

РАЗРАБОТКА МЕТОДОВ УПРАВЛЕНИЯ КЛЮЧАМИ ШИФРОВАНИЯ В СПУТНИКОВЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

DEVELOPMENT OF METHODS FOR MANAGING ENCRYPTION KEYS IN SATELLITE DATA TRANSMISSION NETWORKS

МЕЛЬНИКОВ АЛЕКСЕЙ ОЛЕГОВИЧ,

доцент,

МИРЭА - Российский технологический университет.

РУСАКОВ АЛЕКСЕЙ МИХАЙЛОВИЧ,

старший преподаватель,

МИРЭА - Российский технологический университет.

ШМИТЬКО КИРИЛЛ АНДРЕЕВИЧ,

студент,

МИРЭА – Российский технологический университет.

MELNIKOV ALEKSEY OLEGOVICH,

docent,

MIREA – Russian Technological University.

RUSAKOV ALEKSEJ MIXAJLOVICH,

senior lecturer,

MIREA – Russian Technological University.

SHMITKO KIRILL ANDREEVICH,

student,

MIREA – Russian Technological University.

В статье приводится обзор и анализ современных методов осуществления безопасности спутниковых систем связи на основе программно-аппаратных решений. Предметом исследования являются алгоритмы управления ключами шифрования в спутниковых сетях VSAT. В том числе, оценены преимущества и недостатки беспроводных систем, проведен обзор применяемых способов шифрования спутникового трафика. Представлены основные методы обеспечения безопасности передачи информации в беспроводном спутниковом канале от абонента к абоненту. Проанализированы сильные и слабые стороны различных решений по осуществлению методик шифрования ключей для передачи информации.

The article provides an overview and analysis of modern methods of implementing the security of satellite communication systems based on software and hardware solutions. The subject of the study is encryption key management algorithms in VSAT satellite networks. In particular, the advantages and disadvantages of wireless systems are evaluated, a review of the methods used to encrypt satellite traffic is carried out. The main methods of ensuring the security of information transmission in a wireless satellite channel from subscriber to subscriber are presented. The strengths and weaknesses of various solutions for implementing key encryption techniques for information transmission are analyzed.

Ключевые слова: *управление ключами, VSAT, шифрование, аппаратное шифрование, информационная безопасность.*

Управление ключами играет важнейшую роль в криптографии. Данный механизм является основным для обеспечения безопасности информации. Важнейшей задачей управления ключами является сведение безопасности многочисленных ключей криптосистемы к установлению абсолютной безопасности одного ключа либо малой группы ключей, которые могут использоваться для шифрования основных ключей. Это достигается несколькими способами: изоляция ключей, выбором безопасного хранилища и т.д. Целью управления ключами является нейтрализация таких угроз, как:

1. Компрометация конфиденциальности секретных ключей.
2. Компрометация аутентичности секретных или открытых ключей.
3. Несанкционированное использование секретных или открытых ключей.

Обзор современных технологий

Пользователей интернета в России по данным от 28 сентября 2022 года – около 130 млн. человек, что составляет примерно 90% населения [6]. Большая плотность пользователей приходится на Московскую и Ленинградскую области. Интернет передается проводным способом, так как маршрутизационные пункты располагаются достаточно близко друг к другу, и это не составляет труда провести ответвление для нового пункта. Что касается дальних регионов, то даже для местности на расстоянии 100-200 км от областного центра возникают проблемы с проводным интернетом. Связаны они, в основном, с рельефом местности, погодными условиями и со степенью развития инфраструктуры – факторы, влияющие на передачу информации беспроводным способом. Спутниковые системы связи лишены существенных недостатков проводных систем. К примеру: в системе VSAT к интернету подключены лишь ЦУС (центральные управляющие станции), поэтому исключаются возможные трудности с прокладкой интернет-кабелей к многочисленным потребителям – достаточно подключить один концентратор, который будет осуществлять связь с большим количеством удаленных терминалов; абонентские терминалы подключаются непосредственно у пользователей, поэтому перебои электричества на распределительных центрах так же исключаются.

Исходя из вышеизложенного, спутниковая связь в регионах со сложным рельефом местности, суровыми климатическими условиями и т.д. способна обеспечить потребность населения в таких видах сервиса, как интернет, телевидение и телефония.

Современные системы VSAT за последние несколько лет модернизировались и теперь могут конкурировать по скорости с проводным интернетом. В настоящее время VSAT-терминалы работают в Ku- и Ka- диапазонах. Диаметр антенн, при этом, варьируется от 0,3 до 1,5 м. Такое оборудование уже на порядок доступнее для конечного потребителя, и это способствует более быстрому распространению технологии. Что касается защищенности передачи информации по спутниковым каналам связи – можно сказать следующее: спутниковый канал не скрыть от прослушивания – данные передаются в эфире и их можно перехватить. При этом, легко найти и использовать доступное массам оборудование: антенну и DVB-тюнер (DVB – Digital Video Broadcasting – семейство стандартов цифрового телевидения)[7]. Так, любителям послушать в эфире какие-нибудь частоты, удастся достаточно просто узнавать подобную информацию:

- навигационную информацию летательных аппаратов и морских судов;
- данные для входа в панель управления ветряной электростанцией;
- информация о неисправностях судов, находящихся на рейсах;
- электронные письма и т.д.

Чаще всего, систему защиты данных настраивают на уровне протоколов, с помощью которых эти данные можно передавать. Сам по себе протокол – некий набор соглашений, которым должны следовать участники обмена информацией [2]. В различных стандартах протоколов упоминается степень защищенности передачи, а также, как это влияет на скорость передачи.

Дело в том, что трафик в протоколах шифруется на устройстве отправителя и дешифруется у получателя. Для этого необходимо договориться о правилах шифрования между участниками. Такая договоренность заключается в использовании единого алгоритма шифрования/дешифрования, а также механизме передачи ключа. Информация может шифроваться/дешифроваться не только на программном уровне, но и на аппаратном, при помощи специальных микросхем, в которые с завода установлен уникальный алгоритм шифрования/дешифрования, а также ключ – тем самым исключается возможность перехватить его злоумышленнику. Такие устройства должны быть установлены как у отправителя информации, так и у ее получателя.

Шифрование представляет собой сокрытие информации от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней. Пользователи называются авторизованными, если у них есть соответствующий ключ для дешифрования информации. Важной особенностью шифрования является то, что даже если злоумышленник заполучил зашифрованный текст и знает алгоритм, он не сможет ничего добиться без ключа.

Шифрование подразделяется на симметричное и асимметричное. В первом случае – используется один ключ как для шифрования, так и для дешифрования. Данный вид не может обеспечить процедуру проверки подлинности (аутентификация), поскольку любой пользователь может создавать, шифровать и отправлять действительное сообщение. Во втором случае – используется два ключа, один из которых открытый, то есть может передаваться по открытому каналу, используется только для шифрования информации. При перехвате такого ключа злоумышленник не может нарушить целостность информации. Второй ключ закрытый – остается на концах передачи информации конфиденциальным – используется в паре с открытым ключом для дешифрования.

При этом зашифрованный текст представляет собой тот же текст в той же кодировке, но он видоизменен математическим алгоритмом. В зависимости от реализации алгоритма шифрования, текст может меняться перестановками, с помощью операции XOR, с помощью замены символов и т.д. В компьютере данные вычисления над текстом производятся в специальной кодировке – например, в ASCII, KOI8-г – где символ текста представлен в виде двоичного числа, удобного для различных преобразований.

Существует два способа применения шифрования. Первый из них – программный, а второй – аппаратный. Существенное отличие аппаратного способа от программного состоит в быстродействии первого. Данный способ реализуется специальной микросхемой в оборудовании для передачи данных, которая создана только для шифрования и не задействуется для решения пользовательских задач – избавлена от сторонней нагрузки. Аппаратное шифрование является дорогостоящим решением, и приобретать его необходимо в определенных рассчитанных случаях – как известно, стоимость решения по защите информации должна быть меньше, чем стоимость потери информации [5].

Также существуют программно-аппаратные средства шифрования, которые позволяют производить шифрование на процессорах, которые также используются для пользовательских задач. Это реализовано с помощью внедрения в основной чип сопроцессора, который производит только криптографические вычисления [8].

В случае с программным решением – все достаточно просто. Алгоритмы шифрования стандартизированы и классифицированы. Программисту необходимо использовать тот или иной алгоритм в зависимости от необходимой степени защищенности и скорости передачи данных. Останется только разработать механизм передачи ключей.

В современных спутниковых системах используется комбинированная защита. Это означает, что при производстве удаленных терминалов и концентраторов производитель интегрирует индивидуальный ключ шифрования в специальную микросхему платы, которая может являться как отдельным модульным устройством в архитектуре терминала, так и быть

встроенной в саму материнскую плату конкретного устройства. Таким образом, терминалы используют один ключ для шифрования/дешифрования остальных ключей, которые уже можно использовать для защиты передаваемого трафика.

Цель данной работы состоит в разработке нового метода управления ключами шифрования для передачи данных по спутниковой сети передачи данных.

Достоинства и недостатки современных систем

Во время протокольного общения между терминалами могут отправляться дополнительные ключи для многоуровневой защиты по специальному защищенному каналу. Ключи будут отправляться в двух случаях:

- истек срок жизни ключа;
- удаленный терминал запросил новый ключ.

Например, достаточно распространен следующий подход к безопасности спутниковых сетей. Генерацией и отправкой ключей занимается концентратор.

Он формирует новый ключ с помощью специальной микросхемы. Данный ключ помещается в одно из двух специальных сообщений, в зависимости от причины генерации нового ключа, PACAU (Periodic Adapter Conditional Access Update) и ICAU (Interactive Adapter Conditional Access Update). Данные ключи являются уже производными от ключей, встроенных в плату.

При этом происходит шифрование уровней потока данных в системе передачи для получения большей стойкости информации к взлому. Вложенность уровней упирается в нужную производительность системы [9].



Рис. 2. Процесс инициализации ключей удаленного терминала.

Такой подход к шифрованию трафика является достаточно мощным решением, подходящим для предотвращения большинства атак на конфиденциальную информацию, перехваченную в открытом канале связи.

Стоит отметить, что для реализации высокого уровня безопасности системы, используется передача ключей по защищенному каналу связи.

К примеру, при вводе в эксплуатацию нового терминала осуществляется следующий алгоритм инициализации ключей и синхронизации нового удалённого терминала с концентратором:

1. С удалённого терминала отправляются заводские данные.
2. В концентраторе производится запись в базу данных информации о новом терминале.
3. Осуществляется генерации ключей для нового терминала и ожидается запрос этих ключей с терминала.
4. После запроса ключей происходит авторизация нового терминала, и отправка ключей на терминал.
5. Удалённый терминал, принявший новые ключи, осуществляет их дешифрование с помощью ключа завода-изготовителя.
6. Теперь может происходить защищенный обмен данными между удаленным терминалом и концентратором.

Этот процесс продемонстрирован на Рисунке 2.

Таким образом, основными методами обеспечения безопасности передачи информации в беспроводном спутниковом канале от абонента к абоненту являются:

- ограничение физического доступа к каналу связи;
- применение аппаратно-программных средств защиты информации.

При реализации первого метода, осуществляются мероприятия по физической защите терминала спутниковой связи (пропускной режим, видеонаблюдение и т.д.). При реализации второго метода используются уже описанные методики:

- применение фирменных алгоритмов шифрования данных;
- проверка подлинности терминала при его регистрации в сети оператора (аппаратный ключ);
- шифрование как всего сеанса работы (программный ключ), так и каждого сеанса в отдельности (сеансовые ключи);
- применение фирменных алгоритмов преобразования исходных данных во внутренние форматы (структуры) данных, которые потом передаются через спутниковый канал; тем самым решаются задачи дополнительной защиты информации, доставки служебной информации и коррекции ошибок.

Данные способы применимы для прямых и обратных спутниковых каналов связи [1]. Прямой канал – от концентратора к абонентам, обратный – от абонентов к концентратору.

Преимущество системы управления ключами заключается в том, что если ключевой материал, хранящийся в концентраторе, будет скомпрометирован, ключ на удаленном терминале можно будет сменить с помощью другого зашифрованного ключа, восстановив целостность системы безопасности. Поэтому ответственность за обеспечение безопасности ключа, встроенного в терминал, несет исключительно производитель терминала.

Также усиливает безопасность тот факт, что между удаленным терминалом и концентратором используется схема разделения секрета: концентратор использует зашифрованный уникальный ключ от удаленного устройства для шифрования ключей уровня потока данных, необходимых для услуг, которые разрешено получать удаленному терминалу. Удаленный терминал использует свою копию уникального зашифрованного ключа для расшифровки трафика и, таким образом, получает доступ к этим услугам.

Итак, можно говорить о следующих достоинствах данного подхода к шифрованию передачи данных по спутниковому каналу связи:

- 1) высокая степень защищенности;
- 2) низкая степень компрометации ключей шифрования;
- 3) высокая производительность сетевой архитектуры.

К недостаткам можно отнести:

- 1) сложность реализации;
- 2) дорогостоящее оборудование.

СПИСОК ЛИТЕРАТУРЫ

1. Гурлев И.В. Методы и способы обеспечения безопасности информации, передаваемой по спутниковой сети технологии VSAT // Интернет-журнал «Науковедение». 2017. № 3. 8 с.
2. Столяров А.В. Программирование: введение в профессию. Т.2 Системы и сети. М.ДМК Пресс. 2021. 656 с.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. 2-е изд., испр. и доп. М. Гелиос АРВ, 2002. 480 с..
4. Лаган Е.А., Футерман М.Ю. Сравнительный анализ средств программного и аппаратного шифрования // Инновации, технологии, наука: сборник статей Международной научно-практической конференции. 2016. №2. С.57-59.
5. Мэйволд Е. Безопасность сетей: 3-е издание (эл.) Москва: Национальный Открытый Университет «ИНТУИТ»: Ай Пи Ар Медиа, 2021. 571 с.
6. Сайт правительства России. URL:<http://government.ru/news/46639>(дата обращения:27.02.2023).
7. Перехват трафика кораблей и самолетов // Хабр. URL: <https://habr.com/ru/company/globalsign/blog/515370> (дата обращения: 19.01.2023).
8. Криптография в отдельном блоке: криптографический сопроцессор семейства STM32F4xx. URL: <https://www.compel.ru/lib/54365> (дата обращения: 11.03.2023).
9. Telecommunications Industry Association. URL:<https://tiaonline.org/standard/tia-1008> (дата обращения: 03.01.2023).

© Мельников А.О., Русаков А.М., Шмитько К.А., 2023.