К ВОПРОСУ РАЗРАБОТКИ ПРОТОКОЛА ЗАЩИТЫ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СИСТЕМАХ IP-ТЕЛЕФОНИИ

А.Б. Маховиков, кандидат технических наук, доцент;
К.В. Матрохина.
Санкт-Петербургский горный университет.
Е.Н. Трофимец, кандидат педагогических наук, доцент.
Санкт-Петербургский университет ГПС МЧС России

Рассмотрен оригинальный протокол защищенной передачи информации для организации IP-телефонии в корпоративных системах связи. Проведен анализ известных используемых протоколов защиты информации в IP-телефонии, выявлены их достоинства и недостатки. Дано описание процесса установления соединения, передачи текстовых сообщений и голосовой связи на основе разработанного протокола, обоснованы его практическая значимость и целесообразность внедрения.

Ключевые слова: корпоративная сеть, IP-телефония, протокол передачи информации, шифрование, управление данными

TO THE DEVELOPMENT OF THE INFORMATION PROTECTION PROTOCOL IN CORPORATE IP TELEPHONY SYSTEMS

A.B. Makhovikov; K.V. Matrokhina. Saint-Petersburg mining university.
E.N. Trofimets. Saint-Petersburg university of State fire service of EMERCON of Russia

The paper considers the protocol of secure information transfer for the corporate IP-telephony system. The article analyzes the advantages and disadvantages of the known protocols used. The description of the process of establishing a connection, sending text messages and voice communication in the developed protocol is given. Its practical significance and expediency of use are described.

Keywords: corporate network, IP-telephony, information transfer protocol, encryption, data management

В настоящее время мессенджеры стали неотъемлемой частью нашей жизни. Они используются для совершения звонков и видеоконференций, отправки текстовых и голосовых сообщений. Однако в корпоративном секторе популярные мессенджеры в качестве инструментов IP-телефонии используются достаточно редко. Причина данного обстоятельства состоит в том, что серверы, на которых хранится вся передаваемая информация, принадлежат компаниям-разработчикам, следствием чего является возникновение потенциальной угрозы конфиденциальности корпоративной информации.

Таким образом, актуальной является задача разработки системы, в которой была бы реализована идея объединения использования типовых клиентских приложений, установленных на смартфонах сотрудников, с технологией обработки передаваемой информации на собственном корпоративном сервере. Одним из основных элементов такой системы является протокол передачи данных, который должен обеспечивать гарантированную защиту от возможной утечки конфиденциальной информации.

Используемые протоколы защиты информации в IP-телефонии

Обеспечение безопасности передаваемой информации является одной из важнейших задач любой современной технологии связи, в том числе и IP-телефонии. В данных технологиях реализованы методы, направленные на предотвращение ряда угроз, возникающих при передаче данных по каналам связи: сниффинг, перехват и манипулирование данными, подмена и взлом пользовательских данных, ограничение доступности. Обсуждению данных проблем посвящены работы Б.С. Гольдштейна [1], А.В. Рослякова [2], Г.С. Казиева [3], А.В. Пролетарского [4] и других авторов.

В настоящее время в корпоративном секторе для организации IP-телефонии, видео и аудиоконференций, передачи мгновенных сообщений обычно используются SIP-сервера (рис. 1). При этом следует отметить, что для организации IP-телефонии вместо типовых приложений для смартфонов используются IP-телефоны.

Рис. 1. **Пример организации корпоративной системы связи на базе протокола SIP**

Для обеспечения защиты информации при её передаче в рассматриваемой сети используются три вида протоколов:

– протоколы защиты медиаинформации (SRTP);

– протоколы генерации/распределения ключей для протоколов защиты медиаинформации (ZRTP);

– протоколы защиты сигнализации (SIP) [5].

Вышеупомянутые протоколы имеют недостатки, а значит не могут гарантировать комплексной защиты информации. Протокол TLS использует одинаковый набор ключей (открытого и закрытого) для аутентификации сервера и для обмена ключами протокола SRTP.

Протокол ZRTP использует некриптостойкие ключи для шифрования.

В связи с этим для создаваемой корпоративной системы IP-телефонии было принято решение разработать собственный протокол защищенной передачи информации.

Система включает в себя серверное приложение для операционных систем CentOS или MS Windows, приложение под MS Windows для администрирования системы и клиентские приложения для смартфонов под управлением операционных систем Google Android и Apple iOS, размещенные, соответственно, в Google Play и AppStore. Принципиальная система представлена на рис. 2.

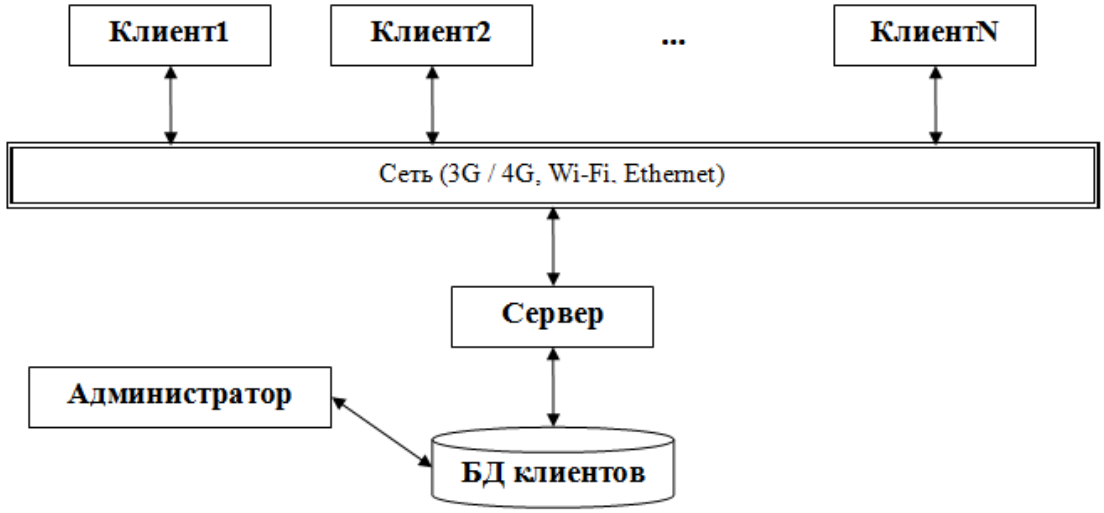

Рис. 2. **Структурная схема системы (БД – база данных)**

Сервер является центральным элементом комплекса и в процессе своего функционирования взаимодействует со всеми остальными элементами по защищенным каналам связи. Базовые и сеансовые ключи генерируются при установке или переустановке сервера.

Сервер является приложением для операционных системы CentOS или MS Windows.

Основными функциями сервера являются:

– хранение основных ключей;

– хранение сведений о сотрудниках компании и их смартфонах;

– обеспечение авторизации клиентов;

– обеспечение клиентов списками контактов;

– установление и разрыв соединения между клиентами;

– генерация базовых и сеансовых ключей.

Структурная схема сервера представлена на рис. 3.

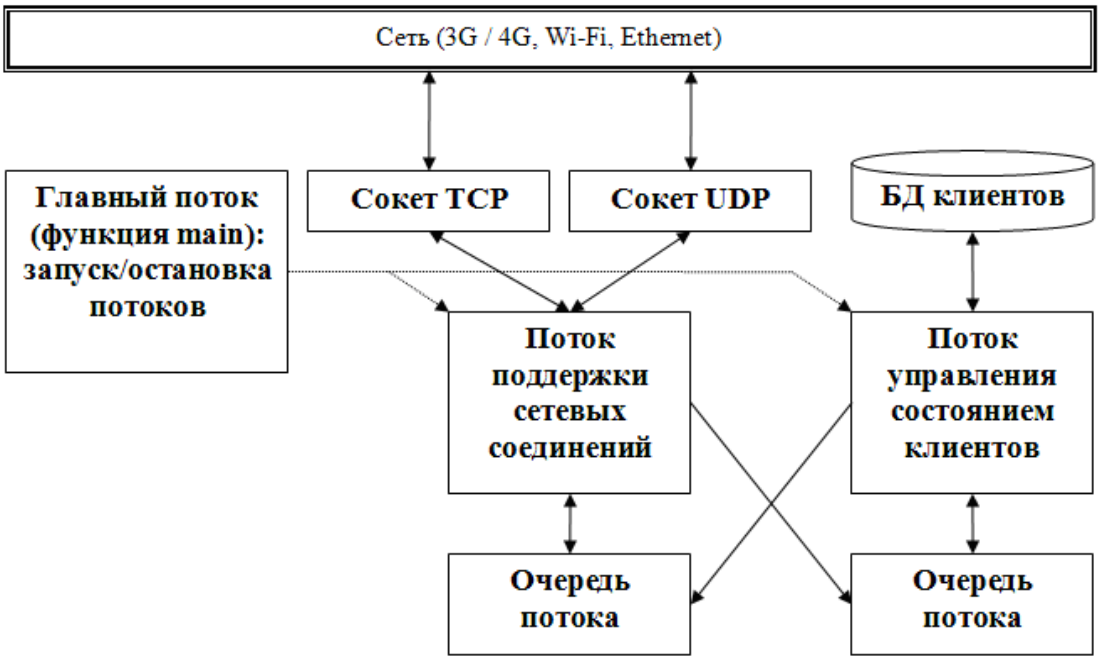

Рис. 3. **Структурная схема сервера**

Клиент представляет собой приложение для смартфонов под управлением операционных систем Google Android, Apple iOS. Ядро системы для Google Android написано Java Native Interface и Си, для Apple iOS на Object Си и Си.

Основными функциями клиента являются:

– осуществление звонков;

– передача текстовых сообщений;

– обмен файлами между абонентами сети.

Структурная схема клиента представлена на рис. 4.

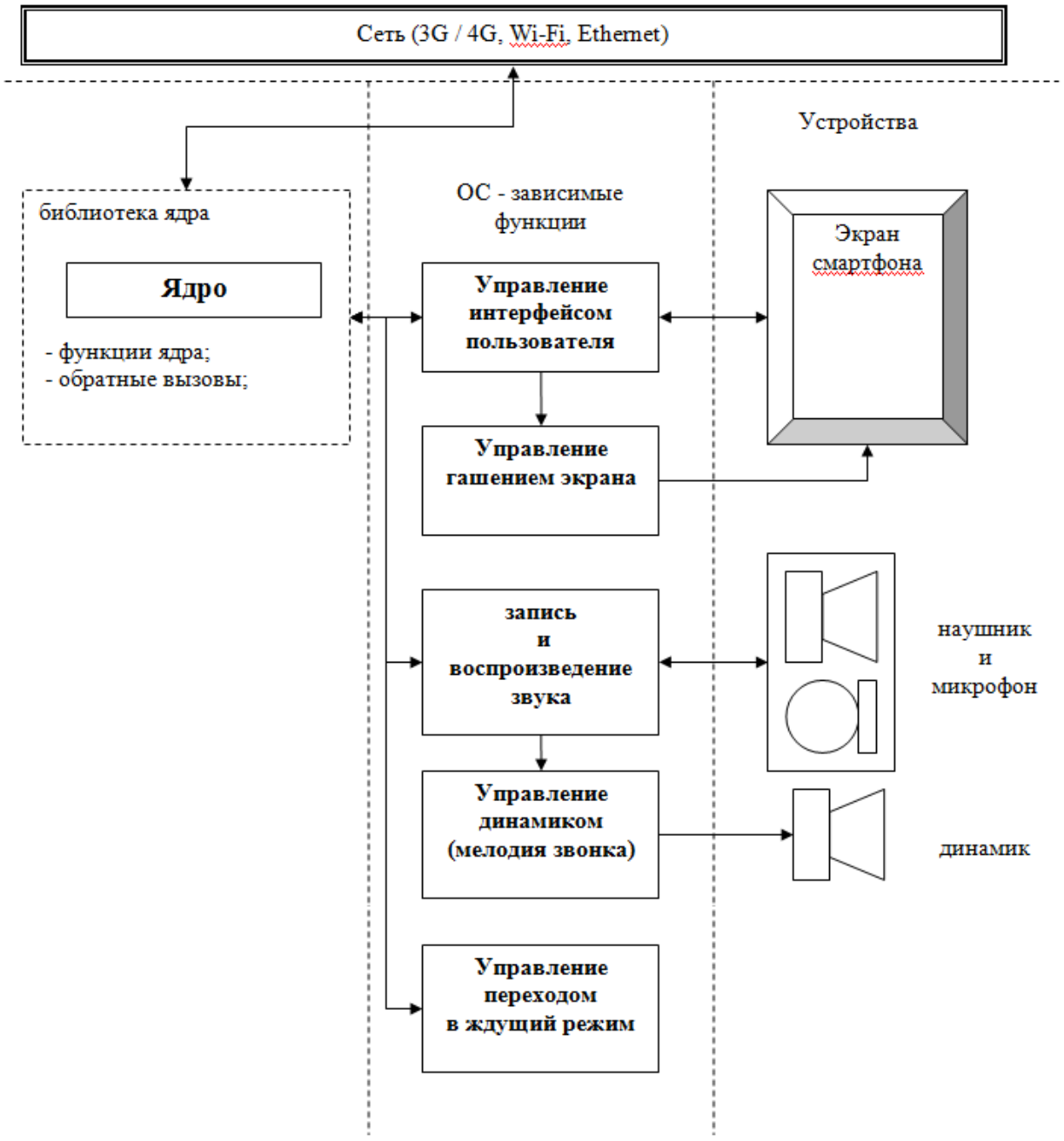

Рис. 4. **Структурная схема клиента**

Так как разрабатываемая система связи является корпоративной, то существует принципиальная возможность настройки абонентских смартфонов непосредственно в офисе компании. В ходе этой настройки в клиентские приложения вводятся базовые ключи

шифрования, которые, таким образом, не нужно передавать по каналам связи. Это означает возможность применения только алгоритмов симметричного шифрования, которые, по сравнению с ассиметричными алгоритмами, отличаются большей криптостойкостью при меньшей длине ключа и меньшими вычислительными затратами. Одним из лучших таких алгоритмов считается российский ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования [6].

Далее описаны процессы, которые осуществляются на основе разработанного протокола, на базе ГОСТ 28147–89 в разработанной системе.

Описание функций разработанного протокола

Авторизация. После запуска клиент переходит в состояние «соединяюсь» и по известным IP-адресу и порту устанавливает TCP-соединение с сервером. В случае успешного соединения сервер переходит в состояние «ожидаю авторизацию», а клиент переходит в состояние «авторизуюсь» и направляет пакет со своим идентификатором и двумя сгенерированными числами, которые являются половиной идентификатора сессии и сессионного ключа. Пакет зашифрован с помощью базового ключа клиента. Если совпадают первые половины идентификатора сессии и сессионного ключа, то авторизация считается успешной.

После успешной авторизации клиент начинает периодически «пинговать» сервер. В каждом зашифрованном пинг-пакете, а также во всех пакетах, передаваемых с клиента, содержится уникальный идентификатор подключения, который использовался при авторизации. IP-адрес и порт клиента запоминаются сервером. Если в течение определенного интервала времени пинг-пакеты не приходят, то авторизация данного клиента пропадает. Дополнительно отключение клиента возможно путем отправки специального сообщения. Как только сервер получает пакет с сообщением об успешной авторизации, он отправляет клиенту список абонентов.

Поддержание канала. Для поддержания канала в активном состоянии клиент через определенные промежутки времени отправляет на сервер «пинг-пакеты». Сервер на них отвечает и определяет время, когда поступил последний пакет, если превышено допустимое время ожидания, то сервер разрывает соединение.

Клиент также непрерывно измеряет время, прошедшее с момента прихода последнего пинг-пакета от сервера, и в случае превышения допустимого его значения (то есть в случае «молчания» сервера), разрывает соединение и предпринимает попытку снова осуществить авторизацию. Попытки авторизации производятся клиентом через равные промежутки времени в бесконечном цикле. При этом абонент имеет возможность в любое время завершить работу клиента. На рис. 5 представлена диаграмма, отражающая функции «Авторизовать и поддерживать соединение».

Передача текстовых сообщений. Для обмена текстовыми сообщениями клиент-отправитель создает у себя сессию смс-структуру данных, содержащую идентификатор клиента-адресата, тип сессии («смс») и информацию об отправленных и принятых сообщениях, включающую текст, время отправки, время жизни, статус («отправлено», «доставлено», «прочитано») и время последнего изменения статуса. Клиент-отправитель с заданной периодичностью просматривает сессию и удаляет из нее сообщения, время жизни которых истекло.

Для отправки сообщения клиент-отправитель формирует пакет «смс», включающий идентификаторы клиента-отправителя, клиента-адресата, сообщения, содержимое сообщения, время жизни и время его создания. Этот пакет шифруется сессионным ключом и отправляется на сервер. Статус сообщения устанавливается равным «отправлено» и в сессию заносится время отправки. Сервер расшифровывает пакет, изымает оттуда идентификатор клиента-адресата, перешифровывает пакет его сессионным ключом и пересылает его ему.

Клиент-адресат расшифровывает пакет, и, если он еще не обменивался сообщениями с данным клиентом-отправителем, то создает сессию, содержащую идентификатор клиента-отправителя и тип сессии («смс»). Содержимое сообщения, время жизни и время его создания, идентификатор сообщения заносятся в сессию. Статус сообщения устанавливается равным «доставлено», время изменения статуса равным текущему времени, и на сервер отправляется пакет «подтверждение смс», содержащий идентификаторы клиента-адресата, клиента-отправителя, сообщения, его статус «доставлено» и время доставки. После прочтения сообщения абонентом статус меняется на «просмотрено» и на сервер посылается пакет со статусом «просмотрено» и временем просмотра. Пакеты «подтверждение смс» шифруются сессионным ключом клиента-адресата.

Сервер расшифровывает пакет, изымает оттуда идентификатор клиента-отправителя, перешифровывает пакет его сессионным ключом и пересылает его ему.

При получении пакета «подтверждение смс» клиент-отправитель заносит в сессию статус сообщения и время изменения статуса.

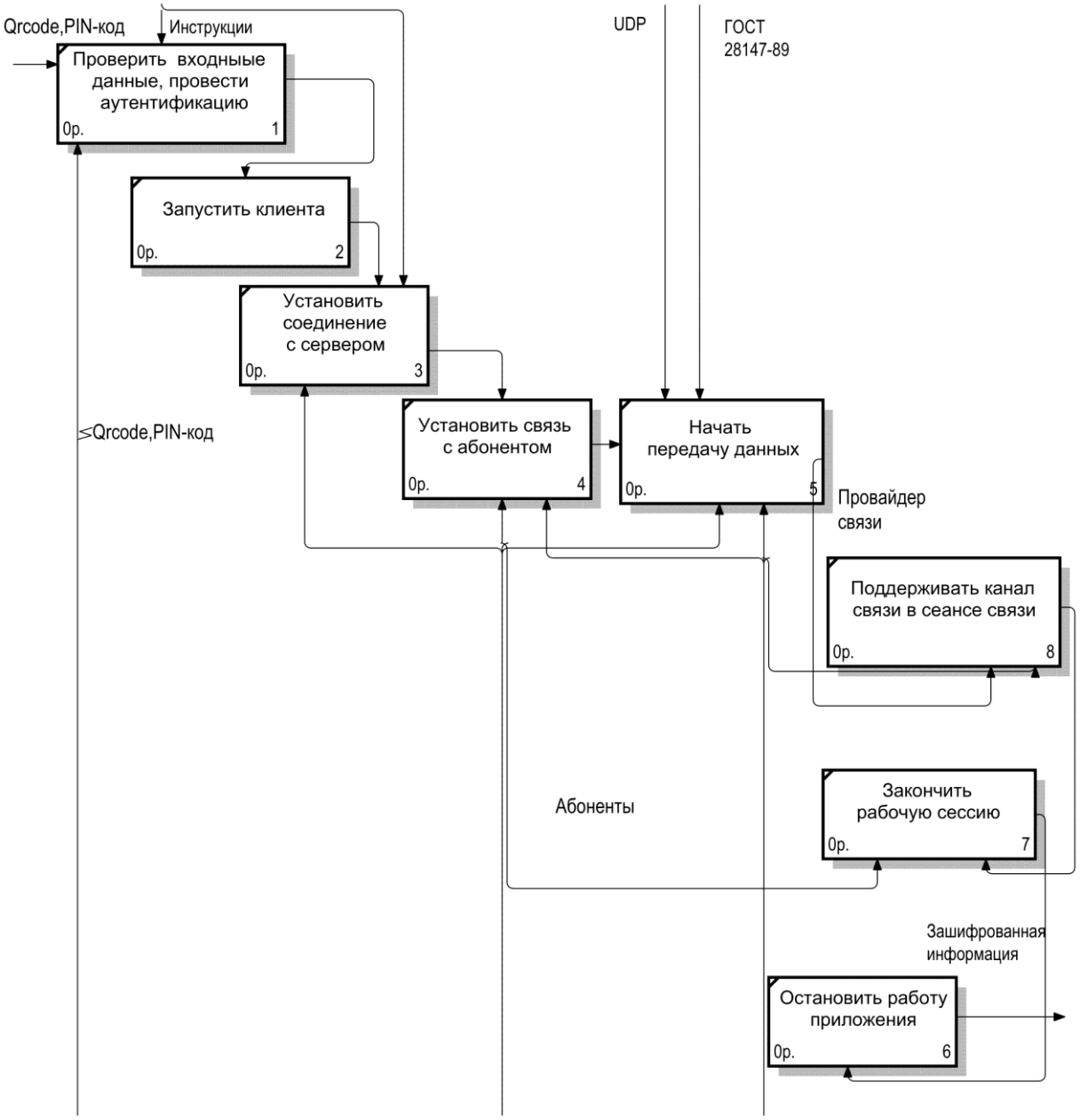

Рис. 5. **Диаграмма декомпозиции «Авторизовать и поддерживать соединение»**

Звонок. Клиент-инициатор организовывает у себя сессию звонка (вызывая абонента) – структуру данных, содержащую идентификатор клиента-адресата, тип сессии («звонок»), состояние сессии («ожидаю ответ») и идентификатор сессии клиента-инициатора. Также он генерирует сеансовый ключ.

Далее клиент-инициатор передает серверу пакет «старт», содержащий тип сессии («звонок»), идентификаторы сессии клиента-инициатора, клиента-инициатора, клиента-адресата и сеансовый ключ. Этот пакет зашифрован сессионным ключом.

При получении стартового пакета сервер инициирует у себя сессию звонка, используя информацию из него. Более того, сервер генирирует идентификатор сессии клиента-адресата. Далее он отправляет клиенту-адресату пакет «старт», содержащий тип сессии («звонок»), идентификаторы сессии клиентов и сеансовый ключ.

Получив стартовый пакет, клиент-адресат уведомляет абонента о входящем звонке.

Сессия переводится в состояние «разговор» в случае, если входящий звонок принят.

Далее клиенты отправляют на сервер короткие UDP-пакеты. Данные пакеты зашифрованы сеансовым ключом. Роль сервера состоит в перенаправлении пакетов между клиентом-инициатором и клиентом-адресатом. Как только будут получены UDP пакеты, сессия переходит в рабочее состояние, и она передает голосовые пакеты на сервер. Пакеты зашифрованы сеансовым ключом.

Если один из клиентов не отвечает в течение определенного времени на звонок, то другой клиент (взаимодействующий) отправляет серверу пакет «конец связи». Когда сервер получает данный пакет, он удаляет рабочую сессию (рис. 6).

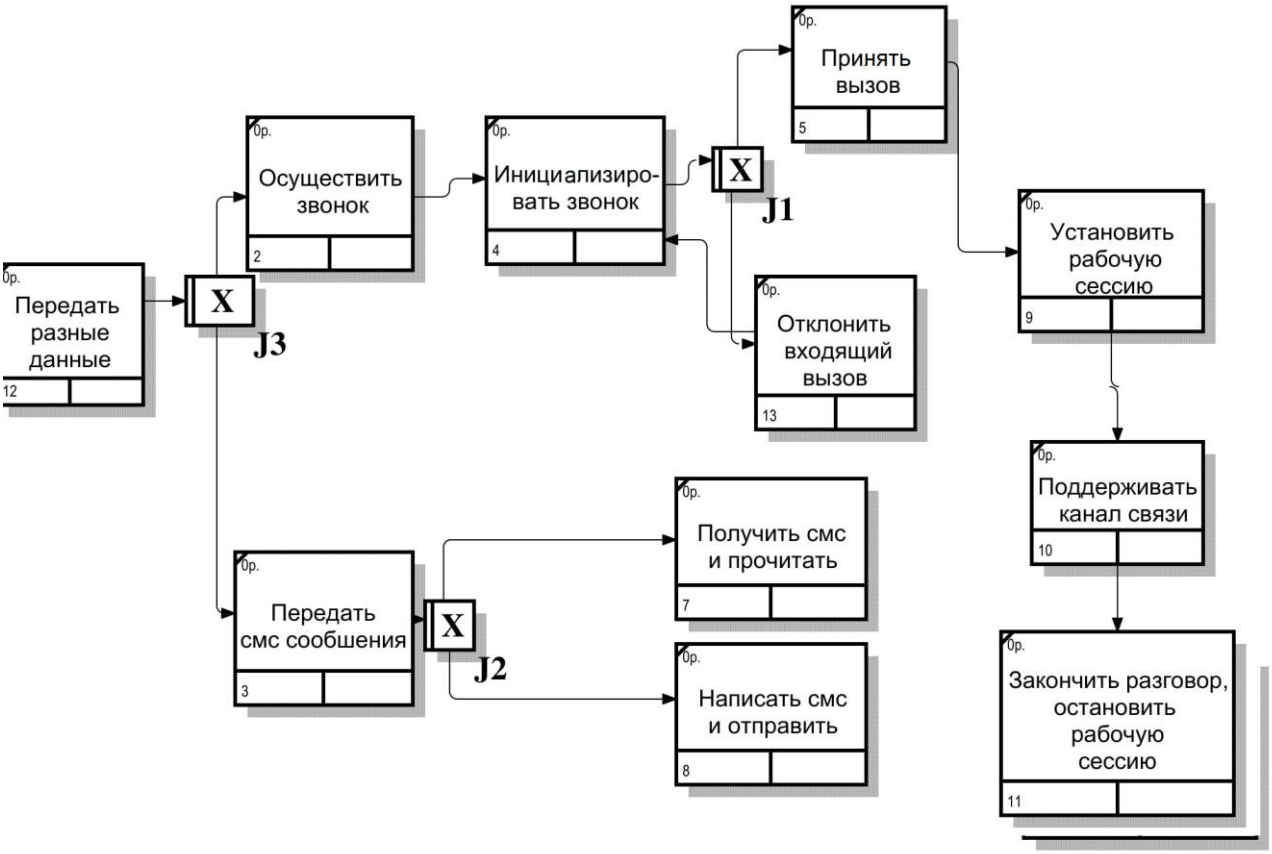

Рис. 6. **Декомпозиция блока «Передавать данные»**

В современном мире информация является одним из ценнейших ресурсов, поэтому ее защита – важная задача. В силу возрастающей популярности IP-телефонии, все острее встает вопрос обеспечения ее безопасности в общем и конфиденциальности разговоров в частности.

Знание основных источников опасности для сетей IP-телефонии, а также понимание методов устранения этих угроз поможет сохранить репутацию и финансовые ресурсы компании.

В данной статье приведено описание функций разработанного защищенного протокола и структурные компоненты системы.

Протокол применен в защищенной корпоративной системе связи Hidden Net, которая прошла тестирование во многих зарубежных и российских компаниях. В результате был сделан вывод, что Hidden Net удобная, надежная система, гарантирующая конфиденциальность информации и целостность данных.

Литература

1. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP-Телефония. СПб.: БХВ-Петербург, 2014. 336 с.

2. Росляков А.В., Самсонов М.Ю., Шибаева И.В. IP-телефония. 2-е изд. М.: Эко-Трендз, 2003. 252 с.

3. Казиева Г.С. IP-телефония и видеосвязь. Алматы: АИЭС, 2007. С. 56.

4. IP-телефония в компьютерных сетях / А.В. Пролетарский [и др.]. 2-е изд., испр. М.: НОУ Интуит, 2015. 226 с.

5. Ковцур М.М. Протоколы обеспечения безопасности IP-телефонии // Первая миля. 2012. Т. 32. № 5. С. 18–27.

6. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. URL: https://ru.wikipedia.org/wiki/ГОСТ 28147–89 (дата обращения: 25.03.2020).

References

1. Gol'dshtejn B.S., Pinchuk A.V., Suhovickij A.L. IP-Telefoniya. SPb.: BHV-Peterburg, 2014. 336 s.

2. Roslyakov A.V., Samsonov M.Yu., Shibaeva I.V. IP-telefoniya. 2-e izd. M.: Eko-Trendz, 2003. 252 s.

3. Kazieva G.S. IP-telefoniya i videosvyaz'. Almaty: AIES, 2007. S. 56.

4. IP-telefoniya v komp'yuternyh setyah / A.V. Proletarskij [i dr.]. 2-e izd., ispr. M.: NOU Intuit, 2015. 226 s.

5. Kovcur M.M. Protokoly obespecheniya bezopasnosti IP-telefonii // Pervaya milya. 2012. T. 32. № 5. S. 18–27.

6. GOST 28147–89. Sistemy obrabotki informacii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya. URL: https://ru.wikipedia.org/wiki/GOST 28147–89 (data obrashcheniya: 25.03.2020).