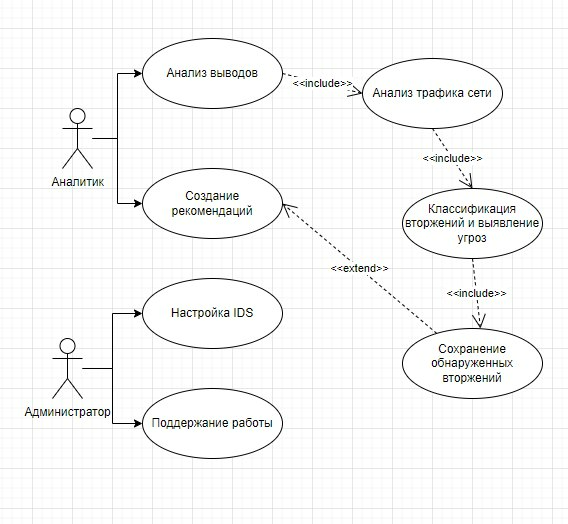


Рисунок 2 – Модель требований в нотации UML

**5. Требования к базе данных ПС.**

* поддержка целостности, достоверности и актуальности данных;
* низкая стоимость хранения и использования;
* защита данных;
* ведение архивов и резервное копирование.

**6. Требования к инструментальному программному обеспечению.**

Система должна быть совместима с операционными системами Windows и Linux. Инструменты должны включать CASE-средства (например, Rational Rose, Enterprise Architect) и средства объектно-ориентированного моделирования (например, UModel). Разработка должна осуществляться с использованием современных интегрированных сред разработки (IDE), таких как PyCharm, Visual Studio или Intellij Idea. При необходимости использования сторонних библиотек или фреймворков должны быть выбраны надежные и проверенные решения с открытым исходным кодом.

**7. Нефункциональные требования.**

* производительность: система должна обеспечивать высокую скорость обнаружения и реагирования на вторжения;
* надежность: обеспечение стабильной работы системы без сбоев;
* масштабируемость: возможность расширения и модификации системы в будущем;
* безопасность: обеспечение защиты от несанкционированного доступа и атак на систему;
* удобство использования: интуитивный интерфейс для операторов и администраторов.