



БПОУ РА «Горно-Алтайский государственный
политехнический колледж им. М. З. Гнездилова»

Модуль обнаружения вредоносного ПО в сетевом трафике

Выполнила: студентка группы 1077

Шабьков Алан Артурович

Руководитель: Завчук Ирина Петровна

Цели и задачи работы

Целью работы является модуль обнаружения вредоносного программного обеспечения в сетевом трафике.

Задачи:

- Определить основные угрозы информационной безопасности
- Изучить проблемы обеспечения безопасности сети
- Исследовать современные методики анализа сетевого трафика

Угрозы информационной безопасности

Отсутствие блокировки компьютера на время отсутствия пользователя.

Несанкционированное отключение элементов защиты пользователями

*Использование сомнительного программного обеспечения
Отсутствие разграничения доступа*

Системы мониторинга и анализ сетевого трафика

- *Системы управления сетью (Network Management Systems)*
- *Встроенные системы диагностики и управления (Embedded Systems)*
Оборудование для диагностики и сертификации кабельных систем
- *Анализаторы протоколов (Protocol analyzers)*
- *Многофункциональные устройства анализа и диагностики.*

Системы обнаружения и предотвращения вторжений

Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS))

Система предотвращения вторжений (СПВ) (англ. Intrusion Prevention System (IPS))

Методики обнаружения аномального и злоумышленного поведения пользователей



ViPNet IDS



ViPNet IDS

The screenshot displays the ViPNet IDS management interface. At the top, there is a navigation bar with a back arrow, the text "Обнаружение Система", and tabs for "Сеть", "Параметры", and "Правила обнаружения". Below the navigation bar, there is a search bar with the text "Искать правило...", a status bar showing "Найдено 24525 правил", and a progress indicator with "1/1", "44/45", "96/96", and "0/0". There are also buttons for "Применить изменения" and "Отменить изменения".

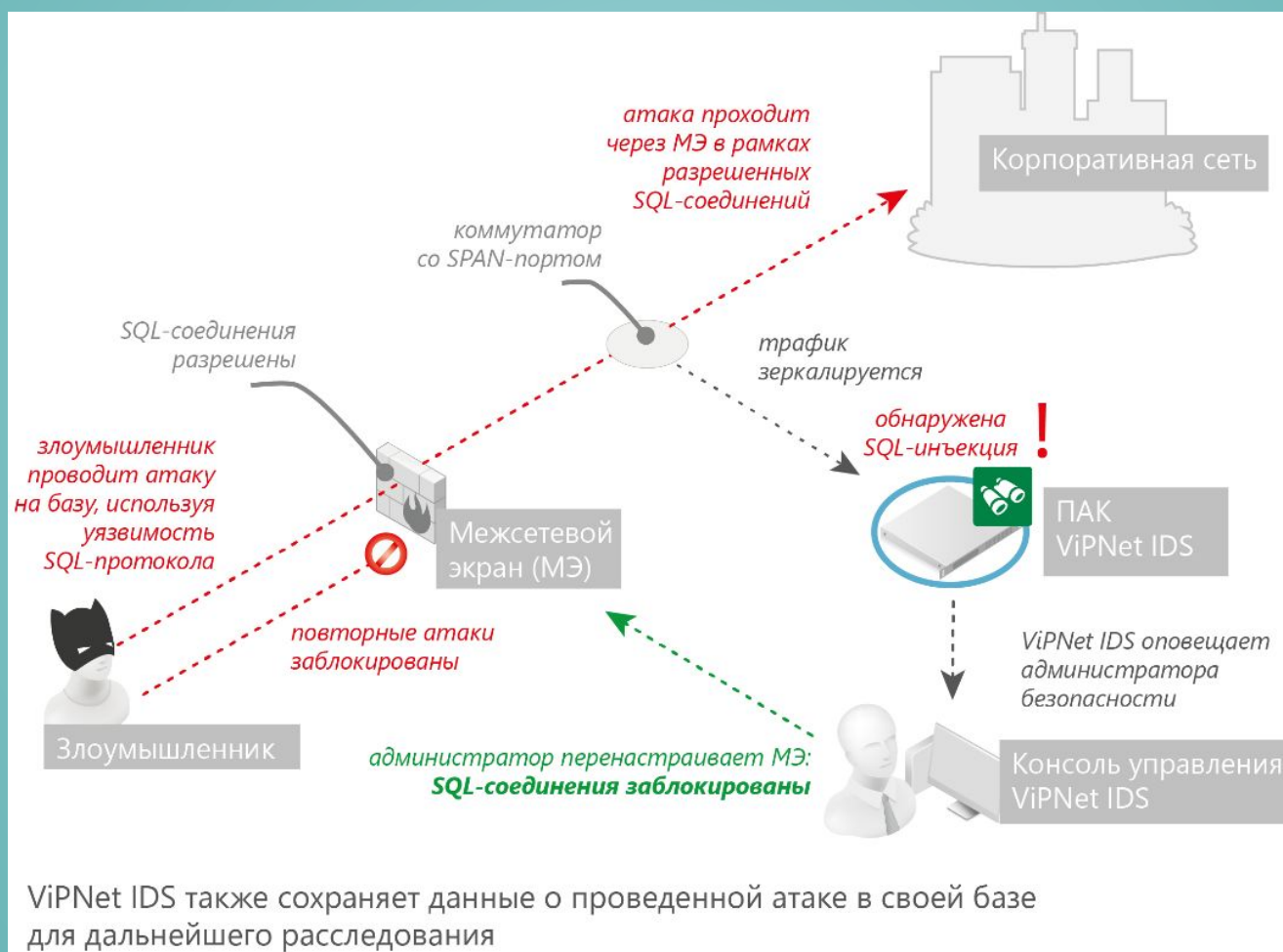
The main content area is divided into two sections. On the left, there is a sidebar titled "Группы правил" (Rule Groups) with a gear icon. It lists several rule groups:

- emerging-exploit (451)**: Сигнатуры атак, направленные на выявление программного кода, использующего для выполнения атаки уязвимости в программном обеспечении (эксплойты). Используется, пакеты сохраняются в базу данных.
- emerging-ftp (124)**: Сигнатуры атак на протокол передачи файлов FTP. Используется, пакеты сохраняются в базу данных.
- emerging-games (75)**: Сигнатуры возможного нарушения политики информационной безопасности – сигнатуры игровых серверов. Используется, пакеты сохраняются в базу данных.
- emerging-icmp (39)**: Сигнатуры атак, охватывающие незаконный или аномальный трафик ICMP, например сканирование портов. Используется, пакеты сохраняются в базу данных.
- emerging-icmp_info (66)**: Сигнатуры атак, охватывающие ICMP сообщения. Используется, пакеты сохраняются в базу данных.

On the right, there is a section titled "Группа правил: decoder". It has a table with columns: "Использование", "Сохранение пакетов", "Добавить тег", "Удалить тег", "Правило", "П...", "Ис...", "С...", "Критичность", "Класс", "Название", and "Теги правила". The table lists 20 rules with their IDs, criticality levels, and names.

| Использование | Сохранение пакетов | Добавить тег | Удалить тег | Правило | П... | Ис... | С... | Критичность | Класс | Название | Теги правила |
|--------------------------|--------------------------|--------------|-------------|---------|-------------------------------------|--------------------------|--------------------------|-------------|-------------------------|----------------------|--------------|
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.450 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Средняя | non-standard-protocol | DECODE_IP_BAD_PR... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.451 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Средняя | attempted-dos | DECODE_ICMP_PATH... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.452 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Средняя | denial-of-service | DECODE_ICMP_DOS_... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.453 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Средняя | misc-attack | DECODE_IPV6_ISATA... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.454 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Высокая | attempted-admin | DECODE_PGM_NAK_... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.455 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Средняя | attempted-dos | DECODE_IGMP_OPTI... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.456 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | misc-activity | DECODE_IP6_EXCESS... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.46 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Средняя | bad-unknown | DECODE_TCP_INVALI... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.47 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Средняя | bad-unknown | DECODE_TCP_LARGE... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.5 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_IPV4OPT_TR... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.54 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_TCPOPT_BA... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.55 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_TCPOPT_TR... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.56 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_TCPOPT_TT... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.57 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_TCPOPT_OB... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.58 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_TCPOPT_EX... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.59 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_TCPOPT_WS... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.6 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_IPV4_DGRA... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.95 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_UDP_DGRA... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.96 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_UDP_DGRA... | |
| <input type="checkbox"/> | <input type="checkbox"/> | | | 116.97 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Низкая | protocol-command-dec... | DECODE_UDP_DGRA... | |

Обнаружение атаки и предотвращение ее развития





БПОУ РА «Горно-Алтайский государственный
политехнический колледж им. М. З. Гнездилова»

Механизм управления продажами продукции предприятия

Выполнила: студентка группы 1077

Шабыков Алан Артурович

Руководитель: Завчук Ирина Петровна