МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Анализ шифрования каналов связи

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Гамаюнова Михаила Борисовича

Научный руководитель
доцент к. ф.-м. н. _____ А. В. Жаркова
21.01.2023 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
21.01.2023 г.

Саратов 2023

ВВЕДЕНИЕ

В XXIвеке трудно представить крупную компанию, ведущую свою деятельность с помощью всевозможных информационных технологий, которая бы не задумывалась о безопасности своих систем и конфиденциальности данных своих клиентов. Злоумышленники обладают широким спектром программного и аппаратного обеспечения, направленного на обман пользователей и работников компаний с целью получения конфиденциальных данных, проникновение в компьютерные сети предприятий и на перехват файлов и сообщений, проходящих по незащищенным каналам связи. Существует ряд правовых и организационных мер, призванных ограничить доступ к конфиденциальной информации внутри конкретного предприятия и обеспечить защищенный доступ к ней уполномоченных лиц, но эти меры не применимы к информации, которая выходит за пределы контролируемой зоны предприятия. У компаний есть работники, которые могут подключиться к корпоративным ресурсам удаленно; клиенты, которые отправляют данные со своих компьютеров на офисные серверы; филиалы предприятия, находящиеся в разных частях страны или мира, которые обмениваются важными данными между собой. С целью решения проблемы передачи данной информации по открытым каналам связи применяется шифрование. Однако рынок шифрования в последние годы значительно вырос, ровно, как и спрос на качественные аппаратные и программные средства, способные защитить данные в публичных сетях.

Целью данной дипломной работы является анализосновных видов шифрования каналов связи для обеспечения криптографической защиты данных при их передаче; изучение разнообразных аппаратных средств, позволяющих компаниям организовать безопасный обмен сообщениями через публичные сети; исследование ряда возможных атак злоумышленников на каналы связи, защищенные шифрованием.В результате требуется написать программу по обмену данными между двумя пользователями с использованием

различных видов шифрования каналов связи и выявить преимущества и недостатки каждого из видов шифрования.

В процессе работы необходимо решить следующие задачи:

1) проанализировать основные виды шифрования каналов связи;

2) рассмотреть актуальные на текущий момент аппаратные средства шифрования данных в каналах связи;

3) изучить различные виды атак и методы защиты от них;

4) написать программу для обмена данными между двумя пользователями с использованием различных видов шифрования каналов связи.

Данная работа частично была представлена на IX Международной научной конференции«Компьютерные науки и информационные технологии» памяти А. М. Богомолова и опубликована в её материалах[1].

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 93 страницы, из них 53 страницы – основное содержание, включая 27 рисунков и 1 таблицу, список использованных источников из 23 наименований.

[1]Гамаюнов, М. Б. О шифровании каналов связи / М. Б. Гамаюнов, А. В. Жаркова[Электронный ресурс] // Компьютерные науки и информационные технологии : Материалы Междунар. науч. конф. – Саратов : ООО Издательство «Научная книга», 2021. – С. 44–47.

КРАТКОЕ СОДЕРЖАНИЕ

В дипломной работе в разделе 1 «Необходимые определения» приводятся необходимые определения, которые используются в данной работе.

Криптография (от греческого «тайнопись») – это совокупность идей и методов, связанных с преобразованием информации с целью ее защиты от непредусмотренных пользователей. Информация считается представленной в виде некоторого текста (сообщения). Это – *открытый текст*. Способ его преобразования в защищенную форму называется *шифром*, процесс применения шифра – *шифрованием*, полученный в результате шифрования измененный текст – *криптограммой*/*шифртекстом*.Перевод криптограммы в исходныйоткрытый текст производится в ходе *дешифрования* (*расшифрования*).

Взаимно обратные действия шифрования и расшифрования осуществляются с помощью некоторой дополнительной информации, называемой *ключом.* Именно в ключе спрятан секрет шифра. Без знания ключа чтение криптограммы должно быть значительно затруднено или практически невозможно в пределах разумного интервала времени.

Шифры, обладающие свойством, что для шифрования и расшифрования в них применяется один и тот же секретный ключ, называют *симметричными.* Если шифр этим свойством не обладает, процедуры шифрования и расшифрования в нем осуществляются на разных ключах, то подобные шифры называются *асимметричными*[2].

Говорят, что криптографический алгоритм реализует *имитозащиту* данных, если он обеспечивает защиту получателя от навязывания ложной информации[3].

---

[2]Салий, В. Н. Криптографические методы и средства защиты информации: учебное пособие [Электронный ресурс] / В. Н. Салий // Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского [Электронный ресурс]. – Саратов, 2017. – 43 с. : ил., табл. – URL: http://elibrary.sgu.ru/uch_lit/622.pdf (дата обращения: 19.11.2022). – Загл. с экрана. – Яз. рус.

[3]Ростовцев, Е. Г. Теоретическая криптография [Электронный ресурс] / Е. Г. Ростовцев, Е. Б. Маховенко. – СПб. : Профессионал, 2004. – 479 с. – Загл. с экрана.– Яз. рус.

Процесс нахождения ключа K (или открытого текста X) по заданной криптограмме Yназывается *криптоанализом*, а противник, занимающийся криптоанализом, – *криптоаналитиком*[4].

Дейтаграммный способ передачи данных основан на том, что все сообщения передаются от одного узла сети другомунезависимо друг от друга на основании одних и тех же правил[5].

Контролируемая зона –пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств[6].

Линия связи – это совокупность технических средств, служащих для организации на единой технической основе одного или нескольких *каналов связи*.Система передачи информации, предназначенная для передачи сообщений по одной линии связи, имеет вид, показанный на рисунке 1.

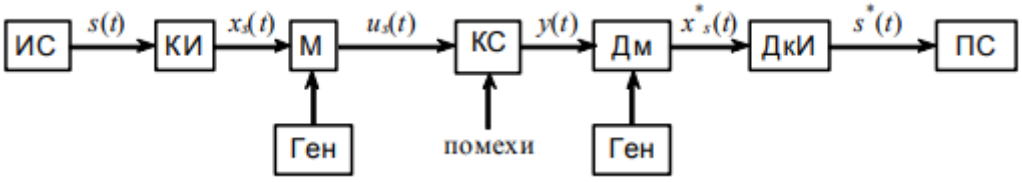

Рисунок 1 – Линия связи[7]

На рисунке 1 обозначено:

ИС – источник сигнала;

$s(t)$ – множество полезных сигналов;

КИ – кодер источника, в нём происходит преобразование сообщения в электрический сигнал;

$x_s(t)$ – кодовая комбинация полезных сигналов $s(t)$;

---

[4]Пилиди, В. С. Криптография. Вводные главы: учебное пособие [Электронный ресурс] / В. С. Пилиди. – Ростов н/Д. : ЮФУ, 2009. – 110 с. – Загл. с экрана. – Яз. рус.

[5]Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов [Электронный ресурс] / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб. : Питер, 2010. – 944 с. : ил. – Загл. с экрана. – Яз. рус.

[6] ГОСТ Р 52863–2007. Защита информации. Автоматизированные системы в защищенном исполнении [Электронный ресурс] // Информационная система МЕГАНОРМ [Электронный ресурс]. – М. :Стандартинформ, 2020. – 40 с. – URL: https://meganorm.ru/Data/474/47480.pdf (дата обращения: 03.12.2022). – Загл. с экрана. – Яз. рус.

[7] Теория электрической связи. Конспект лекций [Электронный ресурс] / В. А. Григорьев, О. И. Лагутенко, О. А. Павлов, Ю. А. Распаев, В. Г. Стародубцев, И. А. Хворов ; под общ. ред. В. А. Григорьева. – СПб. : НИУ ИТМО, 2012. – 148 с. – Загл. с экрана. – Яз. рус.

М – модулятор, предназначен для согласования параметров электрического сигнала на выходе кодера источника с параметрами канала связи;

Ген – генератор электрического сигнала;

$u_s(t)$ – множество электрических сигналов;

КС – канал связи (конкретная физическая среда);

помехи – возможные помехи в канале связи;

$y(t)$ – выходящий из канала связи сигнал;

ДМ – демодулятор, служит для обратного преобразования (по сравнению с модулятором) сигнала из канала связи в сигнал сообщения;

$x_s^*(t)$–кодовая комбинация полезных сигналов $s(t)$на приемной стороне;

ДКИ – декодер источника, преобразует сигнал сообщения в удобный для восприятия абонентом вид;

$s^*(t)$ – множество возможных сообщений;

ПС – получатель сообщения[7].

VPN(англ. VirtualPrivateNetwork,виртуальная частная сеть) – обобщённое название сервисов, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети[8].

В разделе 2 «О шифровании каналов связи» в подразделе «Виды шифрования каналов связи» приводятся 4 вида шифрования каналов связи: канальное, сквозное, комбинированное и туннелирование. В подразделе «Передача данных с использованием симметричной и асимметричной криптографии» рассматриваются особенности передачи данных с использованием упомянутых видов систем шифрования. В подразделе «Аппаратные средства канального шифрования и туннелирования» представлены некоторые аппаратные средства шифрования каналов связи и в подразделе «Возможные атаки на каналы связи» описаны некоторые виды атак на зашифрованные каналы.

[8] Švenčionis, T. WhatIsaVPN [Электронный ресурс] / T. Švenčionis // Cybernews [Электронный ресурс]. – 22.11.2022. – URL: https://cybernews.com/what-is-vpn/ (дата обращения: 26.11.2022). – Загл. с экрана. – Яз. англ.

Шифрование данных для передачи по каналам связи может осуществляться на любом уровне эталонной модели OSI[5]. На практике чаще всего это делается либо на самых нижних, либо на самых верхних уровнях. В случае, когда данные шифруются на нижних уровнях, шифрование называется *канальным*. А когда шифрование происходит на верхних уровнях, оно называется *сквозным*. Использование совокупности из канального и сквозного шифрования называется *комбинированным*. И тот, и другой вид шифрования имеет определенные преимущества и недостатки[9]. Канальное шифрование обеспечивает более высокий уровень защищенности, но требует дополнительные организационные меры безопасности[10]. Сквозное шифрование работает быстрее канального, но не скрывает служебную информацию от злоумышленника.

Иным подходом к шифрованию каналов связи является *туннелирование* (*VPN-туннелирование*, *инкапсуляция протоколов*[11]). Этот подход тесно связан с применением VPN-сервисов, т. к. принцип их работы основан на туннелировании[12]. При данном подходе сообщение перед попаданием в незащищенную сеть проходит через специальный VPN-шлюз, который управляет входящим и исходящим трафиком[13].

Наиболее распространенными на текущий момент протоколами туннелирования являются следующие протоколы:OpenVPN, L2TP/IPsec, PPTP,

---

[9]Криптографические алгоритмы [Электронный ресурс]//Бюро научно-технической информации :[Электронный ресурс].–URL: http://www.bnti.ru/showart.asp?aid=277&lvl=04.03.07. (дата обращения: 19.11.2022). – Загл. с экрана. – Яз. рус.

[10]Макаренко, С. И. Информационная безопасность: учебное пособие [Электронный ресурс] / С. И. Макаренко. – Ставрополь : СФ МГГУ им. М. А. Шолохова, 2009. – 372 с. : ил. – Загл. с экрана. – Яз. рус.

[11]Олифер, В. Г. Стратегии межсетевого взаимодействия [Электронный ресурс] / В. Г. Олифер, Н. А. Олифер // Центр Информационных Технологий [Электронный ресурс]. – URL: http://citforum.ru/nets/tpns/glava_2.shtml (дата обращения: 26.11.2022). – Загл. с экрана. – Яз. рус.

[12]Jančis, M. WhatIsaVPNTunnelandHowDoesItWork [Электронный ресурс] / M. Jančis // Cybernews [Электронный ресурс]. – 02.09.2021. – URL: https://cybernews.com/what-is-vpn/what-is-a-vpn-tunnel/ (дата обращения: 18.12.2022). – Загл. с экрана. – Яз. англ.

[13]Lavigne, D. VPN и IPSec на пальцах [Электронный ресурс] / D. Lavigne // Издательство Nestor [Электронный ресурс]. – 23.01.2005. – URL: https://nestor.minsk.by/sr/2005/03/050315.html (дата обращения: 13.12.2022). – Загл. с экрана. – Яз. рус.

SSTP, IKEv2, IPsec, SSL/TLS, Wireguard[14]. Из них стоит выделить 2 протокола: OpenVPNи IPsec.

OpenVPN–протокол с открытым исходным кодом, с гибкой конфигурацией для множества параметров шифрования и высокой скоростью передачи данных, изначально выпущенный в 2001 году. Используется множеством VPN-сервисов как основа. Поддерживает несколько алгоритмов шифрования, например, AES или Blowfish. К минусам можно отнести сложность ручной настройки для обычного пользователя, поэтому обычно используется в составе какого-нибудь VPN-сервиса. Также поддерживает 2 транспортных протокола: TCP и UDP.

IPsec используется для нескольких целей, одной из которых является туннелирование.IPsecчасто используется в паре с другими протоколами для дополнительной безопасности, но может и использоваться отдельно от них. Криптостойкость IPsecво многом зависит от конкретной настройки[14]. Поддерживаются такие алгоритмы как AES, Blowfish, ChaCha20, 3DES[15].У IPsecесть 2 режима передачи данных: транспортный и туннельный. При туннельном режиме весь оригинальный пакет зашифровывается, после чего к нему добавляется новый заголовок. При транспортном режиме зашифровывается только блок данных пакета, IP-заголовок остается прежним[16].

Существует несколько подходов к обеспечению безопасности данных в компьютерных сетях. Можно использовать сквозное шифрование на конечных узлах сети или установить VPN-клиенты, но это требует настройки со стороны специалистов безопасности, а также данные сервисы оказывают некоторую нагрузку на системы.

---

[14]Bischoff, P. VPN ProtocolsExplainedandCompared [Электронный ресурс] / P. Bischoff // Comparitech [Электронный ресурс]. – 25.08.2021. – URL: https://www.comparitech.com/vpn/protocols/ (дата обращения: 18.12.2022). – Загл. с экрана. – Яз. англ.

[15]Charboneau, T. IPsec Encryption: HowSecureIsItReally [Электронный ресурс] / T. Charboneau // Twingate [Электронный ресурс]. – 07.10.2021. – URL: https://www.twingate.com/blog/IPsec-encryption/ (дата обращения: 03.12.2022). – Загл. с экрана. – Яз. англ.

[16]Sanoja, D. IPsec TunnelModevs. TransportMode [Электронный ресурс] / D. Sanoja // Twingate [Электронный ресурс]. – 19.08.2021. – URL: https://www.twingate.com/blog/ipsec-tunnel-mode/ (дата обращения: 03.12.2022). – Загл. с экрана. – Яз. англ

Поэтому существует другой подход –межсайтовое шифрование. При данном подходе используются доверенные или защищенные каналы, через которые данные передаются к устройствам шифрования, откуда уже отправляются дальше в сеть. Для сетей Ethernet, через которые проходит трафик, нет единого стандарта шифрования, поэтому разные компании предлагают разные устройства и подходы к шифрованию и защите передаваемых данных[17].

Примерами различных устройств аппаратного шифрования каналов связи являются следующие устройства: ViPNetCoordinator HW[18], «Континент»[18] и «Палиндром»[19].

Несмотря на использование шифрования данных при передаче по каналам связи, злоумышленник все равно может попытаться получить информацию путем всевозможных атак.

Примерами таких атак могут быть следующие атаки: вскрытие «человек-в-середине»[20], атака по времени выполнения[21], атаки по потребляемой мощности[21], атаки по ошибкам вычислений[22], атаки по электромагнитному излучению.

В разделе 3 «Программная реализация» в подразделе «Настройка EVE-NG» представлена настройка виртуальной сети для тестирования программы. В подразделе «Демонстрация работы программы» описанаразработанная и реализованнаяпрограмма на языке Java, моделирующая обмен данными между

---

[17]Рожнов, М. Как защитить данные в распределенных сетях Ethernet [Электронный ресурс] / М. Рожнов // CNews [Электронный ресурс]. – 09.04.2020. – URL: https://safe.cnews.ru/articles/2020-04-09_kak_zashchitit_dannye_v_raspredelennyh (дата обращения: 01.12.2022). – Загл. с экрана. – Яз. рус.

[18]Макаров, И. Шесть устройств для сетевого шифрования: плюсы и минусы [Электронный ресурс] / И. Макаров // BIS Journal [Электронный ресурс]. – 25.02.2020. – URL: https://ib-bank.ru/bisjournal/post/1210 (дата обращения: 13.12.2022). – Загл. с экрана. – Яз. рус.

[19]Рожнов, М. Российские высокоскоростные шифраторы L2 для сетей Ethernet [Электронный ресурс] / М. Рожнов // Anti-malware [Электронный ресурс]. – 18.05.2020. – URL: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-L2-encryption-devices-for-Ethernet-networks (дата обращения: 13.12.2022). – Загл. с экрана. – Яз. рус.

[20]Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си [Электронный ресурс] / Б. Шнайер. – М. : Триумф, 2002. – 610 с. – Загл. с экрана. – Яз. рус.

[21]Панасенко, С. П. Алгоритмы шифрования. Специальный справочник [Электронный ресурс] / С. П. Панасенко. – СПб. : БХВ-Петербург, 2009. – 576 с. – Загл. с экрана. – Яз. рус.

[22]Yongbin, Z. Side-ChannelAttacks: TenYearsAfterItsPublicationandtheImpactsonCryptographicModuleSecurityTesting [Электронный ресурс] / Z. Yongbin, F. Dengguo // CryptologyePrintArchive [Электронный ресурс]. – 2006. – 34 с. – URL: https://eprint.iacr.org/2005/388.pdf (дата обращения: 08.04.2021). – Загл. с экрана. – Яз. англ.

двумя пользователями по сети с возможностью выбора одного из нескольких видов шифрования каналов связи и одного из нескольких режимов работы. В подразделе«Сравнение времени работы различных видов шифрования»представлена таблица сравнения времени работы различных видов шифрования.

При запуске программа предлагает выбрать один из двух режимов работы: отправитель или получатель.

Получатель работает в качестве сервера: он ожидает подключения отправителя, после чего начинает с ним обмен данными. Получатель лишь принимает отправляемые ему данные и работает в том режиме, о котором ему сообщит отправитель.

В режиме отправителя можно выбрать один из трех режимов работы: нагрузочное тестирование, бесконечная отправкаили выборочная отправка файлов; выбрать вид шифрования: сквозное, канальное, комбинированное или туннелирование. Режим нагрузочного тестирования позволяет отправлять все файлы из указанной директории, режим бесконечной отправки организует бесконечный обмен сообщениями между отправителем и получателем, режим выборочной отправки позволяет вручную выбрать определенные файлы из директории для точечного тестирования.

Для сквозного, канального и комбинированного шифрования можно выбрать одну из двух шифрсистем: AESили «Кузнечик» (ГОСТ Р 34.12–2015). Обе шифрсистемы используют длину ключа 256 бити работают в режиме CFB. Для отправкиконфигурации шифрования используется RSAс длиной ключа 512 бит. Режим туннелирования использует протокол IPsec, которыйв данной настройке использует шифрсистему AESс длиной ключа 256 бит, туннельный режим и проверку целостности с помощью хеш-функции SHA256.

После запуска обмена сообщениями программа в зависимости от режима либо предложит выбрать файлы для отправки, либо возьмет их из указанной директории, отправит получателю конфигурацию работы и шифрования, после

чего по одному доставит файлы до получателя, проверяя их целостность и отсчитывая время, которое ушло на доставку каждого конкретного файла.

На рисунке 19 представлен пример успешной работы программы.

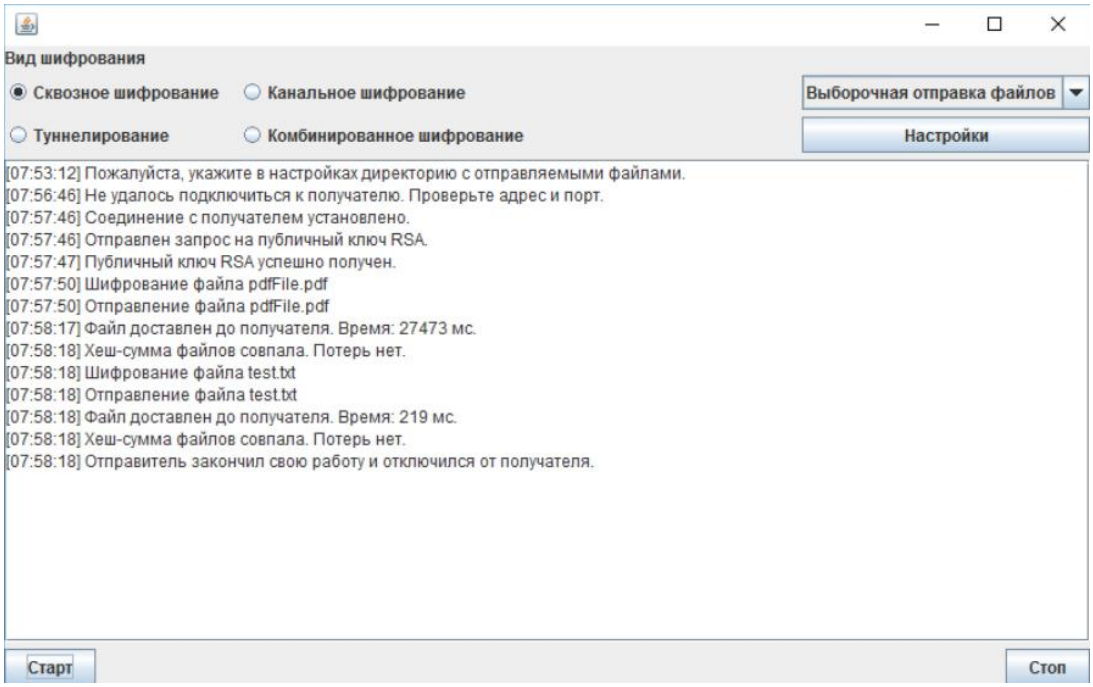

Рисунок 19 – Пример успешной работы отправителя

В таблице 1 приведено сравнение времени работы различных видов шифрования каналов связи, полученное с помощью описанной выше программы. У канального шифрования было 4 промежуточных узла. Для тестирования использовался режим нагрузочного тестирования. Время работы среднее по результатам 10 тестов. Время работы сильно выше аналогичного в реальных системах, поскольку большое количество производительности отводилось на поддержку всех узлов в виртуальной сети EVE-NG.

Таблица 1 – Результат измерения времени доставки сообщения

Размер файла	Время работы			
	Сквозное шифрование	Канальное шифрование	Комбинированное шифрование	Туннелирование
1 КБ	219 мс	344 мс	688 мс	156 мс
100 КБ	813 мс	969 мс	1125 мс	766 мс
1 МБ	7,7 с	9,8 с	10 с	6,8 с
10 МБ	82,6 с	104,6 с	109,6 с	78,8 с
50 МБ	7 мин	7,7 мин	9,5 мин	6,5 мин

Как видно из таблицы 1, туннелирование работает быстрее всего в виду того, что шифрование на маршрутизаторах Cisco, используемых в

работе,оптимизировано лучше, чем на Java. Комбинированное шифрование работает дольше остальных видов, так как оно является комбинацией сквозного и канального шифрования.

ЗАКЛЮЧЕНИЕ

Проанализировав четыре вида шифрования каналов связи, изучив представленные на рынке аппаратные средства защиты и исследовав возможные атаки на зашифрованные каналы связи, можно отметить, что, несмотря на существование угрозы перехвата и несанкционированного доступа к конфиденциальным данным в канале связи, существует ряд аппаратных устройств, протоколов туннелирования и алгоритмов шифрования данных для организации конфиденциального обмена данными между узлами, находящимися друг от друга на любом расстоянии. У каждого из методов защиты есть свои преимущества и недостатки, на основании которых можно принимать решение о внедрении того или иного способа защиты на разнообразных предприятиях.

В результате проделанной работы на языке Javaбыла написана программа, моделирующая передачу данных по каналу связи, с помощью которой было проведено сравнение времени работы описанных в работе видов шифрования.

Дополнения и изменения в работе, предложенные на IXКонференции «Компьютерные науки и информационные технологии» памяти А. М. Богомолова[1], были учтены и успешно реализованы.

Результаты работы могут использоваться, если компании или конечному пользователю необходимо провести сравнение или эмуляцию работы описанных в работе видов шифрования каналов связи в конкретной реальной (виртуальной) сети. Также работа может использоваться для ознакомления с некоторыми атаками на каналы связи, использующие шифрование, с особенностями использующихся на текущий момент протоколов туннелирования, с несколькими типами аппаратных продуктов.

Таким образом, все поставленные задачи решены, цель работы достигнута.