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 №1**

**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: Анализ предметной области.

Цель: изучение и системное представление бизнес-процессов, подлежащих программированию, приобретение навыков системного анализа объектов и процессов реального мира на предмет организации программного управления ими.

Задание:

1. Дать характеристику объекта информатизации: наименование, назначение, структура, задачи, действующие лица.
2. Выполнить системное описание заданного бизнес-процесса и выполнить его декомпозицию на подпроцессы (задачи).
3. Построить модель «Черный ящик» и диаграмму вариантов использования UML. Описать построенные модели. Сформировать реестры инфопотоков.
4. Дать характеристику схеме решения задач в ручном режиме и выделить ее недостатки.
5. Обосновать необходимость усовершенствования и развития существующей схемы решения задач за счет создания специального программного обеспечения.

Индивидуальная тема: ПС обнаружения вторжений в компьютерной сети.

**1. Характеристика объекта информатизации**. Объектом информатизации является отдел мониторинга вторжений и локальная сеть заказчика. Локальная сеть представляет собой набор узлов – рабочих станций и других устройств, с которыми работают сотрудники предприятия. Для обнаружения несанкционированного доступа или различного рода атак, в сети устанавливают IDS (Intrusion Detection System) – систему обнаружения вторжений и пользуются услугами специалистов кибербезопасности. На рисунке 1 представлена упрощенная схема сети, в которой установлена система обнаружения вторжений.

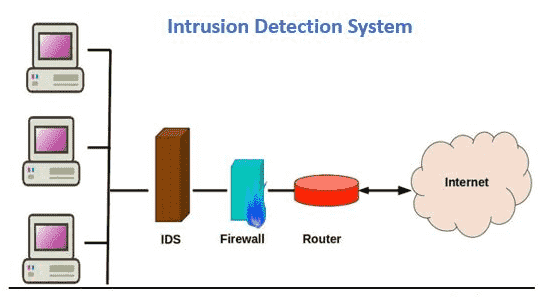


Рисунок 1 – Схема сети с установленной IDS

Обычно IDS отслеживают входящий сетевой трафик, обнаруживая определенные шаблоны и последовательности, которые соответствуют известным сигнатурам атак. Несмотря на свою эффективность, они не способны обнаруживать неидентифицированные атаки без известных шаблонов.

**2. Процесс информатизации.** Предлагается реализация обнаружения вторжений на основе машинного обучения. Это относительно новая технология, предназначенная для обнаружения неизвестных атак и не ограничивающаяся определением сигнатур атак. Этот тип обнаружения использует машинное обучение для анализа больших объемов сетевых данных и трафика.

Среди действующих лиц процесса можно выделить злоумышленника, жертву, администратора и аналитика информационной безопасности. Во время инцидента кибербезопасности система должна уведомить аналитика, чтобы он принял необходимые меры. Для улучшения работы администратор должен периодически конфигурировать работающую систему.

Обобщенную схему можно увидеть на рисунке 2.

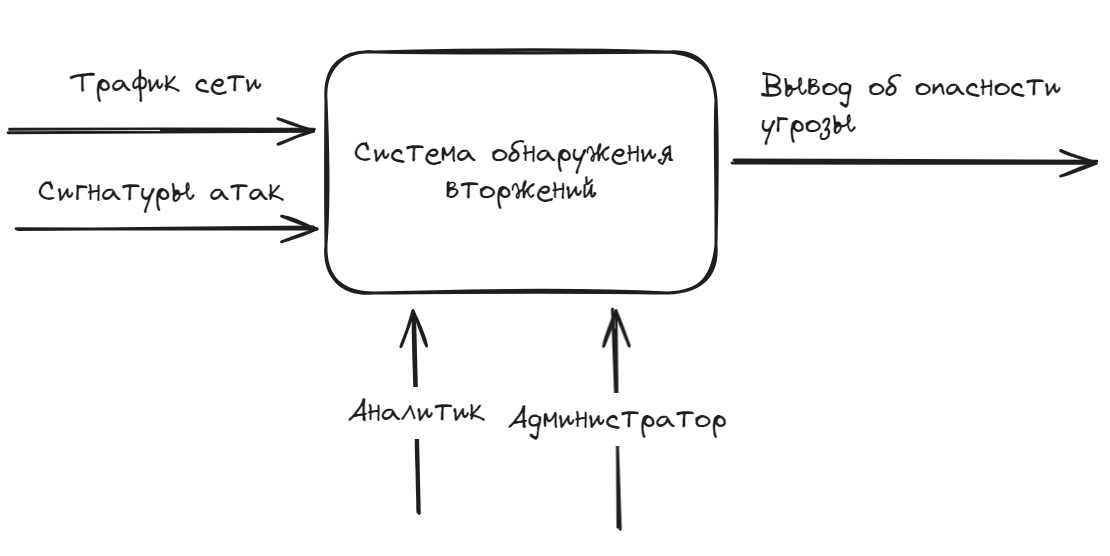


Рисунок 2 – Схема «Черный ящик»

Обнаружение процессов можно декомпозировать (рисунок 3).

Изображение выглядит как текст, диаграмма, зарисовка, Шрифт

Автоматически созданное описание

Рисунок 3 – Декомпозиция бизнес-процесса

Общая информация о задачах:

* Задача сбора трафика;
* Задача хранения полезного трафика сети;
* Задача анализа данных и формирования вывода;
* Задача создания рекомендаций и применения мер;

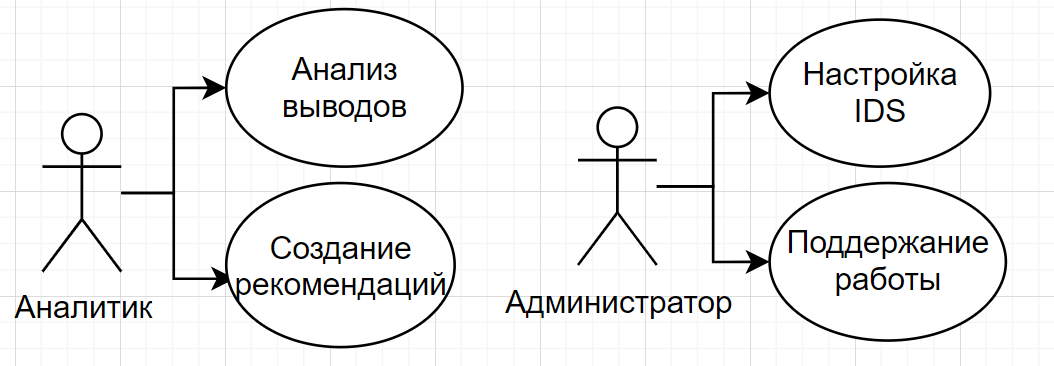


Рисунок 4 – Диаграмма вариантов использования

Таблица 1. Реестр входных информационных потоков

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Наименование и назначение потока | Форма представления | Обработчик (кто обрабатывает) | Корреспондент (откуда поступает) | Характеристики обработки | |
| Трудозатраты, чел.ч | Периодичность, регламент |
| 1 | Трафик сети | Файл | Система обнаружения | Сеть | 0 | Постоянно |
| 2 | Сигнатуры атак | Файл | Система обнаружения | Администратор | 0.5 | Зависит от требований заказчика |

Таблица 2. Реестр выходных информационных потоков

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Наименование и назначение потока | Форма представления | Обработчик (кто обрабатывает) | Корреспондент (откуда поступает) | Характеристики обработки | |
| Трудозатраты, чел.ч | Периодичность, регламент |
| 1 | Вывод об опасности угрозы | Файл/Текст | Аналитик | Система обнаружения | 0.16 | Постоянно |

**3. Необходимость усовершенствования.** В существующем решении IDS собирают данные и обрабатывают их посредством сигнатурного анализа, что может не учитывать некоторые сценарии атак и требовать постоянных доработок. Аналитику в свою очередь чаще требуется перепроверять выводы этой системы, а ложные срабатывания плохо сказываются на его трудозатратах.

По результатам анализа была выявлена возможность улучшить текущее качество обработки данных для обеспечения своевременного реагирования на угрозы безопасности посредством применения машинного обучения.