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

УДК 004.056

Зябкин
Дмитрий Михайлович

Защита информации в IP-сетях

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии

по специальности 1-45 81 01 Инфокоммуникационные системы и сети

Научный руководитель

Астровский Иван Иванович

кандидат технических наук, доцент

Минск 2018

КРАТКОЕ ВВЕДЕНИЕ

Целью диссертации является повышение эффективности информационной безопасности информационных систем предприятия ТЭЦ-2.

В 21 веке важной ценностью на планете считается информация. Все больше и больше информации переводится в электронный формат, широко используются электронные платежи, хранение документов, личные данные человека и т.д.. Понятие информации неразрывно связано с компьютерными технологиями, системами и сетями связи, становится очевидной важность вопроса защиты информации в них. Особенно актуально стоит этот вопрос в области передачи и хранения секретной информации государства и частной коммерческой информации.

В бизнесе добросовестная конкуренция предполагает соперничество, основанное на соблюдении законодательства и общепризнанных норм морали. Однако нередко предприниматели, конкурируя между собой, стремятся с помощью противоправных действий получить информацию в ущерб интересам другой стороны и использовать ее для достижения преимущества на рынке. Криминализация общества и недостаточная эффективность государственной системы охраны правопорядка заставляет представителей бизнеса самим принимать меры для адекватного противостояния имеющим место негативным процессам, наносящим ущерб конфиденциальной информации фирмы.

Причин активизации компьютерных преступлений и связанных с ними финансовых потерь достаточно много, существенными из них являются:

– переход от традиционной «бумажной» технологии хранения и передачи сведений на электронную и недостаточное при этом развитие технологии защиты информации в таких технологиях;

– объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам;

– увеличение сложности программных средств.

В последнее время в современных обзорах по информационной безопасности прослеживается тенденция к увеличению количества нарушений

в области компьютерных преступлений. Учитывая разнообразие угроз и сложность современных сетей, реализация решения для защиты требует глубоких знаний и опыта в целом ряде узкоспециализированных дисциплин. В число распространенных угроз входит умышленное использование опасного программного кода (вирусов, червей, троянских программ), а также атаки типа DoS (отказ в обслуживании).

Данная диссертация посвящена решению задач безопасности предприятия.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

Актуальность темы состоит:

– в разработке политики безопасности предприятия в условиях информационной борьбы;

– в глубокой проработке и решении ряда важных проблем, направленных на повышение информационной безопасности в IP-сетях.

Проблемы защиты информации в IP-сетях постоянно находятся в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей. Под защитой информации понимается использование специальных средств, методов и мероприятий с целью предотвращения утери информации, находящейся в IP-сети.

К основным характеристикам корпоративной сети относятся:

– сеть объединяет в структурированную и управляемую замкнутую систему все принадлежащие компании информационные устройства: отдельные компьютеры и локальные вычислительные сети (LAN), хост-серверы, рабочие станции, телефоны, факсы;

– в сети обеспечивается надежность ее функционирования и мощные системы защиты информации. То есть, гарантируется безотказная работа

системы как при ошибках персонала, так и в случае попытки несанкционированного доступа.

В современных условиях быстрое наращивание объемов бизнеса компании приводит к тому, что инфраструктура предприятий представляет собой множество разнородных систем. Это делает актуальной задачу по переходу на унифицированные коммуникации.

IP-сеть, отвечающая современным стандартам безопасности, позволяет получать доступ к необходимой информации, обеспечивает защиту от несанкционированного доступа к данным, обеспечивая в офисе стабильное информационное взаимодействие.

Цель работы

Целью диссертации является теоретическое и практическое исследование методов и способов повышения эффективности безопасности информационных систем предприятия ТЭЦ-2.

Задачи исследования

Для достижения поставленной цели сформулированы следующие задачи:

1. Провести анализ возможных информационных угроз предприятия, с выявлением наиболее опасных.
2. Рассмотрение существующих средств и методов защиты информации в IP-сети.
3. Разработка и проектирование комплекса мероприятий по защите информации в IP-сети.
4. Провести анализ эффективности реализации политики безопасности в сети предприятия.

Метод исследования

В работе использовался комплексный метод защиты информации: защита от несанкционированного доступа и защита каналов связи с помощью комплекта протоколов IPsec.

Первым этапом является разработка алгоритма функционирования системы Secret Net от несанкционированного доступа. Затем следует организация защиты каналов связи, посредством комплекта протоколов IPsec.

Вторым этапом является моделирование IP-сети предприятия с использованием межсетевых экранов.

Третий этап. Расчет рисков информационной безопасности в программном продукте Mathcad версии 15.

Затем производится анализ полученных данных, обобщение полученных результатов и разработка рекомендаций.

Научная новизна результатов работы

Наиболее значимые новые научные результаты работы:

Предложена упрощенная и более эффективная методика и система комплексной защиты информации в IP-сети предприятия. Разработан алгоритм функционирования программного продукта Secret Net.

Достоверность полученных результатов

Исходные данные для научных исследований были получены из чертежей организационной и структурной схемы сети предприятия ТЭЦ-2. Расчет рисков информационной безопасности производился в программном продукте Mathcad версии 15 и внедряется на предприятии.

Практическая ценность результатов работы

Ценность результатов работы заключается в том, что полученные расчеты рисков информационной безопасности позволяют проанализировать и оценить как слабые так и сильные стороны имеющейся политики безопасности. Был предложен алгоритм функционирования системы Secret Net для защиты от несанкционированного доступа и защита каналов связи с помощью комплекта протоколов IPsec. Разработана новая модель сети предприятия в программе GNS-3. Эти мероприятия позволяют усовершенствовать комплексную систему

защиты информации предприятия ТЭЦ-2.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **Введении** дается краткая характеристика работы, обоснована актуальность темы диссертации, сформулированы ее цель и задачи, практическая значимость, научная новизна и основные этапы исследований.

В **1-ом разделе** произведен анализ потенциальных угроз информации в IP-сетях. Описаны основные цели и модели информационной безопасности. Способы и методы защиты информации в IP-сетях.

Во **2-ом разделе** представлена структурная схема сети ТЭЦ-2. Спроектирована организационная структура предприятия в программе Busines Studio. Разработан алгоритм защиты от несанкционированного доступа системы Secret Net. Представлены основные технические характеристики оборудования. Произведена оценка рисков информационной безопасности для сети ТЭЦ-2.

В **3-ем разделе** описаны средства защиты предприятия. Методы информационной защиты IP-сети. Защита каналов связи с помощью комплекта протоколов IPsec. Оценка протокола Ipsec.

В **4-ом разделе** предложена организация защиты информационной системы предприятия. Рассмотрены и рекомендованы к использованию политики безопасности. Модель сети предприятия с использованием межсетевых экранов в GNS-3, использование прокси-серверов и антивирусных программ для защиты информации.

В **Заключении** диссертации сформулированы основные результаты выполненной работы.

ЗАКЛЮЧЕНИЕ

В ближайшее время прогресс в области развития средств вычислительной техники, программного обеспечения и сетевых технологий даст толчок к

развитию средств обеспечения безопасности, что потребует во многом пересмотреть существующую научную парадигму информационной безопасности. Основными положениями нового взгляда на безопасность должны являться:

– исследование и анализ причин нарушения безопасности компьютерных систем;

– разработка эффективных моделей безопасности, адекватных современной степени развития программных и аппаратных средств, а также возможностям злоумышленников и разрушающих программных средств;

– создание методов и средств корректного внедрения моделей безопасности в существующие вычислительные системы с возможностью гибкого управления и надлежащей безопасностью в зависимости от выдвигаемых требований, допустимого риска и расхода ресурсов;

– необходимость разработки средств анализа безопасности компьютерных систем с помощью осуществления тестовых воздействий (атак).

Широкая информатизация общества, внедрение компьютерной технологии в сферу управления объектами государственного значения, стремительный рост темпов научно-технического прогресса, наряду с положительными достижениями в информационных технологиях, создают реальные предпосылки для утечки конфиденциальной информации.

В диссертации, основной целью которой являлось разработка общих рекомендаций по защите информации в сети ТЭЦ-2, получены следующие результаты:

– рассмотрены основные пути защиты от несанкционированного доступа к информации, циркулирующей в системах обработки данных;

– произведена классификация способов и средств защиты информации;

– осуществлен анализ методов защиты информации в IP-сетях;

– рассмотрены основные направления защиты информации в IP-сети;

– разработана концепция безопасности сети ТЭЦ-2 и вопросы обеспечения безопасности при групповой обработке данных в службах и подразделениях предприятия;

– осуществлена выработка политики безопасности ТЭЦ-2;

– рассмотрен порядок управления доступом к информации в IP-сети и способы повышения безопасности и защиты данных.

Помимо этого представленные методы и средства защиты информации позволяют выявить слабые места в существующей системе защиты информации предприятия, на основе которых есть возможность произвести модернизацию защиты информации в IP-сети.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1 – А. 54-я научная конференция аспирантов, магистрантов и студентов УО «БГУИР» под темой «Защита информации в IP-сетях».

2 – А. QR-алгоритм для вычисления обобщенных собственных значений матриц коэффициентов ковариации/ Материалы международного научно-технического семинара. Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных (Минск, апрель-декабрь 2017г.)/ Борискевич И.А., Аль Хашими А.Э., Наиф М.Н., Зябкин Д.М., Щерба Д.С.