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

УДК 621.391.7

Буйновский
Дмитрий Николаевич

Генерирование и прием кодированных сигналов для систем обработки информации

АВТОРЕФЕРАТ

на соискание ученой степени магистра технических наук
по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Бойправ Ольга Владимировна,
кандидат технических наук

_____

Минск 2017

ВВЕДЕНИЕ

Основной целью науки криптографии и систем защиты данных является обеспечение конфиденциальности, целостности, доступности данных. Однако, с постоянным техническим совершенствованием оборудования и программного обеспечения, с ростом вычислительных возможностей ЭВМ, а также с первыми успешными опытами в направлении создания квантовых компьютеров, существует вероятность того, что в скором времени существующие алгоритмы асимметричного шифрования перестанут быть надежными. Причем это будущее уже не за горами. Летом этого года проведены успешные эксперименты по созданию квантового компьютера, состоящего из 51 кубита.

Исходя из вышесказанного, целью данной работы является проведение исследований по возможности создания систем, методов и алгоритмов, способных обеспечить конфиденциальность, целостность, доступность информации при текущем темпе совершенствования вычислительной техники. Причем, конечной целью автором поставлено исследование возможности создания абсолютно надежной системы связи и методики шифрования данных, то есть системы, которую невозможно взломать даже при обладании бесконечным ресурсом вычислительной мощности. Для этих целей использовались критерии абсолютно стойкой системы шифрования, сформулированные Клодом Шенноном в 1949 году, методика передачи данных отдельными фотонами, а также принцип шумоподобных сигналов.

Важность данного вопроса обусловлена тем, что вся методология современной науки становится сегодня существенно в большей степени информационно ориентированной по сравнению с тем, как это было ранее, в минувшее столетие. Поэтому информатика становится не только одной из быстро развивающихся и перспективных областей современной науки, но также и фундаментальной составляющей всего процесса научного познания, научной базой для формирования общества, основанного на знаниях.

На основании проведения исследований дискретных сигналов, а также путем анализа существующих способов генерирования и приёма КС из отечественных и зарубежных источников, потребуется выработать методику обмена секретными ключами на более надежных принципах чем односторонние хеш-функции. Причем появившееся в настоящее время направление, квантовая криптография (основанная на физических процессах квантовых состояний отдельных атомов), не видится эффективной для широкого использования, так как для реализации такой защиты необходимо построение выделенных линий связи, а также невозможность использования для воздушной связи с подвижными объектами. Данная методика

эффективна только для особых задач. На данный момент уже созданы и применяются подобные устройства, например в Швейцарских банках.

Считается, что криптостойкость алгоритма должна зависеть не от тайны технических особенностей этого алгоритма а только от тайны ключа шифрования. Необходимо исходить из предположения, что все технические данные алгоритма известны потенциальному противнику. Однако в некоторых случаях сама методика шифрования может быть ключом. Также основная проблема теории электросвязи, связанная с отысканием методов передачи и приёма, обеспечивающих получение требуемой достоверности принимаемых дискретных сообщений и повышения скорости передачи все еще остается актуальной.

Автором изучен и систематизирован определенный объем сведений по теме диссертационной работы. Разработан и обоснован алгоритм функционирования программного средства, с помощью которого может быть реализован обмен конфиденциальной информацией. Выбрана программная среда для реализации данного решения, а также проведены его разработка и апробация.

Все результаты и выводы данной работы основаны на существующих основополагающих принципах теории электросвязи.

Теоретическая значимость работы заключается в выполненном аналитическом сравнении критериев оптимального приема КС, а также вариантов реализации оптимальных приемников, в соответствии с чем определены их достоинства и недостатки, а также условия использования. Практическая значимость работы обусловлена возможностью использования разработанного программного средства в целях обмена конфиденциальной информацией.

Некоторые компоненты разработанной системы внедрены в коммерческое использование в компании СООО Мобильные ТелеСистемы

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Цель работы – построение модели канала, предназначенного для передачи информации ограниченного распространения. Для достижения поставленной цели решены следующие задачи:

– анализ способов генерирования кодированных псевдослучайных сигналов;

– анализ математических моделей дискретных случайных процессов;

– исследование характеристик источников случайных и псевдослучайных последовательностей;

– определение критериев оптимального приема кодированных сигналов, известных точно, а также сигналов со случайными параметрами;

– аналитическое сравнение структур оптимальных приемников и варианты их реализаций;

– разработка и апробация программы моделирования кодированного сигнала.

Тема диссертации соответствует приоритетным направлениям научных исследований в Республике Беларусь на 2015–2020 годы, установленным Указом Президента Республики Беларусь от 22 апреля 2015 г. № 166 «О приоритетных направлениях научно-технической деятельности в Республике Беларусь на 2016–2020 годы» п.7.6: «Технологии развития информационного общества».

Личный вклад соискателя

Результаты исследований получены автором самостоятельно. Научный руководитель принимал участие в определении целей и задач исследования, интерпретации промежуточных результатов.

Положения, выносимые на защиту

1. Повышение уровня защищенности конфиденциальных данных, передаваемых по каналам связи осуществляется за счет использования разработанного программного средства и обусловлено тем, что в нем реализованы механизмы шифрования с использованием криптостойкого алгоритма (AES) и ключа большой длины, аутентификации и авторизации пользователей, проверки целостности данных и наличия чужого вмешательства, скрытия канала передачи.

2. Уменьшение объема памяти сервера, необходимого для реализации обмена конфиденциальными данными при использовании разработанного программного средства реализовано за счет усовершенствования алгоритма его функционирования, в соответствии с которым передаваемые данные не хранятся на сервере, а основная обработка передаваемых данных осуществляется на клиентских терминалах.

Апробация результатов диссертации

Основные результаты диссертационной работы докладывались и обсуждались на научных конференциях различного уровня: XXI Международной научно-технической конференции «Современные средства связи» (Минск, 20–21 октября 2016 г.); XIV Белорусско-Российской научно-технической конференции «Технические средства защиты информации» (Минск, 25–26 мая 2016 г.).

По теме диссертации опубликованы 1 тезис доклада и 2 статьи в сборнике материалов конференции.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении определена область исследований. В общей характеристике работы обоснована актуальность исследований, сформулирована цель работы, изложены основные положения, выносимые на защиту.

В первой главе определены основные способы кодирования сигналов, приведена математическая модель анализа кодированных сигналов, а также сделан вывод, что для решения поставленной задачи, в качестве физического переносчика целесообразней всего использовать шумоподобные сигналы.

Во второй главе проанализированы характеристики источников случайных и псевдослучайных последовательностей. Для разработанного программного обеспечения очень важным фактором является генерирование списков ключей шифрования. А для этого необходимо использовать генератор случайных последовательностей. Так как любая вычислительная система, действующая по заранее заданному алгоритму, не способна генерировать истинно случайные значения, имеет место очередная уязвимость системы. Поэтому целесообразно для генерации случайных последовательностей использовать источники белого шума, однако на практике это не всегда возможно.

В третьей главе определены критерии оптимального приема кодированных сообщений, структура оптимальных приемников, а также обоснована необходимость использования помехоустойчивого кодирования. Также приведены критерии оценки криптостойкости приема сигналов. Наиболее важными в данном случае являются критерии Клода Шеннона, которым должен соответствовать абсолютно стойкий алгоритм шифрования, характеризующийся следующими свойствами:

– ключ генерируется для каждого сообщения (каждый ключ используется только один раз);

– ключ статистически надежен (то есть вероятности появления каждого из возможных символов равны, символы в ключевой последовательности независимы и случайны);

– длина ключа равна длине сообщения или больше ее;

– исходный (открытый) текст обладает некоторой избыточностью (что является критерием оценки правильности расшифровки).

Данные критерии были использованы для разработанного программного обеспечения.

В четвертой главе представлены результаты разработки программного обеспечения для передачи конфиденциальной информации. Система, в которой оно должно использоваться, характеризуется модульной

архитектурой, состоящей из среды передачи, которая организуется с помощью протокола OpenVPN, приложений клиентов, реализованных на основе tcp сокетов, базы данных для хранения клиентских сессий (соответствия идентификатора клиента и его IP адреса), а также прокси через который осуществляются внутренние взаимодействия (Soap gateway). Также разработан усовершенствованный способ кодирования данных, повышающий надежность защиты информации. Данный способ основан на принципе одноразового блокнота и криптостойком алгоритме (AES).

ЗАКЛЮЧЕНИЕ

Актуальность обозначенного решения обусловлена ростом вычислительной мощности электронных систем, а также теоретической возможностью появления квантовых компьютеров в будущем.

В данной работе проведены теоретические исследования по возможностям генерирования и приема кодированных сигналов на основании физической среды, а также произведена практическая разработка комплексного программного решения для передачи зашифрованных данных. Стоит отметить, что при разработке были использованы существующие решения криптографии и разработана своя методика. Этот комплексный подход существенно повысил надежность такой линии связи. Разработанное решение возможно использовать для связи через открытые сети (интернет), либо через защищенную изолированную линию передачи (с использованием шумоподобных сигналов через воздушные линии связи, либо методики передачи информации отдельными фотонами). Разработанное решение универсально. Связь можно осуществлять между различными устройствами (мобильными телефонами, стационарными узлами на базе всех существующих операционных систем – IOS, MacOS, Android, Windows, Unix). Ограничений нет. На данный момент автором разработаны клиенты для IOS, Android и Windows.

Разработана модель защищенного канала связи для передачи секретной информации. Данная модель основывается частично на использовании свободно распространяемого программного обеспечения, а частично на собственных разработках автора. Также разработано усовершенствование алгоритма шифрования на основе критериев Шеннона, при котором используется уникальный ключ для каждого сообщения, длина ключа равняется длине сообщения, а ключ этот передается по существующей системе связи в зашифрованном виде. Также используется список предварительно сгенерированных ключей, который должен быть в наличии на обеих сторонах и для расшифровки последующего сообщения необходимо использовать ключ находящийся в самом сообщении и переданный в предыдущем сообщении. Генерация ключа в предыдущем сообщении используется с помощью генератора случайных последовательностей. В разработанном программном обеспечении использована частичная реализация принципа одноразового блокнота, по разработанному автором алгоритму, а также решение плавающей кодировки.

Эта методика основана на простых и надежных принципах, однако не эффективных с точки зрения скорости передачи и быстродействия. Поэтому разработанный алгоритм может представлять собой только временное решение обозначенной проблемы, так как при такой реализации полезная

нагрузка снижается в два раза. Для повышения скорости передачи потребуются дальнейшие исследования.

Проанализированы существующие методы защиты информации. На основании полученных данных, можно сделать вывод, что наиболее эффективная технология с точки зрения сокрытия конфиденциальной информации – передача информации с использованием шумоподобных сигналов.

При текущем положении развития техники и науки криптографии, существующие методы защиты достаточно надежны. Однако, в случае появления квантовых компьютеров, алгоритмы основанные на сложности в решении определенного рода задач (например задачи факторизации) за обозримый промежуток времени, станут ненадежными. Для абсолютно надежной защиты данных в будущем, возможно использовать либо физическую защиту линий связи (технологии которых рассмотрены в разделах 1, 2), либо совершенствование существующих алгоритмов защиты данных. В данной работе произведен теоретический анализ дискретных сигналов и возможности использования шумоподобных сигналов для защиты данных. Также для передачи секретного ключа можно использовать однофотонные линии связи В этом случае защита основана на постулате, заключающемся в том что попытка измерения взаимосвязанных параметров в квантовой системе вносит в неё нарушения. Однако для широкого применения использование таких систем не представляется возможным ни сейчас ни в будущем, так как потребуется строительство дополнительных линий связи плюс такая методика не сработает для беспроводных систем связи.

Следует отметить, что согласно статистическим данным, очень малый процент всех взломов осуществлен с использованием уязвимостей алгоритмов. При текущем развитии науки и техники существующие алгоритмы надежны, а успешные взломы чаще всего связаны с использованием слабых ключей, компрометации ключей и т.д. На данный момент, самой главной угрозой информационной безопасности является человеческий фактор. Поэтому, наиболее безопасная линия – линия созданная с использованием методики NGE (комплексный подход заключающийся не только в использовании эффективных систем шифрования, но и мероприятия по организации процесса обмена конфиденциальной информации с целью предотвращения человеческого фактора).

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Буйновский, Д.Н. Перспективы использования квантовой криптографии в современных системах связи. / Д.Н. Буйновский // XXI Международная научно-техническая конференция «Современные средства связи» УО БГАС. Минск, 20–21 октября 2016 г. – Минск, 2016. – С. 233–234.

2. Буйновский, Д.Н. Применение М-последовательностей для скрытной передачи информации. Помехоустойчивое кодирование. / Д.Н. Буйновский // XIV Белорусско-Российская научно-техническая конференция «Технические средства защиты информации» УО БГУИР. Минск, 25–26 мая 2016 г. – Минск, 2016. – С. 26.

3. Буйновский, Д.Н. Шифрование следующего поколения (NGE). Помехоустойчивое кодирование. / Д.Н. Буйновский // XIV Белорусско-Российская научно-техническая конференция «Технические средства защиты информации» УО БГУИР. Минск, 25-26 мая 2016 г. – Минск, 2016. – С. 26–27.

4. Дмитрий Буйновский. Часть 1. Установка и настройка авторитетного DNS сервера на основе решения PowerDNS. Базовая установка [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/278153/. – Дата доступа : 20.11.2016

5. Реализация асинхронной защищенной системы связи на основе TCP сокетов и центрального OpenVPN сервера [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/346792/. – Дата доступа : 17.01.2018.