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

УДК 004.056:004.7

Могилевчик
Ян Леонидович

Система обеспечения информационной безопасности корпоративной сети ООО "Открытый контакт"

АВТОРЕФЕРАТ

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

_____

Научный руководитель
Охрименко Алексей Александрович
кандидат технических наук, доцент

_____

Минск 2018

ВВЕДЕНИЕ

На сегодняшний день довольно сложно представить какую-либо организацию, которая не владеет существенными информационными активами. В большинстве случаев функционирование определенной организации полностью зависит от сохранности информации, имеющейся у нее.

Информация компании может существовать в разных формах. Она может быть размещена на бумажном носителе, отправлена через почтовое отделение или по электронной почте, может храниться на электронных носителях или демонстрироваться с пленки, а также передаваться при разговоре. Независимо от формы существования информации, способа ее обработки или хранения она, как и все другие важные для организации активы, должна быть соответствующим образом защищена. Для этого и предназначена информационная безопасность.

Для обеспечения безопасности информационных систем и сетей организациям предстоит противостоять большому числу источников угроз безопасности: компьютерное мошенничество, шпионаж, саботаж, вандализм и прочие угрозы. Источники ущерба, такие как атаки хакеров и атаки, вызывающие отказ в обслуживании, становятся более распространенными и более изощренными. Зависимость организации от информационных систем и сервисов подразумевает, что организация становится более уязвимой по отношению к угрозам безопасности. Соединение открытых и локальных сетей, распределение информационных ресурсов увеличивают трудность управления доступом. Тенденция к распределенному применению компьютеров ослабляет эффективность централизованного и специального управления.

Информационная безопасность может быть достигнута применением различных средств управления: политики, действия, процедуры, организационной структуры, программных средств. Эти средства управления должны гарантировать, что задачи безопасности организации решены. Однако следует учитывать, что проблема обеспечения информационной безопасности носит комплексный характер, поэтому для ее решения необходимо сочетание законодательных, административных, организационных и программно-технических мер.

Объектом защиты является крупная компания с реализованной компьютерной сетью. Компьютерная сеть компании охватывает главный офис и все филиалы, размещенные в различных офисах города. Для связи между всеми офисами компания использует выделенные линии. Так как компания является крупной, то все коммутационное оборудование располагается на ее

территории, а не у провайдера, предоставляющего выделенные линии. Компьютерные сети главного офиса и всех филиалов представляют собой иерархические сети, в которых реализован уровень доступа, уровень распределения и центральный уровень (уровень ядра). На уровне доступа располагаются рабочие станции пользователей, сетевые принтеры, локальные серверы, а также коммутационное оборудование первого уровня (коммутаторы). На уровне распределения используются коммутаторы и маршрутизаторы со средней производительностью. На уровне ядра используются мощные, высокоскоростные коммутаторы и маршрутизаторы.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы магистерской диссертации обусловлена повсеместным развитием информационных технологий, ростом количества корпоративных сетей и необходимостью обеспечивать должную защиту информационным активам данных сетей. Корпоративные системы, приложения и данные становятся доступными из сети Интернет, вследствие чего компании сталкиваются с возрастающим числом угроз для своей информационной инфраструктуры.

Технологии глобальных сетей вышли на новый уровень, когда скорости обмена данными в сетях достигли больших величин, особое распространение получили корпоративные сети, которые изначально упрощают ведение бизнеса и способствуют развитию науки. Информация и другие важные для организации активы, должны быть соответствующим образом защищены. Для решения этой задачи и предназначена система обеспечения информационной безопасности корпоративной сети.

Для достижения поставленной цели в этой диссертации поставлены и решены следующие задачи:

1) проведен анализ основных угроз, представляющих опасность для безопасности корпоративной сети;
2) выявлены основные угрозы информационной безопасности корпоративной сети;
3) разработаны и проанализированы сервисы, противостоящие угрозам безопасности;
4) разработана политика безопасности.

Положения, выносимые на защиту: программно-аппаратный комплекс защиты информации в корпоративной сети предприятия.

Теоретическая значимость работы заключается в поиске и анализе новых программно-аппаратных средств защиты информации.

Практическая ценность работы заключается в разработке технических решений (механизмов и сервисов безопасности), которые обеспечивают информационную безопасность корпоративной сети.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении приведен краткий исторический очерк, определено место проблемы обеспечения информационной безопасности в корпоративных сетях. Обосновывается актуальность выбранной темы, определяются объект и предмет исследования, цель и задачи.

В первой главе рассматриваются основные положения относительно информационной безопасности в корпоративных сетях предприятий. Выявлено, что эффективность бизнеса компании напрямую зависит от качества и оперативности управления бизнес-процессами, которые сильно зависят от стабильной работы корпоративной сети передачи данных. Определены общие требования, предъявляемые к элементам корпоративной информационной системе. Так же в главе дана характеристика объекта защиты.

Во второй главе предложены политики безопасности объекта. Эти политики определяет цели и принципы обеспечения информационной безопасности, а так же гарантируют должный уровень безопасности при их соблюдении. Были определены основные положения, касающиеся резервного копирования информации, правил использования паролей, требований к физической защите оборудования, правил пользования сетью Интернет, правил протоколов маршрутизации.

В третьей главе рассматриваются основные технические решения для обеспечения информационной безопасности сети. Наиболее важным в вопросе безопасности в сети является уровень доступа. Без применения механизмов обеспечения безопасности на данном уровне сети многочисленные затраты на защиту уровня распределения, центрального уровня, магистральных каналов будут потрачены впустую. На уровне доступа рассматриваются безопасность рабочих станций пользователей, локальных серверов, сетевых принтеров и беспроводного оборудования. Предложены механизмы обеспечения безопасности всей сети от нежелательного трафика. Для защиты всей сети от нежелательного трафика необходимо использовать аппаратные межсетевые экраны. Межсетевой экран ограничивает виды трафика, пересылка которого разрешена, а также определяет способы обработки трафика. Списки контроля доступа в межсетевых экранах указывают, какие виды трафика следует пересылать или блокировать.

В главе рассмотрены системы обнаружения и предотвращения вторжений, описаны компоненты протокола управления сетью, решена проблема с организацией безопасного удаленного доступа к корпоративной сети. Были оценены риски, связанные с атаками DDoS, а так же предложены пути решения проблем с распределенными атаками класса «отказ в

обслуживании». В ходе испытаний было установлено, что принятые технические решения и политики безопасности полностью удовлетворяют всем функциональным и гарантийным требованиям безопасности, предъявляемым к объекту защиты. Созданная политика и принятые на ее основе решения обеспечивает безопасность в каждой функциональной области корпоративной сети.

В четвертой главе приводятся основные параметры настроек сервисов безопасности. Дан листинг настроек механизма AAA, используемый в сервере Tacacs+, сконфигурированы списки контроля доступа. Показан механизм борьбы со стороны клиента и со стороны поставщика услуг таких атак как «черные дыры».

ЗАКЛЮЧЕНИЕ

В ходе выполнения диссертации была разработана система обеспечения информационной безопасности корпоративной сети компании.

На основании этой работы были определены технические решения (механизмы и сервисы безопасности) для обеспечения информационной безопасности корпоративной сети. В качестве основного решения была использована архитектура Cisco SAFE для безопасности корпоративных сетей. Также были выбраны механизмы для борьбы с DDoS атаками, которые представляют наибольшую угрозу для корпоративных сетей.

Определены показатели эффективности проекта и показано, что разработка политики информационной безопасности корпоративной сети является экономически полностью обоснованной.

Результатами испытаний разработанной политики безопасности для данного объекта оценки подтверждено, что она обеспечивает целостность доступность и конфиденциальность данных, а также их полноту и актуальность. Также разработанная политика обеспечивает уровень безопасности, соответствующий нормативным документам.

В ходе испытаний было установлено, что принятые решения полностью удовлетворяют всем функциональным и гарантийным требованиям безопасности, предъявляемым к объекту защиты.

Проект является экономически целесообразным, так как расходы на защиту не превышают четверть от предполагаемого ущерба от нарушения информационной безопасности.

Созданная политика и принятые на ее основе решения обеспечивает безопасность в каждой функциональной области корпоративной сети.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1 – Могилевчик, Я. Л. Система обеспечения информационной безопасности корпоративной сети компании ООО «Открытый контакт» / Я. Л. Могилевчик // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп. заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 68–81.

2 – Могилевчик, Я. Л. Аудит информационной безопасности в компьютерной сети небольшого предприятия / Я. Л. Могилевчик // Тезисы докладов XV Белор.-российск. НТК (Минск, 6 июня 2017 г.). – Минск: БГУИР, 2017. – 116 с.– С. 21.