DOI 10.37882/2223–2966.2022.03.29

СОВРЕМЕННЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ МОНИТОРИНГЕ НАЗЕМНОГО КОМПЛЕКСА УПРАВЛЕНИЯ СПУТНИКОВОЙ СЕТИ

Савельев Роман Николаевич
Аспирант, Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, г. Красноярск
savelyevroman@mail.ru

Аннотация. Рассмотрены основные преимущества использования спутниковых сетей связи, а также основные проблемы обеспечения информационной безопасности. Установлено, что в последнее десятилетие спутники играют все более важную роль в современных технологиях, от предоставления возможностей геолокации и обеспечения логистики и навигации до сбора разведывательной информации, проводимого национальными государствами. Установлено, что спутниковая индустрия пережила возрождение за последние несколько лет и теперь занимает лидирующую позицию, чтобы играть ключевую роль в удовлетворении постоянно растущих рыночных требований, таких как транспортная сеть 5G, Интернет вещей (IoT) и исследования космоса. Тем не менее, расширение использования спутников сделало спутниковые сети связи мишенью для хакеров, стремящихся скомпрометировать конфиденциальную информацию с потенциально разрушительными последствиями, в том числе и для наземного комплекса управления. Когда дело доходит до защиты данных, переносимых спутниками, безопасность не может быть второстепенной. Обеспечение информационной безопасности при мониторинге наземного комплекса управления спутниковой сети должно играть неотъемлемую часть в проектировании любой спутниковой сети. Цель работы: представление современных технических средств информационной безопасности при мониторинге наземного комплекса управления спутниковой сети. При написании работы были использованы методы анализа, сравнения, обобщения. В результате выполнения работы сформированы рекомендации по обеспечению информационной безопасности для наземных комплексов управления спутниковой сети. Представлен пример системы мониторинга, которую можно использовать в наземном комплексе управления с целью обеспечения информационной безопасности. Представленные результаты могут быть использованы наземными комплексами управления спутниковой сети для повышения информационной безопасности. По результатам написания статьи установлено, что использование современных технических средств при мониторинге наземного комплекса управления спутниковой сети является обязательным для обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, спутниковая сеть, наземный комплекс, мониторинг, криптографическая защита.

MODERN TECHNICAL MEANS OF INFORMATION SECURITY FOR MONITORING OF THE GROUND CONTROL COMPLEX OF THE SATELLITE NETWORK

R. Saveliev

The main advantages of using satellite communication networks, as well as the main problems of ensuring information security, are considered. Over the past decade, satellites have been found to play an increasingly important role in modern technology, from providing geolocation and logistics and navigation capabilities to intelligence gathering by nation states. The satellite industry has been found to have experienced a renaissance over the past few years and is now in a leading position to play a key role in meeting ever-increasing market demands such as 5G transport network, Internet of Things (IoT) and space exploration. However, the increased use of satellites has made satellite communications networks a target for hackers seeking to compromise confidential information with potentially devastating consequences, including for the ground control complex. When it comes to protecting data carried by satellites, security cannot be secondary. Ensuring information security while monitoring the ground control complex of a satellite network should play an integral part in the design of any satellite network. Purpose of the work: presentation of modern technical means of information security during monitoring of the ground control complex of the satellite network. When writing the work, the methods of analysis, comparison, generalization were used. As a result of the work, recommendations were formed on ensuring information security for ground control systems of the satellite network. Example of monitoring systems that can be used in a ground control complex to ensure information security are presented. The presented results can be used by ground control systems of a satellite network to improve information security. Based on the results of writing the article, it was found that the use of modern technical means when monitoring the ground control complex of the satellite network is mandatory to ensure information security.

Keywords: information security, satellite network, ground complex, monitoring, cryptographic protection.

Введение

Спутниковая связь занимает особое место в системе связи. Основным преимуществом является высокая оперативность установления соединения на большие расстояния (в пределах всего земного шара при условии использования систем с глобальным покрытием). В последние годы, с постоянным углублением и инновациями в области сетевой информатизации, ситуация с сетевой безопасностью, в том числе и для спутниковых сетей связи, становится все более серьезной, а продвинутые постоянные атаки стали серьезной угрозой для киберпространства. Процесс атаки тщательно планируется, а методы атаки сложны и запутаны, что часто приводит к серьезной утечке данных или повреждению системы.

Злоумышленники продолжают изменять существующие методы атаки и разрабатывать новые инструменты атаки. Обнаружение в реальном времени не может быть достигнуто с помощью сигнатур вредоносных программ. Полагаясь только на брандмауэры, системы предотвращения вторжений и антивирусное программное обеспечение, нельзя предотвратить эти атаки.

После многих лет развития традиционные спутники связи накопили определенную основу технологии сетевой безопасности, включая технологию защиты от помех на физическом и канальном уровнях, шифрование источника и канала, а также технологию дешифрования.

Однако среда безопасности спутниковых сетей сталкивается с проблемами, которые в основном отражаются в [1]:

- структура сети спутниковой связи изменилась с простой на сложную, сильно интегрированную с IP-технологиями;
- масштаб сетей спутниковой связи изменился с малых до сверхбольших;
- услуги сети спутниковой связи больше не ограничены полосой пропускания и становятся более распространенными;
- оборудование связи переживает новый виток технологических обновлений;
- сети спутниковой связи сталкиваются с более глубокими, широкими и расширенными типами информации и протоколами передачи.

Таким образом, наряду с преимуществами, наземный сегмент спутниковых систем связи создает большие проблемы в области кибербезопасности, которые делают их еще более привлекательными для злоумышленников. Следовательно, актуальным вопросом является исследование технических средств, с помощью которых можно обеспечить информационную безопасность при мониторинге наземного комплекса управления спутниковой связи.

Постановка задачи

Учитывая, что спутниковая связь в настоящее время начинает широко использоваться во многих сферах жизнедеятельности, необходимо исследовать вопрос информационной безопасности подобного рода сетей связи, в том числе необходимо рассмотреть технические средства, которые могут быть использованы для мониторинга наземного комплекса управления. Для поставленной цели необходимо рассмотреть структуру спутниковой сети связи, на основании чего привести список возможных проблем информационной безопасности и представить пример структурной схемы организации подсистемы криптографической защиты информации с применением технических средств обеспечения информационной безопасности наземного комплекса управления.

Основная часть

Применение спутниковой связи [2–9] показало ряд преимуществ по сравнению с другими типами связи, а именно:

- высокая устойчивость и качество связи;
- высокая мобильность, возможность оперативного развертывания земных станций спутниковой связи непосредственно в районах дислокации;
- минимальные затраты (техники и личного состава) при организации спутниковых радиолиний;
- возможность размещения земных станций спутниковой связи на различных типах местности (в ущельях, оврагах), укрытия их за неровностями рельефа земной поверхности (холмами, горами) и искусственными препятствиями (строениями, сооружениями), что обеспечивает повышение защищенности пунктов управления, снижение эффективности действия средств создания радиоэлектронных помех и дополнительной защиты.

Как показал опыт локальных конфликтов последнего времени, во многих случаях средства спутниковой связи оставались единственными средствами связи.

Структура спутниковой сети связи (рис. 1) содержит космический сегмент, пользовательский сегмент и наземный сегмент.

В пользовательский сегмент входят различные спутниковые терминалы; космический сегмент включает группировку спутников, которые можно разделить на созвездие с межспутниковой связью (ISL) и созвез-

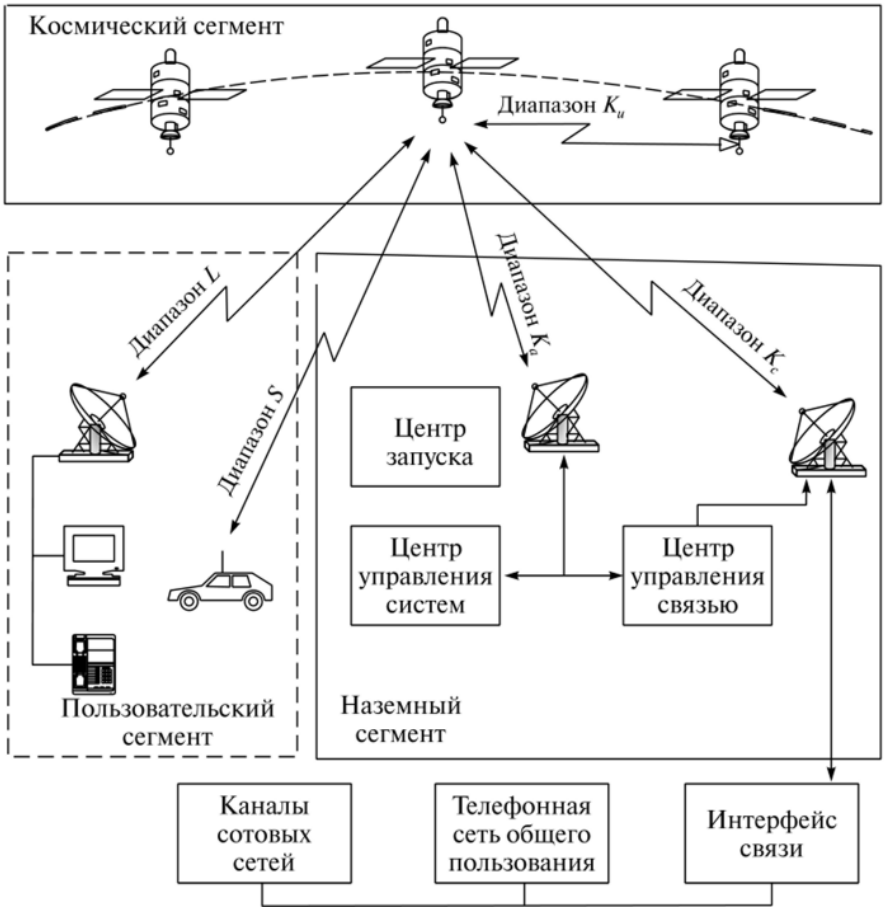

Рис. 1. Структура спутниковой сети связи

дие без ISL; наземный сегмент включает в себя станцию сопряжения (GS), систему управления и контроля эксплуатации (OMCS), систему измерения и контроля (MCS), систему управления сетью (NMS) и т.д.

Поскольку в основе спутниковых операций лежат технологии, размещенные на Земле, наземные точки «входа» предлагают киберпреступникам огромное количество потенциальных возможностей для взлома. Огромное количество точек «входа» также усложняет отслеживание и прекращение кибератаки.

Одним из наиболее значительных недостатков, общих для всех спутниковых систем, является использование телеметрии дальнего действия для связи с наземными станциями. Восходящие и нисходящие каналы часто передаются через открытые протоколы безопасности телекоммуникационной сети, к которым легко могут получить доступ киберпреступники [10,11].

Спутниковые наземные станции особенно уязвимы — если злоумышленник сможет прервать спутниковый сигнал, он сможет получить доступ к любым нисходящим системам, подключенным к спутнику. Таким образом, злоумышленник потенциально может проникнуть в сеть [12].

Возможные проблемы информационной безопасности для спутниковых сетей связи, в том числе и для наземного сегмента, представлены в виде табл. 1 [13,14].

Таким образом, для спутниковых систем связи в настоящее время присуще множество проблем информационной безопасности. Следовательно, отсутствие технических средств информационной безопасности при мониторинге наземного комплекса управления спутниковой связи может привести к разрушительным последствиям.

Таким образом, важно рассмотреть подобного рода технические средства.

В качестве примера технического средства рассмотрим VPN/ брандмауэр GoSilent. Данное средство

Таблица 1. Возможные проблемы информационной безопасности для спутниковых сетей связи

Классификация	Проблема безопасности	Описание
Национальная безопасность	Угрозы национальной и военной безопасности	1. Хакеры могут украсть стратегическую информацию о странах, разместив вредоносные средства для наблюдения на спутниках LEO. 2. Спутник LEO может быть использован как коммуникационная платформа для будущего оружия информационной войны.
	Вмешательство в астрономические исследования	1. Запуск большого количества спутников на низкой околоземной орбите может серьезно помешать астрономическим наблюдениям.
Сетевая безопасность	Выдача себя за другое лицо	1. Хакеры могут быть замаскированы под спутниковый терминал (СТ) для доступа к спутниковой сети с целью разрушения сети 2. Хакер может маскироваться под спутник, чтобы обманом заставить получить доступ к ложной сети.
	Перехват данных	1. Хакеры незаконно получают и анализируют передаваемые данные трафика или данные по беспроводным каналам связи.
	Проблемы с целостностью данных	1. Хакеры могут изменять, вставлять, воспроизводить, удалять пользовательские или данные для нарушения их целостности
	Перехват информации	1. Незаконный перехват информации о местоположении или идентификации пользователя, передаваемой СТ по беспроводным каналам связи
	Создание помех	1. Злоумышленники создают помехи для спутниковой беспроводной связи, испуская мощные электромагнитные волны.
	Отказ в обслуживании	1. Злоумышленники могут создавать помехи для спутника или шлюза
	Анонимная атака	1. Злоумышленники атакуют спутниковый узел в космосе, но спутник не может определить атакующих
	Злонамеренное занятие ресурсов полосы пропускания спутника	1. Отправка незаконных сигналов на спутник через беспроводную связь.
Безопасность оборудования	Вредоносный спутниковый контроль	1. Злоумышленники могут отправлять злонамеренные инструкции или вводя вирусы в спутниковые узлы с наземных или космических объектов для достижения цели контроля над спутниками.
	Вредоносное потребление спутниковых ресурсов	1. Злонамеренное потребление ресурсов спутника для достижения цели сокращения срока службы спутника

предлагает надежные алгоритмы защиты шифрования от киберугроз, в том числе тех, которые наиболее часто нацелены на наземные комплексы связи:

- троян удаленного доступа (RAT) — вредоносный код, который незаметно загружается в виде вложения или программы по запросу пользователя. После установки приложения злоумышленник получает возможность управлять наземным комплексом;
- IP Exfiltration — несанкционированная передача данных с помощью вредоносного кода;
- атака «человек посередине» — злоумышленники получают доступ к сети с помощью грубой силы или внедрения пакетов и незаметно перехватывают, и подслушивают сообщения;
- атака соединения SCADA — злоумышленники используют комплект средств связи, чтобы получить доступ к наземному комплексу управления SCADA предприятия (диспетчерский контроль и сбор данных).

Техническое средство GoSilent соответствует критериям готового решения для спутниковых систем, а также удовлетворяет требованиям безопасности на государственном уровне, например:

- имеет возможность создания виртуального сервера и межсетевой экран приложений уровня 7 с отслеживанием состояния шлюза VPN;
- защита ПК — фильтрует весь трафик данных. Защита от кибератак, кражи личных данных и вредоносных программ;
- изоляция Captive Portal — изолирует устройства конечных пользователей от попыток перехвата и изменения соединения между пользователем и сторонним сайтом (системой), которую они пытаются посетить.
- IP Obfuscation — рандомизирует IP-адреса для всего входящего и исходящего трафика данных.

Также предлагается создать подсистему криптографической защиты. Данную подсистему предлагается реализовать с использованием программно-аппаратных средств комплекса межсетевого экранирования.

Подсистема криптографической защиты должна реализовать следующие функции:

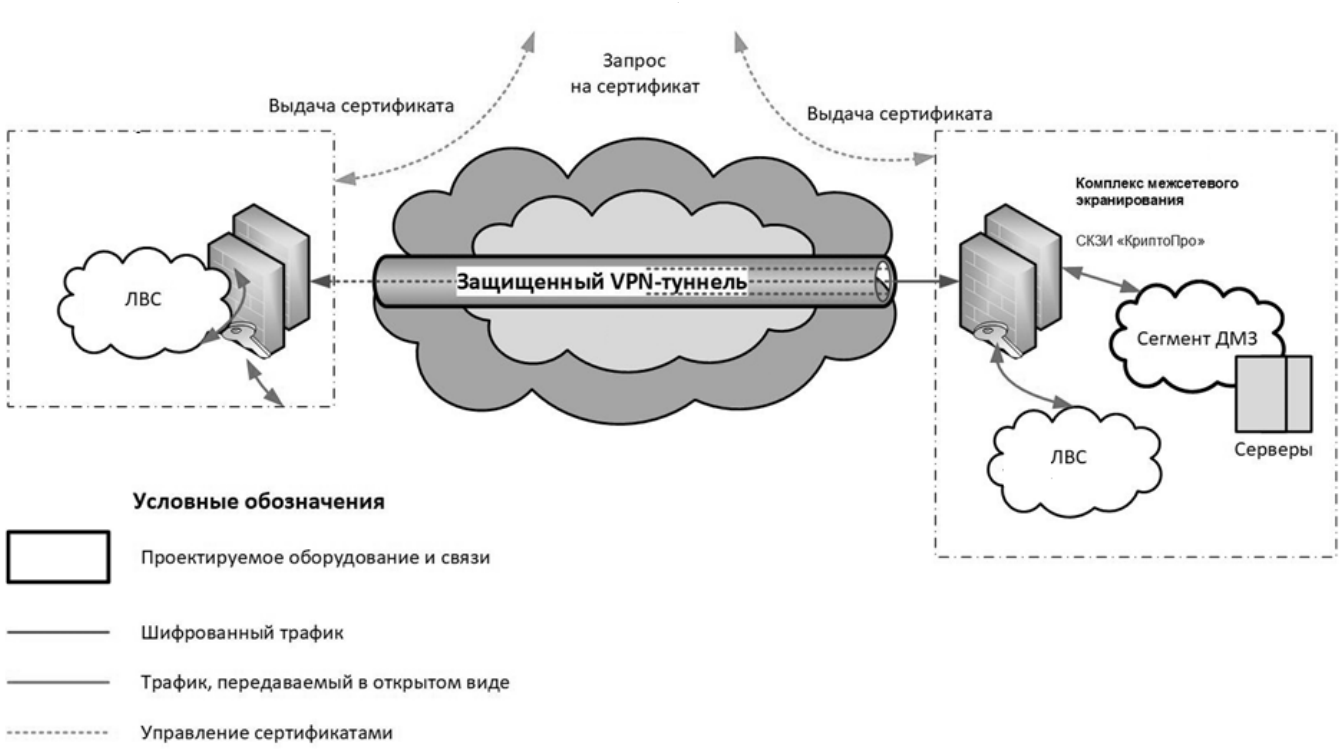

Рис. 2. Общая схема организации подсистемы криптографической защиты для наземного комплекса управления спутниковой сети

- поддержка постоянно действующих туннелей VPN;
- шифрование предаваемой информации;
- аутентификация.

Функции подсистемы криптографической защиты можно реализовать с использованием встроенных средств, например, IPsec VPN МЭ Cisco ASA, функционирующих совместно с установленным СКЗИ. Встроенные средства IPsec VPN МЭ обеспечивают организацию защищенных туннелей виртуальной частной сети (VPN). СКЗИ «КриптоПро» CSP 5.0 обеспечивает применение отечественных криптографических [15].

Общая схема функционирования подсистемы криптографической защиты с использованием предлагаемых средств представлена на рис. 2.

Ниже приведены несколько рекомендаций по кибербезопасности как для частных, так и для государственных предприятий, использующих спутниковые системы связи:

- Сделать кибербезопасность главным приоритетом и уделять ей должное внимание;
- Реализовать надежное шифрование для каждой части данных, передаваемых через наземный комплекс (обычно это достигается с помощью организации VPN, как в представленном примере)
- Использовать методы аутентификации;
- Использовать безопасное туннелирование

Однако стоит отметить, что даже при соблюдении вышеуказанных мер предосторожности все еще существует значительный риск, связанный с использованием устройств в наземном комплексе.

Заключение

Быстрое развитие спутниковых систем связи принесло с собой некоторые риски для информационной безопасности. С одной стороны, необходимо активно развивать индустрию спутниковых сетей, в полной мере используя уникальные преимущества спутников, на которую не влияют географические препятствия и катастрофы; с другой стороны, ввиду различных уровней угроз безопасности, с которыми сталкивается спутниковая сеть, необходимо проводить перспективные исследования безопасности спутниковой сети, чтобы заполнить нормативные пробелы. В работе рассмотрена эффективная система мониторинга, используя которую пользователи наземного комплекса управления могут существенно повысить уровень информационной безопасности всей спутниковой сети.

ЛИТЕРАТУРА

1. Cybersecurity Threats to Satellite Communications [Электронный ресурс]. URL: https://medium.datadriveninvestor.com/cybersecurity-threats-to-satellite-communications-b35d83681723 (дата обращения: 10.11.2021).
2. Кукк К.И. Спутниковая связь: прошлое, настоящее, будущее. М.: Горячая линия.— Телеком, 2015.157 с.
3. Крылов А.М. Спутниковые системы связи и вещания. Состояние и перспективы развития.— М.: Горячая линия.— Телеком, 2014. 182 с.
4. Михайлов Р.Л. Описательные модели систем спутниковой связи как космического эшелона телекоммуникационных систем специального назначения. Монография.— СПб.: Наукоемкие технологии, 2019. 150 с.
5. Системы спутниковой связи и вещания: справочно-аналитичекое издание / Под ред. Ю.А. Подъездкова. М.: Радиотехника, 2018.— 360 с.
6. Макаренко С.И. Описательная модель системы спутниковой связи Inmarsat. Системы управления, связи и безопасности. 2018. № 4. С. 64–91.
7. Цветков К.Ю., Осташов И.Т., Косяков Е.Н. Радиорелейные и спутниковые системы передачи информации специального назначения.— СПб.: ВКА им. А.Ф. Можайского, 2013. 447 с.
8. Быховский М.А. Развитие телекоммуникаций. На пути к информационному обществу. Развитие спутниковых телекоммуникационных систем.— М.: Горячая линия.— Телеком, 2014. 256 с.
9. 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.
10. Сомов, А.М. Спутниковые системы связи: Учебное пособие для вузов.— М.: РиС, 2015.— 244 с.
11. Cyber Concerns For The Satellite Sector [Электронный ресурс]. URL: https://www.attilasec.com/blog/satellite-cybersecurity (дата обращения: 10.11.2021).
12. Защита информации в спутниковой связи [Электронный ресурс]. URL: https://igorosa.com/zashhita-informacii-v-sputnikovoj-svyazi/ (дата обращения: 02.12.2021).
13. Cao H., Wu L., Chen Y., Su Y., Lei Z., Zhao C. Analysis on the Security of Satellite Internet. In: Lu W. et al. (eds) Cyber Security. CNCER. Communications in Computer and Information Science, 2020. Vol.1299. 36 p.
14. De Azúa, J.A.R., Calveras, A., Camps, A.: Internet of Satellites. IoSat, Analysis of Network Models and Routing Protocol Requirements, 2018, 56 p.
15. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем. М.: Инфра-М, 2018. 64 с.

Журнал «Современная наука: актуальные проблемы теории и практики»