Содержание:

Введение

В настоящий момент информация является большим предметом рассуждений, и тут затрагиваются не только такие вопросы как актуальность информации ее новизна или полнота, но и более важная ее сторона – безопасность. Безопасность информации это очень большая сфера, над которой работают разные кластеры людей, так или иначе связанных с сферой IT технологий. Информация является основой для большинства сфер жизни, таких как политическая, экономическая.

С каждым годом мы все больше узнаем о том, как же можно защищать информацию с каждым годом появляются все больше методов защиты информации. Но, так или иначе, информация остается основным источником проблем в настоящем мире, угроза утечки информации по-прежнему есть, как внутри какой-либо ячейки общества, так и снаружи, на политическом уровне. А ведь при неправильной работе с информацией информация может быть похищена, а это в свою очередь может привести к катастрофе огромных масштабов. Безусловно, это зависит о зоны, к которой относится информация. Если это, к примеру, небольшая компания, то это может повлиять на ее работу. Если это более высокий уровень, политический, то это может привести даже к войне между государствами. Поэтому проблема защиты информации на данный момент является актуальной.

Курсовая работа будет посвящена оценке и анализу основных протоколов защиты мгновенных сообщений. Говоря о мгновенных сообщениях, я подразумеваю мессенджеры которые, на данный момент являются актуальными.

Существует разные виды программного обеспечения для обмена мгновенными сообщениями:

- Платное
- Бесплатное
- с поддержкой
- без поддержки
- С Web интерфейсом

- С клиентской частью программы

Вообще рынок программного обеспечения, позволяющего обмениваться информацией быстро, достаточно велик, но в современном мире, используются не так много видов такого программного обеспечения, и каждый вид такого программного обеспечения используется в своей сфере в соответствии со своими потребностями и возможностями.

Каждая компания или отдельное лицо выбирает программное обеспечение из своих соображений, но в большинстве случаев выбор мессенджера диктуется обществом и зачастую общество мало интересует вопрос безопасности передачи сообщений. В основном это интересует компании, которые работают с другими основными ресурсами – людскими и финансовыми.

1.

Аналитическая часть.

Аппаратная архитектура компании

Сеть компании построена по топологии звезда с использованием кабеля типа “Витая пара” категории 5E с пропускной способностью до 100мбит/с

В сети функционируют 25 компьютеров, 1 сервер, 1 маршрутизатор и 1 точка доступа.

Список оборудования

Пользовательское

- Компьютеры на базе процессора Intel Core i5
- Процессор Intel Core i5-7400 Kaby Lake + куллер (3000MHz/LGA1151/L3 6144Kb)
- Материнская плата - GIGABYTE GA-H110M-S2
- Kingston HyperX Fury Black PC4-19200 DIMM DDR4 2400MHz CL15 - 8Gb
- Накопитель - SSD - 120Gb - Kingston A400 SA400S37/120G
- Монитор Samsung S22D300NY
- Клавиатура DEXP K-401BU
- Мышь проводная DEXP CM-904BU

- Корпус mATX FORMULA FA-703B, Mini-Tower, 450Вт.
- Принтер Kyocera P6035CDN

Серверное

- Точка доступа MikroTik wAP ac (Black) RBwAPG-5HacT2HnD-be – выполняет роль WiFi роутера
- Маршрутизатор MikroTik RB2011iLS-IN – выполняет роль фаервола и коммутации каналов
- STSS Flagman MX240.5-008LH – сервер общего назначения(dns-dhcp-ad-fileserver)

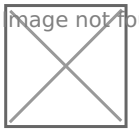


Рисунок 1. Архитектура сети компании ЗАО “Дятлы-77”

Программная архитектура компании

Программное обеспечение

Компьютер пользователя

- Операционная система Windows 10x64
- ESET Endpoint Antivirus 5.0.2265.1
- Браузер Google Chrome v64
- Microsoft Office 2016
- PDF Creator
- Adobe Acrobat

Сервер

- Операционная система Windows Server 2008 R2
- ESET Endpoint Antivirus 5.0.2265.1

Исполняемые роли:

- Domain Controller
- DHCP
- Active Directory

- File Server

Рисунок 2. Программная архитектура компании

Протоколы передачи данных

Любая информационная система, будь то мобильное приложение, программное обеспечение или видео конференция при передаче данных всегда соответствует основным стандартам передачи данных. Регулируется передача данных в интернете сетевыми протоколами.

Сетевой протокол – набор правил, необходимых для передачи информации между узлами сети. Существуют различных уровни передачи информации, которые объединены в общую эталонную модель OSI – открытую систему взаимодействий. С помощью этой системы различные программы и приложения взаимодействуют друг с другом. Модель OSI включает в себя 7 уровней, каждый из которых имеет свои функции. Примерами таких протоколов являются протоколы TCP/IP , TELNET, FTP,SMTP,POP3,HTTP и т.д.

Также существуют протоколы защиты информации, которые с помощью шифрования и кодирования защищают информацию, которой пользователь обменивается с пользователем или сервером. К примеру, при покупке вещей через интернет или переводе денежных средств через интернет, очень часто в проводнике интернет страницы можно увидеть формат написания сайта так https://сайт. HTTP - протокол передачи гипер текста, сам по себе он не является безопасным, а вот буква ‘s’ в конце показывает, что используются дополнительные методы для шифрования данных при передаче в виде протокола TLS или SSL.

Основные технологии и протоколы защиты информации

Существует огромное количество методов защиты информации, которые были разработаны несколько десятков лет назад, а используются и сейчас. В основе методов защиты информации находятся такие технологии и стандарты как: P2P, DES, SQUARE, AES, RSA, SHA, RC, открытые и закрытые ключи.

Ключи шифрования

Прежде всего, нужно сказать, что основой каждого алгоритма шифрования являются ключи шифрования. Ключи шифрования бывают двух типов: открытый ключ и закрытый ключ

Открытый ключ – набор информации находящийся в открытом доступе, передается между различными субъектами и используется для шифрования и генерации закрытого ключа.

Закрытый ключ – ключ, с помощью которого происходит декодирование зашифрованной информации.

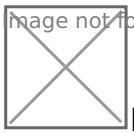


Рисунок 3. Схема шифрования информации с использованием ключей шифрования.

Ключи могут быть подменены 3 лицом, путем перехватывания пакетов. Для защиты от перехвата пакетов была придумана проверка на подлинность с помощью идентификационных сертификатов

Идентификационный сертификат - это информационный носитель, на котором записывается сертификат с закрытым ключом, выдается доверенным центром и передается по закрытому каналу или лично в руки.

Типы шифрования

Шифрование – процесс преобразования информации в зашифрованную путем использования различных способов и алгоритмов шифрования.

Шифры бывают:

Асимметричными – в свою очередь имеют 2 ключа один для шифрования, второй для дешифрования;

Симметричными – симметричные шифры используют одинаковый ключ для шифрования текста и его расшифровки;

В свою очередь, симметричные шифры бывают:

Блочными – шифры, которые преобразуют информацию блоками от 64 байт до 256, особенность в том, что шифр текст может быть получен только после получения все необходимой для шифровки информации.

Рисунок 4. Пример блочного шифра

А – исходное значение

Б – шифрование с помощью ключа

С – преобразованные блоки А

Потоковыми – шифры, шифрующие информацию сразу, как только это нужно без ожидания наполнения блока (как в блочном шифре), использование такого типа шифра дает возможность быстрее шифровать информацию.

Рисунок 5. Процесс выполнения потокового шифра

Протоколы TLS/SSL

SSL – криптографический протокол, использующий асимметричное шифрование для аутентификации ключей шифрования и симметричное шифрование при обмене информацией между различными субъектами. До 2014г очень широко использовался (с 1996г), особенно в решениях, в которых присутствует VoIP телефония. В 2014г в протоколе SSL была найдена критическая уязвимость, на смену SSL пришел протокол TLS. Так же протокол SSL используется при шифровании гипертекста (протокол HTTPS)

Протокол Рукопожатия

Протокол Рукопожатия состоит из трех подпротоколов, использование которых позволяет участникам согласовать криптографические алгоритмы, аутентифицировать друг друга, и сообщить друг другу о возникновении тех или иных ошибок.

Криптографические параметры сессии создаются протоколом Рукопожатия, который выполняется выше протокола Записи. Когда клиент и сервер начинают взаимодействовать, они согласовывают версию протокола, выбирают криптографические алгоритмы, могут аутентифицировать друг друга, используя

технологию с открытым ключом. Для создания разделяемого секрета также используется технология с открытым ключом.

Протокол Рукопожатия состоит из следующих шагов:

1. Обмен сообщениями Hello для согласования алгоритмов, обмена случайными значениями и проверки возобновляемости сессии.
2. Обмен необходимыми криптографическими параметрами, которые позволяют клиенту и серверу согласовать премастер-секрет.
3. Обмен сертификатами и криптографической информацией, которая позволяет клиенту и серверу аутентифицировать друг друга.
4. Предоставление параметров безопасности на уровень Записи.
5. Возможность клиенту и серверу проверить, что они вычислили одни и те же параметры безопасности и что Рукопожатие произошло без вмешательства злоумышленника.

TLS

Протокол TLS использует такие же типы шифрования как и протокол SSL

TLS даёт возможность устанавливать связь клиент-серверным приложениям таким образом, что нельзя производить прослушивание пакетов и осуществить несанкционированный доступ.

Использовать протокол TLS или нет – дело выбора пользователя. Права выбора дается потому, что большая часть протоколов связи может работать как с использованием TLS так и без него. Если требуется использование протокола TLS, клиент должен об этом указать, путем выбора протокола или путем выбора порта. Как только клиент и сервер договорились об использовании TLS, им необходимо установить защищённое соединение.

Это делается с помощью процедуры подтверждения связи с отправкой ключевых сообщений. Во время этого процесса клиент и сервер принимают соглашение относительно различных параметров, необходимых для установки безопасного соединения.

Одной из областей применения TLS-соединения является соединение узлов в виртуальной частной сети. Кроме TLS, также могут использоваться набор протоколов IPSec и SSH-соединение. Каждый из этих подходов к реализации виртуальной частной сети имеет свои преимущества и недостатки.

RSA

RSA – Криптографический алгоритм с открытым ключом, основан на факторизации больших. Является первой криптосистемой использующейся и для шифрования и для вычисления цифровой подписи. Алгоритм используется в таких системах как IPSec, TLS, S/MIME и т.д. К минусам данного алгоритма можно отнести относительно низкую скорость шифрования по сравнению с другими алгоритмами. По этому обычно используются другие алгоритмы, например, AES, позволяющий выбрать случайный сеансовый ключ.

Рисунок 6. Алгоритм работы RSA

Peer-to-peer шифрование (P2P)

P2P шифрование – грубо говоря, шифрование, основанное на методах работы пиринговой сети, в которой каждый пользователь имеет равные права по отношению друг к другу.

Отличие такого шифрования от любых других в том, что информация, которая проходит через сервер на нем не остается. Сервер выполняет транспортную роль передавая информацию из точки А в точку Б напрямую.

Естественно, защищенность информации при использовании подобного типа шифрования достаточно высока, потому как шифрование и дешифрование проводится на компьютерах отправителя и получателя. Украсть данные в этом случае, можно только путем физической кражи компьютера А или Б.

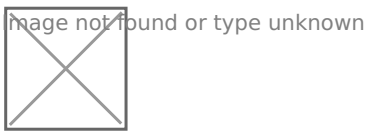


Рисунок 7. Схема выполнения P2P

CRC

Циклический избыточный код - алгоритм нахождения контрольной суммы, используется для проверки целостности данных.

Контрольная сумма – набор случайных символов вычисленных математическим путем, отправляемый при передаче данных в начале файла и в конце, для

исключения потерь во время передачи данных.

Вычисление контрольной суммы происходит по алгоритмам, например, SHA или MD Так же контрольная сумма может быть представлена на ресурсе, откуда идет непосредственно скачивание файла, в дальнейшем контрольные суммы можно сравнить.

SHA

SHA – криптографическая хэш функция, разработанная АНБ совместно с НИСТ и рекомендуемая для генерации хэш сумм

Пример контрольной суммы алгоритма SHA-1

1. SHA-1("В чащах юга жил бы цитрус? Да, но фальшивый экземпляр!") = 9e32295f 8225803b b6d5fdfc c0674616 a4413c1b
2. SHA-1("The quick brown fox jumps over the lazy dog") = 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12
3. SHA-1("Sha") = ba79baeb 9f10896a 46ae7471 5271b7f5 86e74640

Изменение любого из символов влечет за собой полное изменение хэш суммы. Это явление называется лавинным эффектом.

Параметры алгоритма

Одним из основных параметров CRC является порождающий полином.

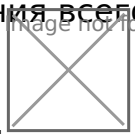
С порождающим полиномом также связана его степень, которая определяет количество битов, используемых для вычисления значения CRC. Чаще всего используются 8, 16 и 32 битные алгоритмы.

Описание работы алгоритма

Из файла берётся первое слово — это может быть битовый (CRC-1), байтовый (CRC-8) или любой другой элемент. Если старший бит в слове «1», то слово сдвигается влево на один разряд с последующим выполнением операции XOR с порождающим полиномом.

Соответственно, если старший бит в слове «0», то после сдвига операция XOR не выполняется. После сдвига теряется старый старший бит, а младший бит освобождается — его значение устанавливается равным нулю. На место младшего бита загружается очередной бит из файла, и операция повторяется до тех пор,

пока не загрузится последний бит файла. После прохождения всего файла, в слове



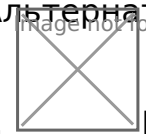
остается остаток, который и является контрольной суммой.

Рисунок 8. Схема формирования контрольной суммы алгоритмом CRC-8

DES

DES – (Data Encryption Standard) – алгоритм использующий симметричное шифрование, разработан компанией Microsoft в 1977г. В основе алгоритма лежит сеть Фейстеля.

Сеть Фейстеля - это принцип построения блочных шифров, при котором на вход первой ячейки шифра поступает информация и ключ, в дальнейшем ключ для каждой новой ячейки генерируется с помощью предыдущей. Большая часть шифров основана на сети Фейстеля. Альтернативой сети Фейстеля является



подстановочно-перестановочная сеть. Рисунок 9. Схема работы блочного шифра с по методу Фейстеля

Алгоритм DES имеет длину блоков в 56 байт + 8 байт проверочных.

Рисунок 10. Схема работы шифра DES

Аналогией нашего времени является 3DES – тот же шифр, но выполняющийся 3 раза

Алгоритм шифрования AES

AES - Advanced Encryption Standard – это симметричный алгоритм блочного шифрования, размер блока 128 бит, ключ может быть от 128 до 256 бит. Стандарт был выбран на основе конкурса, проведенного NIST – (Национальный институт стандартов и технологий) в 1997 году.

Алгоритм является последователем шифра DES и использует в своей основе подстановочно-перестановочную сеть. На данный момент AES является одним из

самых распространенных, широко используется компанией Intel в разрабатываемых процессорах.

В 2003г правительство США постановило, что может быть использован при шифровании секретной и топ-секретной информации.

Подстановочно-перестановочная сеть

SP-сеть подстановочно-перестановочная сеть — разновидность блочного шифра, разработанная Фестелем в 1971г. Представляет собой блок состоящий из двух типов слоев 1 слой – слой с блоком большой разрядности – 2 слой – слой с блоком малой разрядности. Первым криптографическим алгоритмом на основе SP-сети был алгоритм Люцифер, разработанный в 1971г.

Рисунок 11. Пример SP-сети в алгоритме “Люцифер”

1.16.1. Принцип работы SP-сети

Шифр на основе SP-сети получает на вход блок и ключ и совершает несколько чередующихся раундов, состоящих из чередующихся стадий и стадий перестановки

Для достижения безопасности достаточно одного S-блока, но такой блок будет требовать большого объёма памяти. Поэтому используются маленькие S-блоки, смешанные с P-блоками. Линейная стадия перестановки распределяет избыточность по всей структуре данных.

S-блок замещает маленький блок входных бит на другой блок выходных бит. Эта замена должна быть взаимно однозначной, чтобы гарантировать обратимость. Назначение S-блока заключается в нелинейном преобразовании, что препятствует проведению линейного крипто анализа. Одним из свойств S-блока является лавинный эффект, то есть изменение одного бита на входе приводит к изменению всех бит на выходе.

P-блок — перестановка всех бит: блок получает на вход вывод S-блока, меняет местами все биты и подает результат S-блоку следующего раунда. Важным качеством P-блока является возможность распределить вывод одного S-блока

между входами как можно больших S-блоков.

Для каждого раунда используется свой, получаемый из первоначального, ключ. Подобный ключ называется раундовым. Он может быть получен как делением первоначально ключа на равные части, так и каким-либо преобразованием всего ключа.

IMS

IMS – служба мгновенных сообщений. Именно с помощью этой службы работают месенджеры, включающие в себя отправку сообщений по сети мгновенно.

Все программы работающие со службой мгновенных сообщений требуют клиентская и серверная части программы. Разница между IMS и почтовыми клиентами в том, что передача сообщения между субъектами осуществляется онлайн, то есть в реальном времени.

Каждая из сетей разработана разными компаниями и использует в своей работе разные серверы и протоколы. Таким образом разные сети не могут взаимодействовать друг с другом, за исключением сетей использующих XMPP.

У XMPP есть несколько альтернатив, разработанных сторонними производителями, тем не менее, клиентские части этих программ позволяют связываться с пользователями, клиенты которых работают через XMPP. Примером таких программ могут являться QIP и IM+. Оба этих клиента позволяют сочетать в себе несколько различных сетей, но регистрация все равно проводится на разных сайтах разработчиков этих сетей.

Большинство IM-сетей используют закрытые протоколы, поэтому альтернативные клиенты теоретически могут обладать меньшим количеством базовых функций, чем официальные, хотя на практике чаще бывает наоборот. Однако при изменениях протокола на стороне сервера сети альтернативные клиенты могут внезапно перестать работать, примером может быть недавняя блокировка большей части IP адресов РКН.

XMPP

XMPP Extensible Messaging and Presence Protocol — протокол обмена сообщениями и информацией, также известен как Jabber. Jabber - свободный для использования протокол для обмена мгновенными сообщениями в онлайн режиме.

Также может поддерживать передачу голосовых и видео сообщений, а также файлов. Из-за своей расширяемости Jabber позволяет держать свой собственный сервер мгновенных сообщений, а также позволяет хранить профиль локальной программы на локальном компьютере, т.е. не требует регистрации на сайтах разработчиков программ. На основе протокола XMPP уже открыто множество частных и корпоративных серверов XMPP.

Среди них есть достаточно крупные проекты, такие как Google Talk, Одноклассники, LiveJournal и др. Ранее протокол поддерживался также социальными сетями Facebook и ВКонтакте.

Преимущества и недостатки протокола XMPP

Преимущества

- Главным преимуществом XMPP является отсутствие центрального сервера обмена информацией, это означает, что любой человек может сделать свой собственный сервер обмена мгновенными сообщениями.
- XMPP серверы могут быть изолированы от общих сетей XMPP, используя модификацию /isolated при запуске программы, это позволит хранить профиль учетной записи на локальном компьютере. Многие реализации серверов также используют SSL-протокол при обмене между клиентом и сервером.
- Настраиваемая функциональность может быть надстроена поверх XMPP; для поддержки возможности взаимодействия различных сетей стандартные расширения поддерживаются XMPP Software Foundation. Приложения XMPP в дополнение к функциональности клиента сетевого общения включают в себя администрирование сети, распределение ресурсов, утилиты для совместной работы, обмен файлами, игры и мониторинг удалённых систем.

Недостатки

- Главным недостатком протокола XMPP является избыточность передаваемой информации более 70 % меж серверного трафика XMPP составляют статус-сообщения, которые оповещают о присутствии или отсутствии. Для решения этой проблемы компания – разработчик разрабатывает новые протоколы для уменьшения избыточного трафика

1. Практическая часть

Разработка общей структуры

Для реализации плана по модернизации программной архитектуры компании ЗАО “Дятлы-77” выбрано программное средство Skype. По сравнению описанными в данной работе конкурентами выбранное программное средство имеет возможности к расширению до бизнес версии, имеет возможность хранения истории переписок.

Это позволяет получить доступ к истории переписок в любое время и в тоже время позволяет передавать голосовые сообщения используя сервер как узел, связывающий 2 точки. Пользователи могут устанавливать программное обеспечение на локальных компьютерах и телефонах, авторизоваться с помощью уникальной учетной записи скайп и всегда иметь возможность оперативно решить любые вопросы с использованием мгновенных сообщений или голосовой связи. основными уязвимостями протокола XMPP являются:

- Атаки на TLS;
- TCP-атаки;
- Конфигурационные настройки.

Благодаря центру сертификации имеется возможность установить подлинность личности и клиента, и сервера. Клиент может быть уверен, что сервер, который предоставляет ему информацию о соединении, действительно достоверный сервер. И наоборот: сервер компании может быть уверен, что клиент, подключившийся к нему – именно сотрудник компании, а не стороннее лицо.

Обоснование задачи

Компании ЗАО Дятлы-77 понадобилось решение для быстрой коммуникации между пользователями, сотрудники IT отдела компании предложили 3 варианта программных решений

- Skype
- ICQ
- What’s App

Данные мессенджеры являются наиболее распространенными в современное время и могут быть использованы для коммуникации между работниками предприятия.

Программное обеспечение для передачи мгновенных сообщений

В курсовой работе будут предложены 3 варианта мессенджеров: Skype, ICQ, What’s App. Предлагаемые решения я опишу ниже.

Skype

Один из популярных мессенджеров обеспечивающий обмен мгновенными сообщениями, голосовую связь между другими пользователями Skype и звонки на стационарные телефоны.

Все это возможно благодаря VoIP, VoIP – интернет телефония, которая работает по IP протоколу сетевого уровня и поддерживает двустороннее голосовое общение и видео связь.

Для защиты информации Skype использует 256-битный протокол защиты AES. До 2011 года считалось, что разговоры по Skype анонимны, но после приобретения Skype компанией Microsoft дела пошли немного хуже. Компания Microsoft успешно сотрудничает с различными спецслужбами, эти изменения после 2011 года были внесены в соглашение о конфиденциальности между пользователем и Skype и успешно работают, благодаря технологии вмешательства запатентованной компанией Skype для спецслужб. Также компания Skype оставляет за собой право собирать информацию о пользователях.

Основной фишкой Skype является защищенность передачи сообщений

Защищенность передачи сообщений

Сообщения в Skype передаются в зашифрованном виде и в схеме передачи сообщений отсутствуют дополнительные узлы передачи, передача ведется от пользователя к пользователю напрямую с помощью peer-to-peer технологии.

Система авторизации пользователя на сервере авторизации Skype

Рисунок 12. Алгоритм регистрации пользователя в системе Skype

При регистрации нового пользователя Skype использует открытый ключ шифрования – RSA

После этого устанавливается соединение с сервером Skype через 256-битовый протокол AES. При помощи генератора случайных чисел создаётся ключ сеанса. Сервер проверяет логин на уникальность.

Сервер хранит имя пользователя и пароль, повторно прошедший процедуру хэширования. Далее сервер формирует и подписывает идентификационный сертификат на имя пользователя, который подтверждает проверочный и идентификационный ключи.

Сервер Skype хранит закрытый ключ шифрования и распространяет соответствующий ему открытый ключ с каждой копией программного обеспечения. В процессе регистрации пользователь выбирает логин и пароль. Skype на компьютере пользователя генерирует открытый и закрытый ключи.

Далее пользователь проходит авторизацию на сервере Skype, используя полученные учетные данные, проходит проверка на подлинность. Если проверка прошла успешно, пользователь получает доступ к сервисам Skype, в противном случае возвращается сообщение об ошибке.

ICQ

ICQ – бесплатное программное обеспечение для обмена информацией между пользователями, разработано для компьютеров с ОС Windows и Linux и телефонами на базе Android и iOS. . Позволяет пересылать как текстовые, так и видео сообщения через Интернет. Серверная часть ПО используется для централизованного хранения учетных записей. Обмен сообщениями между пользователями может быть осуществлён как через сервер, так и без него.

Служба является коммерческой, но её использование бесплатно. Служба разработана компанией Mirabilis. в 1996 году. В настоящее время служба является частью Mail.Ru Group.

Для использования службы требуется учётную запись для пользователя, которая может быть создана на официальном сайте компании разработчика или непосредственно в клиенте программы. История сообщений на серверах не сохраняется, и может храниться только локально программой-клиентом на устройстве пользователя, и быть доступной через её интерфейс.

Для поиска пользователей, необходимо знать уникальный идентификатор пользователя или его электронное имя (никнейм).

Обмен сообщениями

С каждым из контактов можно вести личную переписку. Если отправитель не отключил эту возможность, то, в зависимости от клиента, получатель информируется о наборе сообщения, что создаёт эффект присутствия отправителя. В случае, если в момент отправки сообщений адресат не находился в сети, они будут сохранены службой и доставлены адресату, как только тот подключится к сети.

Отправка файлов

В ICQ реализована передача файлов по технологии P2P, то есть при непосредственном интернет-соединении двух компьютеров, минуя сервер. Передача файлов возможна только тогда, когда статус у получателя «В сети».

Условия использования

Переписка в ICQ не является личной (конфиденциальной) в прямом смысле этого слова, даже несмотря на то, что активных собеседников, как правило, двое. В соответствии с правилами пользования сервисом, все права на передаваемую в рамках сервиса информацию передаются компании-владельцу в том числе права на публикацию и распространение по своему усмотрению. Факт использования сервиса означает принятие пользователем этих условий.

С признанием правил пользования (acceptable use policy) пользователь передаёт ICQ Inc. все авторские права на данные, которые он опубликовал в рамках службы ICQ.

What’s App

WhatsApp — бесплатное решение для обмена мгновенными текстовыми сообщениями для мобильных телефонов, также имеет веб-интерфейс для общения через компьютер. Также поддерживает видео-звонки и передачу файлов через Интернет

Компания WhatsApp Inc. впервые представила свой мессенджер в 2009 году а, с октября 2014 года принадлежит Facebook Inc. С 2016 года приложение официально стало бесплатным и по сей день является таким, пользователь оплачивает лишь использованный приложением интернет-трафик. Приложением пользуется больше миллиарда человек.

Технические подробности

WhatsApp использует модифицированный протокол Extensible Messaging and Presence Protocol. При установке создаётся аккаунт на сервере s.whatsapp.net, использующий номер телефона в качестве имени пользователя

Мультимедиа-сообщения отправляются путём загрузки изображения, звука или видео на HTTP-сервер и передачей гиперссылки на объект вместе с закодированным в Base64 уменьшенным вариантом изображения.

WhatsApp автоматически синхронизирует список контактов с телефонной книгой телефона. Это возможно благодаря тому, что все пользователи регистрируются по своему телефонному номеру.

Веб-версия WhatsApp расположена по адресу https://web.whatsapp.com/. Работа веб-версии осуществляется совместно с телефоном и возможна только если телефон подключён к сети Интернет.

С ноября 2017 года в приложении появилась функция удаления сообщения не только у себя, но и у собеседника (в том числе из чатов). Удаление возможно только в течение семи минут после отправки сообщения

Безопасность

Алгоритм генерации пароля и отсутствие шифрования в ранних версиях WhatsApp неоднократно критиковались

До августа 2012 года сообщения отправлялись без шифрования. С 15 августа 2012 по заявлению техподдержки WhatsApp сообщения шифруются в приложениях iOS и Android, однако метод шифрования не уточнялся

С апреля 2016 года с выходом обновления версии 2.16.12 WhatsApp включил сквозное шифрование (end-to-en*d*) для всех Шифрование распространяется на все типы сообщений: текст, фото, видео и голосовые сообщения. Шифрование также доступно в групповых чатах. Расшифровать подобные сообщения, по заявлениям компании, может только получатель, содержимое недоступно даже серверам

WhatsApp· В реализации используются алгоритмы ECDH на Curve25519, AES-256, AES-GCM, HMAC-SHA256, HDKF.

Стоимость

Мессенджер WhatsApp стал бесплатным с 18 января 2016 года. Ранее подписку за использование сервисом взималась плата в размере около 1 доллара США каждый год, начиная со второго года использования. На данный момент официальный клиент WhatsApp для всех типов смартфонов и телефонов (iPhone, Android, BlackBerry, Windows Phone, Nokia) бесплатен для скачивания и использования.

Внедрение программного обеспечения

На данный момент в компании функционирует аппаратное обеспечение, указанное на рисунке 1. И программное обеспечение, указанное на рисунке 2. Планируется внедрить в структуру компании программное обеспечение Skype и ICQ для осуществления быстрых коммуникаций между пользователями сети рисунок 14.

Общее сравнение предлагаемых решений

Таблица 1.

Общее сравнение предлагаемых решений

	Skype	ICQ	What’s App
Год разработки	2003	1996	2009
Компания владелец	Microsoft	Mail.ru Group	Facebook
Возможность развернуть ПО на собственном сервере	Нет	Да(в т.ч. с хранением локальной учетной записи)	Нет
Наличие Web-интерфейса программы	Да	Да	Да

Возможность связи с другими сетями	Нет	Да(необходимо создать учетную запись)	Нет
Поддерживаемые ОС	Windows/Linux/Android/iOS	Windows/Linux/Android/iOS	Windows/Linux/Andr
Алгоритм шифрования сообщений	Peer-to-peer	Peer-to-peer	End-to-end
Поддержка голосовых конференций	Да	Да	Да
Поддержка видео конференций	Да	Да	Да
Возможность передачи файлов	Да	Да	Да
Тип лицензии	adware	Adware и проприетарная	проприетарная
Возможность корпоративного использования	Skype-connect	Нет	Нет
Цена	Бесплатно	Бесплатно	Бесплатно

Список оборудования

Пользовательское

- Компьютеры на базе процессора Intel Core i5
- Процессор Intel Core i5-7400 Kaby Lake + куллер (3000MHz/LGA1151/L3 6144Kb)
- Материнская плата - GIGABYTE GA-H110M-S2
- Kingston HyperX Fury Black PC4-19200 DIMM DDR4 2400MHz CL15 - 8Gb
- Накопитель - SSD - 120Gb - Kingston A400 SA400S37/120G
- Монитор Samsung S22D300NY
- Клавиатура DEXP K-401BU
- Мышь проводная DEXP CM-904BU
- Корпус mATX FORMULA FA-703B, Mini-Tower, 450Вт.
- Принтер Kyocera P6035CDN

Серверное

- Точка доступа MikroTik wAP ac (Black) RBwAPG-5HacT2HnD-be – выполняет роль WiFi роутера
- Маршрутизатор MikroTik RB2011iLS-IN – выполняет роль фаервола и коммутации каналов
- STSS Flagman MX240.5-008LH – сервер общего назначения(dns-dhcp-ad-fileserver)

Рисунок 13. Существующая архитектура сети компании ЗАО “Дятлы-77”

Программное обеспечение

Планируется внедрить в программную архитектуру компании 2 мессенджера – Skype версии 8.23 и ICQ версии 10.0

Компьютер пользователя

- Операционная система Windows 10x64
- Браузер Google Chrome v64
- Microsoft Office 2016
- Skype 8.23
- ICQ 10.0.12251
- PDF Creator
- Adobe Acrobat
- ESET Endpoint Antivirus 5.0.2265.1

Сервер

- Операционная система Windows Server 2008 R2
- ESET Endpoint Antivirus 5.0.2265.1

Исполняемые роли:

- Domain Controller
- DHCP
- Active Directory
- File Server

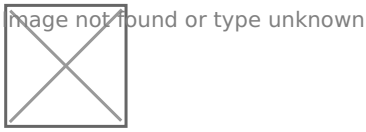


Рисунок 14. Планируемая программная архитектура компании

После внедрения программного обеспечения, сотрудники смогут общаться друг с другом используя как Skype так и ICQ.

Установка программного обеспечения

Для реализации программной модернизации компании, требуется скачать программное обеспечение с официального сайта. Для этого нужно зайти на сайт Skype.com и нажать на кнопку загрузить скайп. Загрузчик автоматически определит операционную систему.

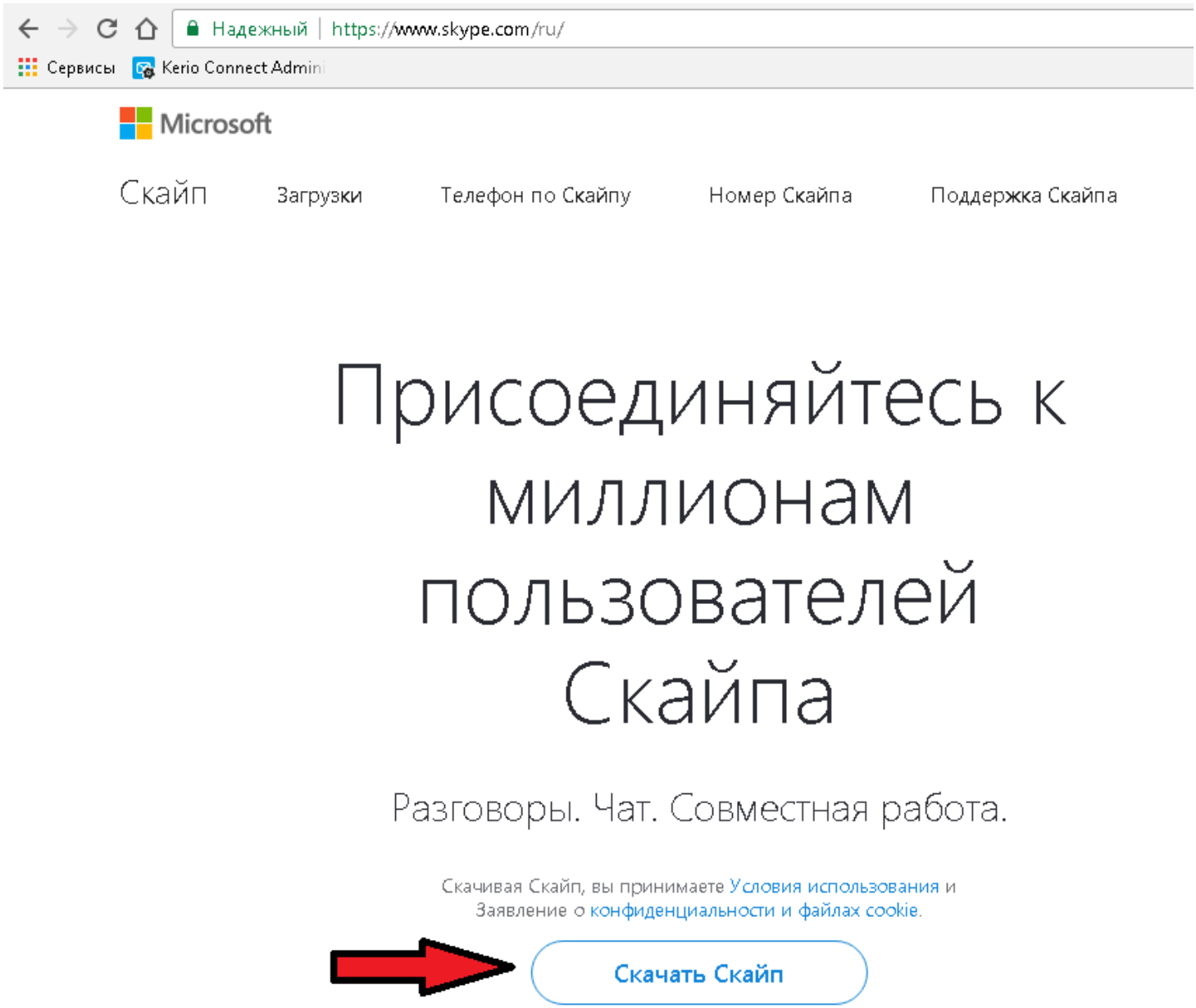


Рисунок 15. Скачивание Skype

Для установки необходимо запустить файл, скачанный с официального сайта компании Skype – www.skype.com/ru и нажать кнопку запустить.

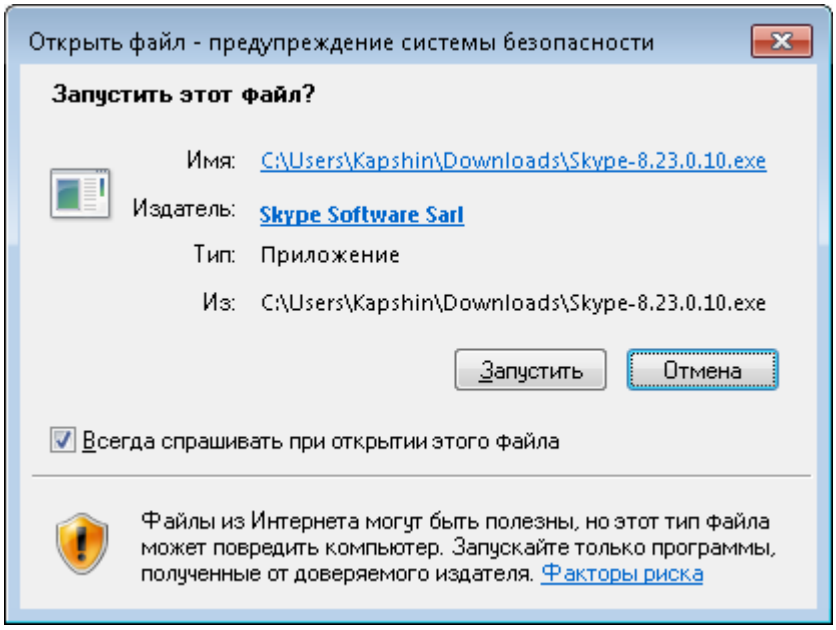


Рисунок 16. Установка Skype

Нажать кнопку *Установить* и дождаться установки программы

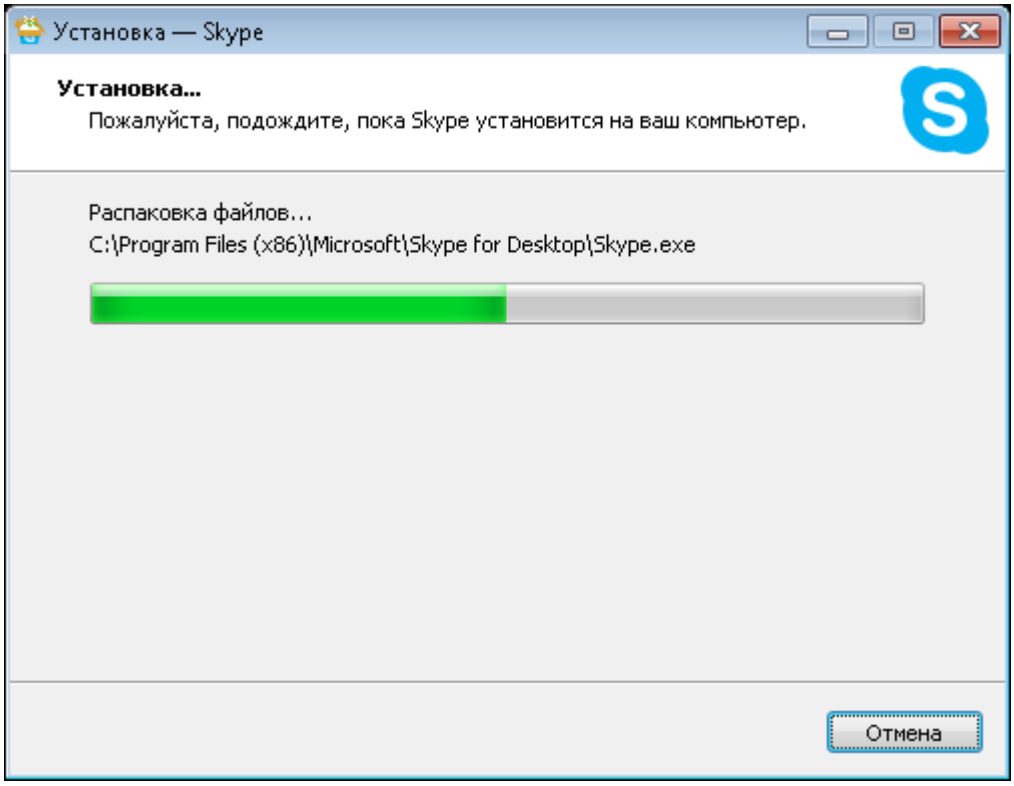


Рисунок 17. Установка Skype

После установки Skype войти в программу с использованием своей учетной записи.

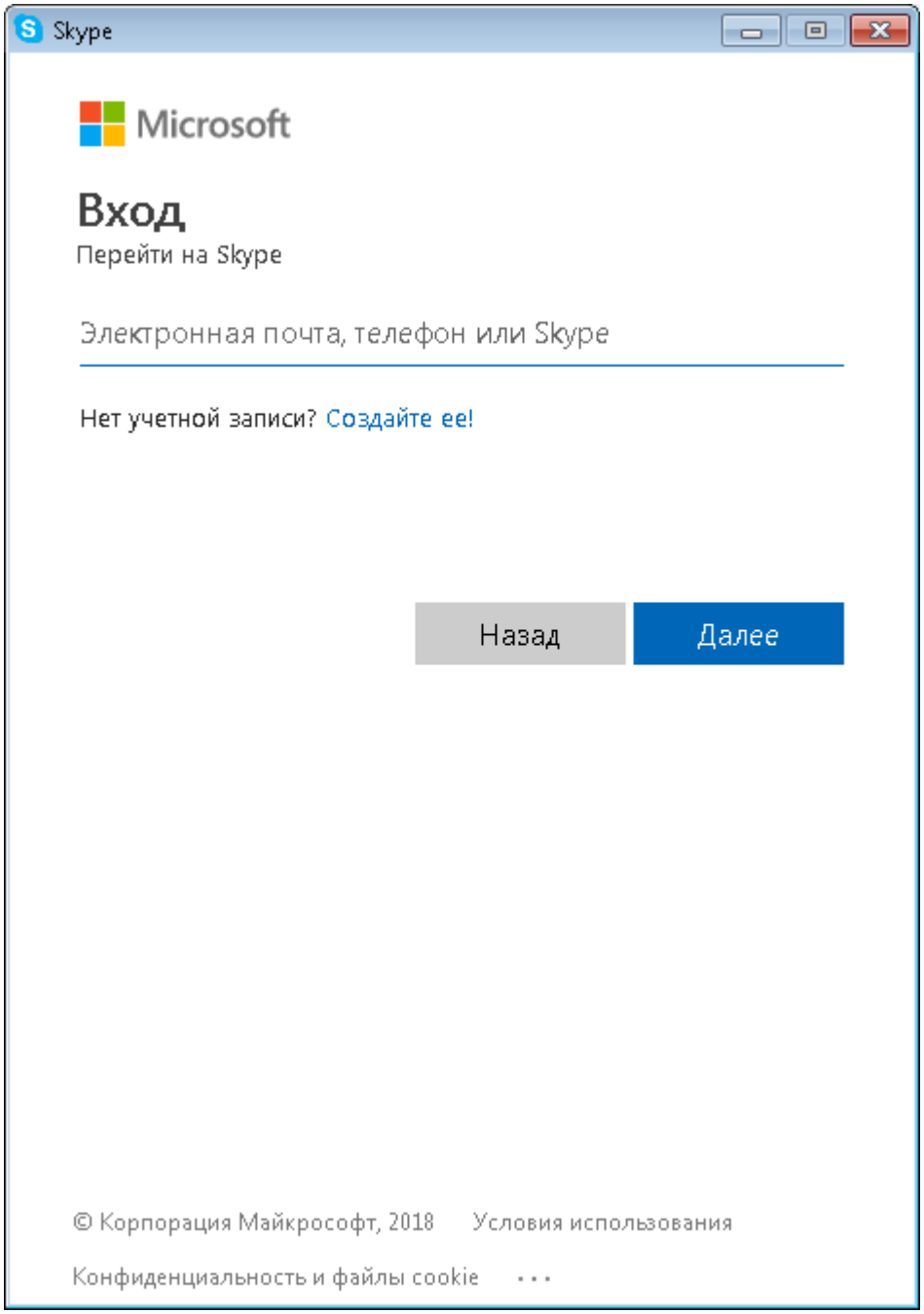


Рисунок 18. Окно логина в Skype

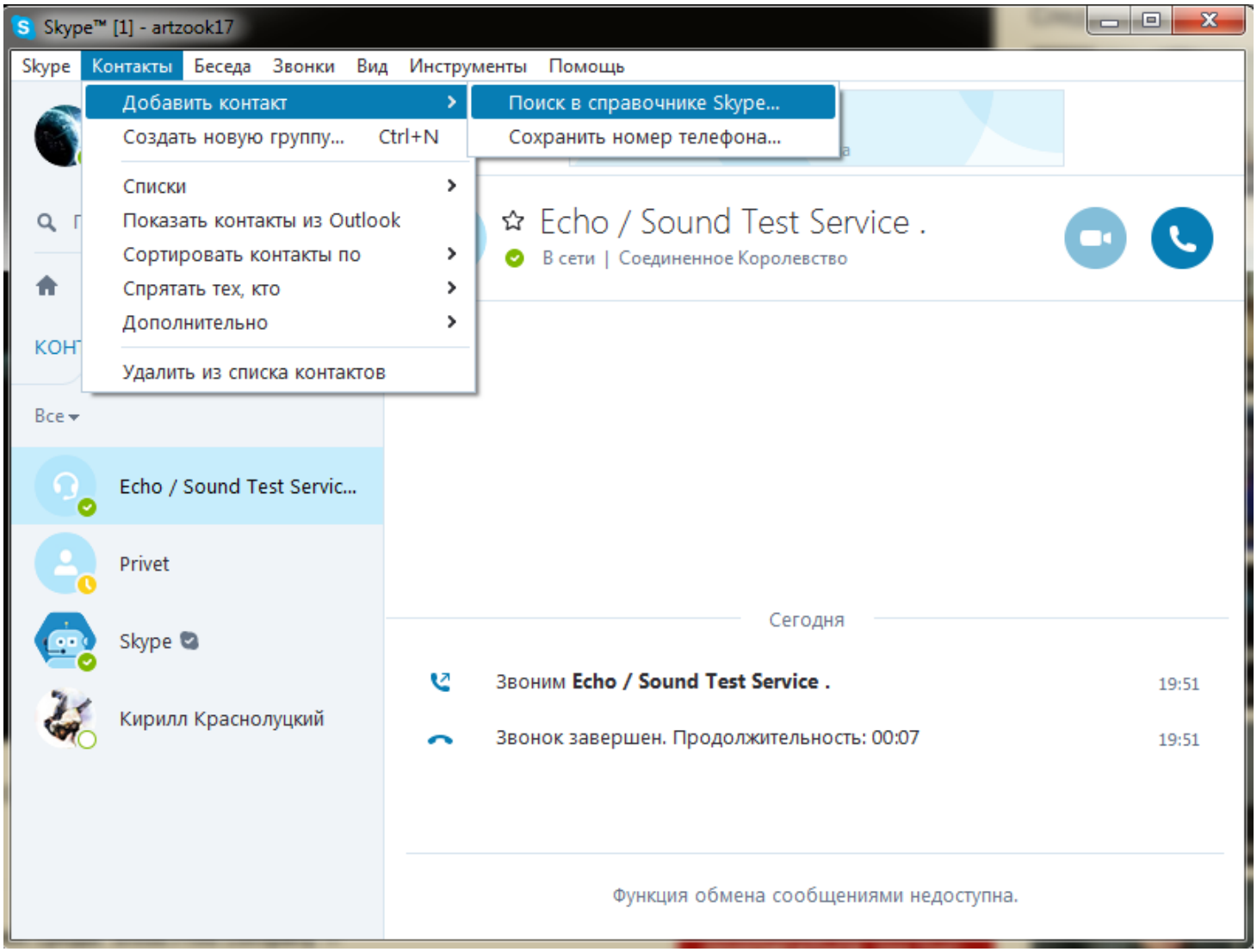
Контрольный пример реализации

Для проверки работоспособности программного обеспечения пробую установить связь с другим пользователем. Для этого, нужно:

- Найти другого пользователя в общем справочнике Skype
- Добавить пользователя в свой справочник Skype
- Написать или позвонить пользователю.

Установка связи с другим пользователем Skype

Во вкладке *Контакты* нажать добавить контакт и выбрать поиск в справочнике Skype.



.Рисунок 19. Поиск пользователей Skype

В строке справочника необходимо ввести никнейм другого пользователя скайп. К примеру, keeper

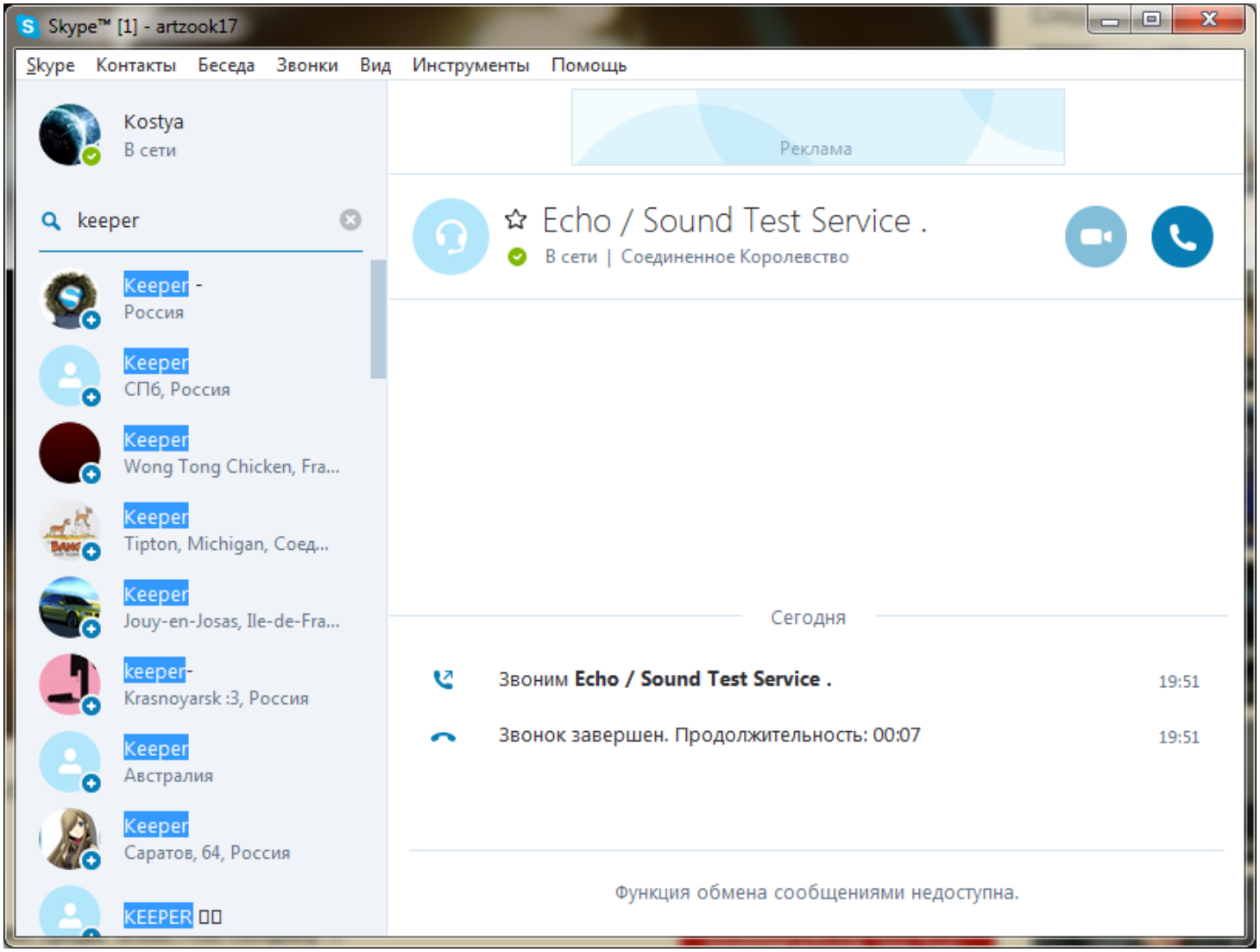


Рисунок 20. Добавление пользователей Skype в своей список контактов

Пример текстового сообщения

Для отправки текстового сообщения необходимо:

- Выбрать собеседника
- Курсором мыши выбрать поле для ввода сообщений
- Используя клавиатуру написать сообщение
- Отправить сообщение нажатием кнопки *Отправить*.

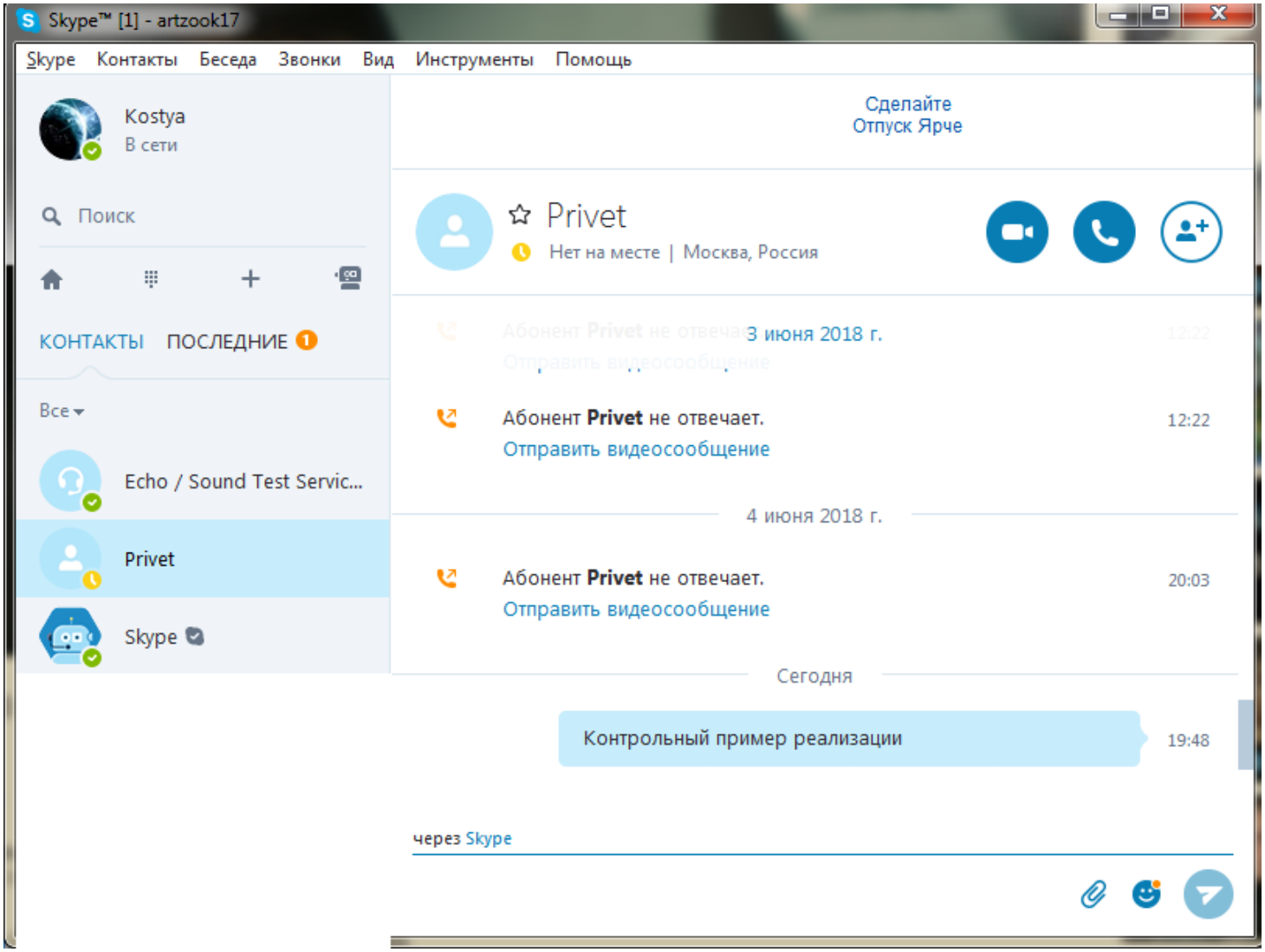


Рисунок 21. Пример отправки текстового сообщения

Пример голосового звонка

Для совершения голосового звонка необходимо:

- Выбрать собеседника
- Курсором мыши нажать на кнопку с изображением трубки вверху экрана
- Дождаться установления связи с собеседником

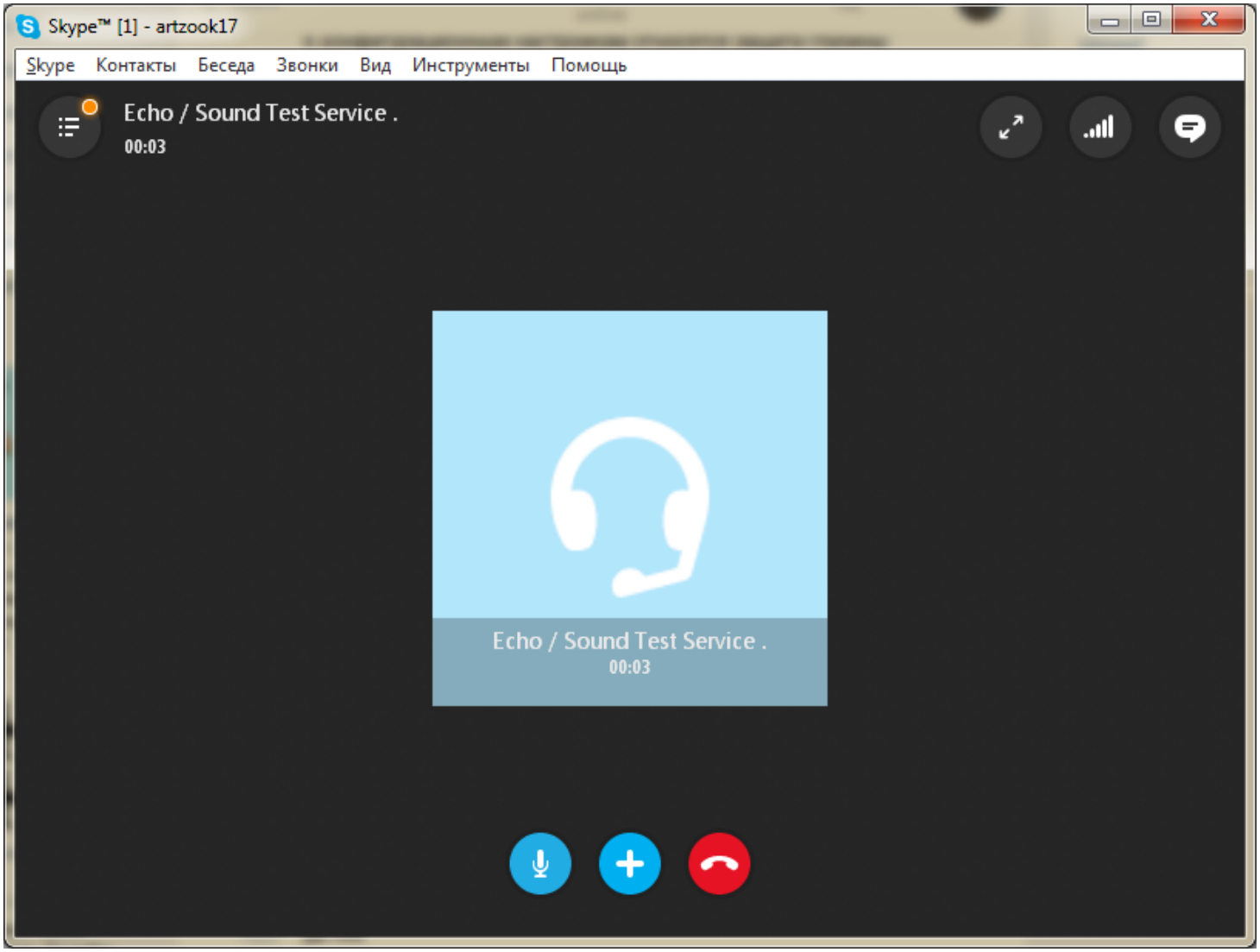


Рисунок 22. Голосовой вызов пользователя в Skype

Защищенность протоколов передачи мгновенных сообщений

Каждый из протоколов, согласно которым работает внедряемое программное обеспечение, использует различные типы шифрования, чем позволяет безопасно обмениться как текстовой, так и голосовой информацией. Также в компании предусмотрен антивирус ESET Endpoint Antivirus версии 5.0, который позволит защитить компьютер от нежелательных приложений. Также в компании предусмотрен встраиваемый межсетевой экран, который настроен на маршрутизаторе MikroTik RB2011iLS-IN-36, который также анализирует трафик и отсеивает нежелательные или инфицированные пакеты информации.

Заключение

В заключении могу сказать, что мессенджеры плотно вошли в жизнь человечества и с каждым годом количество пользователей будет расти. различных сфер деятельности, которые пользуются программами для быстрой коммуникации. Сейчас каждая компания использует квик мессенджер, будь то Skype, ICQ или написанный специально для компании.

Компания ЗАО Дятлы -77 выбрала для себя мессенджер Skype. По сравнению описанными в данной работе конкурентами выбранное программное средство имеет возможности к расширению до бизнес версии, имеет возможность хранения истории переписок.

Это позволяет получить доступ к истории переписок в любое время и в тоже время позволяет передавать голосовые сообщения используя сервер как узел, связывающий 2 точки. Пользователи могут устанавливать программное обеспечение на локальных компьютерах и телефонах, авторизоваться с помощью уникальной учетной записи скайп и всегда иметь возможность оперативно решить любые вопросы с использованием мгновенных сообщений или голосовой связи

С точки зрения постоянности связи это хороший выбор. Решение Skype является достаточно актуальным потому, что оно бесплатно, поддерживает телефонные звонки, видеоконференции, а также благодаря своей популярности решает вопрос конференции с пользователями из других стран.

QIP позволяет развернуть собственный сервер при поддержке XMPP, а также, при желании пользователи могут добавить другие варианты сетей использующих XMPP. Совмещая при этом хороший уровень защиты своих данных, как при использовании Skype, который шифрует всю информацию, начиная с регистрации учетной записи, заканчивая голосовыми сообщениями, используя Peer-to-peer шифрование, являющееся достаточно популярным из-за своей безопасности.

Безусловно, Peer-to-peer имеет свои минусы, но вопрос безопасности для сотрудников компании является достаточно важным, а Peer-to-peer , хранящий информацию на узлах конечных пользователей решает проблему перехвата пакетов при передаче.

С большей вероятностью в ближайшее время IM-системы сравняются и превысят уровень использования в сравнении с почтовыми клиентами. В связи с растущей популярностью, растет и количество угроз на такой вид угроз, но ведущие IT компании не стоят на месте и предлагают варианты решений для защиты информации, как текстовой, так и голосовой.

Литература

- Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2008. — 272 с. — ISBN 978-5-388-00069-9.
- Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.— 544 с.—ISBN 5-94074-383-8
- К. Шеннон. Теория связи в секретных системах с // Перевод С. Александр Венедюхин, Ключи, шифры, сообщения: как работает TLS (Техническое описание TLS), 04/09/2015
- https://privacy.microsoft.com/ru-ru/privacystatement
- http://www1.cs.columbia.edu/~salman/skype/skype2.pdf
- https://cyberleninka.ru/article/v/otsenka-bezopasnosti-sistem-mgnovennogo-obmena-soobscheniyami-metodom-analiza-ierarhiy
- https://xmpp.org/
- https://www.skype.com/ru/
- https://www.skype.com/ru/legal/
- https://icq.com/windows/ru
- https://www.whatsapp.com/