

Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И
РАДИОЭЛЕКТРОНИКИ

УДК 004.056.53(476)

Антонников
Артур Алексеевич

Защита речевой информации передаваемой по телефонной сети предприятия с
применением технологии VPN

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 2016

Библиотека БГУИР

Нормоконтроль

Борботько Тимофей Валентинович

КРАТКОЕ ВВЕДЕНИЕ

В наше время мы можем наблюдать весьма бурное развитие организаций и предприятий имеющих территориально-распределенные корпоративные вычислительные сети. Данная тенденция обусловлена децентрализацией различных подразделений и структур организаций, зачастую находящихся в рамках различных стран. Иными словами, бизнес стремится к территориально-разнесенной структуре по ряду технических причин, связанных с экономической эффективностью

Столь быстрое развитие Интернет сети открыло новые возможности в организации территориально-распределенных корпоративных вычислительных сетей. В свою очередь, такой ход вещей, породил новую тенденцию—организация сети стала более доступной и значительно дешевле.

Важнейшим критерием по организации интернет телефонии и полноценной территориально-распределенной сети с защитой аутентификацией и шифрованием (пакетной передачи информации) на базе существующей распределенной ЛВС является низкий бюджет внедренческих и постоянных затрат, связанных с телефонными переговорами.

Однако такое заманчивое и дешевое решение — передача корпоративных данных, в частности речевой информации (аналоги skype, Viber и т.д.), через публичную сеть, например, Интернет, часто представляет угрозу для безопасности предприятия.

Для решения этих проблем может быть использована технология виртуальных частных сетей VPN (Virtual Private Network). Эта технология позволяет превратить соединения в пакетных сетях общего пользования в защищенные каналы с гарантированной полосой пропускания, обеспечивая безопасность и широкий спектр сервисов при приемлемой стоимости устанавливаемых соединений. Поэтому данная технология востребована многими предприятиями и организациями, не имеющими собственных сетевых ресурсов, прежде всего ввиду ее экономичности, доступности и безопасности. Конкретная реализация VPN-технологии осуществлялась на примере организации ООО «Седьмая степень» имеющая распределенную структуру, филиалы и подразделения которой находятся за пределами РБ. Основными критериями выбора протоколов и технических средств реализации данного решения являлась дешевизна, крайне высокий уровень защищенности, гибкость настройки. В этой связи выбор пал на программный продукт с открытым исходным кодом под названием «OPENVPN».

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью данной магистерской работы является расширение профессиональных знаний, полученных в процессе обучения в магистратуре, формирования практических умений и навыков ведения самостоятельной научной работы и исследования. Для этого необходимо разработать методику обнаружения угроз IP-телефонии на примере компании ООО «Седьмая степень».

Основными задачами являются:

- 1 Определение наиболее важных факторов, влияющих на обнаружение и идентификацию угроз распределенной ЛВС с интеграцией IP-PBX;
- 2 Анализ исходной защищенности речевого трафика на ООО «Седьмая степень»;
- 3 Выбор и анализ существующих средств защиты голосового трафика для ООО «Седьмая степень».
- 4 Внедрение оптимальной системы защиты голосового трафика

Тема является актуальной, так как распределенные сети являются приоритетным направлением в современных бизнес-процессах.

Информатизация хозяйственной деятельности способствует её облегчению, интенсификации и, как следствие, повышению экономической эффективности. Но наряду с передачей, обработкой и хранением информации, важно обеспечить её целостность, конфиденциальность и доступность. Исключить как внешние, так и внутренние угрозы.

Личным вкладом автора является разработка способа защиты системы IP-телефонии для ООО «Седьмая степень»

Результаты работы были апробированы на XX Международной научно-технической конференции «Современные средства связи» в БГАС докладом в секции «Информационные технологии и защита информации» на тему «Обработка трафика колл-центра на основе офисной IP телефонной станции».

КРАТКОЕ СОДЕРЖАНИЕ

В первой главе и во введении была рассмотрена актуальность задачи обеспечения защиты речевой информации компании в условиях децентрализации ее структурных подразделений.

Во второй главе приведено описание структуры распределенной сети компании ООО «Седьмая степень». Был определен основной список угроз интернет-телефонии.

В третьей главе проведен анализ эффективности различных способов защиты голосового трафика. Предложен оптимальный с точки зрения затрат и удобства внедрения вариант защиты.

Сделаны выводы о том, что проблему защиты речевого трафика можно свести к организации VPN-сети.

Показано, что угрозы VOIP подразумевает различные угрозы. Защита (противодействие) во многом будет зависеть от вида угрозы.

Рассмотрены существующие методы обнаружения и противодействия атакам на IP-телефонию:

- 1 Протоколы реализующие защиту сигнальной информации речевого трафика;
- 2 Протоколы реализующие защиту речевой информации;
- 3 Обеспечение системы безопасности как комплекса программно-аппаратных средств для IP-PBX системы (технические мероприятия).

Сделан вывод о комплексности подхода к минимизации вероятности нанесения ущерба от атак на IP-телефонию.

На основе выявленных недостатков, разработана усовершенствованная система (использование программного комплекса OPENVPN) нейтрализация атак для ООО «Седьмая степень».

ЗАКЛЮЧЕНИЕ

В данной магистерской диссертации разработана методика нейтрализация атак и снижение рисков угроз, связанных с системой IP-телефонии для ООО «Седьмая степень».

В рамках поставленной цели, были выполнены все задачи в полном объеме.

Показана актуальность проблемы на конкретных примерах. Проанализированы в полном объеме все актуальные угрозы и способы защиты IP-телефонии.

Сделаны выводы о том, что угрозы бывают разные и что четкой классификации угроз IP-телефонии нет.

Показано, что защита речевой информации в сети с пакетной коммутацией сводится к защите трафика как такового. Защита (противодействие) во многом будет зависеть от самой структуры сети.

Рассмотрены способы противодействия и защиты угрозам передачи речи.

Отмечено, что можно применять отдельные средства защиты для каждого сегмента передачи речевой информации, а также, что можно воспользоваться программными комплексами, подразумевающими централизованное управление сетью. Рассмотрены виды таких средств защиты.

Рассмотрены существующие методы защиты и противодействия атакам на IP-телефонию:

- 1 Протоколы реализующие защиту сигнальной информации речевого трафика;
- 2 Протоколы реализующие защиту речевой информации;
- 3 Обеспечение системы безопасности как комплекса программно-аппаратных средств для IP-PBX системы (технические мероприятия).

Конкретно для РУП «Минскэнерго» проанализирована распределенная сеть, проведено внедрение системы защиты сети путем конфигурирования программного продукта OPENVPN.

Проанализирована исходная информационная защищенность, в контексте передачи речи, конкретно на ООО «Седьмая степень». Для предприятия выявлены возможные источники угроз, проанализированы вероятности возникновения этих угроз и их опасность, оценена актуальность обеспечения защиты.

К актуальным отнесены:

- перехват данных;
- отказ в обслуживании;
- подмена номера;
- кража сервисов;
- неожиданные вызовы;
- несанкционированное изменение конфигурации;
- мошенничество со счетом.

На основе выявленных недостатков, разработана усовершенствованная реализация туннелирования и защиты голосового трафика ООО «Седьмая степень».

Выполнены следующие мероприятия:

- 1 Выработаны рекомендации по разработке структуры сети отвечающие требованиям безопасности;
- 2 Доработано логическое разграничение филиалов сети;
- 3 Осуществлена настройка оборудования и защита стандартными средствами;
- 4 Осуществлена разработка

Предлагаемые решения должны обеспечить приемлемый уровень защиты IP-телефонии ООО «Седьмая степень».

Теоретическая значимость данной работы заключается в изучении различных вариантов реализации защиты голосового трафика с помощью VPN. Предложен оптимальный вариант реализации с точки зрения финансовых затрат и удобства внедрения.

Практическая значимость данной работы заключается в возможности реализации на объекте исследования – ООО «Седьмая степень».

Данная работа может быть полезна специалистам занимающимся защитой информации на предприятиях, так как демонстрирует методику защиты в конкретных условиях.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Антонников А.А., Петров С.Н. Применение VPN технологии для защиты речевой информации в сетях VOIP / А.А. Антонников // Технические средства защиты информации: тезисы докладов XII Белорусско-российской науч.-техн. конф., 4–5 мая 2015 года, Минск, Респ. Беларусь; – Минск: БГУИР, 2015. – с. 40

2-А. Антонников А.А., Петров С.Н. Защита голосового трафика на базе разветвленной сети предприятия ООО «Седьмая степень» с использованием программного продукта OPENVPN/ А.А. Антонников // Технические средства защиты информации: тезисы докладов XII Белорусско-российской науч.-техн. конф., 4–5 мая 2015 года, Минск, Респ. Беларусь; – Минск: БГУИР, 2015. – с. 85

3-А. Антонников А.А., Петров С.Н., Власюк С.В., Пулко Т.А. Обработка трафика колл-центра на основе офисной IP телефонной станции / Антонников А.А. // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы международного научно-технического семинара., декабрь 2015 года, Минск, Респ. Беларусь; – Минск: БГУИР, 2015. – с. 82-86