НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ СЕТЕВОЙ СТЕНД КАК МНОГОФУНКЦИОНАЛЬНЫЙ КОМПЛЕКС СРЕДСТВ ИЗУЧЕНИЯ СЕТЕВЫХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Абрамова Т.В., Аралбаев Т.З., д-р техн. наук, профессор,
Каменева Е.В., Синицын Ю.И., канд. техн. наук, доцент
Оренбургский государственный университет

Одним из важных факторов успешного проведения учебного процесса является материально-техническое обеспечение изучаемых дисциплин. Настоящая работа посвящена результатам построения учебно-лабораторного комплекса (УЛК) для изучения методов и средств защиты информации в компьютерных сетях, в частности, для изучения аномалий сетевых трафиков.

По результатам исследования Лабораторией Касперского в 2015 году 17% российских компаний столкнулись с DDos-атаками, а сама страна оказалась в первой пятерке государств, чьи веб-ресурсы вызывали наибольший интерес у киберзлоумышленников. По данным компаний Qrator и Wallarm, в 2014 году среднее число зловредных запросов на одного клиента увеличилось в 2.5 раза, при этом для одной атаки, как правило используются запросы с группы IP-адресов [6]. Таким образом, рост количества сетевых угроз определяет необходимость подготовки квалифицированных специалистов в области защиты от сетевых атак, в частности специалистов, занимающихся вопросами анализа сетевого трафика на наличие аномалий.

Следует отметить, данная задача достаточно успешно решается в центрах специальной подготовки и переподготовки специалистов в области сетевых технологий, например, в центрах обучения академии Cisco. Однако в условиях учебного процесса вузов имеются ряд сложностей организационного, методического и финансового характера, преодоление которых возможно лишь на основе системного подхода, учитывающего специфику учебных стандартов, перечня компетенций, дидактического материала, существующей лабораторной базы, квалификационных характеристик разработчиков и других факторов.

Представленный учебно-лабораторный комплекс разработан на кафедре вычислительной техники защиты информации Оренбургского государственного университета на базе кафедральных компьютерных лабораторий и учебно-исследовательского сетевого стенда, установленного в одной их лабораторий. Разработке УЛК предшествовал ряд исследований, в ходе которых проведен аналитический обзор публикаций, посвященных структурным, архитектурным и функциональным особенностям УЛК, определена концепция его построения, выявлены требования и принципы его разработки. В частности, анализ публикаций [1; 2; 5] позволил определить концепцию построения структуры и выбор архитектуры УЛК.

Перечень работ [1; 4] позволил сформировать систему дидактического материала, определить структуру лабораторных работ и порядок их проведе-

ния. На основе анализ работ [3-5] определены функциональные требования к УЛК и особенности его реализации.

Известно, что создание учебно-лабораторного комплекса, как системы, является достаточно сложной, многовариантной задачей, решение которой достигается различными подходами, в частности: на основе методов целочисленного линейного программирования, морфологического анализа, экспертной оценки и других. В данном случае УЛК формировался на базе существующих средств кафедры вычислительной техники и защиты информации. Поэтому основные требования к нему определялись выбором тематики учебно-методического материала по защите информации в компьютерных сетях. Для этого был проведен анализ существующих комплексов лабораторных работ, позволивший определить структуру лабораторных работ и перечень дидактических единиц для изучения.

В указаниях для специализированных курсов имеется свой ряд недостатков, в частности: в частности, недостаточная функциональная полнота, требования повышенной первоначальной подготовки. Целью разработки представленного в работе УЛК является устранение перечисленных недостатков.

В основу концепции разработки положен принцип представления УЛК как учебно-методической системы для изучения аномалий сетевых трафиков [7]. В соответствии с этим:

- УЛК построен с учетом компетенций и дидактического материала специальности «Комплексная защита объектов информатизации» (КЗОИ);
- использован критерий обеспечения функциональной полноты для решения учебно-исследовательских задач мониторинга и отражения сетевых вторжений;
- оптимизация технических и функциональных характеристик УЛК проведена в условиях стоимостных и временных ограничений вуза.

При реализации концепции были разработаны и использованы: реляционная модель выбора и обоснования перечня дидактических единиц и модулей, реляционная модель выбора аппаратно-программных средств и лабораторно-стендового оборудования. Применение данных моделей позволили оптимизировать структуру и качественный состав обеспечивающих подсистем УЛК.

Структура УЛК представляет собой кафедральную локальную вычислительную сеть из 24 компьютерных станций, включающую в себя сетевые узлы, размещенные в стендовой стойке, имеющие возможность подключения к Интернету как посредством средств беспроводной связи, так и через прокси-сервер вуза.

Архитектурно УЛК реализована на базе стационарных компьютерных станций, мобильных компьютеров (ноутбуков), обеспеченных проводной и беспроводной связью. Коммутаторы, маршрутизаторы и межсетевой экран стенда выбраны по принципу доступности из линейки сетевого оборудования фирм DLink и Cisco.

На рисунке 1 представлена стойка и основное сетевое оборудование учебно-исследовательского стенда, используемого в составе УЛК для проведения лабораторных работ по сетевым технологиям.

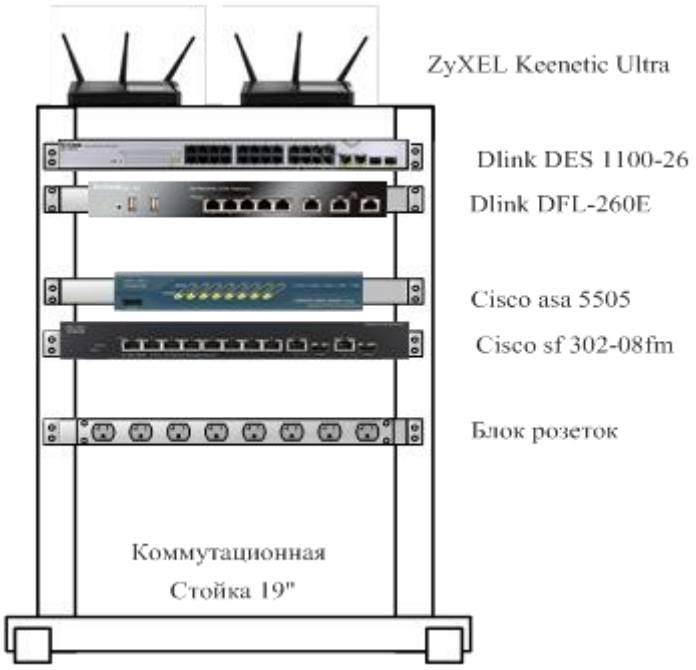

Рисунок 1 - Внешний вид учебно-исследовательского сетевого стенда

В коммутационную стойку установлено следующее сетевое оборудование:

- настраиваемый коммутатор DLink DES-1100-26;
- межсетевой экран DLink DFL-260E;
- межсетевой экран Cisco asa 5505;
- управляемый коммутатор Cisco sf302-08mp;
- беспроводной маршрутизатор ZyXEL Keenetic Ultra.

В перечень программно-аппаратных и программных средств УЛК включены:

- программно-аппаратный комплекс защиты информации от несанкционированного доступа «Аккорд»;
- персональное средство криптографической защиты информации «ШИПКА»;
- сканер сетевого трафика “Wireshark”;
- программное средство защиты информации от несанкционированного доступа “Secret Net 7”;
- сетевой сканер уязвимостей хостов “XSpider 7.7”;
- программное средство подбора паролей архивов “Advanced Archive Password Recovery 4.54.55” и ряд других программ.

Представленный УЛК обеспечивает выполнение лабораторных работ практически по всем сетевым дисциплинам специальности КЗОИ, в перечень которых входят: «Комплексная защита информации в распределенных вычислительных системах», «Сети и системы», «Программно-аппаратные средства защиты информации», «Защита информационных процессов в компьютерных системах».

Технические и функциональные характеристики УЛК позволили разработать и применить в учебном процессе комплекс из 12 лабораторных работ, тематика которых включает вопросы построения и исследования компьютерных сетей различной конфигурации, установки, настройки и исследования сетевого оборудования и программного обеспечения, в частности:

- построение локальных вычислительных сетей на базе учебно-исследовательского сетевого стенда;
- построение и настройка защищенной беспроводной сети;
- безопасное администрирование сетей;
- создание и противодействие простой сетевой атаке;
- анализ трафиков и уязвимостей в сетях с использованием программных средств;
- создание и противодействие DDos-атакам;
- моделирование игровых ситуаций по получению доступа к сетевому ресурсу;
- дистанционное управление и сканирование уязвимостей;
- оперативная идентификация аномалий сетевого трафика и определение мер по их нейтрализации.

Учебно-лабораторный комплекс применяется для физического и имитационного моделирования компьютерных сетей с различной технологией и для реализации различных аномальных ситуаций, необходимых для генерации и регистрации данных в научно-исследовательских разработках студентов и аспирантов.

В частности, на базе УЛК успешно выполнены следующие научно-исследовательские разработки студентов:

- оперативный поиск информации в базах данных сетевого трафика на основе ассоциативного подхода;
- моделирование сетевого трафика и обнаружение аномалий на основе методов нейронных сетей, классификатора Байеса и спектрального анализа;
- дистанционное управление и сканирование уязвимостей в компьютерной сети удаленных автоматизированных систем.

УЛК успешно использован на курсах повышения квалификации по основам информационной безопасности преподавательского состава кафедры.

Достоинства работы сетевого стенда наглядно видны при проведении лабораторных работ среди студентов и магистрантов кафедры. В качестве примера можно рассмотреть эксперимент по организации атаки ping flooding [8] и сбору экспериментальных данных для анализа активности сетевого трафика,

наглядно показывающих студентам возможности сбора и обработки данных при выявлении сетевых атак. Структурная схема сети при проведении атаки представлена на рисунке 2.

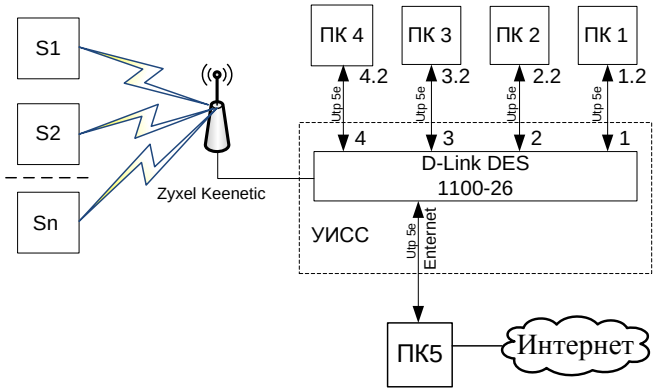

Рисунок 2 – Структурная схема построения сети

На рисунке приняты следующие условные обозначения: ПК1 – ПК2 – компьютеры лаборатории, подключенные посредством проводной связи к коммутатору D-Link, ПК5 – компьютер сети, выполняющий функции DHCP-сервера, Zyxel Keenetic – маршрутизатор, S1 – Sn – компьютеры сети, участвовавшие в атаке, подключенные к сети посредством беспроводной связи.

В ходе моделирования атаки, атакующие были разбиты на 6 групп. С периодичностью, кратной 2, первая группа атаковала каждые 2^3=8 секунд, вторая группа каждые 2^4=16 секунд, третья группа каждые 2^5=32 секунды, четвертая каждые 2^6=64 секунды, пятая каждые 2^7=128 секунд, шестая каждые 2^8=256 секунд. Общее время атаки – 300 секунд. Временная диаграмма режима атаки представлена на рисунке 3.

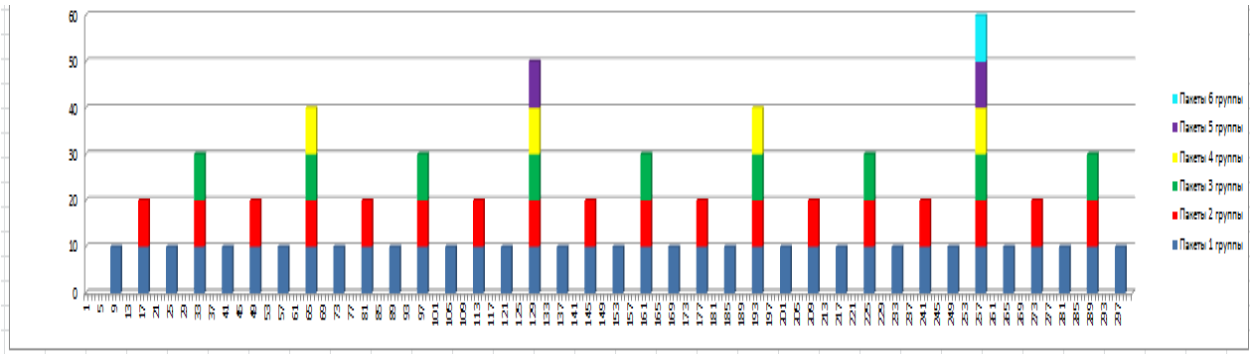

Рисунок 3 – Временная диаграмма экспериментального сетевого трафика в режиме атаки

После проведения атаки с помощью табличного процессора Microsoft Excel была произведена обработка данных и построен график экспериментального сетевого трафика по состоянию сети в нормальном режиме и в режиме

атаки. При анализе графика интенсивности сетевой активности в режиме атаки наблюдается определенная периодичность в активности пользователей сети, в соответствии с проведенными экспериментальными атаками. Рост скачков интенсивность в каждом следующем периоде связан с подключением к атаке новых групп атакующих.

Результаты представлены на рисунке 4.

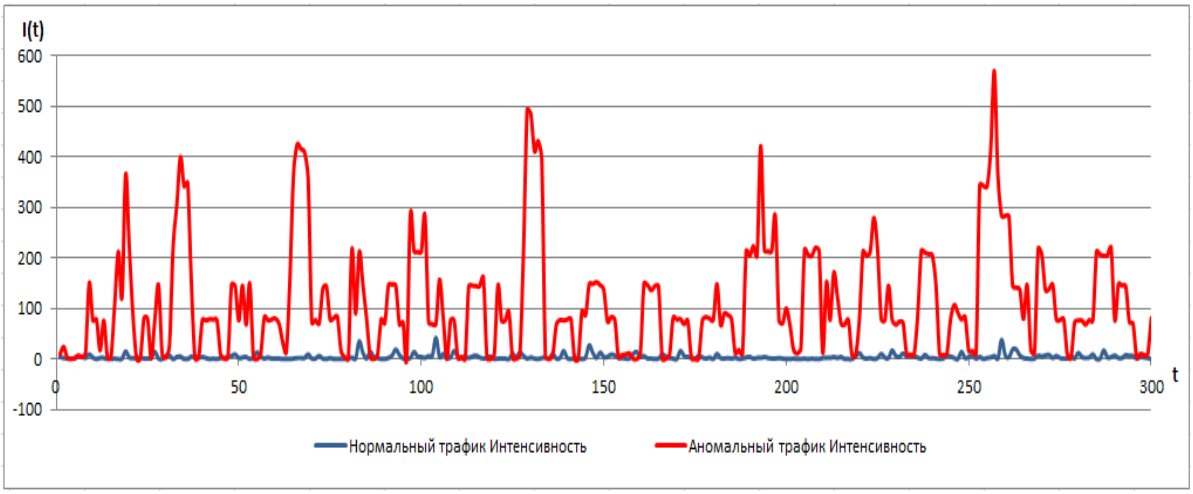

Рисунок 4 – Интенсивность сетевого трафика в режимах покоя и атаки

Полученные графики наглядно показывают, что показатель интенсивность сетевого трафика значительно меняется при смене вида деятельности пользователей. В штатном режиме сетевой трафик удовлетворяет стандартному шаблону. Сетевая активность пользователей не превышает 45 пакетов в секунду. На графике наблюдаются временные скачки интенсивности, связанные с работой сетевого оборудования. В режиме атаки, напротив, интенсивность трафика резко возрастает, вследствие перегрузки при обработке ICMP-сообщений сетевым оборудованием. При этом интенсивность сетевого трафика в режиме атаки в разы превышает интенсивность трафика в нормальном режиме. Это обусловлено высокой активностью пользователей сети и сетевого оборудования.

Полученные данные дают обучающимся наглядное представление о происходящих в сети процессах. Кроме того, их можно использовать для дальнейшего моделирования и прогнозирования сетевых процессов, для генерации и регистрации данных в научно-исследовательских разработках студентов и аспирантов. Например, получив график интенсивности трафика при проведении сетевой атаки и построив линию тренда полученного графика, можно проводить дальнейший прогноз сетевой активности и надежности работы сети при проведении того или иного вида сетевой атаки.

Результаты проведенной работы показывают, что использование сетевого стенда для имитации сетевой атаки дает наглядное представление о сетевых процессах, возможность проанализировать воздействие атаки на сетевое обору-

дование, настроить оборудование для обеспечения информационной безопасности сети. Кроме того, подобный подход способен привести к повышению интереса студентов к учебному процессу и получению практических навыков и, в конечном счете, повышению качества подготовки будущих специалистов в области сетевой безопасности и сетевых технологий.

Список литературы

1. *Богданова Е.А., Руденков Н.А. и др. / Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет- маршрутизаторы. 2013 г. – 743 с.*
2. *Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: учебное пособие / А.К. Гуц, Т.В. Вахний. – Омск: Изд-во ОМГУ, 2013. – 160 с.*
3. *Методические указания по выполнению лабораторных работ по дисциплине «Защита информации» – Утв. 2003 г. – Уфа: УГАТУ, 2003. – Режим доступа. – URL: http://www.studfiles.ru/dir/cat32/subj1166/file9309.html (Дата обращения 15.04.2015).*
4. *Основная образовательная программа высшего профессионального образования. Направление подготовки: 090900 – Информационная безопасность. Профиль подготовки – Комплексная защита объектов информатизации. Квалификация – Бакалавр. Форма обучения – Очная. – Утв. 2011-04-16. – Оренбург: ОГУ, 2011. – 43 с.*
5. *Смирнова Е.В., Пролетарский А.В. и др. / Построение коммутируемых компьютерных сетей: учебное пособие, 2012. – 367 с.*
6. *DDos-атаки 2014: реже, но крупнее – [Электронный ресурс] – / БЕСТСЕЛЕРЫ Аналитического рынка ИТ. – Режим доступа. – URL: http://www.itbestsellers.ru/companies-analytics/detail.php?ID=30073 (Дата обращения 15.04.2015).*
7. *Аралбаев Т.З., Романенко С.Ю. УЧЕБНО-ЛАБОРАТОРНЫЙ КОМПЛЕКС ДЛЯ ИЗУЧЕНИЯ АНОМАЛИЙ СЕТЕВЫХ ТРАФИКОВ // Технические науки - от теории к практике: сб. ст. по матер. LVI междунар. науч.-практ. конф. № 3(51). – Новосибирск: СибАК, 2016. – С. 17-24.*
8. *Ping-флуд– [Электронный ресурс] — Режим доступа. – URL: https://ru.wikipedia.org/wiki/Ping-D1%84%D0%BB%D1%83%D0%B4 (Дата обращения 11.01.2017).*