Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.7

СИЛИЧ
Светлана Сергеевна

МОДЕЛИ УГРОЗ ЛОКАЛЬНОЙ СЕТИ В УЧРЕЖДЕНИИ ОБРАЗОВАНИЯ

Автореферат
на соискание степени магистра
по специальности 1–45 80 01 Системы и сети инфокоммуникаций

_____

Научный руководитель
Кандидат технических наук,
доцент
ШЕВЧУК Оксана Геннадьевна

_____

Минск 2024

ВВЕДЕНИЕ

Локальные сети в учреждениях образования играют важную роль в обеспечении эффективной работы и обмена информацией. Однако с ростом использования сетевых технологий возрастает и уровень угроз безопасности, с которыми они сталкиваются.

Данные о сотрудниках, документации интересны преступникам, которые для несанкционированного доступа к ним используют все возможные средства. Поэтому к системам защиты конфиденциальной информации предъявляются особые требования.

Учреждение образование всегда была связана с обработкой и хранением большого количества данных. В первую очередь это персональные данные сотрудников и студентов.

Модели угроз локальной сети в учреждении являются ключевым инструментом для понимания и противодействия потенциальным атакам и нарушениям безопасности. В данной статье мы рассмотрим основные типы угроз, с которыми может столкнуться локальная сеть в учреждении образования, и методы их предотвращения.

Актуальность данной магистерской диссертации заключается в том, что с помощью использования различных методов, связанных с информационной безопасностью, можно обеспечить защищенность распределённой корпоративной сети.

Объектом исследования работы является угроза локальной сети. Предметом исследования диссертационной работы является нахождение методов для защиты локальной сети.

Целью диссертационной работы является организация защиты локальной сети учреждения образования на основе модели угроз.

Для достижения поставленной цели необходимо решить следующие задачи:

1 Провести обзор литературы и рассмотреть основные модели угроз локальной сети.

2 Проектирование модели угроз локальной сети учреждения образования;

3 Определение политик безопасности для организации защиты локальной сети. Практическая ценность исследования позволяет использовать полученные результаты для обеспечения защиты локальной сети в учреждении образования.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту 6 приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь №156 от 7 мая 2020 г. «О совершенствовании организационной структуры Национальной академии наук Беларуси». Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Целью диссертационной работы является организация защиты локальной сети учреждения образования на основе модели угроз.

Для достижения поставленной цели необходимо решить следующие задачи:

1 Провести обзор литературы и рассмотреть основные модели угроз локальной сети.

2 Проектирование модели угроз локальной сети учреждения образования;

3 Определение политик безопасности для организации защиты локальной сети. Практическая ценность исследования позволяет использовать полученные результаты для обеспечения защиты локальной сети в учреждении образования.

Личный вклад соискателя ученой степени:

Содержание диссертации отображает личный вклад автора. Он заключается в научном обосновании нахождения методов защиты сети, моделирование и реализации их, а также обработке и анализе полученных результатов, формулировке выводов.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем кандидат технических наук, доцент О.Г. Шевчук

Апробация диссертации и информация об использовании ее результатов.

Основные положения и результаты диссертационной работы докладывались на: 59-й и 60-й научных конференциях аспирантов, магистрантов и студентов

Опубликование результатов диссертации.

По результатам исследований, представленных в диссертации, опубликована 2 тезиса в сборниках и материалах конференцией.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, трёх глав с выводами по каждой главе, заключения, библиографического списка, восьми.

Общий объем диссертационной работы составляет 76 страница, из них 38 страниц текста, 23 рисунков на 20 страницах, 1 таблиц на 2 страницах, список использованных библиографических источников (22 наименований на 2 страницах), список публикаций автора по теме диссертации (2 наименование на 0.5 страницах), графический материал на 5 страницах.

Проверка на уникальность

Проведена экспертиза диссертации Силич Светланы Сергеевны «Модели угроз локальной сети в учреждении образования» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в online режиме 24.05.2024 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 88,66 %).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** приведена и описана простейшая модель угроз сети учреждения образования, которая включает в себя описание информационной системы и ее структурно-функциональных характеристик, перечень угроз безопасности сети университета, а также используемые средства защиты сети от рассмотренных потенциальных угроз, такие как SIEM, LDAP, файрвол и другие. Приведены и описаны основные атаки на локальные сети. Выявлены основные уязвимости локальной сети учреждения образования.

Стоит отметить, что модели угроз локальной сети в учреждении образования играют важную роль в защите исследовательских и личных данных студентов и сотрудников, предотвращении финансовых потерь и сохранении репутации университета, что приносит значительную экономическую ценность для университетской среды.

В первой главе описываются существующие модели угроз для локальной сети в учреждении образования. Описывается проблема несанкционированного доступа к сети. Перечислены пути несанкционированного доступа, сколько требуется технических знаний или программных разработок со стороны взломщика. Рассмотрены любые утечки конфиденциальной информации.

Рассматривается вредносносное программное обеспечение. Развернуто описаны какие они бывают как заражают сеть. Описывается, как быстро они заражают программу. Рассказывается, кем пишутся и создаются вируса. Какие классы вирусов бывают по различным признакам.

Во второй главе рассматривается структура локально-вычислительной сети 5 корпуса БГУИРА. Расписывается отдельно одна из кафедр учреждения. Описывается как состоит сеть, что в создание сети входит. Как подлечена на сетевом уровне. Что будет происходить с данными в случае аварийного отключения электричества. Произведен анализ программного обеспечения деятельности предприятия. Что именно используют на кафедре, какие программы. А также произведен анализ серверной инфраструктуре.

В третьей главе была рассмотрена сеть кафедры ЭВМ. Методы защиты кафедральной локальной сети.

Защита с помощью Kaspersky Security Center, который позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений. Одним из основных инструментов обеспечения безопасности ЛС является файрволлы. Они

играют ключевую роль в предотвращении несанкционированного доступа и защите от различных видов кибератак.

Также мы рассмотрели, что в университете резервное копирование не менее играет важную роль для обеспечения сохранности и доступности информации, необходимой для учебного процесса, исследований, административных задач и других функций.

ЗАКЛЮЧЕНИЕ

В ходе работы над магистерской диссертацией был проведен анализ особенности существующей сети. В процессе анализа различных моделей угроз были выявлены следующие уязвимости:

– использование отдельных сетей, вместо разбиения единой сети на подсети;

– недостаточная обученность пользователей;

– слабые пароли;

– устаревшее программное обеспечение.

В изучения были приведены основные риски:

– масштабные атак на сеть, такие как DDoS – атаки, которые могут привести к отказу в обслуживании и нарушению работы сети.

– утечка конфиденциальной информации, с учетом большого количества студентов, преподавателей и административного персонала, университеты могут столкнуться с риском утечки конфиденциальной информации, такой как личные данные студентов или результаты исследований.

– вредоносные программы и фишинг, университетские сети могут быть подвержены вредоносным программам, включая программное обеспечение – вымогатели, шпионское ПО и фишинговые атаки, которые могут использоваться для получения доступа к чувствительной информации.

– социальная инженерия, атаки с использованием социальной инженерии могут быть направлены на членов университетского сообщества для получения конфиденциальной информации или учетных данных.

Учитывая необходимость сохранности и защиты большого количества персональных данных, такие уязвимости необходимо ликвидировать и проводить дополнительные тестирования для выявления возможных сценариев взлома сети. Например, ЦИИР БГУИР внедрил систему анализа почтовых сообщений и, при выявлении критериев спама, в теме письма добавляется ключевая фраза «SPAM..», тем самым информируя пользователей о нежелательных письмах.

Наличие уязвимостей были выявлены в процессе анализа различных моделей угроз и их последствий в процессе работы над магистерской диссертацией. Анализ и понимание потенциальных угроз позволяет принимать эффективные меры по предотвращению инцидентов безопасности и минимизации ущерба от возможных атак. Необходима комплексная защита всех элементов организации, что достигается путем применения системы обнаружения и предотвращения вторжений, которая реализуется в основном благодаря Kaspersky Security Center и Cisco, но также необходимы и дополнительные функции, и сервисы, рассмотренные ранее для того, чтобы достигнуть максимального показателя безопасности.

Таким образом, модели угроз локальной сети в учреждении образования играют важную роль в обеспечении безопасности информационных ресурсов и защите конфиденциальности данных. Внедрение соответствующих политик безопасности, обучение персонала и использование современных технологий помогут обеспечить надежную защиту сетевой инфраструктуры и обеспечить безопасность данных в учреждении образования.

Эффективная защита локальной сети в университете требует постоянного внимания, ресурсов и обновления стратегий, чтобы адаптироваться к постоянно меняющимся угрозам в сфере кибербезопасности.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1–А Силич С. С. Модели угроз локальной сети в учреждении образования / Силич С. С., Шевчук О. Г. // 59–я конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 17–21 апреля 2023 г., БГУИР, Минск. – С. 53.

2–А Силич С. С. Классификация угроз, возникающих в локальной сети / Силич С. С., Шевчук О. Г. // 60–я конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 26 апреля 2024 г., БГУИР, Минск, (принята к опубликованию).