

STARLINK: ВЫЗОВЫ КИБЕРБЕЗОПАСНОСТИ И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ СПУТНИКОВОМУ ИНТЕРНЕТУ

Карцан И. Н.¹, Аверьянов В. С.², Красников М. Д.³

DOI: 10.21681/2311-3456-2025-1-18-27

Цель исследования: исследование уязвимостей низкоорбитальной спутниковой группировки, а также методы противодействия и нейтрализации угроз, связанных с предоставлением несанкционированного доступа пользователям к сети Internet.

Метод исследования: аналитический обзор релевантной научной информации, метод оценки информационной защищённости.

Результат исследования: представлен аналитический обзор для проведения оценки помехозащищённости спутниковой группировки Starlink с применением технических параметров Signal-to-Noise Ratio. Выявлены общие уязвимости для серий космических аппаратов Starlink 1.0, Starlink 1.5, Starlink 2.0 и Starlink 2.0 mini. Показано технологическое устройство системы спутникового интернета Starlink, разработанной компанией SpaceX, включая информацию о защите от помех, взлома и кибератак. Рассмотрены методы создания помех с использованием фазового сдвига сигнала, адаптивных радиочастотных помех, когерентных и виртуальных помех, электромагнитных импульсов, рефлекторов и дефлекторов, резонансное рассеивание, а также использование бионических устройств и микродронов. На все рассматриваемые методы представлены как недостатки, так и преимущества. Выявлены методы создания помех с наиболее перспективным подходом.

Практическая полезность заключается в том, что на основе анализа методов создания помех предлагаются технические решения по эксплуатации уязвимостей сетевого оборудования и программного обеспечения.

Ключевые слова: фазовый сдвиг сигнала, адаптивные радиочастотные помехи, когерентные помехи, виртуальные помехи, электромагнитные импульсы, рефлектора, дефлектора, резонансное рассеивание, бионическое устройство, микродрон.

Введение

Система спутниковой связи Starlink, от компании SpaceX, представляет собой технологическое решение по обеспечению глобального интернет-покрытия. В отличие от традиционных спутниковых систем, основа Starlink – низкоорбитальные космические аппараты (КА), что позволяет кратное уменьшить временные задержки информативного сигнала и увеличить скорость передачи данных. По мнению разработчика, технология обещает революционизировать доступ к интернету, обеспечив покрытие в удаленных регионах и труднодоступной местности.

Однако, наряду с преимуществами, Starlink вызывает серьезные опасения у ряда стран в области обеспечения национальной безопасности. Массированное развертывание КА на низкой околоземной орбите создает новые предпосылки по утечке конфиденциальной информации, похищенной хакерскими группировками у органов государственной власти, организаций сферы информационных технологий,

транспорта, финансов, связи, торговли, здравоохранения, страхования и электронной коммерции [1, 2]. Актуальность исследования обусловлена малой степенью разработанности и исчерпывающих методов противодействия. Авторы ставят перед собой цель восполнить научный пробел, предоставив анализ критических уязвимостей сети связи Starlink, возможных методов перехвата и подмены данных, а также стратегий и тактик противодействия спутниковому интернету.

Рассмотрим текущую ситуацию перехода к фазе 2 на базе космических аппаратов класса Generation 2:

1. переход к спутникам второго поколения (Gen 2) характеризуются улучшенной пропускной способностью и совершенными технологиями связи. КА предназначены для значительного повышения производительности сети Starlink;
2. улучшенные возможности. Спутники Gen 2 обладают повышенной пропускной способностью

1 Карцан Игорь Николаевич, доктор технических наук, доцент, главный научный сотрудник ФГБНУ «Аналитический центр», Москва, Россия. E-mail: kartsan2003@mail.ru, ORCID 0000-0003-1833-4036.

2 Аверьянов Виталий Сергеевич, начальник отдела Информационной безопасности Красноярского краевого клинического онкологического диспансера имени А. И. Крыжановского, Красноярск, Россия. E-mail: averyanov124@mail.ru, ORCID: 0000-0001-6069-2537.

3 Красников Максим Дмитриевич, студент кафедры «БИТ» ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева», Красноярск, Россия. E-mail: maks.krasnikov.76@bk.ru

и улучшенными характеристиками для обеспечения связи, включая технологию Direct to Cell по предоставлению широкополосного доступа в сеть интернет, и услуги мобильной связи для удаленной и труднодоступной местности;

3. масштабируемость сети. Вторая фаза включает в себя увеличение числа низкоорбитальных КА, позволяя обеспечить покрытие при увеличенной пропускной способности каналов связи. В перспективе при растущем спросе на услуги связи общее количество спутников Starlink на орбите кратно возрастет;
4. запуски и достижения. SpaceX осуществляет регулярные пуски, включая миссии с большим числом спутников на борту. Несмотря на отдельные неудачи, такие как инцидент 11 июля 2024 года, общая тенденция указывает на успешное наращивание орбитальной группировки.

Преимущества и цели фазы 2 и Generation 2:

- расширение глобального покрытия за счет увеличения числа спутников второго поколения,

позволяющих обеспечить стабильное и высокоскоростное интернет-подключение в удаленных и малообеспеченных регионах, где традиционная инфраструктура недостаточна;

- увеличение пропускной способности за счет новых спутников, разработанных с учетом возросшего спроса на данные и подключение, что позволит увеличить общее количество пользователей, которым предоставлена услуга;
- улучшение качества связи при технологических улучшениях во второй фазе, что поможет уменьшить задержки и повысить надежность предоставляемых услуг.

В последние месяцы проект Starlink продолжает активно развиваться. SpaceX уже запустила множество спутников на низкую околоземную орбиту, и значительная часть этих спутников оснащена технологией Direct to Cell, позволяющей использовать их как вышки сотовой связи, обеспечивая покрытие в зонах без традиционной инфраструктуры.

Таблица 1.

Общие характеристики КА Starlink 1.0, 1.5, 2.0, 2.0 mini

Характеристика	Starlink 1.0	Starlink 1.5	Starlink 2.0	Starlink 2.0 mini
Масса	~260 кг	~300 кг	~1250 кг	~800 кг
Размер	2.8 м x 1.1 м	2.8 м x 1.1 м	7 м x 2.8 м	4.1 м x 2.7 м
Орбита	550 км	550 км	340-614 км	340-614 км
Пропускная способность	10-20 Гбит/с	20-30 Гбит/с	100-200 Гбит/с	50-100 Гбит/с
Частотный диапазон	Ku, Ka	Ku, Ka	Ku, Ka, E	Ku, Ka
Продолжительность жизни	5-7 лет	5-7 лет	7-10 лет	7-10 лет
Солнечные панели	2 панели (~60 м ²)	2 панели (~60 м ²)	4 панели (~100 м ²)	3 панели (~80 м ²)
Навигация и ориентация	Реактивные колёса, ионный двигатель			
Связь	Фазированные антенные решётки	Фазированные антенные решётки	Фазированные антенные решётки	Фазированные антенные решётки
Антенны	1 большая антенна	1 большая антенна	4 антенны	3 антенны
Энергетический потенциал	Средний	Средний	Высокий	Средний
Криптозащита	AES-256	AES-256	AES-256	AES-256
EIRP	23 dBW (200 Вт)	30 dBW (1000 Вт)	40 dBW (10,000 Вт)	35 dBW (3,162 Вт)
Коэффициент усиления антенны (G)	316.23	1000	10000	3162
Расстояние (R)	500000 м			
Температура шума (T)	300 К			

1. Анализ характеристик системы спутниковой связи Starlink

Космические аппараты Starlink представляют собой спутники на низкой околоземной орбите (LEO), разработанные компанией SpaceX для предоставления глобальных услуг широкополосного интернета. В таблице 1 приведены тактико-технические характеристики (ТТХ) спутников Starlink включая необходимую информацию о защите от помех, взлома и кибератак.

Для оценки помехозащищенности КА Starlink применим параметр Signal-to-Noise Ratio (SNR), который показывает отношение мощности полезного сигнала к мощности шума (помех) [3]. Высокое значение SNR указывает на высокую устойчивость к помехам. Формула для расчета SNR:

$$SNR = \frac{P_r}{N}, \quad (1)$$

где P_r – мощность полезного сигнала на приемной антенне, N – мощность шума (помех).

Для проведения анализа используем обозначения:

- EIRP (Effective Isotropic Radiated Power). Мощность, излучаемая спутником, определяется как продукт передаваемой мощности и коэффициента усиления антенны;
- C/N (Carrier-to-Noise ratio). Отношение мощности несущего сигнала к мощности шума;
- G/T (Gain-to-Noise Temperature). Коэффициент, определяющий эффективность антенны приемника относительно температуры шума.

Проведем оценку помехозащищенности для разных версий спутников Starlink после расчетов мощности на приёмнике (P_r):

$$P_r = \frac{EIRP \cdot G}{4\pi R^2}. \quad (2)$$

Расчет мощности шума (N):

$$N = kTB, \quad (3)$$

где (k) – постоянная Больцмана (1.38×10^{-23} Дж/К).

Отношение несущей к шуму (C/N):

$$\frac{C}{N_{dB}} = 10 \cdot \log_{10}\left(\frac{P_r}{N}\right). \quad (4)$$

Коэффициент усиления к температуре шума (G/T):

$$\frac{G}{T_{dB}} = 10 \cdot \log_{10}\left(\frac{G}{T}\right). \quad (5)$$

По полученным результатам проведен следующий анализ:

Starlink 1.0 имеет базовый уровень защиты от высокочастотных помех, делая её уязвимой в условиях высоких плотностей сигнала. Подавление сигнала возможно при наличии помех в том же частотном диапазоне, как в Ku- и Ka- диапазонах. Основные ограничения связаны со слабой антенной и меньшей

эквивалентной изотропно излучаемой мощностью (EIRP), что снижает способность поддерживать сильный сигнал при наличии помех;

Starlink 1.5 – улучшенные антенны и управление частотами снижают вероятность помех, однако сигнал всё ещё будет заглушен сильными источниками помех в близлежащих частотах. Увеличенная мощность и улучшенные антенны позволяют значительно улучшить качество связи и устойчивость к помехам;

Starlink 2.0 – существенно улучшена помехозащищенность. Широкий частотный диапазон и мощные антенны позволяют более эффективно управлять спектром и избегать помех. Заглушить сигнал значительно сложнее, требуется более мощный источник помех;

Starlink 2.0 mini – сигнал защищен достаточно хорошо, но из-за меньшей мощности (в сравнении с полной версией 2.0) будет снижение эффективности примерно на 10–15 % в условиях очень сильных помех. Версия mini предназначена для использования в условиях, где размер и вес имеют значение, сохраняя при этом значительную часть функциональности полной версии.

Общие уязвимости.

1. Физическая уязвимость. Возможность кинетических атак или воздействия космического мусора.
2. Зависимость от наземных станций. Атаки на наземные станции управления приводят к потере телеметрической информации.
3. Электромагнитные помехи. Энергетические вспышки на Солнце и других источниках временно ухудшают качество услуг связи.

Эволюция спутников Starlink от версии 1.0 до 2.0 mini показывает значительное улучшение в производительности и устойчивости к помехам. Улучшенные антенны, повышенная EIRP и расширенные частотные диапазоны позволяют справляться с более сложными условиями предоставления услуг связи минимизируя влияние внешних помех. Однако остаются уязвимости, связанные с физическими атаками и электромагнитными помехами, которые необходимо учитывать при разработке и эксплуатации спутниковых систем.

Система спутникового интернета Starlink от компании SpaceX приобрела значительную популярность благодаря своей способности обеспечивать высокоскоростной доступ в интернет в отдаленных и труднодоступных регионах. Однако, наряду с очевидными преимуществами, рост популярности Starlink вызывает обеспокоенность у различных государственных и коммерческих структур по всему миру. В условиях современных геополитических и экономических реалий вопрос контроля над информационными потоками становится особенно актуальным. В связи с этим

возникают предложения по разработке и внедрению методов борьбы с незаконной эксплуатацией системы связи Starlink. Ограничительные меры направлены как на частичное, так и на полное блокирование доступа к её услугам.

Основные методы противодействия включают:

1. методы подавления сигнала [4]. Использование специализированного оборудования для создания помех и блокировки сигнала спутников, что делает невозможным подключение абонентских терминалов к сети;
2. кибератаки [4, 5]. Проведение кибератак на инфраструктуру Starlink с целью выведения из строя отдельных элементов сети и нарушения её функционирования;
3. юридические меры [4, 6]. Принятие законов и нормативных актов, ограничивающих или запрещающих использование спутникового интернета в определенных регионах или для определенных категорий пользователей;
4. физическое уничтожение [7]. Использование противоспутникового оружия для уничтожения КА на орбите.

2. Методы противодействия, их преимущества и недостатки

Рассмотрим несколько инновационных, теоретических методов, которые могли бы быть использованы для создания помех, но при этом они требуют высокой технической сложности и значительных ресурсов [8, 9].

2.1. Фазовый сдвиг

Фазовый сдвиг – это метод, используемый для создания помех в сигнале, поступающем от спутников, изменяя фазу волны, что приводит к искажению информации и ухудшению качества сигнала. Это один из эффективных методов для заглушения или блокировки спутникового интернета, включая системы Starlink. Принцип работы фазового сдвига основан на изменении фазы волны сигнала, что приводит к интерференции. Когда две волны с одинаковой частотой и амплитудой встречаются с разными фазами, они могут создавать зоны усиления и затухания сигнала. Этот принцип лежит в основе фазового сдвига для создания помех.

Для создания фазового сдвига необходимы генератор сигнала создающий сигнал той же частоты, что и целевой сигнал (сигнал спутника Starlink), фазовый модулятор, который изменяет фазу сигнала, созданного генератором, антенна для излучения фазово-сдвинутого сигнала в направлении целевого сигнала.

Основные формулы, связанные с фазовым сдвигом, включают фазовый угол и частотные параметры. Фазовый угол:

$$\Delta\phi = \phi_2 - \phi_1, \quad (6)$$

где $\Delta\phi$ – разница фаз, ϕ_2 и ϕ_1 – фазы двух встречающихся волн.

Фазовая скорость:

$$v_p = \frac{\omega}{k}, \quad (7)$$

где v_p – фазовая скорость, ω – угловая частота, k – волновое число.

Интерференция волн, если две волны с амплитудой A и фазами ϕ_2 и ϕ_1 встречаются, результирующая амплитуда A_r определяется как:

$$A_r = 2A \cos\left(\frac{\Delta\phi}{2}\right). \quad (8)$$

Преимущества метода фазового сдвига.

- ✓ Высокая эффективность. Фазовый сдвиг может существенно снизить качество сигнала и сделать интернет-соединение неработоспособным.
 - ✓ Точность. Возможность точного управления фазой позволяет нацеливаться на конкретные сигналы и частоты.
 - ✓ Гибкость, будет использован в различных условиях и сценариях.
- Недостатки.

- ✓ Сложность реализации. Требует точного оборудования и настроек.
- ✓ Высокие затраты. Необходимы значительные финансовые вложения в оборудование и технологии.

2.2. Адаптивные радиочастотные помехи

Адаптивные радиочастотные помехи (АРЧП) представляют собой один из методов противодействия спутниковым системам связи, таким как Starlink. Данный метод направлен на создание помех в радиочастотном диапазоне, в котором работают спутники связи, с целью нарушения их работы [10].

Основные принципы работы АРЧП.

1. Изучение целей. Для успешного подавления систем связи необходимо понимать их технические характеристики, такие как рабочие частоты, тип модуляции, протоколы передачи данных, и режимы работы.
2. Излучение помех. АРЧП подразумевает генерацию и излучение радиосигналов, которые могут создавать помехи в диапазоне частот, используемых целевой системой. Эти помехи могут быть как узкополосными (на определенной частоте), так и широкополосными (охватывающими широкий спектр частот).
3. Адаптивность. АРЧП включает в себя способность адаптироваться к изменениям в работе системы связи. Например, если система изменяет частоту передачи для обхода помех, то генератор помех также должен уметь оперативно изменять свои параметры.

4. Интеллектуальное управление. Современные системы АРЧП используют алгоритмы машинного обучения и искусственного интеллекта для анализа сигнала и динамического формирования помех. Это позволяет более эффективно противодействовать сложным и адаптивным системам связи.

Методы создания радиочастотных помех.

1. Шумовые помехи. Генерация белого шума или шума с определенными характеристиками для заполнения всего частотного диапазона, используемого системой связи.
2. Модулированные помехи. Генерация помех, модулированных аналогично сигналам целевой системы, чтобы затруднить их распознавание и фильтрацию.
3. Направленные помехи. Использование направленных антенн для создания помех в конкретном направлении, минимизируя при этом воздействие на другие системы.
4. Пульсирующие помехи. Создание помех с переменной мощностью и частотой для затруднения их фильтрации и адаптации системы связи к ним.

Для расчета эффективности адаптивных радиочастотных помех (АРЧП) против спутниковых систем связи, таких как Starlink, необходимо учитывать несколько ключевых параметров и использовать определенные формулы.

Основные параметры.

- ✓ Мощность передатчика помех (P_j). Мощность сигнала, генерируемого устройством помех.
- ✓ Мощность сигнала спутника (P_s). Мощность сигнала, передаваемого спутником.
- ✓ Расстояние до спутника (d_s). Расстояние от генератора помех до спутника.
- ✓ Эффективность антенны передатчика помех (G_j). Усиление антенны устройства помех.
- ✓ Эффективность антенны спутника (G_s). Усиление антенны спутника.
- ✓ Полоса частот сигнала (B_s). Ширина полосы частот передаваемого сигнала.
- ✓ Полоса частот помех (B_j). Ширина полосы частот генерируемых помех.
- ✓ Уровень шума на приемнике спутника (N_0). Удельная спектральная плотность мощности шума на приемнике спутника.

Основные формулы. Соотношение сигнал/шум (SNR) на входе приемника спутника:

$$SNR_s = \frac{P_s \cdot G_s}{Re B_s} \quad (9)$$

Соотношение помех/сигнал (J/S) на входе приемника спутника:

$$J/S = \frac{P_j \cdot G_j}{P_s \cdot G_s} \cdot \frac{B_s}{B_j} \quad (10)$$

Уровень помех на входе приемника спутника:

$$P_{i,s} = \frac{P_i \cdot G_i}{(4\pi d_s)^2} \quad (11)$$

Для успешного подавления сигнала необходимо, чтобы соотношение помех к сигналу (J/S) было больше, чем определенный порог, который зависит от чувствительности приемника спутника.

2.3. Электромагнитные импульсы

Электромагнитный импульс (ЭМИ) представляет мощный выброс электромагнитной энергии, который может вызвать временные или постоянные повреждения электронных систем, включая спутниковые системы связи, такие как Starlink. ЭМИ создается как естественным путем (например, солнечные вспышки), так и искусственно (например, ядерные взрывы или специальные генераторы ЭМИ).

ЭМИ основан на быстром высвобождении энергии, создающем сильное электромагнитное поле. Это поле индуцирует высокие напряжения и токи в проводниках, что может повредить или разрушить электронные компоненты [11].

Ядерный ЭМИ (NEMP) возникает при ядерных взрывах на больших высотах. Образующийся гамма-луч вызывает эмиссию вторичных электронов, что создает интенсивное электромагнитное поле.

Неядерный ЭМИ (NNEMP) будет создан при помощи специальных устройств, таких как генераторы микроволновых импульсов (НРМ) или взрывные магниты (FCG).

Основные параметры ЭМИ:

1. амплитуда поля (E). Интенсивность электромагнитного поля, измеряемая в Вольтах на метр (В/м);
2. длительность импульса (τ). Время существования импульса;
3. полоса частот (B). Спектральный диапазон импульса;
4. энергия импульса (W). Общая энергия, высвобождаемая в ходе импульса;
5. расстояние до цели (d). Расстояние от источника ЭМИ до поражаемой цели.

Для получения данных проводится расчет интенсивности поля на заданном расстоянии от источника $E(d) = \frac{E_0}{d}$. Индуцированное напряжение в проводнике длиной L :

$$V = E(d) \cdot L \quad (12)$$

Индуцированный ток при сопротивлении R :

$$I = \frac{V}{R} = \frac{E(d) \cdot L}{R} \quad (13)$$

КА, включая спутники Starlink, уязвимы к ЭМИ из-за своей чувствительной электроники и недостаточной защиты от мощных импульсов. ЭМИ может вызвать следующие эффекты:

1. нарушение работы систем связи и навигации. Временные сбои или постоянное повреждение радиочастотной аппаратуры;
2. повреждение электроники. Выход из строя микропроцессоров, память и другие электронные компоненты;
3. сбой питания. Нарушение работы систем питания, приводящее к отключению спутника.

Защитные меры:

- ✓ Экранирование. Использование защитных экранов и материалов для поглощения или отражения ЭМИ;
- ✓ Фильтрация. Установка фильтров на входах и выходах электронных систем для блокировки высокочастотных импульсов;
- ✓ редундантность систем. Дублирование ключевых систем и компонентов для повышения надежности.

2.4. Рефлекторы и дефлекторы

Рефлекторы и дефлекторы используются для управления направлением электромагнитных волн, таких как сигналы со спутников, в другую сторону. Такие устройства могут быть полезны для защиты от нежелательных сигналов или для манипуляции сигналами связи [12]. Рассмотрим использование дронов и наземных устройств с отражающими или отклоняющими поверхностями.

Основные концепции рефлекторов и дефлекторов.

- ✓ Рефлекторы отражают электромагнитные волны. Они могут быть пассивными (не требуют внешнего питания) или активными (используют внешнее питание для усиления или изменения характеристик сигнала).
- ✓ Дефлекторы отклоняют направление распространения электромагнитных волн без полного отражения. Фазированные решетки (используют множество элементов антенн, фазировка которых позволяет изменять направление излучаемого сигнала). Диэлектрические призмы (применяют изменения показателя преломления для отклонения сигнала).

Для использования рефлекторов и дефлекторов могут быть использованы как дроны, так и наземные устройства.

Дроны могут нести на себе отражающие или отклоняющие поверхности для манипуляции сигналами спутников. Такие дроны могут быть использованы в ситуациях, где необходимо быстро и гибко изменить направление сигнала.

Наземные устройства могут быть более мощными и долговечными по сравнению с дронами и использоваться для постоянного отклонения или отражения сигналов.

Преимущества:

- ✓ Гибкость. Возможность быстрой настройки и перенастройки направления сигнала;
- ✓ Мобильность. Дроны могут перемещаться, обеспечивая адаптивное управление сигналом;
- ✓ Масштабируемость. Возможность использования нескольких устройств для увеличения зоны покрытия.

Недостатки:

- ✓ Энергозатраты. Дроны требуют энергии для полета и управления рефлекторами/дефлекторами;
- ✓ точность позиционирования. Необходимо точное управление дронами для эффективного отражения/отклонения сигналов;
- ✓ сложность конструкции. Фазированные решетки и другие сложные устройства требуют точной настройки и калибровки.

2.5. Резонансное рассеяние

Резонансное рассеяние – это явление, при котором электромагнитные волны (свет, радиоволны и т.д.) взаимодействуют с частицами, атомами или молекулами таким образом, что происходит их эффективное рассеяние. В контексте борьбы с спутниковыми системами связи, такими как Starlink, резонансное рассеяние будет использовано для создания помех или отклонения сигналов. Рассмотрим, как это работает и как можно применить данное явление на практике.

Резонансное рассеяние возникает, когда частота электромагнитного волнового сигнала совпадает с собственной частотой колебаний частиц или молекул в материале. Это вызывает сильное взаимодействие и приводит к эффективному рассеянию волны. При применении резонансного рассеивания в спутниковых системах связи используются устройства и материалы, которые резонируют на частотах, используемых спутниками [13].

Преимущества:

- ✓ Точность. Резонансное рассеяние позволяет точно настраивать взаимодействие с сигналами на заданных частотах;
- ✓ Эффективность. Высокая эффективность рассеяния на резонансных частотах;
- ✓ Гибкость. Возможность создания метаматериалов и резонаторов с нужными характеристиками.

Недостатки:

- ✓ сложность разработки. Создание метаматериалов и резонаторов требует сложных технологий и точного проектирования;
- ✓ ограниченность диапазона. Резонансное рассеяние эффективно на узком диапазоне частот, что требует точной настройки под конкретные задачи;
- ✓ Стоимость. Высокая стоимость материалов и технологий.

2.6. Когерентные помехи

Когерентные помехи создаются путем генерации сигнала с теми же характеристиками (частота, фаза, амплитуда), что и целевой сигнал, но с измененными параметрами для создания интерференции. В результате целевой сигнал становится искаженным или подавленным. Когерентные помехи работают на основе принципа интерференции, где два сигнала с одинаковыми частотами и фазами могут складываться, образуя конструктивную или деструктивную интерференцию [14].

Когерентные помехи могут быть использованы для создания помех спутниковым сигналам, направленным на приемные станции или терминалы пользователей.

Преимущества:

- ✓ высокая эффективность. Возможность точного подавления целевого сигнала;
- ✓ Адаптивность. Возможность изменения параметров сигнала помех в реальном времени для поддержания интерференции.

Недостатки:

- ✓ точность синхронизации. Необходимость точной синхронизации по частоте и фазе с целевым сигналом;
- ✓ сложность реализации. Требуются сложные технологии для создания и поддержания когерентных помех;
- ✓ Контрмеры. Спутники и приемные станции могут использовать методы для защиты от когерентных помех, такие как изменение частот или фазирование сигналов.

2.7. Бионические устройства и микродроны для создания помех

Бионические устройства и микродроны – это малые, высокотехнологичные устройства, которые могут перемещаться в атмосфере и создавать помехи на микроскопическом уровне [15]. Такие устройства могут использоваться для различных целей, включая создание помех спутниковым системам связи, таким как Starlink.

Бионические устройства используют принципы биологии и инженерии для выполнения определенных задач. Они могут включать в себя элементы, которые имитируют природные системы, такие как крылья насекомых для полета.

Микродроны – это миниатюрные летательные аппараты, которые могут быть оснащены различными сенсорами и средствами связи для выполнения специфических задач. Они могут летать в воздухе, перемещаться в тесных пространствах и создавать целенаправленные помехи.

Варианты создания помех спутниковой связи:

1. запуск микродронов. Несколько микродронов запускаются вблизи целевой зоны;
2. Синхронизация. Дроны синхронизируются для создания когерентных РЧ-помех на частоте спутникового сигнала;
3. создание помех. Передатчики на дронах начинают генерировать помехи, вызывая интерференцию с целевым сигналом;
4. ЭМИ-атака. Некоторые дроны запускают ЭМИ для временного выведения из строя приемного оборудования;
5. оптические помехи. Дроны с лазерами нацеливаются на оптические сенсоры спутников для создания засветки и помех.

Преимущества:

- ✓ Мобильность. Микродроны могут перемещаться в различные точки для создания локализованных помех;
- ✓ Незаметность. Малый размер и способность к маневрированию делают их трудными для обнаружения и нейтрализации;
- ✓ Адаптивность. Микродроны могут быстро адаптироваться к изменениям в окружающей среде и задачах.

Недостатки:

- ✓ Энергозависимость. Ограниченное время полета из-за небольших размеров и емкости батарей;
- ✓ комплексность управления. Требуется высокоточная система управления и координации для эффективной работы;
- ✓ Контрмеры. Возможность разработки технологий для обнаружения и нейтрализации микродронов.

2.8. Виртуальные помехи

Виртуальные помехи включают использование программных методов для создания помех или искажения работы приемных устройств [16, 17]. Это будет достигнуто через хакерские атаки, внедрение вредоносного программного обеспечения (ПО), манипуляции с программным обеспечением, работающим на приемных устройствах, или через сетевые атаки, направленные на инфраструктуру спутниковой связи.

Хакерские атаки направлены на уязвимости в программном обеспечении приемных устройств или сетевой инфраструктуры спутниковых систем. Они могут включать:

- ✓ Взлом. Получение несанкционированного доступа к системам;
- ✓ DoS/DDoS атаки. Атаки отказа в обслуживании, которые перегружают систему и делают её недоступной;
- ✓ MITM атаки. Атаки типа «человек посередине», перехват и изменение данных в реальном времени.

Вредоносное ПО (malware) будет использовано для создания помех или искажения работы приемных устройств. Это будет достигнуто через:

- ✓ Трояны. Программы, скрывающиеся под видом легитимного ПО;
- ✓ Вирусы. Программы, которые распространяются и внедряются в другие программы;
- ✓ Черви. Самовоспроизводящиеся программы, распространяющиеся через сеть.

Вариант алгоритма атаки на систему спутниковой связи:

1. Разведка. Хакеры проводят разведку для выявления уязвимых систем и приемных устройств;
2. Фишинг. Рассылка фишинговых писем с целью получения данных доступа к административным панелям;
3. внедрение вредоносного ПО. Использование полученных данных для установки вредоносного ПО на приемные устройства;
4. создание помех. Вредоносное ПО изменяет параметры обработки сигналов, создавая помехи;
5. удаленный контроль. Установка бэкдоров для возможности дальнейших манипуляций и атак.

Преимущества:

- ✓ Скрытность. Трудно обнаружить программные атаки, особенно если они хорошо замаскированы;
- ✓ Удаленность. Возможность проведения атак из любой точки мира;
- ✓ Гибкость. Атаки могут быть адаптированы и изменены в зависимости от ситуации.

Недостатки:

- ✓ техническая сложность. Требуется высокий уровень технической экспертизы;
- ✓ законодательные ограничения. Проведение таких атак может нарушать законы и международные соглашения;
- ✓ риски обнаружения. Если атака будет обнаружена, это может привести к серьезным последствиям.

Выводы

Исследование содержит всестороннюю оценку методов по созданию паразитных помех спутниковой системы связи Starlink. Каждый из предложенных методов проанализирован с точки зрения технической

реализуемости, эффективности и потенциальных последствий. Особое внимание уделено бионическим устройствам и микродронам, а также виртуальным помехам, так как они представляют наиболее перспективные подходы, однако и другие методы имеют свои достоинства и могут быть успешно применены в комбинации.

Методы создания помех можно условно разделить на несколько категорий: физические, электронные и киберметоды. Каждый из них обладает своими уникальными характеристиками и требует специфических технических средств и условий для реализации.

Физические методы включают в себя использование дронов, лазеров и других устройств для прямого вмешательства в работу спутников. Применение дронов для создания помех позволяет осуществлять мобильные и точные атаки на спутниковую связь. Лазеры могут быть использованы для ослепления оптических сенсоров спутников, что приведет к временной потере связи.

Электронные методы создания помех основаны на использовании радиочастотных генераторов и других электронных устройств. Эти методы позволяют создавать когерентные и некогерентные помехи, которые значительно ухудшают качество связи. Применение низкочастотных генераторов и микродронов, оснащенных передатчиками, предоставляет возможность для широкомасштабного воздействия на спутниковую систему.

Киберметоды включают в себя использование вредоносного программного обеспечения, фишинг и атаки на программное обеспечение. Эти методы направлены на нарушение работы наземных станций управления и приемных устройств, что может привести к потере контроля над спутниками или снижению качества передачи данных.

В целом, работа демонстрирует, что создание помех спутниковой системе Starlink вполне возможно реализовать различными способами. Однако каждый из предложенных методов требует детальной проработки и учета всех возможных последствий, как технических, так и правовых. Комплексный подход, сочетающий различные методы, представляется наиболее эффективным для достижения поставленных целей.

Литература

1. Рябов А. В., Алексеев А. Е. Направления повышения помехоустойчивости систем радиосвязи // *Охрана, безопасность, связь*. 2022, № 7-1, с. 117–122.
2. Яковишин А., Кузнецов И., Дроздов И., Письменский Д. Перспективы развития информационной безопасности: глобальные вызовы и стратегии защиты // *Информационные ресурсы России*. 2024, № 2 (197), с. 93–103. DOI: 10.52815/0204-3653_2024_2197_93
3. Карцан И. Н., Кобозев Д. С. Аспекты безопасности спутниковой связи // *Естественные и технические науки*. 2024, № 6 (193), с. 310–312.

4. Пашаев Ф. Г., Зейналов Д. И., Наджафов Г. Т. Разработка программно-технических средств защиты технологических процессов от киберугроз // Проблемы информационной безопасности. Компьютерные системы. 2024, № 2 (59), с. 104-116. DOI: 10.48612/jispr/p79a-z1nu-71vk
5. Никифоров И. А. Роль искусственного интеллекта в кибербезопасности // Сборник научных трудов вузов России «Проблемы экономики, финансов и управления производством». 2024, № 54, с. 230-237.
6. Логинов Е. А. Роль и значимость искусственного интеллекта в обеспечении информационной безопасности // Научный аспект. 2024, Т. 21, № 5, с. 2805-2809.
7. Аверьянов В. С., Карцан И. Н. Методы оценки защищенности автоматизированных систем на базе квантовых технологий согласно CVSS V2.0/V3.1 // Защита информации. Инсайд. 2023, № 1 (109), с. 18-23.
8. Данилюк А. И., Гладких Д. С., Мельник В. Н., Полищук В. Р. Факторы, оказывающие воздействие на системы связи в условиях боевых действий // Тенденции развития науки и образования. 2024, № 107-9, с. 167-170. DOI: 10.18411/trnio-03-2024-489
9. Ромащенко М. А., Васильченко Д. В., Белецкая С. Ю. Использование искусственных нейронных сетей для оценки воздействия электромагнитных помех // Радиотехника. 2023, Т. 87, № 8, с. 21-27. DOI: 10.18127/j00338486-202308-04
10. Дементьев А. Н., Новиков А. Н., Арсеньев К. В., Куркин А. Н., Жуков А. О., Карцан И. Н. Метод обработки сигналов в адаптивной антенной решетке // Южно-Сибирский научный вестник. 2023, № 4 (50), с. 60-63. DOI: 10.25699/SSSB.2023.50.4.009
11. Zhang D., Cheng E., Wan H., Zhou X., Chen Y. Prediction of Electromagnetic Compatibility for Dynamic Datalink of UAV // IEEE Transactions on Electromagnetic Compatibility. 2019, Vol. 61, № 5, pp. 1474-1482. DOI:10.1109/TEMC.2018.2867641
12. Петренко А. С., Петренко С. А., Ожиганова М. И. О киберустойчивости и безопасности изобразительных нейросетей // Защита информации. Инсайд. 2023, № 6 (114), с. 50-54.
13. Ожиганова М. И. Архитектура безопасности киберфизической системы // Защита информации. Инсайд. 2022, № 2 (104), с. 5-9.
14. Ожиганова М. И., Калита А. О. Анализ и применение алгоритмов машинного обучения для идентификации вредоносного программного кода // Информатизация и связь. 2019, № 5, с. 51-56.
15. Калита А. О., Ожиганова М. И., Тищенко Е. Н. Основы организации адаптивных систем защиты информации // НБИ технологии. 2019, Т. 13, № 1, с. 11-15. DOI: 10.15688/NBIT.jvolsu.2019.1.2.
16. Ромащенко М. А., Васильченко Д. В., Пухов Д. А. Современное состояние задач повышения помехоустойчивости канала управления беспилотных авиационных систем на основе искусственного интеллекта // Вестник Воронежского государственного технического университета. 2023, Т. 19, № 6, с. 142-146. DOI: 10.36622/VSTU.2023.19.6.022
17. Zhang R., Cui J. Application of Convolutional Neural Network in multi-channel Scenario D2D Communication Transmitting Power Control // 2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL), Chongqing, China, 2020, pp. 668-672. DOI:10.1109/CVIDL51233.2020.000-3

STARLINK: CYBERSECURITY CHALLENGES AND COUNTERMEASURES FOR THE SATELLITE INTERNET

Kartsan I. N.⁴, Averyanov V. S.⁵, Krasnikov M. D.⁶

Keywords: signal phase shift, adaptive RF interference, coherent interference, virtual interference, electromagnetic pulses, reflector, deflector, resonant scattering, bionic device, microdrone.

Purpose of the research: investigation of vulnerabilities of low-orbit satellite constellation, as well as methods of counteraction and neutralization of threats related to providing unauthorized access to the Internet to users.

Research method: analytical review of relevant scientific information, information security assessment method.

Research result: the analytical review is presented to assess the interference immunity of the Starlink satellite constellation using Signal-to-Noise Ratio technical parameters. Common vulnerabilities for the Starlink 1.0, Starlink 1.5, Starlink 2.0 and Starlink 2.0 mini-series of spacecraft are identified. The technological design of the Starlink satellite Internet system developed by SpaceX is shown, including information on defenses against jamming, hacking, and cyberattacks. Interference techniques utilizing signal phase shifting, adaptive RF interference, coherent and virtual interference, electromagnetic pulses, reflectors and deflectors, resonant scattering, and the use of bionic devices and microdrones are discussed. Both disadvantages and advantages are presented for all the methods considered. Interference techniques with the most promising approach are identified.

Practical usefulness lies in the fact that, based on the analysis of interference techniques, technical solutions for exploiting vulnerabilities in network hardware and software are proposed.

References

1. Ryabov A. V., Alekseev A. E. Directions of increasing the immunity of radio communication systems // Safety, security, communications. 2022, № 7-1, s. 117-122.
2. Yakovishin A., Kuznetsov I., Drozdov I., Pismensky D. Perspectives of information security development: global challenges and protection strategies // Information Resources of Russia. 2024, № 2 (197), s. 93-103. DOI: 10.52815/0204-3653_2024_2197_93
4. Igor N. Kartsan, Dr.Sc., Associate Professor, Chief Scientist Analytical Center, Moscow, Russia, E-mail: kartsan2003@mail.ru, ORCID 0000-0003-1833-4036.
5. Vitaliy S. Averyanov, Head of Information Security Department, Krasnoyarsk Regional Clinical Oncologic Dispensary named after A.I. Kryzhanovskiy, Krasnoyarsk, Russia. E-mail: averyanov124@mail.ru, ORCID: 0000-0001-6069-2537.
6. Maksim D. Krasnikov, student of the BIT Department, FSBEI VO «Siberian State University of Science and Technology named after Academician M.F. Reshetnev», Krasnoyarsk, Russia. E-mail: maks.krasnikov.76@bk.ru

3. Kartsan I. N., Kobozev D. S. Aspects of satellite communication security // *Natural and Technical Sciences*. 2024, № 6 (193), s. 310–312.
4. Pashayev F. G., Zeynalov D. I., Najafov G. T. Development of software and hardware means of protection of technological processes from cyber threats // *Problems of information security. Computer Systems*. 2024, № 2 (59), s. 104–116. DOI: 10.48612/jisp/p79a-z1nu-71vk
5. Nikiforov I. A. The role of artificial intelligence in cyber security // *Collection of scientific papers of Russian universities «Problems of economics, finance and production management»*. 2024, № 54, s. 230–237.
6. Loginov E. A. The role and significance of artificial intelligence in ensuring information security // *Scientific Aspect*. 2024, Vol. 21, No. 5, s. 2805–2809.
7. Averyanov V. S., Kartsan I. N. Methods of evaluation of automated systems security on the basis of quantum technologies according to CVSS V2.0/V3.1 // *Zashhita informacii. Insajd*. 2023, № 1 (109), s. 18–23.
8. Danilyuk A. I., Gladkikh D. S., Melnyk V. N., Polishchuk V. R. Factors affecting the communication systems under combat conditions // *Tendencies of Science and Education Development*. 2024, № 107-9, s. 167–170. DOI: 10.18411/trmio-03-2024-489
9. Romashchenko M. A., Vasilchenko D. V., Beletskaya S. Yu. Using artificial neural networks to assess the impact of electromagnetic interference // *Radiotekhnika*. 2023, Vol. 87, No. 8, s. 21–27. DOI: 10.18127/j00338486-202308-04
10. Dementiev A. N., Novikov A. N., Arseniev K. V., Kurkin A. N., Zhukov A. O., Kartsan I. N. Signal processing method in the adaptive antenna array // *South Siberian Scientific Bulletin*. 2023, № 4 (50), c. 60–63. DOI: 10.25699/SSSB.2023.50.4.009
11. Zhang D., Cheng E., Wan H., Zhou X., Chen Y. Prediction of Electromagnetic Compatibility for Dynamic Datalink of UAV // *IEEE Transactions on Electromagnetic Compatibility*. 2019, Vol. 61, № 5, pp. 1474–1482. DOI:10.1109/TEM.2018.2867641
12. Petrenko A. S., Petrenko S. A., Ozhiganova M. I. About cyber resistance and security of image neural networks // *Zashhita informacii. Insajd*. 2023, № 6 (114), s. 50–54.
13. Ozhiganova M. I. Security architecture of cyber-physical system // *Zashhita informacii. Insajd*. 2022, № 2 (104), s. 5–9.
14. Ozhiganova M. I., Kalita A. O. Analysis and application of machine learning algorithms for identification of malicious software code // *Informatization and communication*. 2019, № 5, s. 51–56.
15. Kalita A. O., Ozhiganova M. I., Tishchenko E. N. Fundamentals of organization of adaptive information protection systems // *NBI Technologies*. 2019, Vol. 13, No. 1, s. 11–15. DOI: 10.15688/NBIT.jvolsu.2019.1.2
16. Romashchenko M. A., Vasilchenko D. V., Pukhov D. A. Current state of the problems of improving noise immunity of the control channel of unmanned aircraft systems based on artificial intelligence // *Bulletin of Voronezh State Technical University*. 2023, Vol. 19, No. 6, s. 142–146. DOI: 10.36622/VSTU.2023.19.6.022
17. Zhang R., Cui J. Application of Convolutional Neural Network in multi-channel Scenario D2D Communication Transmitting Power Control // *2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL)*, Chongqing, China, 2020, pp. 668–672. DOI:10.1109/CVIDL51233.2020.000-3

