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

УДК 004.773

Перцев
Игорь Юрьевич

Анализ и разработка средств защиты почтовых сообщений

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности 1-40 80 05 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Ярмолик В.Н.
д.т.н., доцент

Минск 2016

КРАТКОЕ ВВЕДЕНИЕ

В двадцать первом веке движущей силой и главным объектом всех отраслей человеческой деятельности становится информация. По мнению некоторых экспертов, информация – главная международная валюта. Новые технологии, стремительно развивающиеся технологии вызывают изменения в общественной жизни, в профессиональной и иных видах деятельности. Однако вместе с колоссальным ростом популярности сети Интернет, возникает беспрецедентная угроза разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т.д., которые передаются посредством сети Интернет.

На сегодняшний день к сети Интернет подключены миллионы различных устройств, существуют миллионы ресурсов, которые могут быть использованы в глобальном масштабе. С развитием Интернета развиваются и возможности нанесения вреда ресурсам в сети Интернет. К сожалению, современные, даже сложные сетевые технологии достаточно уязвимы для целенаправленных атак. Причем такие атаки могут производиться удаленно, в том числе и из-за пределов национальных границ. Все это ставит новые проблемы перед разработчиками и строителями информационной инфраструктуры.

Некоторые современные формы бизнеса полностью базируются на сетевых технологиях (электронная торговля, IP-телефония, сетевое провайдерство и т.д.) и по этой причине особенно уязвимы. В 2009 году встала проблема унификации методики названия различных видов вредоносных кодов, так как возникла необходимость обмена данными и предотвращения атак в рамках международного сообщества. В современной машине вредоносные коды могут находиться не только на дисках или в оперативной памяти, на флэшках или CD, но и в чипах управления внешних устройств, в BIOS и т.д.

Электронной почтой пользуются не только для общения с людьми, но также и для передачи конфиденциальной и дорогой информации. Бухгалтерские данные, договоры и прочие документы передаются по электронной почте между компаниями и в пределах одной фирмы. При этом пользователи не задумываются о том, насколько данная информация защищена и аутентична. Такая информация ввиду своей важности должна быть максимально защищена не только от несанкционированного изменения, но в том числе и от несанкционированного доступа. Для обеспечения безопасности информации в электронной почте используются различные криптографические методы.

Основной целью данной работы является анализ и разработка программных средств защиты почтовых сообщений.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является анализ и разработка алгоритмов защиты почтовых сообщений.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Определить границы применимости ОС семейства Windows для решения поставленной задачи.
2. Разработать архитектуру программного средства защиты почтовых сообщений, работающего под управлением многозадачной операционной системы.
3. Разработать методы и алгоритмы защиты почтовых сообщений в реальном времени.
4. Разработать методы и алгоритмы распределения ключей шифрования для защиты почтовых сообщений в реальном времени.
5. Провести экспериментальные исследования разработанной системы.

Объектом исследования являются почтовые сообщения, атаки на них и способы защиты от атак.

Предметом исследования является математические и программные алгоритмы для решения задач защиты почтовых сообщений, методы и алгоритмы распределения ключей шифрования.

Основной *гипотезой*, положенной в основу диссертационной работы, является возможность использования компьютеров общего назначения с ОС Windows для решения задач защиты почтовых сообщений от несанкционированного доступа в режиме реального времени, а также задачи распределения ключей шифрования между адресатами почтовых сообщений.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Работа выполнялась в соответствии научно-техническими заданиями и планами работ кафедры «Программное обеспечение информационных технологий».

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя В. Н. Ярмолика, заключается в формулировке целей и задач исследования.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались и обсуждались на 50-ой научной конференции аспирантов, магистрантов и

студентов БГУИР. Также были опубликованы 2 статьи в научно-методическом журнале “Наука, образование и культура”.

Опубликованность результатов диссертации

По теме диссертации опубликовано 3 печатных работ, из них 2 статьи в рецензируемом издании, 1 работа в сборниках трудов и материалов международных конференций.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, пяти глав, заключения, списка использованных источников и списка публикаций автора. В первой главе представлен анализ предметной области, выявлены основные существующие атаки в сети Интернет. Вторая глава посвящена обзору способов защиты от угроз, перечисленных в первой главе. В третьей главе рассмотрены примеры программных средств, обеспечивающих защиту почтовых сообщений, проведен анализ их преимуществ и недостатков. В четвертой главе рассмотрены методы реализации защищенной сети передачи данных, а также предложена практическая реализация ПО для защиты почтовых сообщений. В пятой главе представлены результаты экспериментальных исследований оценок скорости работы предложенных методик.

Общий объем работы составляет 71 страница, из которых основного текста – 41 страницf, 34 рисунка на 26 страницах, 1 таблица на 1 страницах и список использованных источников из 37 наименований на 3 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во **введении** определена область и указаны основные направления исследования, показана актуальность темы диссертационной работы, дана краткая характеристика исследуемых вопросов, обозначена практическая ценность работы.

В **первой главе** проведен анализ наиболее распространенных атак, применяемых в сети Интернет на почтовые протоколы и протоколы передачи данных. Данная область является постоянно развивающейся, так как идет постоянное соперничество между злоумышленниками и организациями, обеспечивающими безопасность данных. Несмотря на возможное применение комплексных мер по защите компьютера, наиболее надежным способом защиты компьютера является использование проверенных электронных ресурсов, чтение писем из проверенных источников, поскольку наибольшую защиту от атак может обеспечить сам пользователь, соблюдая меры предосторожности.

Результаты исследований, проведенных в этих направлениях, отражены в работах Г. Хоглунда (G. Hoglund), В. Деффи (W. Diffie), Д. Ньюланда (D. Newland), К. Паара (C. Paar), М. Рии (M. Rhee), В. Сталлингса (W. Stallings), Дж. Хартога (J. Hartog) и др.

Вторая глава посвящена исследованию и анализу существующих способов защиты от угроз, перечисленных в первой главе. Были рассмотрены основные подходы (программные и технические) к обеспечению безопасности при работе в сети интернет

Водход к защите информации, в частности, почтовых сообщений в сети Интернет должен быть всесторонним и комплексным – необходимо сочетать организационные меры с использованием соответствующих технических средств. К организационным мерам относятся разработка и внедрение в компании политики использования электронной почты. В настоящее время на рынке информационной безопасности существуют несколько систем контроля содержимого электронной почты с открытой архитектурой. В стандартный комплект поставки таких систем, как правило, входят несколько модулей, каждый из которых позволяет обеспечить защиту от определенного вида угроз или решает отдельную задачу безопасности функционирования системы электронной почты.

В **третьей главе** рассмотрены примеры программных средств, обеспечивающих защиту почтовых сообщений, проведен анализ их преимуществ и недостатков.

На основе рассмотренных приложений можно сказать, что самый простой способ защиты электронной почты – это использование симметричного шифрования. Для его реализации можно использовать плагины браузера SecureGmail и Encrypted Communication или вообще обойтись без них, а использовать программы, позволяющие создавать архивы, защищенные паролем (например, WinRAR, 7-Zip). Расчет прост: вы защищаете архивом файл, помещаете в него сообщение с возможными вложениями и отправляете другому человеку. Он, зная пароль, открывает архив. Самый простой в реализации, но не очень простой в использовании способ. Создавать архив для каждого нового сообщения – довольно рутинно. Плагины SecureGmail и Encrypted Communication делают симметричное шифрование более удобным, но безопаснее оно от этого не становится.

Более надежная система асимметричного шифрования. Она реализована множеством самых разных способов. Можно использовать стандарт S/MIME (что позволяет использовать асимметричную криптографию даже на мобильных устройствах), можно использовать PGP и производные продукты (OpenPGP, PGP Mail, GnuPG).

В идеале мы как раз и рекомендуем использовать стандарт S/MIME как наиболее надежный и универсальный. Надежность его заключается в том, что в самом почтовом клиенте сообщения хранятся в зашифрованном виде и

расшифровываются только по мере обращения к ним (то есть если кто-то завладеет вашим жестким диском, он не сможет расшифровать ваши сообщения). При расшифровке запрашивается пароль, который знаете только вы (в отличие от симметричного шифрования, где пароль знают, как минимум двое).

Универсальность заключается в том, что один раз создав свой сертификат, вы можете использовать его в любых почтовых клиентах (разумеется, с поддержкой S/MIME), а также в любых операционных системах, в которых работают эти почтовые клиенты.

Например, можно сгенерировать сертификат Windows-программой, установить его в Outlook и в мобильном почтовом клиенте MailDroid. Никаких ограничений на использование сертификатов нет.

Главное при использовании S/MIME выбрать удобную программу для создания самих сертификатов. Желательно, чтобы она позволяла публиковать сертификаты на сервере ключей и управлять ними.

В **четвертой главе** рассмотрены методы реализации защищенной сети передачи данных, а также предложена практическая реализация ПО для защиты почтовых сообщений. Диаграмма использования ПО приведена на рисунке 1.

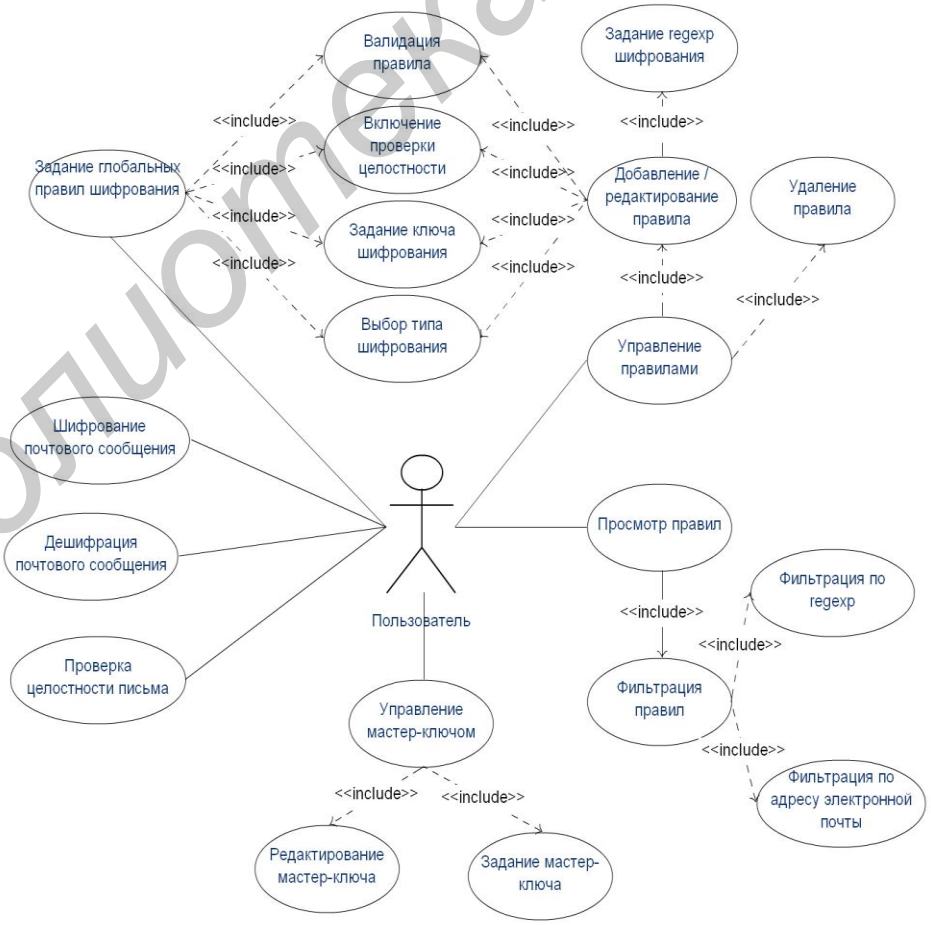

Рисунок 1 –Диаграмма use case для пользователя системы

В **пятой главе** представлены результаты экспериментальных исследований оценок скорости работы предложенных методик.

Предложенный вариант организации защищенной сети позволяет получить простой и легкий в использовании способ распределения ключей шифрования между пользователями. Однако, в случае получения контроля над сервером обновлений, злоумышленник получает доступ ко всем пользовательским ключам. Также необходимо учитывать возможность DOS-атак на данный сервер с целью отказа в обслуживании.

Использование поточного шифрования данных является оправданным в случае, когда скорость шифрования данных превалирует над качеством шифрования. В обратных ситуациях оправданным решением будет являться отказ от поточного шифрования и использования ассиметричных шифров. Предложенная схема реализация защищенной сети позволяет сделать без ущерба в скорости распределения ключей.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Предложена архитектура программной системы для решения задач защиты почтовых сообщений, обеспечивающая шифрование почтовых сообщений при их отправке адресатам, и позволяющая упростить процесс распределения ключей шифрования для различных пользователей.
2. Предложен метод формирования защищенной сети передачи ключей шифрования для автоматизации работы системы.
3. Проведен анализ эффективности существующих решений по защите почтовых сообщений, выделены их достоинства и недостатки.
4. Разработано экспериментальное программное обеспечение защиты почтовых сообщений.

Рекомендации по практическому использованию результатов

1. Полученные результаты формируют теоретическую и практическую базу для разработки ПО компьютерных систем для решения задач защиты почтовых сообщений с применением компьютеров общего назначения, функционирующих в режиме реального времени. Они могут быть использованы для модернизации и дальнейшего развития существующих систем.
2. Разработанные методы и алгоритмы построения защищенной сети могут применяться для реализации систем распределения данных между клиентами в системах защиты почтовых сообщений.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Перцев, И.Ю. Анализ существующих угроз компьютерной безопасности в сети / Перцев И.Ю., Зинькевич В.Н. // Наука, образование и культура. – 2015. - №3(3). – с. 9-13

2. Зинькевич, В.Н Безопасность при передаче файлов в образовании / Зинькевич В.Н., Перцев И.Ю. // Наука, образование и культура. – 2015. - №3(3). – с. 7-8

3. Перцев, И.Ю. Защита почтовых сообщений от несанкционированного доступа // Компьютерные системы и сети: материалы 50-ой научной конференции аспирантов, магистрантов и студентов. – Минск: БГУИР, 2014. – с. 27-28.