На правах рукописи

Нопин Сергей Викторович

ПЕРЕДАЧА МУЛЬТИМЕДИЙНЫХ ДАННЫХ ПО ЦИФРОВЫМ КАНАЛАМ В РЕЖИМЕ, ЗАЩИЩЕННОМ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Специальность 05.12.13

«Системы, сети и устройства телекоммуникаций»

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Новосибирск – 2008

Работа выполнена на кафедре “Средства связи и информационная безопасность” ГОУ ВПО “Омский государственный технический университет”

Научный руководитель:
доктор технических наук, профессор Василий Андреевич Майстренко

Официальные оппоненты: доктор физико-математических наук, профессор Попков Владимир Константинович
кандидат технических наук, доцент Новиков Сергей Николаевич

Ведущая организация: ГОУ ВПО “Московский инженерно-физический институт (государственный университет)”

Защита состоится «___» июля 2008 г. в «___» часов на заседании диссертационного совета Д.219.005.01 в ГОУ ВПО “Сибирский государственный университет телекоммуникаций и информатики” по адресу: 630102, Новосибирск, ул. Кирова 86.

С диссертацией можно ознакомиться в библиотеке ГОУ ВПО “Сибирский государственный университет телекоммуникаций и информатики” по адресу: 630102, Новосибирск, ул. Кирова 86.

Автореферат разослан «____» мая 2008 г.

Ученый секретарь
диссертационного совета
Д.219.005.01, д.т.н., профессор Мамчев Г.В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность проблемы. Услуги телефонной связи предоставляются потребителям множеством компаний по всему миру уже несколько десятков лет. Параллельно с этим существовали и развивались сети передачи двоичной информации, используемые для передачи данных между электронными вычислительными машинами. Результатом укрупнения корпоративных сетей явилось образование глобальной сети Интернет, объединяющей многомиллионную аудиторию пользователей, расположенных по всему миру.

Развитие информационных технологий на рубеже двадцатого и двадцать первого веков позволило реализовать новую услугу – передачу речи в реальном времени через универсальные каналы связи. Передача речи через вычислительные сети, которые используют протокол IP, называется IP-телефонией**.** Основной аспект оптимистичных прогнозов к данной технологии – это потенциал роста выделенных каналов и независимость цены доступа от удаленности точки доступа для конечного клиента, благодаря чему резко снижается цена сеансов связи. Значительными преимуществами IP-телефонии являются цена, качество связи и возможность передачи факсов в реальном времени. Дополнительно IP-телефония вносит новые аспекты в сферу телекоммуникаций: аудио- и видеоконференции, одновременный доступ к приложениям, быстрый поиск абонента и другие.

Перспективные технологии передачи речи и видео поставили перед специалистами проблему использования уже ставших привычными ПЭВМ с установленными ОС Windows для реализации телефонных переговоров и видеоконференций в защищенном от несанкционированного доступа режиме. Использование IP-сетей для организации связи в защищенном режиме предъявляет особые требования как к методам сжатия и передачи речи и видео, так и к системам защиты от несанкционированного доступа.

В настоящее время проводится большое количество научных исследований в области защиты информации, сжатия речи, видео, сетевых технологий и прикладного программного обеспечения. Исследования в области защиты информации отражены в работах отечественных и зарубежных ученых: В.А. Герасименко, Б.Я. Рябко, П.Д. Зегжды, Д.П. Зегжды, А.А. Молдовяна, Н.А. Молдовяна, Б.Я. Советова, В.Г.Шахова, М.А. Иванова, К. Шеннона, Р.Л. Ривеста, Б. Шнайера и др.; в области сетевых технологий в работах: В.Г. Олифер, Н.А. Олифер, М.В. Кульгина; в области сжатия речи и видео в работах Д. Л. Фланагана, Г.Фанта, Дж. Д. Маркела, А.Х. Грея, Д. Сэломона, Д.С. Ватолина и др. Однако остается недостаточно освещенным вопрос использования и анализа современных встроенных в операционные системы прикладных интерфейсов, а также ряд проблем, относящихся к реализации результатов всех этих исследований в составе программного обеспечения мультимедийной системы IP-телефонии, защищенной от несанкционированного доступа, функционирующей в современных операционных системах Windows.

Целью диссертационной работы является разработка системы передачи речи через вычислительные сети, защищенной от несанкционированного доступа, на основе прикладных интерфейсов операционной системы Windows. Для достижения этой цели в диссертационной работе были поставлены и решены следующие **задачи**:

1. Разработка программной архитектуры мультимедийной системы IP-телефонии, защищенной от несанкционированного доступа, с учетом существующих и перспективных возможностей операционной системы Windows.
2. Разработка общего критерия оценки качества и формулировка технических требований к системе передачи речи через вычислительные сети, работающей в защищенном режиме.
3. Разработка модели потенциального нарушителя для анализа защищенности систем IP-телефонии, с учетом всех потенциальных угроз несанкционированного доступа.
4. Создание программного комплекса, позволяющего осуществлять запись/ воспроизведение, компрессию/декомпрессию речевого сигнала, защиту данных от несанкционированного доступа, а также передачу сжатой речи через IP-сети в режиме, защищенном от несанкционированного доступа.

Методы исследования. Для решения поставленных задач использовались методы теории вероятностей, теории графов, математической статистики. При создании программного комплекса использовалось объектно-ориентированное программирование.

Научная новизна.

1. Предложена программная архитектура мультимедийной системы IP-телефонии, реализующая сценарий “компьютер” – “компьютер” в защищенном от несанкционированного доступа режиме, отличающаяся от аналогов принципами создания процессов компрессии и шифрования за счет использования интерфейсов Audio/Video Compression Manager и CriptoApi 1.0. Предложенная программная архитектура позволяет передать процессы компрессии и шифрования из пользовательского приложения на уровень операционной системы.
2. Разработана модель нарушителя для предложенной архитектуры системы IP-телефонии, содержащая классификацию возможных атак с их описанием, а также разработку математических моделей атак, основанных на вероятностных характеристиках. Модель нарушителя отличается от известных учетом следующих атак: на модули ввода/вывода звука DirectSound, на модули компрессии/декомпрессии, на модули защиты данных от несанкционированного доступа, атак связанных с полной подменой программного обеспечения IP-телефонии.
3. Получена новая аналитическая зависимость для расчета параметров алгоритма, позволяющего уменьшить битовую длину пароля за счет времени задержки по операциям генерации ключа.

Практическая значимость и внедрение результатов исследований.

Разработаны, программно реализованы и апробированы компьютерные методики:

- защиты данных от несанкционированного доступа (свидетельство об официальной регистрации в реестре программ для ЭВМ №2006610291);
- защиты речи от несанкционированного доступа, передаваемой через IP-сети (свидетельство об официальной регистрации в реестре программ для ЭВМ №2006612351);
- компрессии речи (свидетельство об официальной регистрации в реестре программ для ЭВМ №2006612352).

Разработанное программное обеспечение VoiceOverNet и CriptoProject, внедрено в ОАО НИИ технологии, контроля и диагностики железнодорожного транспорта (г. Омск) и используется для защиты от несанкционированного доступа речи и данных, передаваемых в локальной вычислительной сети.

Программные компоненты VoiceOverNet и CriptoProject внедрены на кафедре анатомии и физиологии и НИИ ДЭУ СибГУФК (г. Омск), и используются для шифрования данных в учебно-методических комплексах “Физиология”, “Анатомия”, “Спортивная хронобиология”, а также для защиты указанного программного обеспечения и программы “Исследователь временных и пространственных свойств человека” от несанкционированного копирования.

Результаты работы используются в преподавании курсов “Безопасность вычислительных процессов” и “Вычислительные сети” в ОмГТУ, «Математические основы теории систем» и «Информационная безопасность и защита информации» в ОмГУПС.

Основные результаты и положения, выносимые на защиту:

1. Программная архитектура мультимедийной системы IP-телефонии, защищенной от несанкционированного доступа, на основе прикладных интерфейсов ОС Windows, позволяющая передать процессы компрессии и шифрования из пользовательского приложения на уровень операционной системы.
2. Модель нарушителя, содержащая:
   - классификацию возможных атак на систему IP-телефонии;
   - вероятностные характеристики атак;

   позволяет проводить анализ защищенности мультимедийных систем.
3. Полученная аналитическая зависимость позволяет рассчитать параметры алгоритма, уменьшающего битовую длину пароля за счет времени задержки по операциям генерации ключа.
4. Программные средства, реализующие основные подсистемы комплекса IP-телефонии и позволяющие осуществлять компрессию звука, защиту файлов от несанкционированного доступа и передачу речи через IP-сети в режиме, защищенном от несанкционированного доступа.

Достоверность результатов работы подтверждается применением методов системного проектирования прикладного программного обеспечения, обусловлена представительностью объема изученной литературы по теме рабо-

ты, а также внедренными в производственный, научно-исследовательский и учебный процесс программными компонентами разработанного комплекса программного обеспечения. Полученные теоретические и экспериментальные данные согласуются с результатами, полученными другими исследователями. Верификация разработанного программного обеспечения заключалась в отладке и оценке работоспособности программного комплекса, а также его отдельных компонентов, реализующих различные функции, в том числе ввода/вывода звукового сигнала, его компрессии и хранения, защиты данных от несанкционированного доступа и тестирования программных модулей ОС Windows.

Апробация работы. Основные материалы диссертационной работы докладывались на II Международной научно-практической конференции “Актуальные проблемы развития железнодорожного транспорта”, г.Самара, 7-8 декабря, 2005 г.; XIII Всероссийской научной конференции “Проблемы информационной безопасности в системе высшей школы” г.Москва, 23-27 января, 2006 г.; 13-ой Всероссийской межвузовской научно-технической конференции студентов и аспирантов г.Москва, 19-21 апреля, 2006 г.; Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых “Научная сессия ТУСУР-2007” г.Томск, 3-7 мая, 2007 г.

По материалам диссертации составлено и издано учебное пособие “Защита информационных процессов в компьютерных системах” – Омск: ОмГТУ, 2006. – 76 с.

Публикации. Результаты диссертации отражены в 12 публикациях, в том числе семь публикаций в изданиях, рекомендованных ВАК.

Структура и объем работы. Диссертация состоит из введения, четырех глав, заключения, списка использованных источников и приложений. Работа изложена на 182 страницах основного текста, содержит 17 таблиц, 36 рисунков, список литературы включает 224 источника, из них 136 иностранных. Приложения представлены на 51 странице.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность проводимых исследований, сформулированы цели и задачи работы, представлены структура диссертации и основные положения, выносимые на защиту.

В первой главе проводится анализ возможностей реализации системы передачи речи через вычислительные сети, функционирующей в защищенном от несанкционированного доступа режиме, на основе операционной системы Windows. Рассмотрены проблемы реализации архитектуры управления обслуживанием вызовов, проблемы реализации транспортного механизма для речевого трафика, сценарии функционирования систем IP-телефонии.

Проанализированы алгоритмы компрессии / декомпрессии звукового сигнала, защиты данных, в том числе с использованием возможностей операционной системы Windows по обработке звука и защите данных.

Обобщены характеристики ряда специализированных абонентских программных продуктов IP-телефонии, реализующих сценарий “компьютер” – “компьютер” в защищенном от несанкционированного доступа режиме (табл. 1). На основе анализа их основных характеристик сделано заключение, что имеющиеся в настоящее время программные решения систем IP-телефонии, защищенные от несанкционированного доступа, характеризуются следующими недостатками:

- имеют монолитную архитектуру, что, не позволяет использовать динамическое наращивание функциональных возможностей, например, путем использования кодеков и/или алгоритмов защиты от несанкционированного доступа на основе прикладных интерфейсов ОС Windows;
- не позволяют вести контроль и настройку режимов защиты трафика IP-телефонии от несанкционированного доступа;
- не используют сертифицированные ФСБ РФ алгоритмы защиты от несанкционированного доступа и программные модули, что не позволяет их официально применять в органах государственной власти и силовых ведомствах.

Таблица 1

Сравнительный анализ защищенных от несанкционированного доступа абонентских систем IP-телефонии

Название программного продукта	Основные характеристики			
	Используемые алгоритмы для защиты от несанкционированного доступа	Компрессия речи (кодек)	Возможность добавления функциональных возможностей пользователем	Возможность контроля и настройки режимов шифрования
SpeakFreely	DES, IDEA	ADPCM, GSM 6.10, LPC, LPC-10	Нет	Нет
PGPfone	Тройной DES, CAST5, Blowfish	GSM 6.10	Нет	Нет
Nautilus	Blowfish, Тройной DES, IDEA	ADPCM, LPC-10	Нет	Нет
Zfone	ZRTP	Нет данных	Нет	Нет
Skype	AES	Нет данных (до 33 кбит/сек)	Нет	Нет

Решения отечественных производителей средств и систем защиты от несанкционированного доступа (фирм “Анкад”, “КРИПТО-ПРО”, “Аладдин”, “Информзащита”, “Сигнал-КОМ”, “ОКБ САПР”) для решения задач защиты речи от несанкционированного доступа, передаваемой через IP-сети, представляют собой либо программно-аппаратные комплексы (например, КРИПТОН AncNet 10/100 фирмы “Анкад”) либо средства, обеспечивающие защиту от несанкционированного доступа непосредственно в каналах связи (например, телефонный аппарат Voice Coder-AT фирмы “Сигнал-КОМ”). Отечественных абонентских программных продуктов IP-телефонии, реализующих сценарий

“компьютер” – “компьютер” в защищенном от несанкционированного доступа режиме на российском рынке не представлено.

Таким образом, на сегодня не существует специализированных абонентских программных продуктов IP-телефонии, реализующих сценарий “компьютер” – “компьютер” в защищенном от несанкционированного доступа режиме, позволяющих динамически настраивать процессы компрессии речи, защиты трафика, в том числе с помощью сертифицированных ФСБ РФ алгоритмов и программных модулей.

Во второй главе определены основные идеи построения программной архитектуры абонентских систем IP-телефонии, защищенных от несанкционированного доступа.

При проектировании системы IP-телефонии был рассмотрен комплекс вопросов, связанных с выбором методологии проектирования, разработкой программной архитектуры и выбора программной платформы, применением методов оценки качества программных приложений, гибкости реализации и тестирования функционального содержания, формирования требований рекомендательного характера, ориентированных на повышение качества программного продукта системы IP-телефонии.

Суть архитектурного представления системы состоит в том, чтобы, не затрагивая детали реализации, алгоритмы и представление данных, описать поведение и взаимодействие «черных ящиков», реализующих функциональность системы, а также представить набор стратегических решений по организации программной системы, выбору ее структурных элементов и их интерфейсов.

Структурно мультимедийная система связи, работающей на основе ПЭВМ в защищенном от несанкционированного доступа режиме состоит из следующих подсистем:

- ввода-вывода звукового или видео сигнала;
- цифровой обработки звукового или видео сигнала (компрессия и шифрование);
- управления, визуализации и регистрации статистической и диагностической информации, отражающих процесс функционирования системы;
- сетевых телекоммуникационных интерфейсов.

С точки зрения формализации структуры и информационных потоков системы более универсальным является информационный подход (рис. 1), поскольку он предоставляет возможность проанализировать внутреннюю структуру связей системы на основе графоаналитических методов, а также определить наиболее важные с точки зрения безопасности участки.

Центральным узлом представленной системы связи является модуль управления, модуль интерфейса пользователя и модуль прикладных протоколов взаимодействия между системами IP-телефонии (модуль №5, №6, №8). Остальные модули выполняют функции по обработке, преобразованию и передаче звуковых данных.

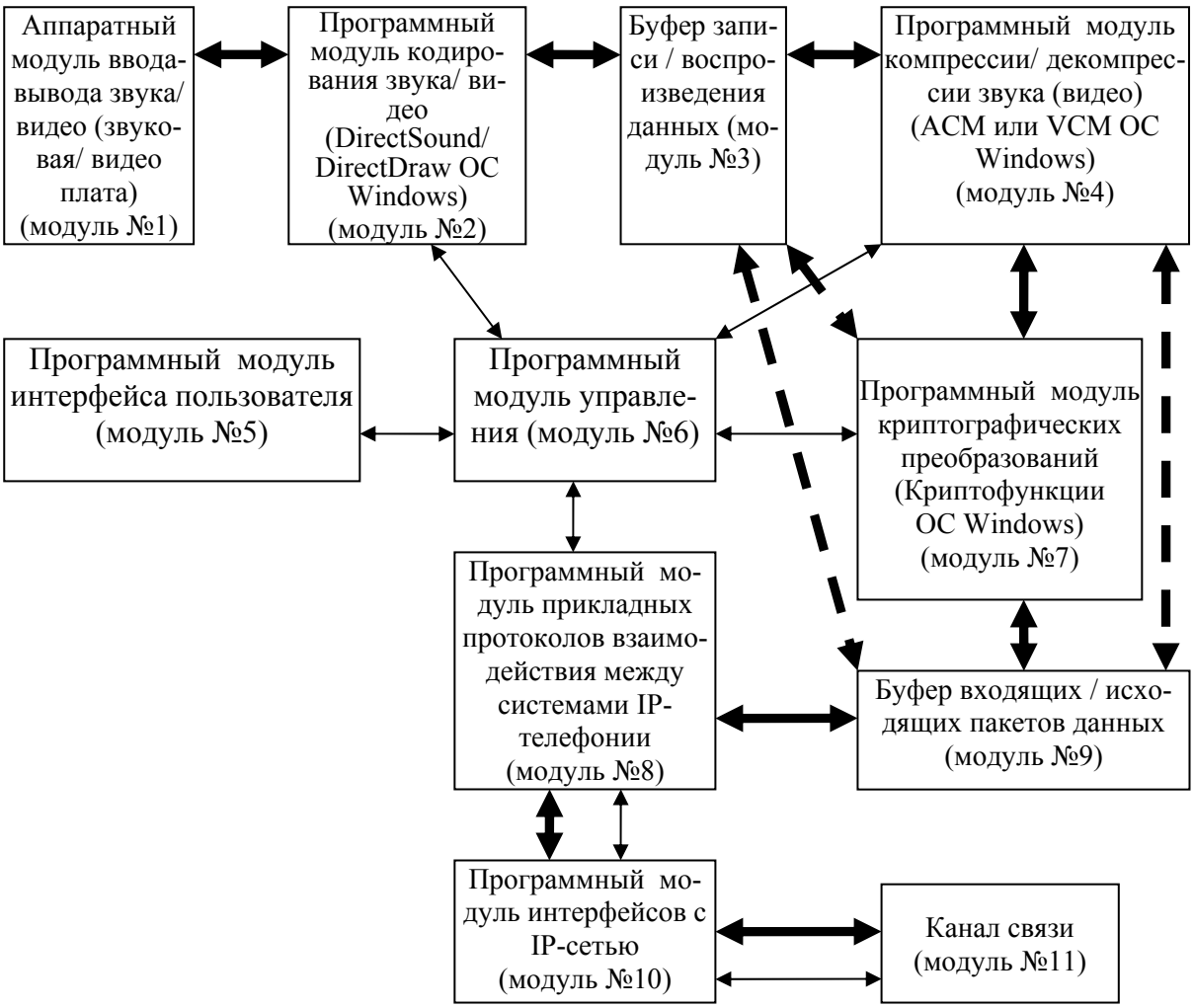

Рис. 1. Схема информационных потоков в системе IP-телефонии, защищенной от несанкционированного доступа

На схеме использованы следующие обозначения:

Управляющие воздействия (потоки команд)

Основные маршруты потока данных

Возможные маршруты потоков данных при отсутствии или отсутствии работоспособности некоторых модулей

Информационный подход позволяет также графически выделить основные отличия в построении программной архитектуры системы связи от соответствующих аналогов представленных в таблице 1. В частности в разработанной системе связи компрессия звука (видео) и шифрование в модулях №4 и №7 принципиально идет другим способом (используя интерфейсы Audio/Video Compression Manager и CriptoApi 1.0), что позволяет передать процессы компрессии и шифрования из пользовательской программы на уровень операционной системы Windows. Данный способ позволяет упростить разработку и увеличить функциональные возможности системы передачи речи или видео за счет вызова внешних по отношению к системе алгоритмов компрессии и шифрования.

Для сложных информационных систем невозможна выработка какого-либо единого совокупного критерия, поэтому оценка эффективности может быть проведена на основании исследования нескольких групп частных показателей, вес которых может быть различным в каждом конкретном случае. Оценка по каждому частному показателю может выводиться по трехбалльной шкале: 2 - хорошо, 1 - удовлетворительно, 0 - неудовлетворительно. В случае необходимости могут быть применены и другие шкалы.

Методики оценок качества программного обеспечения и недостатки существующих систем IP-телефонии позволили получить критерии, характеризующие качество мультимедийной системы IP-телефонии, функционирующей в защищенном от несанкционированного доступа режиме (рис. 2).

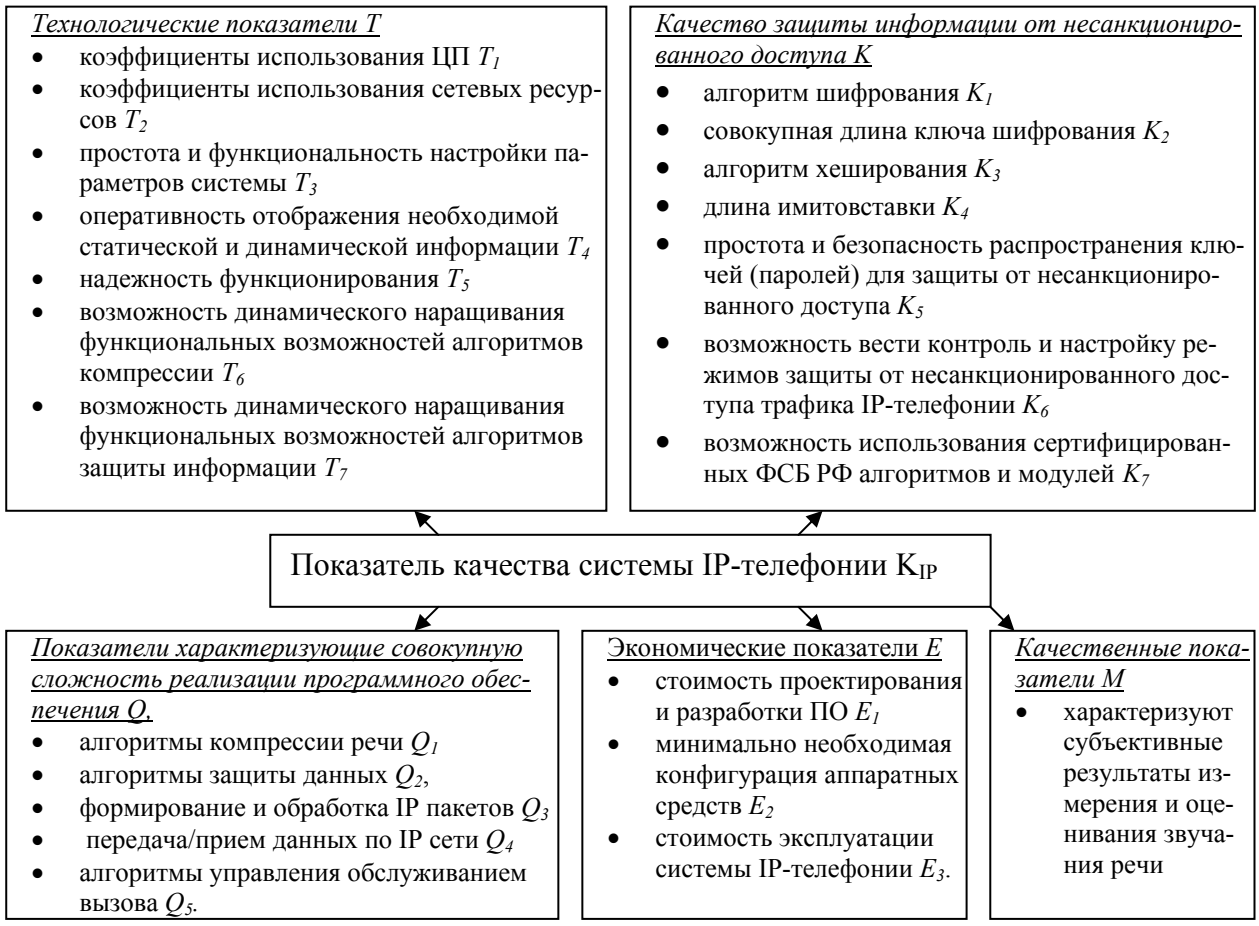

Рис. 2. Атрибуты эффективности IP-телефонии, функционирующей в защищенном от несанкционированного доступа режиме

Методика оценки эффективности включает оценку по 5 основным критериям: 1) оценка качественных показателей, которые характеризуют субъективные результаты измерения и оценивания звучания речи; 2) оценка по технологическим показателям, характеризующим качество программных решений с общих позиций современной технологической базы; 3) оценка по показателям, характеризующим качество защиты информации; 4) оценка по показателям, характеризующим совокупную сложность реализации программного обеспечения; 5) оценка по экономическим показателям, характеризующим затраты, свя-

занные с обеспечением требуемых функциональных характеристик системы IP-телефонии.

Сворачивание частных показателей (атрибутов качества) $T_1 \ldots T_7$, $K_1 \ldots K_7$, $Q_1 \ldots Q_5$, $E_1 \ldots E_3$, представленных на рис. 2, в показатели качества T, K, Q, E соответственно производится с помощью соответствующих весовых коэффициентов $(t_1 \ldots t_7)$, $(k_1 \ldots k_7)$, $(q_1 \ldots q_5)$, $(e_1 \ldots e_3)$.

Для численной оценки показателей качества M, T, K, Q, E предлагается интегральный подход, при котором формулы оценки качества по отдельным показателям примут вид:

$$T = \sum_{i=1}^{7} (t_i \cdot T_i) \tag{1}$$

$$K = \sum_{i=1}^{7} (k_i \cdot K_i) \tag{2}$$

$$Q = \sum_{i=1}^{5} (q_i \cdot Q_i) \tag{3}$$

$$E = \sum_{i=1}^{3} (e_i \cdot E_i) \tag{4}$$

Для оценки общего критерия качества также используется аддитивная методика:

$$K_{IP} = k_M \cdot M + k_T \cdot T + k_K \cdot K + k_Q \cdot Q + k_E \cdot E, \tag{5}$$

где k_M, k_T, k_K , k_Q, k_E – весовые коэффициенты значимости для системы в целом качественных показателей звучания речи, технологических показателей, совокупной сложности реализации программного обеспечения, значимости защиты информации и экономических показателей соответственно. Определение численных значений весовых коэффициентов может быть сделано на основе метода анализа иерархий, разработанного американским ученым Т.Саати. Однако, на всем множестве мест применения систем связи защищенных от несанкционированного доступа оценки весовых коэффициентов атрибутов качества, как правило, оказываются частными и субъективными. Поэтому единственным способом универсальной оценки является отказ от ранжирования и принятие всех атрибутов качества одинаковозначимыми.

В соответствии с выбранными шкалами оценок исходных показателей лучшим вариантом мультимедийной системы IP-телефонии, функционирующей в защищенном от несанкционированного доступа режиме, может считаться тот, для которого выполняется условие максимальной численной оценки:

$$K_{IP} = K_{IPMAX} \tag{6}$$

Кроме того, в задаче оценки показатели $M, T, K, Q, E, T_i, K_i, Q_i, E_i$ ограничиваются следующими условиями:

$$M \geq \varphi_m,\ T \geq \varphi_t,\ K \geq \varphi_k,\ Q \geq \varphi_q,\ E \geq \varphi_e \tag{7}$$

$$T_i \geq \varphi_{ti},\ K_i \geq \varphi_{ki},\ Q_i \geq \varphi_{qi},\ E_i \geq \varphi_{ei} \tag{8}$$

Где φ_m, φ_t, φ_k, φ_q, φ_e, φ_{ti}, φ_{ki}, φ_{qi}, φ_{ei} – постоянные величины, устанавливаемые лицом принимающим решение в зависимости от начальных требований к системе и от специфических особенностей частных показателей $M, T, K, Q, E, T_i, K_i, Q_i, E_i$ соответственно.

В случае не выполнения всех соответствующих условий делается вывод об отсутствии соответствия анализируемой системы заданным требованиям.

В соответствии с разработанным критерием качества сформулированы следующие основные технические требования к мультимедийной системе передачи речи через вычислительные сети, работающей в защищенном режиме по сценарию “компьютер”-“компьютер”:

1) Обеспечение возможности создания буфера разной длины при воспроизведении звука для регулирования качества обслуживания пользователя.
2) Унифицированный интерфейс управления системой.
3) Возможность интеграции (реинтеграции) необходимых компонентов (модулей) для изменения архитектуры системы в каждом сеансе связи.
4) Возможность компрессии (декомпрессии) звуковых данных разными алгоритмами.
5) Возможность защиты данных от несанкционированного доступа с помощью разных алгоритмов, функционирующих в различных режимах.

В третьей главе проводится анализ методов защиты системы IP-телефонии от несанкционированного доступа.

Процесс передачи речи через IP-сети в защищенном режиме является результатом взаимодействия:

1) злоумышленника (нарушителя), изучающего защиту системы и реализующего несанкционированный доступ;
2) пакетов с данными, циркулирующих в системе;
3) способности системы обрабатывать и передавать речевые пакеты, подлежащие защите;
4) созданной разработчиком (разработчиками) системы передачи речи через IP-сети, функционирующей в режиме защищенном от несанкционированного доступа.

Для построения модели нарушителя использовалась информация о существующих средствах доступа к информации и ее обработки, о возможных способах перехвата данных на стадии передачи и обработки, об объекте защиты, об имевших место свершившихся случаях хищения информации и т. п.

Разработанная модель потенциального нарушителя включает типы нарушителей, цели нарушителей и сценарии их возможных действий. В таблице 2 приведен список возможных атак и угроз несанкционированного доступа. Рассмотренные отдельные атаки не всегда могут привести нарушителя к положительному для него конечному результату, поэтому активность нарушителя в общем случае может складываться из некоторых последовательностей атак (стратегий), зависящих как от целей нарушителя, так и от его возможностей. В каждом конкретном атакующем воздействии может быть реализована только одна из возможных стратегий.

Таблица 2

Атаки на систему IP-телефонии, работающую в защищенном режиме

Индекс	Название атаки
A1	Доступ к речевой информации в обход системы IP-телефонии, в обход ОС Windows и в обход ПЭВМ
A2	Доступ к речевой информации в обход системы IP-телефонии
A3	Получение речевой информации внедрением закладок в модули ввода/вывода звука DirectSound ОС Windows
A4	Получение речевой информации внедрением закладок в модули компрессии/ декомпрессии ОС Windows
A5	Получение ключа и/или речевой информации внедрением закладок в программные модули защиты от несанкционированного доступа ОС Windows
A6	Сбор паролей программой типа “Троянский конь”
A7	Перехват пакетов с данными
A8	Навязывание пользователю ложного сообщения
A9	Отказ в обслуживании (DOS)
A10	Подмена программного обеспечения IP-телефонии

Граф возможных стратегий действий нарушителя, направленных на несанкционированный доступ к информации или на нарушение работы системы передачи речи, представлен на рис. 3.

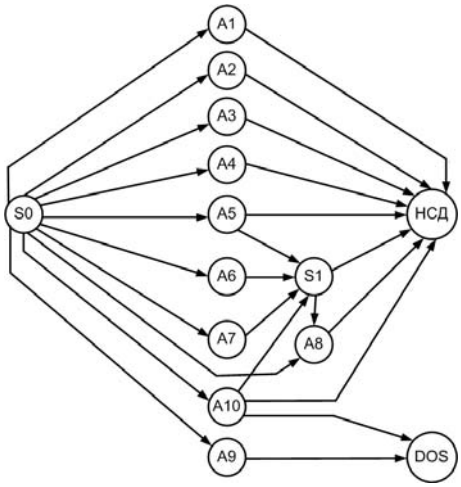

Рис. 3. Граф возможных стратегий действий нарушителя

На рис. 3 элементы A_i обозначают атаки, S_1 – промежуточный результат (S_0 соответствует исходному состоянию), *НСД* и *DOS* – обозначают результат действий нарушителя.

Для увеличения стойкости пароля генерация ключа реализуется согласно рекомендациям исследовательской лаборатории RSA Laboratories. Найдены новые количественные характеристики параметров данного алгоритма, позволяющие при более короткой длине пароля добиться сопоставимой стойкости с алгоритмом защиты от НСД использующим обычную для него длину ключа.

$$П \geq K - \log_2(1 + J \times \frac{S_K}{S_J}) \qquad (9)$$

здесь $П$ – длина пароля в битах, K – длина ключа в битах, J – количество раз, которое должна повториться функция преобразования, участвующая в ге-

нерации ключа на основе пароля, S_K – скорость опробования одного ключа (единиц / сек.), S_J – скорость генерации одного ключа на основе пароля (единиц / сек.).

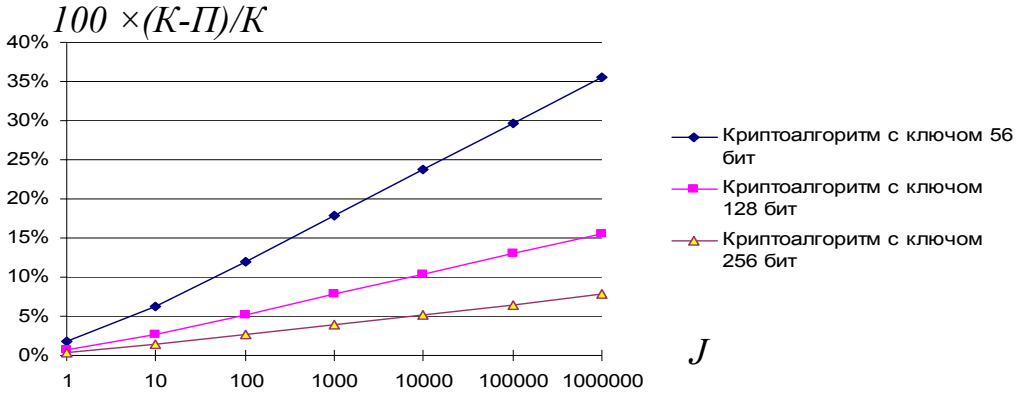

Рис. 4. Эффективность генерации ключей из паролей в зависимости от J при $S_K / S_j = 1$

На рис. 4 показан расчетный график эффективности генерации ключей из паролей (для длин ключей 56, 128, 256 бит).

Вероятность успеха той или иной стратегии действий нарушителя будет равна произведению вероятностей успеха составляющих её атак:

$$p_i(t) = \prod_{j=1}^{N_i} p_j(t) \qquad (10)$$

где $p_j(t)$ - вероятность успеха атаки принадлежащей i-й ветви;

N_i - количество атак i-й ветви.

Вероятность успеха атаки определяется её математической моделью с учётом действия политики безопасности. Под математической моделью атаки понимается её формализованное описание, построенное с точки зрения принятой модели защищённости. В рамках вероятностной модели безопасности значимой будет вероятность предотвращения атаки системой защиты, вероятности её обнаружения и локализации. Эта вероятность в общем случае будет зависеть от времени; характер этой зависимости и будет составлять суть модели атаки. Перечисленным выше атакам соответствуют две математические модели: модель перебора и модель проверки.

Атаки, связанные с проверкой некоторого числа вариантов, можно описать моделью перебора. Типичным примером таких атак является характерная для большинства современных систем, в том числе и для системы IP-телефонии, атака подбором пароля или ключа методом “Грубая сила” (атаки А7.1 и А7.2). Примечание: J, S_K, S_J определены в формуле 7, $N_П$ – количество вариантов пароля (емкость множества паролей).

$$p_{A7.1}(t) = \begin{cases} \dfrac{t}{N_П \times (1/S_K + J/S_J)}, \text{если } \dfrac{t}{N_П \times (1/S_K + J/S_J)} \le 1 \\ 1, \text{если } \dfrac{t}{N_П \times (1/S_K + J/S_J)} > 1 \end{cases} \qquad (11)$$

Атаки, основанные на ошибках (недостатках) в системе безопасности и им подобные, можно описать при помощи модели проверки. Такие атаки используют уязвимость системы защиты, проверяя единственный вариант: наличие или отсутствие данной уязвимости. Вероятность успешного завершения в этом случае не зависит от времени и целиком определяется наличием или отсутствием используемой уязвимости:

$$p(t) = \begin{cases} 1, \text{если уязвимость существует} \\ 0, \text{если уязвимости нет} \end{cases} \qquad (12)$$

Данная математическая модель отражает большинство существующих в настоящее время атак (A1-A6, A8-A10), поскольку под понятие уязвимости подпадают как ошибки (недостатки) в системе безопасности, так и ошибки администрирования.

Для случая максимальной защищённости системы IP-телефонии приведены графы возможных стратегий действий нарушителя (рис.5, рис.6).

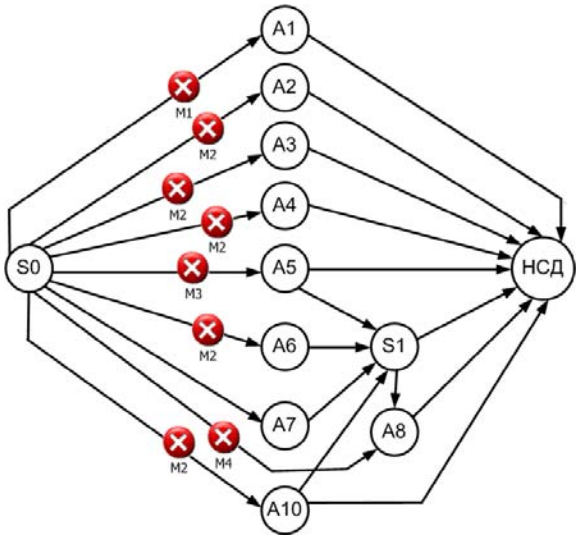

Рис. 5. Граф несанкционированного доступа

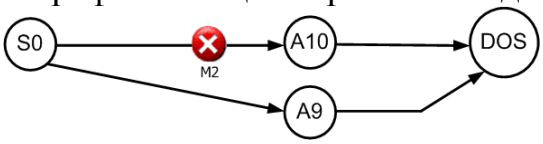

Рис. 6. Граф “отказа в обслуживании”

Где M1-M4 – методы предотвращения атак (табл. 3).

Таблица 3

Методы предотвращения атак

Индекс	Описание
M1	организационные и инженерно-технические методы, направленные на обеспечение надежной защиты помещения против физического проникновения в помещение случайных лиц, способных принести записывающие или радиопередающие устройства, а также меры направленные на нейтрализацию записывающих или радиопередающих устройств.
M2	использование только сертифицированного программного обеспечения, качественная антивирусная защита, способная предотвратить заражение программного обеспечения вредоносными троянскими программами, а также ограничение прав обычных пользователей в части установки программного обеспечения. А также организационные и инженерно-технические методы, направленные на обеспечение целостности компьютерного оборудования и ограничение доступа в помещение и физического доступа к компьютерам, в том числе жёсткая регламентация порядка работы на компьютерах информационной системы, порядка их ремонта, замены и т.д.
M3	ограничение загрузки альтернативных операционных систем, чтобы предотвратить замену библиотеки advapi32.dll, осуществляющей проверку цифровой подписи модулей защиты данных в ОС Windows.
M4	использование режимов шифрования в которых невозможна манипуляция блоками шифроданных или добавление к каждому пакету с открытой информацией некоторых данных характеризующих уникальность пакета, например время и/или порядковый номер пакета.

Таким образом, из всех стратегий действий нарушителя принципиально реализуемы три стратегии (табл. 4).

Таблица 4

Принципиально реализуемые стратегии действий нарушителя

№	Путь прохождения графа	Вероятности успеха*
10	A7 – S1 – НСД	$p_{10} = p_{A7}$
11	A7 – S1 – A8.1 – НСД	$p_{11} = p_{A7} \cdot p_{A8.1}$
16	A9 – DOS	$p_{16} = p_{A9}$

Критическим будет путь №10 или №11, если нарушителю удастся определить ключ к шифру, защищающему трафик системы IP-телефонии. Однако вероятность успеха этих стратегий действий за приемлемое время низка при выборе стойкого шифра. Для общедоступных сетей критический путь №16 всегда имеет вероятность успеха равную 1 на основании чего можно прийти к выводу, что обеспечить качественную связь через IP-сети, не используя дополнительные методы защиты, затруднительно (особенно в случае если нарушитель обладает значительными техническими средствами, рассредоточенными по разным сегментам сети).

* где $p_i(t), i = 1...17$ – вероятности успеха возможных стратегий действий.

При анализе качества защиты реальной информационной системы во внимание необходимо принимать административные, организационные и инженерно-технические методы, а также используемые дополнительные программные или аппаратные средства защиты. Наибольшее значение при этом будут иметь средства защиты от атак, входящих в стратегии действий нарушителя, не предотвращаемые средствами системы IP-телефонии:

1) ограничение физического доступа в помещение, где расположены компьютеры;
2) ограничение физического доступа к компьютерам;
3) использование сертифицированного программного обеспечения;
4) ограничение использования средств сетевого и локального администрирования;
5) наличие развернутого плана действий по противодействию атакам “Отказ в обслуживании”.

В четвертой главе приводятся примеры реализации и апробации мультимедийной программной архитектуры и алгоритмов, предложенных во второй и третьих главах.

Разработан комплекс, включающий в себя ряд программных продуктов: ПО, осуществляющее запись / воспроизведение звука и его обработку (Gamma), в том числе компрессию / декомпрессию и сохранение полученных результатов в звуковые файлы стандартных форматов (Converter); ПО, осуществляющее защиту файлов от несанкционированного доступа, с сохранением данных в файлы специально разработанного авторского формата (CriptoProject); ПО, предназначенное для передачи сжатой речи через IP-сети в режиме, защищенном от несанкционированного доступа (VoiceOverNet).

Разработанное программное обеспечение, осуществляющее защиту данных от несанкционированного доступа, имеет следующие технические особенности и в ОС Windows позволяет осуществлять:

1) определение технических характеристик модулей защиты от несанкционированного доступа, установленных в ОС Windows;
2) шифрование, дешифрование, хеширование файлов и отдельных блоков данных;
3) определение скоростных характеристик модулей защиты от несанкционированного доступа, установленных в ОС Windows.

Разработанное программное обеспечение, предназначенное для передачи сжатой речи через IP-сети в режиме, защищенном от несанкционированного доступа, имеет следующие технические особенности и позволяет осуществлять в ОС Windows:

1) выбор и настройку параметров алгоритмов компрессии / декомпрессии звука на основе аудиокодеков, установленных в ОС Windows;
2) выбор алгоритмов защиты блоков звуковых данных от несанкционированного доступа и настройку их параметров;
3) ввод / вывод звука с разрядностью звука 8 двоичных разрядов на отсчет, с частотой дискретизации 8000 Гц;

4) компрессию / декомпрессию звуковых блоков данных с помощью выбранных пользователем аудиокодеков;
5) защиту от несанкционированного доступа через шифрование, хеширование блоков звуковых данных;

Проведено исследование возможностей по компрессии/декомпрессии речи с помощью разработанной нами программы Converter, содержащей аудиоинтерфейсы управления менеджером сжатия звука ОС Windows, примененных в системе IP-телефонии. Определены свойства стандартно установленных в ОС Windows аудиокодеков.

Непосредственное исследование аудиокодеков, установленных в ОС Windows для компрессии-декомпрессии звука, проводилось в следующей рабочей конфигурации и последовательности:

В ОС Windows XP с помощью разработанной программы Gamma была записана речь (фразы, команды по ГОСТ 16600-72) в файлы формата Microsoft Wave RIFF. Полученные 10 файлов общей длительностью 356 секунд и объемом 2846452 байта с помощью программы Converter были преобразованы аудиокодеками ОС Windows во все доступные для преобразования форматы представления звуковых данных. Для сжатых файлов вычислялся средний коэффициент сжатия и битрейт (bitrate) – количество единиц информации, необходимых для хранения (передачи) одной секунды потока звуковых данных.

Исходный формат звука (формат PCM, моно, частота дискретизации 8000 Гц, 8 двоичных разрядов на отсчет, битрейт 64000 бит/сек). В таблице 5 представлены основные результаты проведенных экспериментов в части определения свойств аудиокодеков, установленных в ОС Windows XP.

Таблица 5

Аудиокодеки ОС Windows

Тип аудио кодека	Атрибуты	Средний коэффициент сжатия	Битрейт, бит/с
DSP Group TrueSpeech™	8,000 кГц; 1 бит; Моно	7,50	8529
GSM 6.10	8,000 кГц; Моно	4,92	13008
IMA ADPCM	8,000 кГц; 4 бит; Моно	1,97	32428
Microsoft ADPCM	8,000 кГц; 4 бит; Моно	1,95	32769
MPEG Layer-3	8 кбит/сек; 8,000 кГц;Моно	8,06	7940
	16 кбит/сек; 8,000 кГц;Моно	4,02	15939
CCIT A-Law	8,000 кГц; 8 бит; Моно	1	64000
CCIT u-Law	8,000 кГц; 8 бит; Моно	1	64000
Alex AC3 Audio	5 кбит/сек; 8 кГц; Моно	12,81	4996
	6 кбит/сек; 8 кГц; Моно	10,68	5995
	8 кбит/сек; 8 кГц; Моно	8,01	7993

С помощью программы CriptoProject, содержащей интерфейсы управления модулями защиты от несанкционированного доступа (криптомодулями) ОС Windows, примененных в системе IP-телефонии, были исследованы криптомодули ОС Windows в следующей рабочей конфигурации и последовательности:

На компьютерах с ОС Windows Vista, Windows XP, Windows 2003, Windows 2000, Windows 98 была протестирована указанная выше программа. Дополнительно к стандартным криптопровайдерам был установлен свободно распространяемый криптопровайдер ООО Мегасофт, который поддерживает рос-

сийские стандарты криптопреобразований: 1) ГОСТ Р 34.10-94; 2) ГОСТ Р 34.11-94; 3) ГОСТ Р 28147-89. Скорость криптографических преобразований исследовалась при шифровании и/или хешировании файла размером 1.5 МБ и блока данных размером 160 МБ (1000000 блоков по 160 байт) при 30 повторах на компьютере Pentium IV Celeron 1700 МГц, ОЗУ 256 Мб, ОС Windows XP.

Были получены следующие результаты: количество стандартных криптомодулей лежало от трех в ОС Windows 98 до двенадцати в ОС Windows 2003/XP. Были успешно протестированы следующие алгоритмы шифрования (в скобках указана длина ключа в битах): RC2 (40-128), RC4 (40-128), DES (56), Two Key Triple DES (112), Three Key Triple DES (168), American Encryption Standard (128, 192, 256), ГОСТ Р 28147-89 (256). Также были работоспособны алгоритмы хеширования SHA-1, MD2, MD4, MD5, HMAC, ГОСТ Р 34.11-94. При шифровании данных из оперативной памяти получена скорость 2-91 МБ/сек (табл. 6), причем наиболее скоростным оказался потоковый алгоритм шифрования RC4. Низкой оказалась скорость алгоритмов шифрования RC2 и DES в режиме гаммирования с обратной связью, что можно объяснить неэффективной реализацией данного режима в базовых криптомодулях ОС Windows. При хешировании данных из оперативной памяти получена скорость 5-105 МБ/сек (табл. 7), наиболее скоростным является алгоритм MD5, наиболее медленными оказались алгоритмы MD2 и HMAC, что соответствует их теоретической производительности.

Таблица 6

Скоростные характеристики некоторых алгоритмов шифрования ОС Windows при обработке данных, находящихся в оперативной памяти

Режим	Шифр простой замены			Шифр простой замены с зацеплением			Гаммирования с обратной связью		
Алгоритм	RC2	RC4	DES	RC2	RC4	DES	RC2	RC4	DES
Скорость (МБ/сек)	15,49±0,05*	93,82±0,19*	20,20±0,02*	14,12±0,01*	93,78±0,27*	17,84±0,02*	1,83±0,001*	94,03±0,11*	2,35±0,001*
Алгоритм	Two Key Triple DES	AES 128-bit	AES 256-bit	Two Key Triple DES	AES 128-bit	AES 256-bit	Two Key Triple DES	AES 128-bit	AES 256-bit
Скорость (МБ/сек)	8,44±0,11*	19,72±0,03*	15,45±0,10*	7,98±0,08*	18,26±0,09*	14,69±0,01*	1,02±0,02*	1,35±0,004*	1,05±0,01*
Алгоритм	ГОСТ Р 28147-89			ГОСТ Р 28147-89			ГОСТ Р 28147-89		
Скорость (МБ/сек)	4,69±0,02*			4,68±0,03*			4,71±0,01*		

Примечание. * - $p < 0,01$ по критерию Фишера

Таблица 7

Скоростные характеристики некоторых алгоритмов хеширования ОС Windows при обработке данных, находящихся в оперативной памяти

Алгоритм	SHA-1	MD2	MD4	MD5	HMAC	ГОСТ Р 34.11-94
Скорость (МБ/сек)	87,18±0,17*	4,76±0,003*	106,46±0,18*	102,00±0,96*	4,73±0,002*	15,67±0,0004*

Примечание. * - $p < 0,001$ по критерию Фишера

Исследование возможностей программы IP-телефонии VoiceOverNet проводилось в следующем порядке:

Для организации сеанса связи через компьютерную сеть в защищенном от несанкционированного доступа режиме были использованы компьютеры Pentium IV Celeron 1700 МГц, ОЗУ 256 Мб, ОС Windows XP, гарнитуры Sven AP-830, локальная сеть Ethernet 10/100 Мбит и программа VoiceOverNet.

В режиме дуплексной связи получено хорошее качество речи (разборчивость звуков по требованиям ГОСТ 16600-72 больше 90 %) в следующих режимах работы программы VoiceOverNet: без компрессии, без шифрования и хеширования; с компрессией, с шифрованием и хешированием; с компрессией, с шифрованием, без хеширования; с компрессией, без шифрования, с хешированием; без компрессии, с шифрованием и хешированием; без компрессии, с шифрованием, без хеширования; без компрессии, без шифрования, с хешированием. Из алгоритмов компрессии звука успешно апробированы в составе программы следующие аудиокодеки (в скобках битовая скорость, кбит/сек): GSM 6.10 (13), DSP Group TrueSpeech™ (8,5), IMA ADPCM (32,4), Microsoft ADPCM (32,7), Alex AC3 Audio (4,9; 5,9; 7,9). Также успешно использованы следующие алгоритмы шифрования (в скобках указана длина ключа в битах): RC2 (40-128), RC4 (40-128), DES (56), Two Key Triple DES (112), Three Key Triple DES (168), American Encryption Standard (128, 192, 256), ГОСТ Р 28147-89 (256). Среди алгоритмов хеширования были работоспособны алгоритмы SHA-1, MD2, MD4, MD5, HMAC, ГОСТ Р 34.11-94. Шифрование успешно протестировано в трех режимах: а) Режим гаммирования с обратной связью (Cipher Feedback Mode, CFB), б) Шифр простой замены с зацеплением (Cipher Block Chaining Mode, CBC или режим выработки имитовставки), в) Шифр простой замены (Electronic CodeBook Mode, ECB).

В ходе экспериментов получена статистическая информация о времени передачи пакетов с данными для разработанной системы IP-телефонии по локальной сети для интервала наблюдения – 1000 принятых пакетов. Результаты ее обработки приведены в таблице 8. Сопоставив эту составляющую с функциональной задержкой кодека либо с обычной буферизацией перед передачей пакета (≥80 мс) сделан вывод, что для высокоскоростных локальных сетей она играет небольшую роль (ее вклад менее 2 %).

Таблица 8

Время передачи пакетов разработанной системы IP-телефонии по локальной сети

Тип локальной сети Ethernet	Стандарт IEEE 802.3u (100 Мбит)				Стандарт IEEE 802.3 (10 Мбит)			
Длина пакета, байт	200	400	800	1600	200	400	800	1600
Среднее время передачи пакета данных от абонента А к абоненту Б, мс	0,48± 1,81*	1,12± 2,71*	0,79± 2,38*	0,66± 2,16*	1,17± 1,45*	0,75± 2,23*	1,22± 2,88*	1,21± 2,81*

Примечание. * - $p < 0{,}001$ по критерию Фишера

В соответствии с разработанной методикой оценки эффективности системы IP-телефонии (см. рис. 2), проведена независимая экспертная оценка программы VoiceOverNet и пяти её ближайших аналогов с учетом ограничений, которые вытекают из принципа возможности вести разговор через вычислительную сеть с удовлетворительным качеством в защищенном режиме от не-

санкционированного доступа ($M \geq 1, T_1 \geq 1, T_2 \geq 1, T_3 \geq 1, K_1 \geq 1$). Оценка по каждому показателю выводилась по трехбалльной шкале: 2 - хорошо, 1 - удовлетворительно, 0 - неудовлетворительно. Экспертная группа была сформирована из 10 опытных специалистов, имеющих большой стаж работы в области передачи речи и информационных технологий. Все эксперты были достаточно хорошо обеспечены информацией о сравниваемых системах IP-телефонии и методикой их сопоставления. Как следует из проведенного экспертами анализа в таблице 9, универсальная оценка разработанной система IP-телефонии VoiceOverNet количественно превосходит имеющиеся аналоги почти в два раза.

Таблица 9

Групповые экспертные оценки систем IP-телефонии, защищенных от несанкционированного доступа

Итоговая оценка	Название программного продукта					
	SpeakFreely	PGPfone	Nautilus	Zfone	Skype	VoiceOverNet
K_{IP}	**13,1**	**13,1**	**13,0**	**9,9**	**14,9**	**23,8**

На основании полученных результатов можно сделать вывод о функционировании исследуемой программной системы. Экспериментальные данные (о компрессии звука различными аудиокодеками, функциональных возможностях криптомодулей ОС Windows, использованных при построении системы IP-телефонии, информация о разборчивости звуков при передаче речи через IP-сети в защищенном режиме) подтверждают соответствие результатов работы цели исследования, в частности о соответствии разработанной системы IP-телефонии, защищенной от несанкционированного доступа, заданным на этапе проектирования требованиям.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1) Разработана программная архитектура системы IP-телефонии, защищенной от несанкционированного доступа, которая представляет собой структуру программы (функциональную, информационную модель, представляющих программную систему множеством компонентов), отличающаяся от аналогов принципами создания процессов компрессии и шифрования за счет использования интерфейсов Audio/Video Compression Manager и CriptoApi 1.0 и позволяет передать процессы компрессии и шифрования из пользовательского приложения на уровень операционной системы.

2) Создан количественный критерий оценки качества абонентских систем IP-телефонии, реализующих сценарий “компьютер” – “компьютер” в защищенном от несанкционированного доступа режиме. Критерий отличается учетом качества программных решений с позиций современной технологической базы и затрат на реализацию системы IP-телефонии, и предназначен для обоснования выбора её структуры.

3) Разработана модель потенциального нарушителя, которая может применяться для анализа защищенности как мультимедийных систем IP-

телефонии, так и других информационных систем на основе операционной системы Windows. Модель нарушителя отличается от известных учетом атак на модули ввода/вывода звука DirectSound, на модули компрессии/декомпрессии, модули защиты данных от несанкционированного доступа, а также атак связанных с полной подменой программного обеспечения IP-телефонии.

4) Предложены рекомендации, позволяющие снизить риски несанкционированного доступа к защищаемой речевой информации и нарушения нормального функционирования системы IP-телефонии, работающей в защищенном режиме.

5) Найдены новые количественные характеристики параметров алгоритма генерации ключа из пароля, позволяющего при более короткой длине пароля добиться сопоставимой стойкости с исходным алгоритмом защиты от несанкционированного доступа за счет времени задержки на генерацию ключа.

6) На основе предложенной программной архитектуры разработан и апробирован экспериментальный программный комплекс, включающий в себя ряд программных продуктов: ПО, осуществляющее запись / воспроизведение звука, его обработку, в том числе компрессию / декомпрессию и сохранение полученных результатов в звуковые файлы стандартных форматов; ПО, осуществляющее защиту файлов от несанкционированного доступа с сохранением данных в файлы специально разработанного авторского формата; ПО, предназначенное для передачи сжатой речи через IP-сети в режиме, защищенном от несанкционированного доступа.

7) Оценена эффективность разработанного программного обеспечения, предназначенного для передачи сжатой речи через IP-сети в режиме, защищенном от несанкционированного доступа, а также его ближайших аналогов на основе разработанного критерия качества. Установлено, что потенциал разработанной системы количественно превосходит имеющиеся аналоги в среднем в два раза.

В приложениях приведен материал, посвященный методам компрессии речи, методам защиты информации от несанкционированного доступа, приведен листинг разработанной модели системы передачи речи на языке имитационного моделирования GPSS, приводятся сведения о полученных в результате экспериментов основных технических характеристиках криптопровайдеров в ОС Windows. Также приложены пять актов практического использования результатов работы.

ОСНОВНЫЕ РАБОТЫ, ОПУБЛИКОВАННЫЕ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Нопин С.В. Моделирование защиты речевой информации с помощью персонального компьютера. / С.В. Нопин, В.Г. Шахов.// Омский научный вестник. – 2004. – №4(29). – С. 124-126.
2. Нопин С.В. Свидетельство об официальной регистрации программ для ЭВМ. Шифратор / С.В. Нопин. - № 2006610291 – Программы для ЭВМ… (офиц. бюл.). – 2006. - № 2(55) - С. 70.

3. Нопин С.В. Свидетельство об официальной регистрации программ для ЭВМ. Преобразователь звуковых форматов / С.В. Нопин. - № 2006612352 – Программы для ЭВМ… (офиц. бюл.). – 2006. - № 4(57) - С. 21.
4. Нопин С.В. Свидетельство об официальной регистрации программ для ЭВМ. Система защищенной IP-телефонной связи / С.В. Нопин. - № 2006612351 – Программы для ЭВМ… (офиц. бюл.). – 2006. - № 4(57) - С. 20.
5. Нопин С.В. Использование возможностей операционной системы (ОС) Windows при разработке систем IP-телефонии. / С.В. Нопин // Микроэлектроника и информатика – 2006. 13-я Всероссийская межвузовская научно-техническая конференция студентов и аспирантов: Тезисы докладов. М.: МИЭТ, 2006. – С.287.
6. Нопин С.В. Защита информационных процессов в компьютерных системах / С.В. Нопин – Омск: ОмГТУ, 2006. – 76 с.
7. Нопин С.В. Моделирование защиты речевой информации с помощью персонального компьютера. / С.В. Нопин, В.Г. Шахов, Д.А.Бесов // Научная сессия МИФИ-2006. XIII Всероссийская научная конференция “Проблемы информационной безопасности в системе высшей школы”. Сборник научных трудов. М.: МИФИ, 2006. – С.88-89.
8. Нопин С.В. Преобразование речевой информации с помощью Audio Compression Manager (ACM) в системах IP-телефонии. / С.В. Нопин, В.Г. Шахов // Актуальные проблемы развития железнодорожного транспорта, материалы II Международной научно-практической конференции 7-8 декабря 2005 года. Самара: СамГАПС, 2006. – С.174-176.
9. Нопин С.В. Возможности использования встроенных звуковых кодеков операционной системы (ОС) Windows в системах IP-телефонии / С.В. Нопин, В.Г. Шахов// Омский научный вестник. 2006. – №1(34). – С.155-157.
10. Нопин С.В. Защита данных с помощью встроенных криптографических интерфейсов операционной системы Windows / С.В. Нопин, В.Г. Шахов// Омский научный вестник. 2006. – №7(43). – С.131-134.
11. Нопин С.В. Разработка защищенных от несанкционированного доступа систем IP-телефонии на основе операционной системы Windows / С.В. Нопин, В.Г. Шахов// Омский научный вестник. 2006. – №9(46). – С.137-142.
12. Нопин С.В. Разработка защищенной от несанкционированного доступа системы IP-телефонии, функционирующей в операционной системе Windows / С.В. Нопин // Научная сессия ТУСУР-2007: Материалы докладов всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 3-7 мая, 2007 г. Томск: В-Спектр, 2007. Ч.2. с. 177-179.

Подписано к печати 2008. Бумага офсетная. Формат 60х84 1/16
Отпечатано на дупликаторе. Усл. печ. л. 1,5. Тираж 100 экз. Заказ .

Издательство ОмГТУ. 644050, г. Омск, пр-т Мира, 11
Типография ОмГТУ