УДК 004.056

РАЗРАБОТКА КОНЦЕПЦИИ ЛАБОРАТОРНОГО СТЕНДА ПО ИЗУЧЕНИЮ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА БАЗЕ IDS INFOTECS

Коркачев Д.В., специальность 10.05.03, группа ИБс-211
Научный руководитель: Киренберг А.Г.,
доцент кафедры информационной безопасности,
Кузбасский государственный технический университет им. Т.Ф. Горбачева,
Россия, г. Кемерово

Современный образовательный процесс в области информационной безопасности сталкивается с парадоксальной ситуацией: с одной стороны, требуется подготовка специалистов, способных работать со сложными системами защиты, с другой стороны – образовательные учреждения зачастую располагают лишь ограниченным набором инфраструктурных ресурсов, не всегда позволяющих моделировать реальные условия работы корпоративных систем. Особенно остро это проявляется в области систем обнаружения вторжений (IDS), где для эффективного обучения требуется возможность тестирования и настройки оборудования в условиях, максимально приближённых к практическому применению. Традиционные подходы к созданию учебных лабораторий предполагают использование разнообразных компонентов инфраструктуры и специализированных систем, которые в ряде случаев ориентированы на корпоративный сектор и не всегда учитывают особенности образовательного процесса.

В основе методологии лежит принцип "минимальной достаточности" – создание среды, которая при минимальных ресурсах обеспечивает максимальную образовательную ценность. Это достигается за счет:

- Применения виртуализации для изоляции тестовых сред
- Использования открытого программного обеспечения
- Реализации постепенного усложнения сценариев

Важным аспектом методологии является поэтапное построение сценариев тестирования – от простых сканирующих атак к сложным многоступенчатым атакам, что позволяет студентам постепенно осваивать методы обнаружения и анализа угроз.

Предлагаемая концепция основана на создании гибридной среды, сочетающей физическое оборудование IDS с виртуальной инфраструктурой, генерирующей тестовый трафик. Ключевая идея заключается в использовании принципа "зеркалирования трафика" (SPAN) для направления, сгенерированного виртуальными машинами трафика на физическое оборудование IDS.

Архитектура системы включает следующие компоненты:

Виртуальная инфраструктура:

- Kali Linux - генерация атак (nmap, Metasploit, OWASP ZAP)

- Ubuntu Server - целевая система с веб-сервером
- Windows Client - рабочая станция пользователя
- Grafana + Loki - платформа для визуализации логов и генерации легитимного веб-трафика

Физическая инфраструктура:

- Сетевой коммутатор с SPAN-портом
- Аппаратная IDS для анализа трафика

Целевые системы на базе Ubuntu Server с развернутыми сервисами:

- Веб-сервер Apache с тестовыми приложениями
- Система управления базами данных MySQL
- Службы удаленного доступа (SSH, RDP)

Система мониторинга и визуализации на базе стека Grafana:

- Grafana - платформа для визуализации метрик и логов
- Loki - система для сбора и хранения логов
- Promtail - агент для транспортировки логов

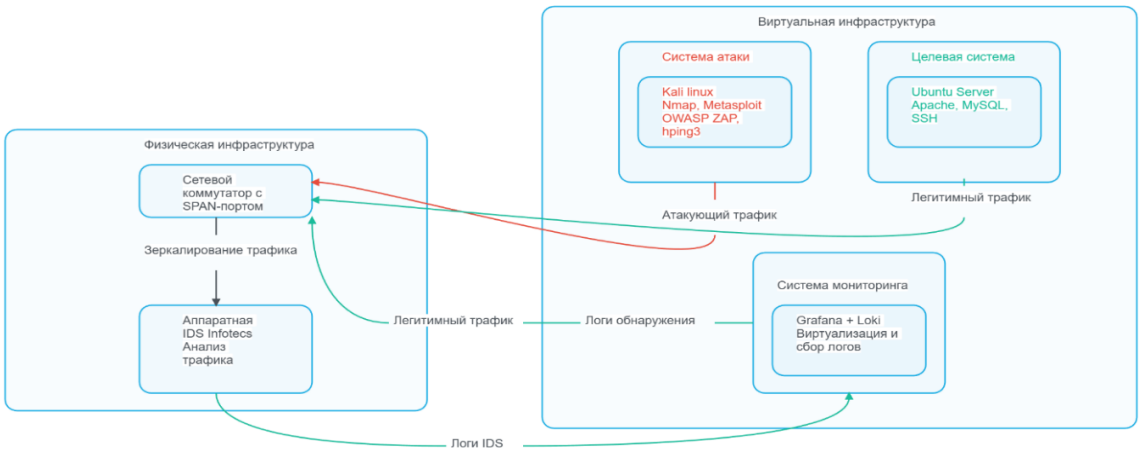

Рисунок 1 – Схема архитектуры системы

Виртуальные машины генерируют смешанный трафик (легитимный от Grafana и атакующий от Kali Linux), который через зеркалированный порт коммутатора поступает на IDS для анализа. Grafana обеспечивает визуализацию процесса обнаружения угроз через сбор логов в Loki. Основным преимуществом предложенной концепции является ее модульность – каждый компонент может быть масштабирован или заменен в зависимости от доступных ресурсов и конкретных образовательных задач.

Внедрение предложенной концепции через создание стенда позволит решить несколько ключевых проблем профильных дисциплин, связанных с изучением систем обнаружения вторжении (IDS/СОВ):

1. Доступность – снижение стоимости создания учебных лабораторий за счет использования виртуализации и открытого ПО.

2. Масштабируемость – возможность постепенного наращивания функциональности по мере развития образовательной программы.

3. Безопасность – изолированная среда позволяет проводить тестирование реальных атак без риска для производственных систем.

4. Наглядность – визуализация процессов обнаружения атак способствует лучшему пониманию принципов работы IDS.

Концепция предусматривает также и разработку комплекса учебных материалов и сценариев, охватывающих основные аспекты работы с системами обнаружения вторжений:

- Настройка и калибровка IDS
- Анализ сетевого трафика
- Классификация типов атак
- Создание правил обнаружения
- Ответ на инциденты безопасности

Дальнейшее развитие концепции предполагает несколько направлений:

1. Создание библиотеки типовых сценариев атак для различных отраслей экономики.

2. Разработка облачной версии платформы для удаленного доступа.

3. Интеграция с системами мониторинга и управления инцидентами безопасности.

4. Создание модулей для тестирования новых классов угроз, таких как атаки на IoT-устройства и промышленные системы.

Важным направлением развития является также создание сообщества пользователей и разработчиков, что позволит постоянно пополнять базу знаний и сценариев тестирования.

Предложенная концепция разработки стенда вместе с имитационной средой для изучения систем обнаружения вторжений представляет собой сбалансированный подход к решению проблемы практической подготовки специалистов ИБ, особенно в условиях ограниченных ресурсов. Использование современных технологий виртуализации и открытого программного обеспечения делает решение доступным для широкого круга образовательных учреждений, выпускающих специалистов укрупнённой группы специальностей 10.00.00.

Список литературы:

1. Белов Е.Б. Основы информационной безопасности: учебное пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

2. Галатенко В.А. Основы информационной безопасности: курс лекций: учеб. пособие для вузов по специальностям в обл. информ. технологий / В. А. Галатенко; Под ред. В. Б. Бетелина. – М.: Интернет-Университет Информационных Технологий, 2006. – 205 с.

3. Grafana Labs. Официальная документация Grafana [Электронный ресурс]. – URL: https://grafana.com/docs/ (дата обращения: 18.11.2025).

4. Grafana Labs. Официальная документация Loki [Электронный ресурс]. – URL: https://grafana.com/docs/loki/latest/ (дата обращения: 18.11.2025).

5. Семенов А.В. Технологии моделирования кибератак для образовательных целей // Информационная безопасность. – 2021. – № 2. – С. 67-74.

6. Петров И.С. Виртуальные лаборатории в образовательном процессе // Высшее образование в России. – 2019. – № 8. – С. 112-118