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

УДК 004.72, 004.772

Ахраменко
Дмитрий Викторович

РАЗГРАНИЧЕНИЕ ДОСТУПА В ЛОКАЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 Методы и системы защиты информации,
информационная безопасность

_____

Научный руководитель
Петров Сергей Николаевич
кандидат технических наук, доцент

_____

Минск 2018

ВВЕДЕНИЕ

Актуальность темы магистерской диссертации: проблема обеспечения защиты и разграничения доступа к информации является одной из важнейших при построении надежной сетевой информационной структуры любого предприятия. В понятие защиты данных включаются вопросы сохранения целостности данных и управления доступа к данным. Большинство систем представляют собой средство единого централизованного хранения данных. Это значительно сокращает избыточность данных, упрощает доступ к данным и позволяет более эффективно защищать данные. Однако, на практике возникает ряд проблем, связанных, например, с тем, что различные пользователи должны иметь доступ к одним данным и не иметь доступа к другим. Поэтому, не используя специальные средства и методы, обеспечить надежное разделение доступа в локальной сети практически невозможно. Большинство современных локальных сетей имеют встроенные средства, позволяющие администратору системы определять права пользователей по доступу к различным частям данных, вплоть до конкретного элемента. Поэтому вопрос о разграничении прав доступа один из основных актуальных компонентов защиты информации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Целью диссертационной работы являлось разработка рекомендаций по защите локальной сети предприятия от несанкционированного доступа сотрудников (инсайдерских атак) на основе разграничения доступа, с использованием базовых настроек имеющегося оборудования. Предлагается использование профилей доступа на основе MAC-адресов (MAC-based Access Control).

Задачи исследования:

1.Изучить протоколы доступа к сетевым ресурсам используемые в локальных сетях.

2.Проанализировать угрозы информационной безопасности локальных сетей.

3.Создать натурную модель локальной сети организации гостиничного бизнеса, включающая персональные компьютеры, модем ZTE ZXHN H208N с поддержкой функций WiFi-точки доступа и коммутатор DES-1210-52, который обеспечивал объединение указанных устройств в сеть.

4. Провести тестирование сети на проникновение. Осуществить контактное подключение к витой паре и провести пассивное исследование локальной сети с целью определения: ее топологии, используемых портов, MAC–и IP–адресов работающих устройств, списка посещенных Web-ресурсов, определение операционных систем работающих устройств. Провести атаку типа «человек по середине» (arp-spoofing, dns-spoofing, DHCP-spoofing и DoS-атака) для сбора логинов/паролей и перехвата конфиденциальной информации.

5.Разработать методику настройки сетевого оборудования с использованием коммутатора DES-1210-52 для разграничения доступа на канальном уровне.

Объект исследования: натурная модель локальной сети организации гостиничного бизнеса.

Предмет исследования: MAC, IP-адреса и параметры протоколов IEEE 802.1Q, ACL, IMPB, IEEE 802.1X, Safeguard Engine.

Апробация результатов диссертации.

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на XVI Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, Беларусь, 5 июня 2018 г.).

Опубликованность результатов диссертации.

2 печатные работы, включая 1 тезис материалов конференции и 1 статью в журнале из перечня ВАК.

Структура и объем диссертации.

Работа состоит из введения, трех глав, заключения, списка использованной литературы. Работа содержит 74 страницы основного текста, 79 рисунков. Список использованной литературы включает 40 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются объект и предмет исследования, цель и задачи.

В **первой главе** приведен обзор построения современных локальных сетей, возможных угроз, и методов разграничения доступа в локальных сетях, осуществлен обзор существующих решений, а также выбраны ключевые положения из нормативных источников и обусловлен выбор направлений деятельности при реализации методики защиты информации.

Во **второй главе** приведены результаты сетевых атак на натуральную модель локальной сети. Были получены следующие результаты: топология локальной сети, запущенные сетевые сервисы, открытые/закрытые порты, определенна операционная система, перехват трафика с получением конфиденциальной информацией (данные, а также логин и пароль), а также перенаправление на фишинговые сайты. Также проведена атака типа отказ в обслуживании, с целью выведения рабочего графика предприятия

В **третьей главе** рассмотрены механизмы защиты данных и разграничения доступа на основе протоколов: IEEE 802.1Q, ACL, IMPB, IEEE 802.1X, Safeguard Engine. Представлены результаты исследования и рекомендации по настройке сетевого оборудования коммутатора DES-1210-52.

ЗАКЛЮЧЕНИЕ

Из отчетов аналитических центров за 2017 год видно, что утечки конфиденциальной информации в 60% случаев произошли вследствие действий внутренних нарушителей. На сетевой канал пришлось 70% зафиксированных утечек, причем подавляющее число случаев компрометации носило намеренный характер. При проведении тестирования различными центрами безопасности на проникновение в локальную сеть организации, от лица внутреннего нарушителя, был получен полный контроль над ресурсами ЛВС, несмотря на используемые технические и программные средства защиты на

предприятии. Многие организации не всегда располагают денежными ресурсами на покупку лицензионного и специализированного программного обеспечения для защиты информационных активов.

В диссертационной работе были разработаны рекомендации по защите локальной сети предприятия от внутреннего нарушителя на основе разграничения доступа с использованием базовых настроек имеющегося оборудования. В качестве сетевого оборудования был выбран коммутатор DES 1210-52. Коммутатор DES 1210-52 является недорогим и распространенным на территории Республики Беларусь, он представляет собой законченное и недорогое решение для сетей малого и среднего бизнеса.

В ходе проделанной работы были настроены механизмы защиты данных и разграничения доступа на основе протоколов коммутатора DES 1210-52: IEEE 802.1Q, ACL, IMPB, IEEE 802.1X, Safeguard Engine. Разработанные рекомендации по настройкам коммутатора DES 1210-52 смогли обеспечить защиту натуральной модели от пассивных (в том числе врезки в канал) и активных атак.

Созданная методика разграничения доступа на канальном уровне может применяться в качестве базовой для настройки системы сетевой безопасности без покупки специальных средств защиты и программного обеспечения, а также позволяет разграничивать доступ пользователей в локальной сети.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Петров, С.Н. Система охранного телевидения с дополнением видеоаналитики / С.Н. Петров, Д.В. Ахраменко, С.В. Власюк // Технические средства защиты информации: Тезисы докл. К XVI Белорусско-российской научно-технической конференции – Минск, – С.108.

2. Петров, С.Н. Разграничение доступа в локальной сети с использованием базовых настроек сетевого оборудования / С.Н. Петров, Д.В. Ахраменко, С.М. Горошко, Т.А. Пулко // Системный анализ и прикладная информатика (объем 7стр., по состоянию на 1 июня 2018 проходит рецензирование).