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

УДК 004.056

Михейчик
Александр Дмитриевич

Исследование способов повышения информационной безопасности корпоративной сети связи

АВТОРЕФЕРАТ
на соискание степени магистра техники и технологии
по специальности 1-45 81 01 «Инфокоммуникационные системы и сети»

_____

Научный руководитель
Хацкевич Олег Александрович
канд. техн. наук, доцент

_____

Минск 2019

КРАТКОЕ ВВЕДЕНИЕ

Выбор темы связан с тем, что на данный момент в мире и в Республике Беларусь наблюдается повышенный интерес к обеспечению информационной безопасности государственных секретов, корпоративных сетей различных организаций, личности человека и т.п. Основная задача перед специалистами по информационной безопасности состоит в том, чтобы обеспечить невозможность злоумышленниками осуществить нарушение конфиденциальности, целостности и доступности информации.

На сегодняшний день современные инфокоммуникационные технологии сумели оказать существенное влияние почти на каждую ключевую сферу жизнедеятельности человека, включая государства, различные организации и т.п. В то же время, параллельно с развитием инфокоммуникационных технологий развиваются новые угрозы, которые направлены как на личность, так и на государственные органы, организации. В качестве существенных угроз можно выделить:

– проведение атак на защищенные системы киберзлоумышленниками;

– использование новейших информационных технологий, с помощью которых злоумышленники могут осуществить государственные кибервойны.

В последнее время активно начали развиваться и внедряться злоумышленниками новые, более сложные сетевые атаки, задача которых заключается в осуществлении дестабилизации работы определенных корпоративных сетей организаций. В настоящий момент можно выделить следующие инструменты, используемые злоумышленниками, для проведения хакерских атак: DDoS-атаки, фишинг, вирусные программы, снифферы, спуфинги, руткиты, инъекции и т.п.

Многие специалисты рекомендуют использовать следующие средства для обеспечения безопасности в корпоративной сети: системы обнаружения и предотвращения вторжений, антивирусные программы, межсетевые экраны, системы обнаружения и предотвращения утечек информации.

Актуальность данной магистерской диссертации заключается в том, что с помощью использования различных способов, связанных с информационной безопасностью, можно максимально повысить защищенность корпоративной сети связи.

Объектом исследования работы является корпоративная сеть связи. Предметом исследования диссертационной работы является нахождения способов и методов для осуществления повышения информационной безопасности корпоративной сети.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Работа выполнялась по теме: «Исследование способов повышения информационной безопасности корпоративной сети связи».

Проведенная работа по диссертационной тематике соответствует мировым тенденциям в области обеспечения информационной безопасности в сетях связи. Рассмотренные средства защиты информации позволяют осуществить повышение защищенности корпоративной сети связи.

Целью диссертации являлось исследование способов, направленных на повышение информационной безопасности корпоративной сети связи, а также на практике продемонстрировать эффективность исследуемых способов.

Для достижения цели были решены следующие задачи:

– проведен обзор литературы и описаны основные сетевые атаки, направленные на корпоративную сеть связи;

– осуществлено исследование и проанализированы традиционные средства защиты информации согласно белорусским стандартам;

– исследованы дополнительные средства защиты информации, а также на практике доказана эффективность данных средств;

– разработана защищенная корпоративная сеть связи с помощью исследуемых способов повышения информационной безопасности.

Научная новизна темы данной магистерской диссертации заключается в том, что результаты практического применения исследуемых способов, направленных на защиту информации, позволяют доказать их эффективность для повышения информационной безопасности.

Основные положения и результаты магистерской работы докладывались и обсуждались на 54-й научной конференции аспирантов, магистрантов и студентов; XVI Белорусско-российской научно-технической конференции «Технические средства защиты информации»; международном научно-техническом семинаре «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных».

Основные результаты и положения диссертации, выносимые на защиту, разработаны и получены лично автором. Соавтором опубликованных работ являлся научный руководитель канд. техн. наук, доцент О.А. Хацкевич, вклад которого связан с определением цели и задач исследований, выбором методов исследований, интерпретацией и обобщением результатов.

КРАТКОЕ СОДЕРЖАНИЕ

Во введение рассматривается проблема информационной безопасности в современном мире, обосновывается актуальность выбранной темы диссертационной работы, дается краткая характеристика ее разработанности, определяются объект и предмет исследования.

В общей характеристике работы сформирована цель, научная новизна, практическая ценность данной диссертационной работы, а также основные задачи, используемые для достижения поставленной цели.

Первая глава «Обзор основных сетевых атак на корпоративные сети» включает в себя исследование международной и национальной литературы по информационной безопасности, а также дается краткая характеристика об известных на сегодняшний день сетевых атаках. Первая глава состоит из группы подразделов.

В подразделах первой главы осуществляется анализ основных международных и национальных источников, связанных с защитой информацией. Рассматриваются и описываются известные сетевые атаки: переполнение буфера, использование специализированных программ (вирусов, снифферов, троянских коней, почтовых червей, rootkit-ов и т.д.), IP-спуфинг, man-in-the-middle, инъекция (SQL-инъекция, PHP-инъекция, межсайтовый скриптинг, XPath-инъекция), отказ в обслуживании, phishing-атаки. В конце даются основные выводы по первой главе.

Вторая глава «Оценка традиционных средств защиты информации» описывает основные средства, предназначенные для обеспечения безопасности корпоративной сети, согласно белорусским стандартам. Вторая глава состоит из группы подразделов.

В подразделах второй главы проводится анализ следующих средств защиты информации: межсетевые экраны, система обнаружения и предотвращения утечек информации, система обнаружения и предотвращения вторжений, антивирусные программы. В конце даются недостатки представленных средств, а также выводы по второй главе.

Третья глава «Способы повышения информационной безопасности сети» включает в себя несколько подразделов, в которых описываются предлагаемые способы повышения информационной безопасности корпоративной сети, на практике демонстрируется и доказывается их эффективность для дальнейшего использования. В конце даются основные выводы по третьей главе.

Четвертая глава «Разработка защищенной корпоративной сети» состоит из нескольких подразделов, в которых осуществляется анализ выбора программных и программно-аппаратных средств, служащих для обеспечения

информационной безопасности. Разрабатывается защищенная корпоративная сеть связи с использованием выбранного оборудования и программ. В конце даются основные выводы по четвертой главе.

ЗАКЛЮЧЕНИЕ

По результатам данной работы были выбраны средства безопасности, с помощью которых можно осуществить повышение информационной безопасности корпоративной сети. Рассмотрены основные международные и национальные источники литературы по безопасности, а также подробно рассмотрены сетевые атаки на корпоративные сети. Были исследованы традиционные средства безопасности, согласно белорусским стандартам, а также показаны недостатки данных средств. На практике доказана эффективность использования дополнительных программных и программно-аппаратных средств защиты информации для повышения информационной безопасности сети. Проведено исследование и выбор средств по информационной безопасности, используя которые была разработана защищенная корпоративная сеть связи.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Михейчик, А.Д. Повышение информационной безопасности с помощью сканера уязвимостей / А.Д. Михейчик // Инфокоммуникации : материалы 54-й научной конференции аспирантов, магистрантов и студентов, Минск, 23–27 апреля 2018 г. – Минск : БГУИР, 2018. – С. 137.

2–А. Михейчик, А.Д. Использование межсетевого экрана нового поколения в корпоративных сетях / А.Д. Михейчик, О.А. Хацкевич // Технические средства защиты информации : тезисы докладов XVI Белорусско-российской научно – технической конференции, Минск, 5 июня 2018 г. – Минск : БГУИР, 2018. – С. 65.

3–А. Михейчик, А.Д. Оценка безопасности сети с помощью online-пентестов / А.Д. Михейчик // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных : материалы международного научно-технического семинара (Минск, ноябрь – декабрь 2018 г.) – Минск : БГУИР, 2018. – С. 86-89.