Интернет-журнал «Науковедение» ISSN 2223-5167 http://naukovedenie.ru/

Том 9, №3 (2017) http://naukovedenie.ru/vol9-3.php

URL статьи: http://naukovedenie.ru/PDF/85EVN317.pdf

Статья опубликована 22.06.2017

Ссылка для цитирования этой статьи:
Гурлев И.В. Методы и способы обеспечения безопасности информации, передаваемой по спутниковой сети технологии VSAT // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №3 (2017) http://naukovedenie.ru/PDF/85EVN317.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 621.391:654.1

Гурлев Игорь Валентинович
ФГКОУ ВО «Академия управления МВД России», Россия, Москва
Доктор технических наук, старший научный сотрудник
Действительный член РАЕН
Главный научный сотрудник Академии управления МВД России
E-mail: gurleff@mail.ru

Методы и способы обеспечения безопасности информации, передаваемой по спутниковой сети технологии VSAT

Аннотация. Обеспечение информационной безопасности является одним из ключевых факторов при выборе систем связи государственными учреждениями, финансовыми структурами, крупными кампаниями и другими организациями, а также правоохранительными органами, успех деятельности которых во многом зависит от сохранности передаваемой информации.

В настоящее время активно развиваются спутниковые системы связи, которые по сравнению с наземными кабельными и радиорелейными сетями связи прямой видимости имеют ряд существенных преимуществ: обладают гораздо более широким охватом, а значит, в удаленных и малонаселенных регионах России являются наиболее оптимальным техническим и экономическим решением.

В статье рассматриваются преимущества спутниковой системы связи в малонаселенных районах Крайнего Севера и Дальнего Востока с антеннами, имеющими малую апертуру, по сравнению с проводными сетями, а также физические и программно-аппаратные методы и способы защиты информации, передаваемой по каналам связи спутников, находящихся на геостационарной орбите.

При реализации метода физической защиты информации обеспечивается физическая охрана объекта, инженерная защита: устанавливаются ограждения вокруг объекта, сигнализация, ведется видеонаблюдение и др.

Программно-аппаратные методы и способы защиты информации предполагают использование специальных протоколов, кодирование и шифрование информации.

Ключевые слова: спутниковая сеть; геостационарная орбита; связь; безопасность информации; методы; способы защиты; физическая защита; инженерная защита; аппаратно-программный метод; протоколы; кодирование; шифрование

Новые информационные технологии способствуют осуществлению активных качественных преобразований в социально-экономической системе России [7, с. 40].

В настоящее время активно развиваются спутниковые системы связи. Спутниковые системы связи по сравнению с кабельными сетями имеют ряд существенных преимуществ: обладают гораздо более широким охватом, т.к. не зависят от инфраструктуры наземных коммуникаций, а значит, в удаленных и малонаселенных регионах России, например, на Крайнем Севере и Дальнем Востоке, являются наиболее оптимальным техническим и экономическим решением. Кроме того, наличие спутниковой системы связи позволяет обеспечить связью многочисленные кочевья оленеводов, геологические партии, а также объединить внутренние коммуникации филиалов добывающих компаний, населённых пунктов, подразделений правоохранительных органов министерства внутренних дел и др. в единую информационную сеть [1, с. 21].

С учетом регулярных ротаций вахтовых смен, приезжающих и отъезжающих с многочисленных добывающих и других предприятий Крайнего Севера и Дальнего Востока страны, когда количество завербованных на работы людей превышает численность местного населения, опасность роста правонарушений резко увеличивается и потребность правоохранительных органов в надёжной связи и защищённой информации, передаваемой по спутниковым каналам, в том числе и персональных данных, становится ещё более актуальной [4, с. 39-40; 5, с. 64].

Исходя из вышеизложенного, спутниковая связь на сегодняшний день является востребованной технологией, с помощью которой осуществляются: телефонная и факсимильная связь; доступ в Интернет; трансляция видеоконференций и т.п.

Для построения сетей связи крупные территориально-распределённые компании в настоящее время широко используют спутниковые системы технологии VSAT.[1] Обозначение «VSAT» было введено в техническую литературу в 1983 году с целью отличать абонентские станции с антеннами малых диаметров (до 2,4 м) от наземных станций с антеннами больших размеров. Сети спутниковой связи технологии VSAT строятся на базе космических аппаратов (спутников-ретрансляторов), находящихся на геостационарной орбите Земли. Одним из самых существенных достоинств спутниковой связи технологии VSAT является её возможная полная независимость от наличия местных наземных интернет-провайдеров. Для осуществления связи с использованием технологии VSAT необходимо только электричество и прямая видимость на спутник [3, с. 8].

Кроме космического аппарата сеть спутниковой связи включает в себя также центральную управляющую станцию (ЦУС) оператора спутниковой связи и абонентские терминалы VSAT.

В состав ЦУС входят приёмо-передающая аппаратура, антенно-фидерные устройства и комплекс контрольного оборудования, который осуществляет функции контроля и управления всей абонентской спутниковой сетью, перераспределение её ресурсов, выявление неисправностей, сопряжение сети с наземными линиями связи, а также тарификацию предоставляемых услуг связи. Компактные терминалы VSAT размещаются непосредственно в удалённых точках, поддерживая широкий спектр современных мультисервисных услуг.

На рис. 1 показана упрощенная схема «абонент-абонент» спутниковой сети связи технологии VSAT.

[1] VSAT (Very Small Aperture Terminal) - терминал с очень малой апертурой.

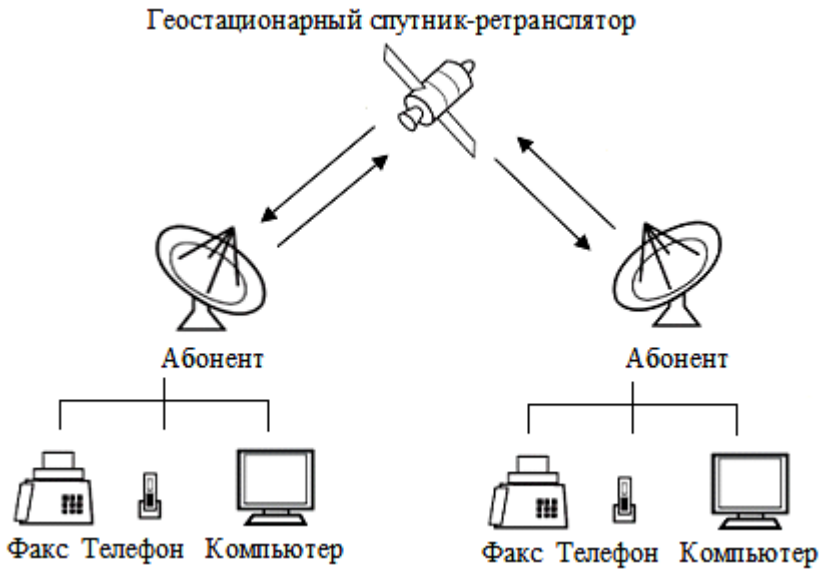

Рисунок 1. *Схема спутниковой связи «абонент-абонент» (составлено автором)*

В отличие от наземных проводных сетей связи, которые подвержены таким опасностям, как отказ сетевого оборудования, сбои и аварии в сетях электрооборудования, в том числе обрыв и повреждение кабеля (по разным причинам, например, грызунами или перемещением замороженных грунтов), спутниковая связь избавлена от этих недостатков.

В соответствии с Регламентом Международного союза электросвязи (МСЭ) для систем спутниковой связи выделено несколько диапазонов частот (таблица 1).

Телекоммуникационный и информационный ресурс российского рынка космической связи технологии VSAT практически полностью обеспечивается геостационарными спутниками двух отечественных компаний: ФГУП «Космическая связь» (космические аппараты серии «Экспресс-АМ») и ОАО «Газпром космические системы» (космические аппараты серии «Ямал») [6, с. 36].

Российские системы спутниковой связи и вещания работают, в основном, в C- и Ku-диапазонах. В последние годы происходит переход спутниковой связи технологии VSAT на более высокочастотный Ka-диапазон, при котором антенны имеют меньшие размеры и цену, что, как следствие, должно привести к увеличению числа пользователей [10].

Таблица 1

№ п/п	Наименование	Полоса частот (ГГц)	Диаметр антенны (м)	Область применения
1	L-диапазон	1,452-1,550 и 1,610-1,710		Подвижная спутниковая связь
2	S-диапазон	1,93-2,70		Подвижная спутниковая связь
3	C-диапазон	3,40-5,25 и 5,725-7,075	2,4-2,5	Фиксированная спутниковая связь
4	Ku-диапазон	10,70-12,75 и 12,75-14,80	0,6-1,5	Фиксированная спутниковая связь, спутниковое вещание
5	Ka-диапазон	15,40-26,50 и 27,00-30,20	0,3-0,9	Фиксированная спутниковая связь, межспутниковая связь

Составлено автором

С помощью спутников связи, находящихся на геостационарных орбитах, можно достаточно быстро сформировать сетевую инфраструктуру с высокими показателями надёжности, поэтому спутниковые каналы VSAT широко применяются при построении распределённых корпоративных и государственных сетей.

Для таких каналов предусматривается достаточно высокий уровень шифрования и защиты данных. Системы связи технологии VSAT предохраняют передаваемую информацию гораздо надёжнее, чем другие технологии связи и выбираются пользователями для резервирования имеющихся каналов как заведомо более безопасные с технической точки зрения и максимально защищённые от повреждений и сбоев.

Передача цифровой информации в сетях VSAT характеризуется низким уровнем ошибок - не более одной на 10 млн. переданных бит информации (примерно одна ошибка на 500 страниц текста) и надёжной работой - до 100 тыс. часов (более 10 лет круглосуточной бесперебойной связи) [2, с. 40].

Скорость работы по спутниковому каналу для терминала VSAT составляет от 16 Кбит/с до 10 Мбит/с и более (до 100 Мбит/с), что сопоставимо со скоростью передачи данных в наземном канале.

Вместе с тем, спутниковые сигналы, так же как сигналы радиорелейных линий связи, подвержены существенному ослаблению во влажной атмосфере (дождь, туман, низкая облачность), поэтому в конкретной местности, с учетом многолетних климатических наблюдений, влияние погодных условий необходимо учитывать при проектировании и снижать их воздействие путем оптимального выбора места установки антенного поста.

В начале 90-х гг. прошлого века технология VSAT была ориентирована в основном на предоставление операторам связи закреплённых одиночных каналов SCPC[2] и организацию удалённого доступа к сетям телефонии. Затем, с увеличением технических возможностей, изменились потребности рынка пользователей и акцент сместился с предложения исключительно голосовых услуг к комбинированным телематическим услугам, включая услуги передачи данных.

Производители оборудования VSAT, прежде всего каналообразующего, всё в большей мере ориентируются на использование протоколов IP[3] и Frame Relay[4] на транспортном уровне своих систем. Специализированные программы необходимые для передачи данных с одного компьютера и приёма их другим компьютером в технической литературе называются «протоколами». Транспортный уровень - TL (Transport Layder) это уровень сети связи, который организует доставку информации без ошибок, потерь и дублирования в переданной последовательности. Протокол IP - один из самых основных протоколов, который объединил отдельные компьютерные сети в глобальную сеть, он входит в стек (набор) протоколов TCP/IP. Протокол TCP (Transmission Control Protocol) - протокол управления передачей.

По мере развития глобальных сетей связи, образованием многомиллионного числа пользователей, появилась настоятельная потребность в защите передаваемой информации.

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.

---

[2] SCPC (Single Channel Per Carrier) - один канал на несущую частоту.

[3] IP (Internet Protocol) - межсетевой протокол.

[4] Frame Relay (ретрансляция кадров) - высокоскоростная технология, основанная на коммутации пакетов, для передачи данных между интеллектуальными оконечными устройствами типа маршрутизаторов или FRAD, работающих со скоростью от 56 Кб/с до 1.544 Мб/с

При реализации первого метода обеспечения безопасности спутниковой связи осуществляется комплекс организационных и административных мероприятий по защите узла связи (ЦУС). Безопасность объекта обеспечивается мерами физической и инженерной защиты:

- обеспечивается физическая охрана объекта;
- устанавливаются ограждения вокруг объекта;
- устанавливается сигнализация;
- ведется видеонаблюдение;
- действует пропускной режим.

К средствам защиты информации от несанкционированного доступа также относятся:

- идентификация - опознание (отождествление) пользователя по его уникальному имени и коду;
- аутентификация - установление подлинности пользователя, представившего идентификатор или проверка того, что лицо или устройство является тем, за кого себя выдает (наиболее распространённым способом аутентификации является пароль);
- авторизация - проверка полномочий или проверка права пользователя на доступ к конкретным ресурсам (авторизация проводится с целью разграничения прав доступа к сетевым и компьютерным ресурсам).

Техническими специалистами выполняются регламентные работы по полному резервному копированию баз данных и конфигурации всех ключевых серверов.

Если наличие внешней физической и инженерной защиты направлено против проникновения на объект снаружи, то против несанкционированного доступа злоумышленников, находящихся внутри объекта, к каналам связи используются логины, пароли и ключи.

Второй метод обеспечения безопасности информации, передаваемой по спутниковой сети технологии VSAT, связан с аппаратно-программными средствами защиты информации в каналах связи и обеспечивается благодаря кодированию и шифрованию данных.

Кодирование информации - процесс преобразования передаваемых данных из формы, удобной для непосредственного использования информации, в форму, удобную для передачи, хранения или автоматической обработки (например, двоичный код).

Шифрование данных - процесс преобразования информации с помощью ключа (шифра) так, чтобы её не мог прочитать посторонний.

Кроме уже разработанных открытых протоколов необходимых для передачи данных с одного компьютера и приёма их другим компьютером, были разработаны стандарты защищённых протоколов, например, протокол IPsec, который обеспечивает безопасность на сетевом уровне. Сетевой уровень - NL (Network Layer) определяет пути передачи данных, адрес, маршрутизацию. В настоящее время существуют 12 стандартов протокола IPsec: RFC2401, …, RFC2412.

Протокол IPsec (набор протоколов) обеспечивает:

- целостность виртуального соединения, аутентификацию источника информации по протоколу AH (Authentication Header);

- шифрование передаваемой информации по протоколу ESP (Encapsulating Security Payload);
- первичную настройку соединения, взаимную аутентификацию и обмен конфиденциальными ключами.

Протоколы являются аппаратно-программными способами защиты информации и входят в аппаратно-программный метод защиты информации, т.к. являются специализированными программами, а реализуются с помощью технических средств (блок питания, блок памяти, генераторы частоты, приемо-передающие устройства и т.д.).

В настоящее время в современных двусторонних сетях VSAT используются мощные системы кодирования на программно-аппаратном уровне, что делает перехват информации по радиоканалу практически невозможным.

Спутниковый канал в направлении от ЦУС к терминалу пользователя является прямым спутниковым каналом (DVB-S, DVB-S2, Frame Relay)[5]. Этот канал - единый для всей сети терминалов оператора. По нему осуществляется передача конфигурационных параметров и управляющих команд оператора, а также пользовательских данных.

Все передаваемые по спутниковому каналу данные проходят многоступенчатую систему преобразований и шифрования, в результате которой осуществляется:

- 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;
- ускорение данных, передаваемых по протоколу TCP/IP;
- в создаваемых виртуальных каналах исходные данные в сеансах TCP группируются, сжимаются и получают приоритеты [8].

Спутниковые каналы в направлении от терминалов к ЦУС являются обратными спутниковыми каналами. Сети терминалов оператора могут работать сразу с несколькими обратными каналами. Само их устройство и метод работы позволяет говорить о них, как о защищенных.

В настоящее время самыми распространенными способами функционирования терминалов в таких каналах являются принципы доступа с временным и частотно-временным разделением каналов TDMA/FDMA (TDMA - способ использования радиочастот, когда в одном частотном интервале находятся несколько абонентов. FDMA - способ использования радиочастот, когда в одном частотном диапазоне находится только один абонент)[6].

[5] DVB (Digital Video Broadcasting) - цифровое видео вещание.

[6] TDMA (Time Division Multiple Access) - множественный доступ с разделением по времени; FDMA (Frequency Division Multiple Access) - множественный доступ с разделением по частоте.

Каждый обратный канал работает в своей определённой частотной полосе или со своей несущей модулированной частотой и с определённым алгоритмом кодирования для выявления и коррекции ошибок, передаваемых данных - Turbo Coding[7].

Конкретный терминал может осуществлять передачу только в одном обратном канале. Однако многие производители спутникового оборудования уже реализовали возможность изменения частот несущих обратных каналов, на которых терминалы осуществляют передачу FDMA от одного пользовательского сеанса к другому, что позволяет, с одной стороны, выполнять перераспределение всех передающих терминалов по обратным каналам в рамках их группы (балансировку нагрузки), а с другой - значительно усложняет перехват передаваемых данных.

Каждый обратный канал делится на временные составляющие. С точки зрения терминалов он не является непрерывным, а представляет собой последовательность импульсных сигналов, причем длительность каждого не превышает несколько миллисекунд. При методе многостанционного доступа с временным разделением TDMA передатчики множества терминалов передают данные в выделенные им временные интервалы по одному каналу или в рамках группы каналов.

Шифрование данных в спутниковом канале осуществляется при участии как спутниковых терминалов на стороне пользователя, так и специализированных высокопроизводительных серверов на ЦУС оператора. На специальном сервере оператора размещается защищенная база данных ключей шифрования и сеансовых ключей всех спутниковых терминалов. Чтобы терминал смог работать в сети оператора, информация в базе ключей оператора должна соответствовать аппаратному ключу, который хранится на интегральной схеме терминала. Это исключает несанкционированное подключение терминалов «чужого» оператора. За генерацию ключей и их распространение отвечает компания-производитель спутникового оборудования. Терминалы изготавливают таким образом, чтобы они были защищены от извлечения ключей шифрования, воздействия любых внешних сигналов, а также от вскрытия оборудования для анализа.

На серверах ЦУС для межсерверного сетевого взаимодействия операторы часто используют модифицированные транспортные протоколы в целях обеспечения полного контроля за серверными сетевыми интерфейсами, а также для защиты от несанкционированного доступа к ним. Каждый сервер имеет дублирующий, отдельно стоящий идентичный сервер, который берет на себя всю работу в случае выхода из строя основного устройства. Кроме того, сетевое взаимодействие оборудования логически разделено на виртуальные сети по технологии VLAN (IEEE 802.1Q)[8], чтобы данные для управления и контроля были изолированы от пользовательских. В результате возможные атаки на сеть оператора со стороны пользователей или из Интернета становятся невозможными, а распространение вирусов в сети блокируется.

Спутниковые абонентские терминалы имеют необходимый набор средств для обеспечения, как собственной безопасности, так и для защиты подключенных к ним сетей. Главным инструментом является сетевой фильтр - его функционала достаточно, чтобы исключить большинство атак по портам и протоколам на сети клиентов через спутниковые каналы связи. Расширенные возможности по регистрации различных ошибок, попыток несанкционированного доступа и взлома предоставляет сервис генерации событий.

[7] Turbo Coding - метод помехозащищенного кодирования.

[8] VLAN (IEEE 802.1Q) - (Virtual Local Area Network) - виртуальная локальная компьютерная сеть стандарта IEEE 802.1Q.

Информация о событиях автоматически передается на центральный пульт управления ЦУС оператора. Для более детального анализа работы терминала также анализируются записи в журнале событий.

Информационная безопасность в спутниковой сети технологии VSAT повышается также за счет сложности используемых методов организации функционирования обратных каналов, а также применения фирменных алгоритмов по работе с ними. Например, если терминал по какой-то причине не сможет получить управляющую информацию от серверов по зашифрованному прямому каналу, то ему не удастся передать свои данные в обратном канале. И наоборот, если он некорректно работает по обратному каналу, то не сможет правильно принимать данные по прямому каналу.

При применении специальной шифрующей аппаратуры спутниковые каналы используются также и для передачи закрытой информации, имеющей самые высокие уровни грифа. Такие устройства подключаются через стандартные по́рты (синхронным и асинхронным интерфейсам) между компьютером или другим средством обработки информации и терминалом VSAT и обеспечивают криптографическую защиту информации [2, с. 43].

Таким образом, при осуществлении всего комплекса мер защиты реализуется телекоммуникационное решение, отвечающее требованиям обеспечения безопасности передаваемой информации по спутниковой сети технологии VSAT. По мере развития технология спутниковой связи также совершенствуются и методы защиты информации.

Крупнейшими провайдерами спутниковой связи технологии VSAT на российском рынке являются компании: «АльтегроСкай», «Вэб Медиа Сервисез», «Ай Пи Нэт», «Амтел-связь» и др., в числе пользователей которых присутствуют МВД России, ФСИН России, ФМС России, ФТС России, МЧС России и другие государственные и правоохранительные органы [9].

ЛИТЕРАТУРА

1. Высоцкий Г. Услуги сетей VSAT и их потребители // Теле-Спутник, № 3, 2011. - С. 20-28.
2. Гладченков А. Спутниковые технологии VSAT и информационная безопасность сети // Журнал сетевых решений / LAN, № 9, 2007. - С. 40-44.
3. Колюбакин В. Что такое VSAT // Теле-Спутник, № 7, 2015. - С. 6-8.
4. Лебедев В.Н. Система технической защиты персональных данных в органах внутренних дел Российской Федерации: основные положения и элементы. // Труды Академии управления МВД России, № 1 (29), 2014. - С. 38-41.
5. Лебедев В.Н. Мероприятия по обеспечению безопасности персональных данных как элемент системы технической защиты персональных данных в органах внутренних дел. // Труды Академии управления МВД России, № 3 (35), 2015. - С. 63-67.
6. Мальцев Г.Н. Сетевые информационные технологии в современных спутниковых системах связи // Информационно-управляющие системы, № 1, 2007. - С. 33-39.
7. Степанов О.А. О перспективах использования информационных технологий в рамках государственного строительства в российском обществе // Труды Академии управления МВД России, № 2 (34), 2015. - С. 39-41.
8. http://satinet.info/zashhita-sputnikovogo-kanala-svyazi/ (дата обращения: 15.03.2017).
9. http://www.kp.ru/guide/sputnikovye-operatory.html (дата обращения: 15.03.2017).
10. https://www.roilcom.ru/VSAT (дата обращения: 16.03.2017).

Gurlev Igor Valentinovich
Academy of the interior Ministry of Russia, Russia, Moscow
E-mail: gurleff@mail.ru

Methods and techniques for the security of information transmitted over the satellite network VSAT technology

Abstract. information security is one of the key factors when choosing communication systems, government agencies, financial institutions, large companies and other organizations, as well as law enforcement agencies, the success of which largely depends on the security of the transmitted information.

Currently actively developing satellite communication systems, which compared to terrestrial cable and radio relay networks direct line of sight have a number of significant advantages: have a much wider coverage and, therefore, in remote and sparsely populated regions of Russia are the most optimal technical and economic solution.

The article discusses the benefits of satellite communications systems in the sparsely populated far North and Far East with an antenna having a small aperture, compared to wired networks as well as physical, software and hardware methods and means of protection of information transmitted via communication channels of satellites in the geostationary orbit.

When implementing the physical protection of information provided by physical security, engineering protection: installed fencing around the facility, alarm system, video surveillance, etc.

Software and hardware methods and means of information protection require the use of special protocols, encoding and encryption of information.

Keywords: satellite network; geostationary orbit; communications; information security; methods; ways of protection; physical protection; engineering protection; hardware and software method; protocols; encoding; encryption