МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ТЕРМИНАЛОВ СПУТНИКОВОЙ СВЯЗИ STARLINK ОТ СРЕДСТВ РАДИОЭЛЕКТРОННОГО ВЛИЯНИЯ ПРОТИВНИКА

ПРЕДИСЛОВИЕ

Методические рекомендации по защите терминалов спутниковой связи Starlink от средств радиоэлектронного воздействия противника (далее - Методические рекомендации) разработаны рабочей группой офицеров Научного центра связи и информатизации Военного института телекоммуникаций и информатизации имени Героев Крут, в соответствии с распоряжением Командования Войск связи и кибербезопасности Вооруженных Сил Украины от 01.05.2023 № 308/98/4671.

В Методических рекомендациях приведены теоретические основы и практические рекомендации по защите терминалов спутниковой связи Starlink (первого и второго поколения) от радиоэлектронного воздействия противника, которые учитывают опыт применения средств спутниковой связи и результаты практических проверок (испытаний) в полевых условиях. В то же время, понимание теоретических основ радиоэлектронного воздействия на терминалы спутниковой связи позволит должностным лицам развивать практику применения методов защиты и не ограничиваться терминалами только одного производителя.

Материалы Методических рекомендаций целесообразно использовать творчески, в соответствии с условиями сложившейся обстановки.

Все вопросы и предложения, касающиеся этих Методических рекомендаций, направлять в Военный институт телекоммуникаций и информатизации имени Героев Крут по адресу: 01011, г. Киев, ул. Князей Острожских, 45/1 (контактный телефон разработчиков для предоставления замечаний и предложений - 38-431).

СОДЕРЖАНИЕ

Введение

Система Starlink - проект американской компании SpaceX по разработке высокопроизводительной спутниковой платформы для изготовления спутников связи и запусков большого их количества (созвездия) в космическое пространство. Система предоставляет доступ к широкополосному Интернету с использованием абонентских терминалов в любой точке планеты, в том числе на всей территории нашего государства.

В Украине широкое использование доступа к широкополосному Интернету системы Starlink для резервирования линий связи критической инфраструктуры началось в 2022 году с началом полномасштабного вторжения российской федерации на территорию нашего Государства.

В то же время, радиодоступу с использованием абонентских терминалов Starlink присущи те же недостатки, что и любой радиосвязи, а именно - возможность воздействия (обнаружения и подавления) средствами радиоэлектронной борьбы (РЭБ) противника. Поэтому разработка Методических рекомендаций по защите терминалов спутниковой связи Starlink от средств радиоэлектронного воздействия противника является актуальной задачей для обеспечения устойчивого управления войсками.

Все положения Методических рекомендаций следует применять творчески, с учетом конкретных условий обстановки.

РАЗДЕЛ 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАДИОЭЛЕКТРОННОГО ВОЗДЕЙСТВИЯ НА ТЕРМИНАЛЫ СПУТНИКОВОЙ СВЯЗИ STARLINK

1.1. Характеристика системы спутниковой связи как организационной системы.

Спутниковая связь (СЗ) представляет собой воздушный эшелон системы электронных коммуникаций ВС Украины, является важнейшим, а во многих случаях и единственным родом связи, которой способен обеспечить управление войсками в сложной обстановке, в том числе во время нахождения командиров и штабов в движении.

Системы спутниковой связи (ССЗ), как системы открытого типа, характеризуются чувствительностью к случайным и преднамеренным помехам, ограничением пропускной способности в занимаемой полосе частот, значительной доступностью для средств радиоразведки и минимально определенным отношением сигнал-помеха в точке приема.

Процесс передачи информации по линиям спутниковой связи (ЛСЗ) должен соответствовать требованиям по достоверности, своевременности и скрытности, совокупность которых характеризует и определяет качество ССЗ. При функционировании военных ЛСЗ, вследствие воздействия различных неблагоприятных факторов, качество СЗ может оказаться ниже необходимого.

ССЗ ВС Украины строятся на технических и информационно-коммуникационных ресурсах иностранных операторов СЗ с использованием аппаратных и программных средств предоставленных в пользование.

ССЗ - это комплекс технических средств, способных объединить информационно-коммуникационные каналы в единую систему географически рассредоточенных пунктов управления и систем вооружения.

В целом в состав системы ССЗ входят следующие основные элементы:

терминалы (земные станции) спутниковой связи, а также центры (шлюзы) СЗ, образующие группировку наземных средств;

космические аппараты, имеющие в своем составе ретрансляторы связи, образующие орбитальную группировку средств СЗ;

центр управления ССЗ;

наземный комплекс управления космическими аппаратами.

Именно наземные станции предназначены для передачи всех видов информации с использованием оборудования космических аппаратов в интересах соответствующих органов (объектов) управления.

Наземные станции (терминалы) представляют собой комплекс аппаратуры связи, включающий приемно-передающее оборудование, модем (аппаратуру каналообразования), антенно-фидерное устройство и другое оборудование.

Средством поддержания устойчивого функционирования всего оборудования в ССЗ и сопряжения его с сетями операторов телекоммуникаций является синхронизация. В большинстве современных ССЗ коммерческого назначения в качестве источников синхронизации применяются сигналы глобальной системы спутникового позиционирования GPS.

Таким образом, для достижения установленных предельных показателей

В качестве функционирования СЗ используются необходимые организационные и технические мероприятия.

1.2. Цели, задачи и методы радиоэлектронного противодействия системам спутниковой связи

Радиоэлектронная борьба - совокупность согласованных мероприятий и действий войск (сил) по радиоэлектронному поражению (подавлению) радиоэлектронных объектов (радиоэлектронных средств) систем управления войсками (силами) и оружием противника и по радиоэлектронной защите радиоэлектронных объектов (радиоэлектронных средств) своих систем управления войсками (силами) и оружием.

Из всех видов разведки противника, направленных на раскрытие системы связи для нарушения их функционирования, самым эффективным остается радиоразведка, которая позволяет в реальном масштабе времени определять местоположение и оперативно-тактическую принадлежность радиоизлучающих средств, а по их совокупности - линий и узлов связи.

Цели РЭБ достигаются выполнением ряда задач, основными из которых являются: раскрытие (обнаружение) радиоэлектронной обстановки (РЭО); радиоэлектронное поражение (подавление) систем и средств управления войсками, оружием, разведкой и РЭБ противника;

дезорганизация систем боевого управления противника в принятии оперативных (боевых) решений с целью повышения эффективности ведения боевых действий своими войсками;

разрушение, уничтожение и (или) искажение программного обеспечения и информации в автоматизированных системах управления (АСУ) противника;

снижение эффективности применения противником средств радиоэлектронного поражения;

обеспечение электромагнитной совместимости (ЭМС) радиоэлектронных средств.

Основным методом радиоэлектронного поражения является радиоэлектронное подавление.

Радиоэлектронное подавление заключается в снижении эффективности (качества) функционирования радиоэлектронных средств противника путем действия на их приемные устройства активными и пассивными радиоэлектронными помехами.

Радиоподавление ведется в определенном диапазоне радиоволн и заключается, в том числе, в нарушении работы терминалов СЗ и средств радионавигации, путем воздействия на их приемные устройства электромагнитным излучением.

Способность ССЗ противостоять всем видам разведки противника характеризуется разведывательной защищенностью.

Разведзащищенность ССЗ достигается:

прогнозированием возможностей группировки разведки противника и его влияния на систему и войска связи;

установлением и строгим соблюдением режимов работы средств СЗ;

выбором соответствующих средств и способов обеспечения связи;

размещением пунктов управления и других ВС вне населенных пунктов, развертыванием и перемещением их с учетом маскирующих свойств местности и использованием табельных средств маскировки;

выносом радиоизлучающих средств на максимально возможные расстояния от ВС пунктов управления и дистанционным управлением их работой:

планированием и проведением мероприятий по защите системы связи от технических средств разведки противника;

рациональным выбором способов обеспечения связи: сохранением в тайне от противника мероприятий по организации ССЗ;

организацией охраны и обороны узлов и линий связи.

1.3. Особенности подавления спутниковых средств связи

Разведка и подавление ССЗ являются технически сложной задачей, так как при применении на космическом аппарате (КА) узко направленных антенн с диаграммой направленности 1 ° и менее (что возможно в миллиметровом и оптическом диапазонах волн) обеспечивается высокая скрытность связи. При этом прием сигналов по боковым лепесткам диаграмм направленности спутниковой антенны требует высокой чувствительности приемника разведки: от - 140 дБ/Вт и выше.

Для оценки помехоустойчивости ССЗ общепринятым является использование так называемого коэффициента защиты ($К_З$), представляющего собой минимально допустимое отношение сигнал/(шум + помеха), на входе приемника, при котором обеспечивается необходимое качество связи (задана достоверность приема). Обычно значения $_К З$ представляются в виде нескольких сомножителей, учитывающих способы модуляции, быстрые и медленные замирания сигналов на трассах связи, виды помех и другие.

Для оценки эффективности подавления (полного нарушения связи) обычно используют коэффициент подавления ($К_П$), что является минимально возможным значением отношения помеха/сигнал на входе приемника, при котором достигается полное нарушение связи.

Реальную помехозащищенность станции СЗ может оцениваться через максимально допустимые значения мощности помехи на входе ее приемного устройства ($Р_{П\,ВХ}$) для близкой к штатной протяженности интервала радиосвязи, при которой в канале ССЗ происходит полное нарушение связи:

$$Р_{П\,ВХ} = Р_{С\,ВХ} \cdot К_П \cdot К_{З\,АНТ\,(\alpha)},$$

где $Р_{П\,ВХ}$ соответствует мощности сигнала на входе приемника станции СЗ для близкой к штатной протяженности ее интервала (км);

$К_П$ - коэффициент подавления;

$К_{З\,АНТ}$ - коэффициент защиты приемной антенны со стороны ее боковых и обратных лепестков ($К_{З\,АНТ}$ 1 для , $К_{З\,АНТ}$ 10^{-3} для -).

Значения реальной помехозащищенности зависят от мощности информационного сигнала в точке приема (от мощности передатчика, коэффициентов усиления приемной и передающей антенн, протяженности трассы связи и условий прохождения радиоволн), технических значений параметра $К_П$ и направлений прихода в точку приема защитных свойств

антенн.

Взаимодействие между ССЗ, станциями помех КА в процессе радиоэлектронного воздействия условно приведено на рисунке 1.1.

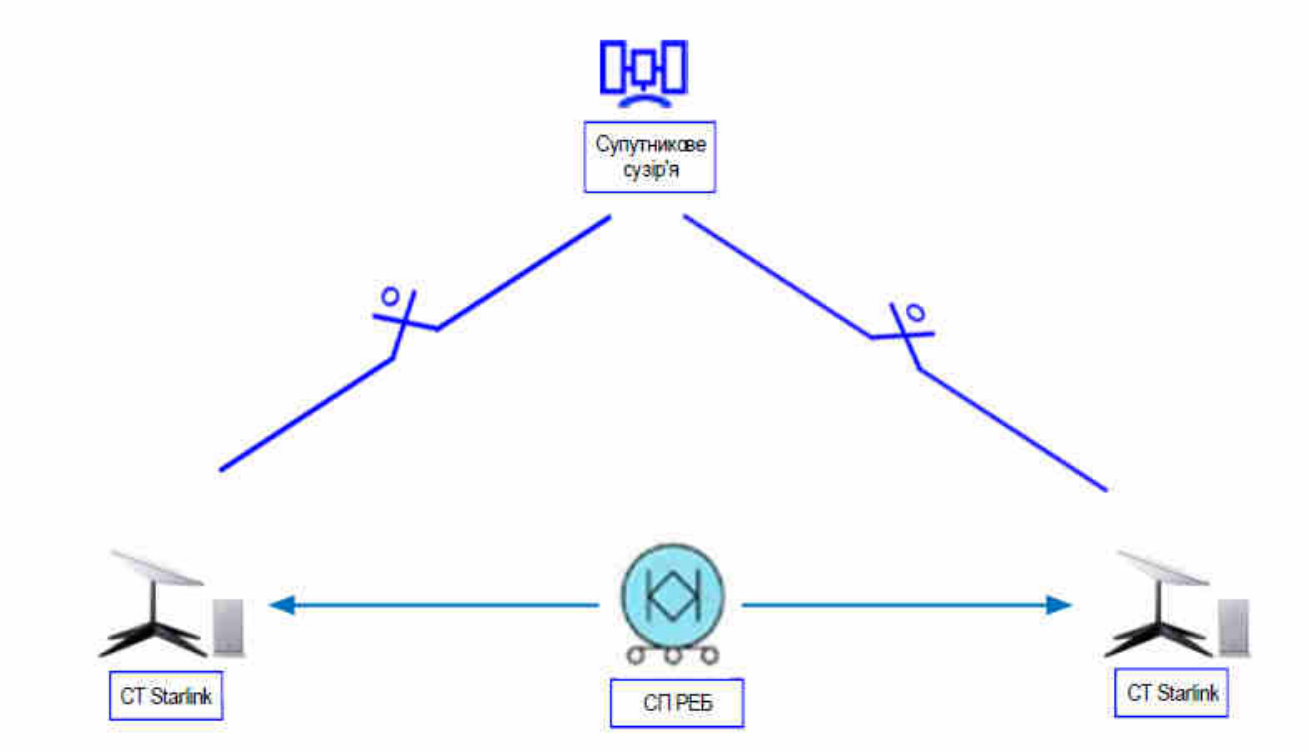

Рисунок 1.1 - Взаимодействие между ССЗ, станциями помех и КА в процессе радиоэлектронного воздействия

Из анализа помехозащищенности ЛСЗ возможно сделать следующие выводы: значения реальной помехозащищенности (значения $P_{П\ ВХ}$) зависят в первую очередь от реальных значений мощности полезных сигналов ($P_{С\ ВХ}$) на входах их приемников. Чем они выше, тем больше значение $P_{С\ ВХ}$ необходимы нарушения связи (тем выше реальная помехозащищенность);

реальная помехозащищенность $P_{П\ ВХ}$ зависит от направлений прихода радиопомех (значений $K_{З\ АНТ}$), их структуры (значений $K_{П}$) и для одного и того же типа ЛСЗ, с учетом значений сомножителя $K_{П \cdot K З\ АНТ}$, может отличаться от средних значений к $\pm (10^3 \div 10^4)$ раз

Для линий спутниковой связи наиболее вероятна постановка заградительных помех (шумовых, частотно- и дискретносканирующих) в пределах рабочих диапазонов терминалов СЗ.

Особенностями разведки и подавления сигналов ССЗ, использующих синхронизацию сети с применением спутниковых радионавигационных средств заключается в том, что без обмена сигналами позиционирования невозможно установление связи в сети, а также поддержание устойчивой работы конечных станций (терминалов) в сети.

Примером такой сети является сеть Интернет Starlink от компании SpaceX. Функционально сеть Интернет Starlink мало чем отличается от Wi-

Fi: для подключения к соответствующей точке доступа (КА) необходимо ввести только правильные данные. Разница заключается в способе получения данных - наземная станция постоянно излучает радиосигнал в сторону одного из более чем 3 тысяч спутников SpaceX, расположенных на орбите Земли, и таким же образом принимает данные.

Взаимодействие между ССЗ Starlink, станциями помех, GPS и КА в процессе радиоэлектронного воздействия изображено на рисунке 1.2.

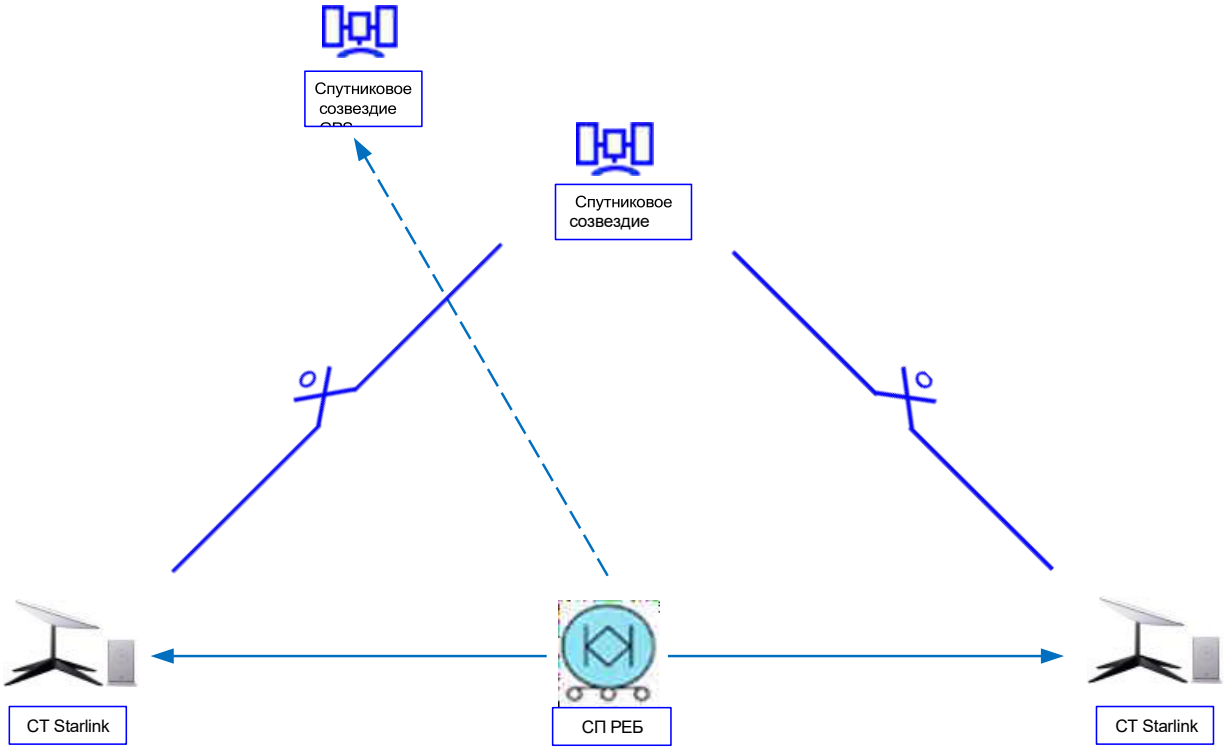

Рисунок 1.2 - Взаимодействие между ССЗ Starlink, станциями помех, GPS и КА в процессе радиоэлектронного воздействия

Подавление сигналов всей системы СЗ SpaceX возможно лишь теоретически - на практике нет готовой технологии, способной обрушить большую сеть, насчитывающую тысячи спутников.

Еще одним преимуществом повышенной помехозащищенности сети Интернет Starlink является разветвленность сети. В отличие от традиционных ССЗ ее аппараты не зависают над одной точкой, а сочетают усилия для глобального покрытия. Благодаря такому подходу выход из строя отдельных спутников не приведет к обрыву соединения, для этого противнику придется уничтожить значительное их количество.

Терминал спутниковой связи Starlink излучает узконаправленный радиосигнал вертикально вверх, тогда как станции радиоэлектронной борьбы накрывают большую площадь в горизонтальной плоскости.

Для реализации радиоподавления сети Интернет Starlink понадобится создание мощной системы радиопомех, организованных непосредственно возле антенн пользователя с помощью мощного передатчика. Станция помех должна располагаться идеально между наземным терминалом и КА, поэтому такой вариант маловероятен.

Наиболее вероятным сценарием нарушения работы ЛСЗ Starlink является

подавление СРНЗ на территории размещения СЗЗ. Поэтому на практике рассматриваются случаи радиоэлектронного подавления отдельных терминалов СЗ, и соответственно - методы защиты.

1.4. Особенности подавления спутниковых радионавигационных систем

Организация доступа к спутниковой радионавигационной системе GPS предусматривает три основных уровня обслуживания:

служба точного позиционирования;

служба стандартного

позиционирования;

дифференциальный режим.

Служба точного позиционирования позволяет получать точное определение составляющих вектора скорости и координат потребителя и имеет ограниченный доступ (для военных потребителей). В этом режиме используются защищенные сигналы P (Y) и M коды.

Служба стандартного позиционирования доступна всем пользователям системы GPS и предусматривает два режима с селективным доступом (с внедрением дополнительных преднамеренных ошибок в значении эфемерид навигационных спутников Земли (НСЗ)) и без него. В стандартном режиме используются сигналы C/A, L1C, L2C и L5 коды.

Дифференциальный режим использования системы основан на исключении разнообразных систематических погрешностей при совместной обработке результата в навигационной аппаратуре и аппаратуре опорной станции передачи данных.

Основные характеристики сигналов в диапазоне L1 СРНЗ GPS приведены в таблице 1.1.

Таблица 1.1

Основные характеристики сигналов в диапазоне L1 СРНЗ GPS

Наименование	C/A	L1C	P(Y)	M
Несущая частота, МГц	1575.42	1575.42	1575.42	1575.42
Частотный диапазон	L1	L1	L1	L1
Метод доступа	CDMA	CDMA	CDMA	CDMA
Компонент сигнала	Данные	Данные	Данные	н/д
Модуляция	BPSK(1)	TMBOC(6,1,1/11)	BPSK(10)	BOC-sin(10,5)
Частота символов, МГц	1.023	1.023	10.23	5.115
Скорость данных, бит/с	50	50	50	н/д

Задачей подавления тракта приема системы GPS является искажение навигационных сигналов, принимаемых потребителями от навигационных систем, входящих в группировки, которые наблюдаются, по обоим каналам связи.

Эти эффекты достигаются за счет:

значительного увеличения отношения помеха/сигнал;

существенного повышения веса паразитных составляющих в корреляционном отзыве обработанных навигационных сигналов;

трудностей или полного срыва в течение длительного времени режима захвата и слежения за навигационными сигналами.

В качестве помех могут быть использованы:

прицельный (по частоте и спектру) шумовой процесс;

сигнал на рабочей частоте с изменяемой фазой по закону цифровой моделирующей функции - псевдоимитирующий сигнал (однако такая реализация процесса требует знания тактовой частоты в формирователях псевдослучайной последовательности, а также ожидаемых значений доплеровских сдвигов);

помехи, имитирующие навигационные сигналы.

Первые две помехи требуют повышенных энергетических затрат.

Третья помеха является наиболее эффективной и относительно простой для технической реализации.

Реализация имитации осуществляется приемом навигационных сигналов на рабочих несущих частотах, усиление их и ретрансляции на тех же рабочих частотах в сторону бортовой приемной станций СЗ, при предварительном обогащении ее рециркуляционными компонентами (заградительное препятствие по задержке).

Что касается системы спутниковой связи Starlink, то ее терминалы оборудованы бортовым GPS приемником. С его помощью терминалы определяют собственное положение и адаптируют параметры работы соответственно доступности спутников в своей локации. Следовательно средства РЭБ могут повлиять на их работу. Это могут быть как средства РЭБ противника, так и собственные средства РЭБ.

По опыту выполнения задач по связи, чаще всего противником используются следующие методы радиоэлектронного воздействия.

GPS jamming («глушилка GPS»): подавление работает по принципу создания радиопомех на частотах, используемых приемниками GPS модулей. В результате работы такой «глушилки» большинство GPS приемников в зоне подавления не имеют возможности определить свое положение.

Для терминалов спутниковой связи Starlink в случае первого включения и активації терминала, передача данных с точным определением положения терминала является обязательным. Поэтому первое включение терминала для его активації в системе Starlink нужно планировать и проводить вне зоны действия любых средств РЭБ (как своих, так и противника).

В случае очередного включения уже активированных терминалов спутниковой связи Starlink в зоне действия GPS «глушилки», терминалы способны устанавливать связь со спутниками и работать с сетью Starlink. Но при этом возможно существенное увеличение времени на установление связи, а также уменьшение скорости передачи информации. Также могут появляться уведомления-предупреждения о невозможности определения положения в мобильном приложении (или в веб-версии) Starlink.

GPS spoofing (подмена сигналов GPS спутников): работает по принципу отправки специально модулированных сигналов, получение которых GPS приемниками в зоне средств РЭБ приводит к ошибочному и/или неточному определению положения приемника. Действие таких средств может влиять на

терминалы Starlink и приводить к ухудшению и даже к потере связи с спутниками. Проявлениями таких проблем могут быть предупреждение в мобильном приложении, ошибки относительно плохой видимости (Visibility), при работе близко к зоне разграничения боевых действий и государственной границы (20-30 км). Обычно идентифицировать использование врагом средств РЭБ по методу

GPS Spoofing возможно в мобильном приложении Starlink, вкладка NETWORK STATISTICS (рисунок 1.3).

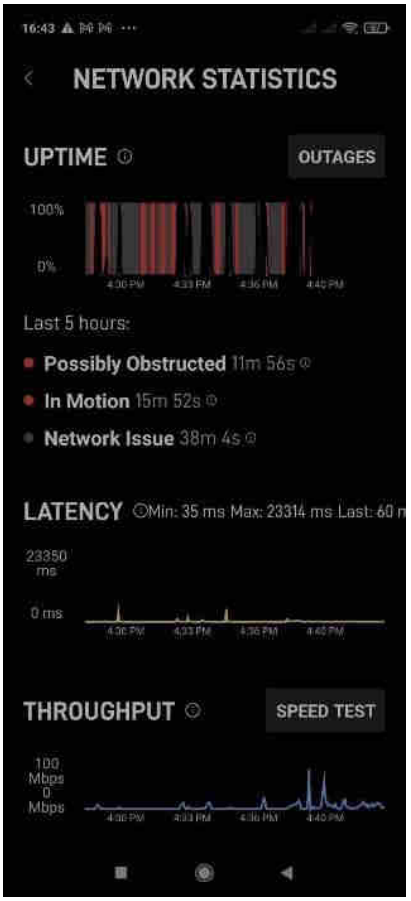

Рисунок 1.3 - Идентификация использования противником средств РЭБ на частотах GPS

Таким образом, в условиях ведения полномасштабной войны российской федерации против Украины, противник активно применяет средства РЭБ с целью разведки и подавления развернутой системы связи, а также нарушения функционирования системы управления Вооруженными Силами и Государства в целом. Поэтому специалистам связи важно понимать теоретические основы и методы по воздействию и защите от средств РЭБ спутниковых терминалов, в том числе Starlink.

Следует отметить, что полностью исключить возможность воздействия средств РЭБ противника на терминалы спутниковой связи невозможно, поэтому специалистам связи необходимо владеть практическими методами защиты и выполнять организационно-технические мероприятия для мінімізації их возможного негативного воздействия.

РАЗДЕЛ 2. ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО МЕТОДАМ ЗАЩИТЫ ТЕРМИНАЛОВ СПУТНИКОВОЙ СВЯЗИ STARLINK

По опыту выполнения задач по связи, с учетом имеющейся информации представителей подразделений ВС Украины, которые выполняют боевые задачи в районах выполнения задач (боевых действий) с наивысшей интенсивностью, были выявлены неединичные случаи эффективного использования врагом средств РЭБ, которые делают невозможным и/или влияют на работу терминалов спутниковой связи Starlink Принципы работы средств РЭБ противника предположительно основаны на методах GPS spoofing и GPS jamming. В свою очередь, использование средств радиоэлектронного подавления требует от специалистов связи выполнения адекватных действий по защите терминалов от воздействия РЭБ и обеспечения необходимого качества связи.

По результатам натурных испытаний (проверок), наиболее эффективными методами защиты терминалов спутниковой связи Starlink оказались следующие:

углубление терминалов в землю;

использование «клетки Фарадея»;

отключение модуля GPS на терминалах программным методом;

комбинации указанных выше методов.

В качестве имитации работы средств РЭБ противника во время проведения натурных испытаний (проверок) использовалось отечественное средство РЭБ «Нота» первого и второго поколения (рис. 2.1), позволяющее практически исследовать влияние средств РЭБ на работу терминала спутниковой связи Starlink.

Рисунок 2.1 - Внешний вид отечественного средства РЭБ «Нота»

Расстояние между станцией РЭБ и спутниковыми терминалами Starlink в ходе натурных испытаний менялось в зависимости от характеристик сигнала подавления станций радиоэлектронной борьбы.

2.1. Практическая проверка работоспособности терминалов спутниковой связи Starlink

Для оценки влияния средства РЭБ на терминалы Starlink, базовой выбрана проверка скорости передачи информации, сущность которой приведена ниже.

Для проведения проверки работоспособности терминалов спутниковой связи Starlink следует развернуть терминалы по схеме организации доступа к сети Интернет (рис. 2.2).

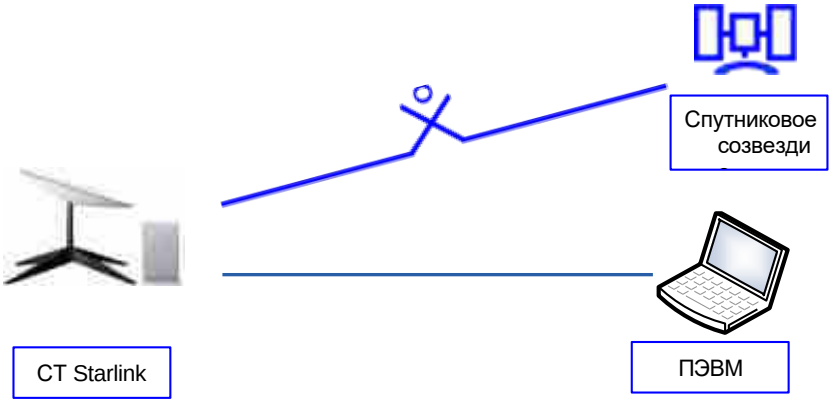

Рисунок 2.2 - Схема организации доступа к сети Интернет

Внешний вид развернутых и настроенных терминалов спутниковой связи Starlink к сети Интернет во время проведения практических проверок приведен на рис. 2.3.

Рисунок 2.3 - Пример развернутых и настроенных терминалов спутниковой связи Starlink (разных поколений) к сети Интернет

Для практической проверки эффективности любого метода защиты от воздействия РЭБ следует осуществить следующее.

Настроить терминалы с помощью программного обеспечения Starlink, при этом программное обеспечение отчитается об успешном соединении и установлении доступа к сети Интернет.

Проверить скорость передачи данных терминалов спутниковой связи Starlink, например с использованием веб-интерфейса «**Speedtest**» по ссылке: https://www.speedtest.net/(рис. 2.4).

Рисунок 2.4 - Пример оценки показателей функционирования и реальной скорости передачи данных терминалов Starlink

Вывод: В условиях успешного соединения и установления доступа к сети Интернет программное обеспечение во вкладке измерения скорости передачи данных **«Speedtest»** показывает реальную скорость передачи данных в данный момент времени (пример оценки скорости и других характеристик приведен в таблице 2.1).

Таблица 2.1

Результаты проверки функционирования и реальной скорость передачи данных терминалов спутниковой связи Starlink

№ з/п	Версия терминала	Время настройки	Скорость нисходящая (Download), Мбит/сек	Скорость выходная (Upload), Мбит/сек	Время задержки (Ping), мсек
1.	1 поколение	5 мин.	47.26 Мбит/сек	9.74 Мбит/сек	58 мсек
2.	2 поколения	4 мин.	38.06 Мбит/сек	4.33 Мбит/сек	72 мсек

2.2. Определение влияния средств РЭБ на работоспособность терминалов спутниковой связи Starlink

Для определения влияния средств РЭБ на работоспособность терминалов спутниковой связи Starlink следует развернуть и настроить терминалы согласно схемы организации доступа к сети Интернет под воздействием средствами РЭБ (рис. 2.5).

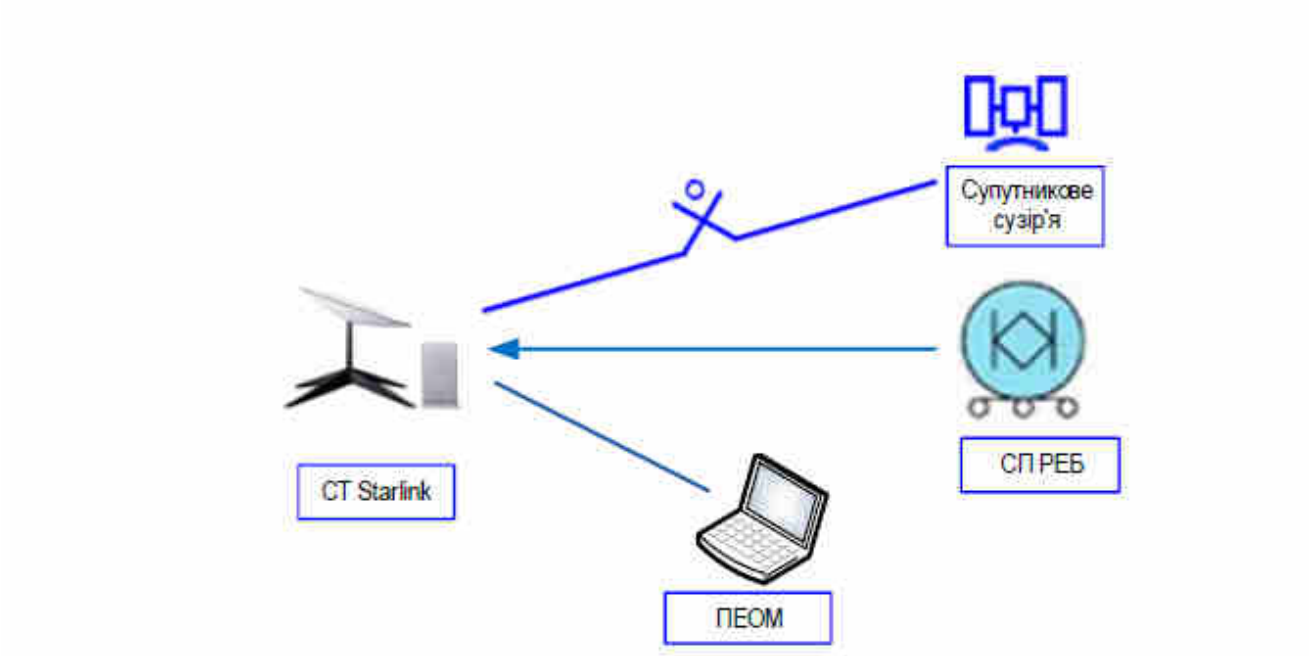

Рисунок 2.5 - Схема организации доступа к сети Интернет с использованием терминалов спутниковой связи Starlink во время воздействия средствами РЭБ

2.2.1. ровести проверку функционирования и возможности влияния средствами РЭБ доступа к сети Интернет с использованием терминалов спутниковой связи Starlink в условиях настроенных терминалов.

Для практической проверки указанного метода следует осуществить следующее. Настроить терминалы с помощью программного обеспечения

Starlink (программное обеспечение отчитается об успешном соединении и установлении доступа к сети Интернет).

Проверить скорость передачи данных терминалов спутниковой связи Starlink, например с использованием веб-интерфейса **«Speedtest»** по ссылке: https://www.speedtest.net/(рис. 2.6).

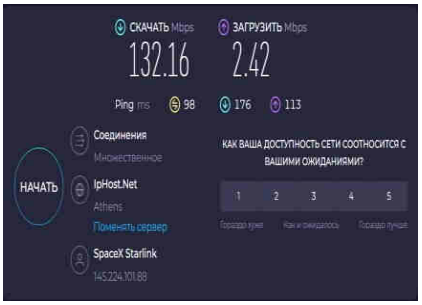

Рисунок 2.6 - Пример показателей скорости передачи данных терминалов спутниковой связи Starlink при воздействии средств РЭБ в условиях настроенных терминалов

2.2.2. Осуществить подключение к сети Интернет терминалов спутниковой связи Starlink под воздействием средств РЭБ из производного положения в условиях полной настройки.

Для практической проверки указанного метода следует осуществить следующее.

Аналогичным образом настроить терминалы с помощью программного обеспечения Starlink, а также проверить скорость передачи данных терминалов (рис. 2.4).

Если подключение к сети Интернет невозможно программное обеспечение Starlink отчитается, пример приведен на рис. 2.7.

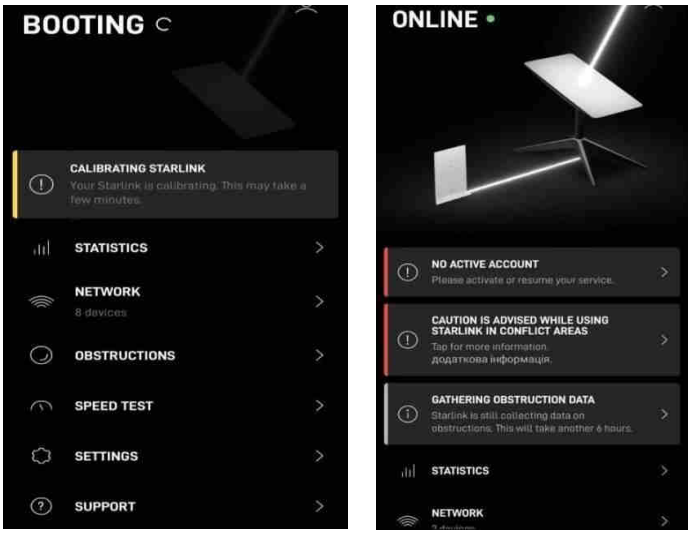

Рисунок 2.7 - Пример сообщения программного обеспечения Starlink о невозможности подключения к сети Интернет

Вывод:

В условиях успешного соединения и установки доступа к сети Интернет программное обеспечение во вкладке измерения скорости передачи данных «**Speedtest**» показывает реальную скорость передачи данных, как приведено на рис 2.6 (пример полученных измеренных параметров приведен в таблице 2.2).

Таблица 2.2

Результаты проверки функционирования терминалов спутниковой связи Starlink под влиянием средств РЭБ в условиях настроенных терминалов

№ з/п	Версия терминала	Скорость нисходящая (Download), Мбит/сек	Скорость выходная (Upload), Мбит/сек	Время задержки (Ping), мсек
1.	1 поколение	132.16 Мбит/сек	2.42 Мбит/сек	98 мсек
2.	2 поколения	30.23 Мбит/сек	7.89 Мбит/сек	115 мсек

Если не произойдет соединение с сетью Интернет программное обеспечение отчитается о невозможности подключения к сети Интернет.

Использование табличной формы обобщения и представления данных позволит в удобном виде сравнить полученные результаты, например оценить влияние РЭБ, или оценить метод защиты от РЭБ по сравнению, и тому подобное.

2.3. Практические рекомендации по защите терминалов спутниковой связи Starlink от воздействия средств РЭБ с использованием метода углубления в землю

Для защиты терминалов спутниковой связи Starlink от воздействия средств РЭБ целесообразно использовать метод углубления в землю по схеме, приведенной на рис. 2.8.

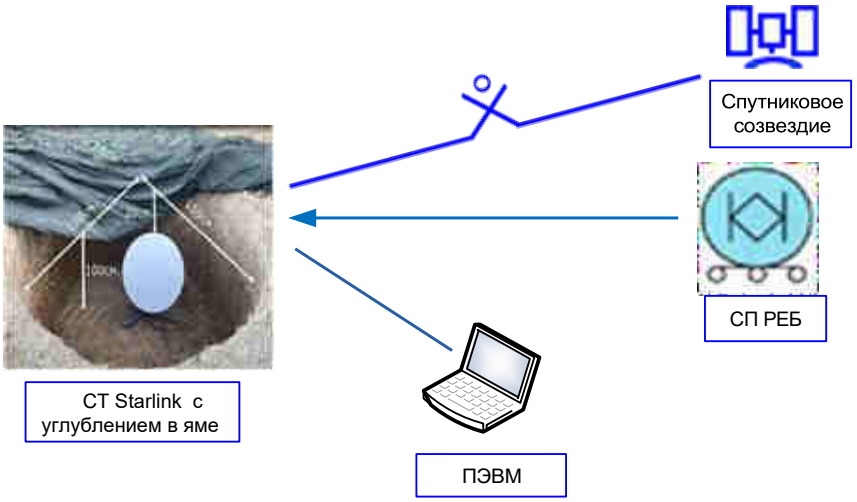

Рисунок 2.8 - Схема организации доступа к сети Интернет с использованием терминалов спутниковой связи Starlink с защитой от воздействия средств РЭБ методом углубления в землю

Образец развернутых терминалов спутниковой связи Starlink, защищенных от воздействия средств РЭБ методом углубления в землю, приведен на рис. 2.9.

Рисунок 2.9 - Пример развернутых терминалов спутниковой связи Starlink защищенных от воздействия средств РЭБ методом углубления в землю

При использовании метода углубления в землю терминалов спутниковой связи Starlink рекомендуется углублять их на глубину от поверхности земли на 1 метр и диаметром ямы 1,5 метра.

Для практической проверки указанного метода следует осуществить операции, приведенные в п.2.1 этих Рекомендаций (результаты приведены на рис. 2.10 и в табл. 2.3.)

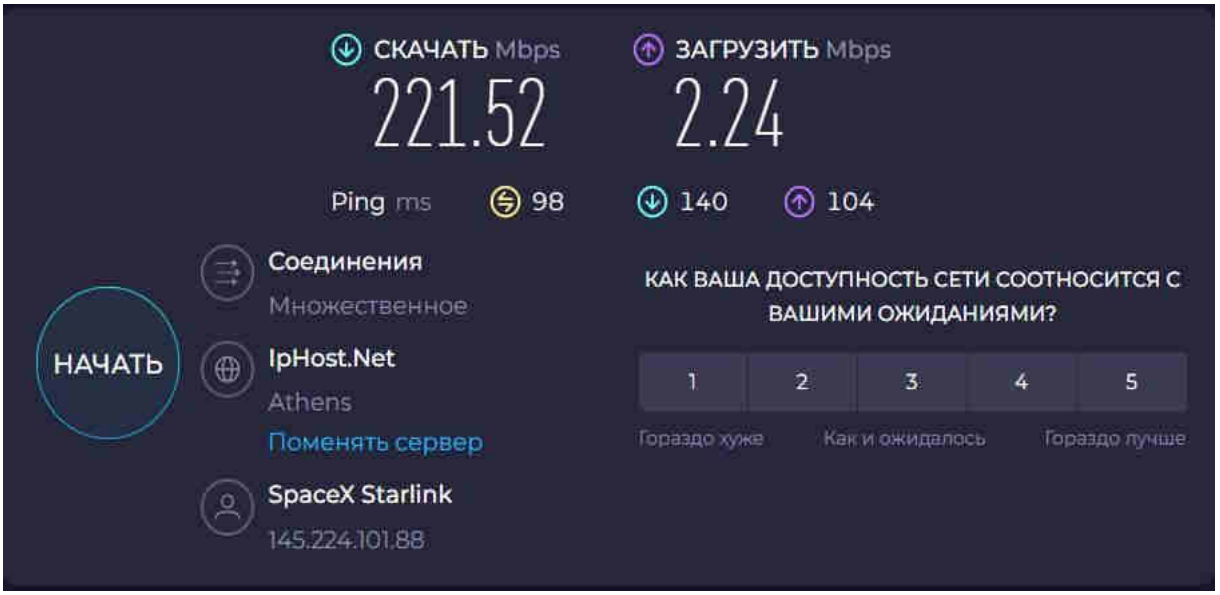

Рисунок 2.10 - Пример показателей скорости передачи данных терминалов спутниковой связи Starlink защищенных методом углубления в землю под воздействием средств РЭБ

Вывод: В условиях успешного соединения и установления доступа к сети Интернет терминалов спутниковой связи Starlink защищенных от воздействия средств РЭБ методом углубления в землю программное обеспечение во вкладке измерения скорости «**Speedtest**» показывает реальную скорость передачи данных, как приведено на рис 2.10. Время на установление связи и скорость передачи данных по сравнению с вариантом нахождения терминала Starlink на земле (без углубления) при этом не меняются. Результаты проверки приведены в таблице 2.3.

Таблица 2.3

Результаты проверки функционирования терминалов спутниковой связи Starlink защищенных методом углубления в землю под воздействием средств РЭБ

№ з/п	Версия терминала	Время настройки	Скорость нисходящая (Download), Мбит/сек	Скорость выходная (Upload), Мбит/сек	Время задержки (Ping), мсек
1.	1 поколение	5 мин.	221.52 Мбит/сек	2.24 Мбит/сек	98 мсек
2.	2 поколения	4 мин.	48.08 Мбит/сек	12.10 Мбит/сек	59 мсек

2.4. Практические рекомендации по защите терминалов спутниковой связи Starlink от воздействия средств РЭБ с использованием «клетки Фарадея»

Проверка защиты терминалов спутниковой связи Starlink от воздействия средств РЭБ с использованием метода защиты «клетки Фарадея» осуществлялась по схеме, приведенной на рис. 2.11.

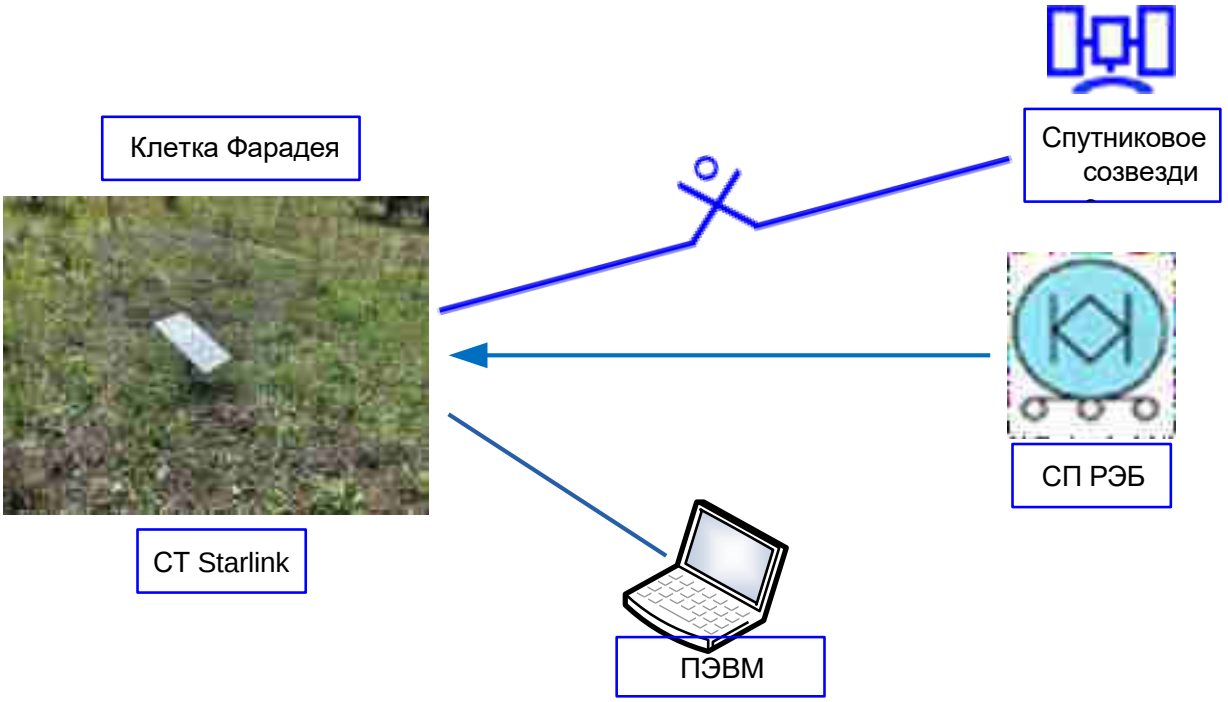

Рисунок 2.11 - Схема организации доступа к сети Интернет с использованием терминалов спутниковой связи Starlink, защищенных «клеткой Фарадея», во время воздействия

средств РЭБ

При использовании терминалов спутниковой связи Starlink защищенных «клеткой Фарадея» во время воздействия средствами РЭБ следует заметить, что накрывать дополнительно сеткой сверху **не нужно!**

В качестве «клетки Фарадея» рекомендуется использовать стальные сетки для армирования с размером ячейки от 2 см до 6 см. Внешний вид таких сеток, как пример, приведен на рис. 2.12.

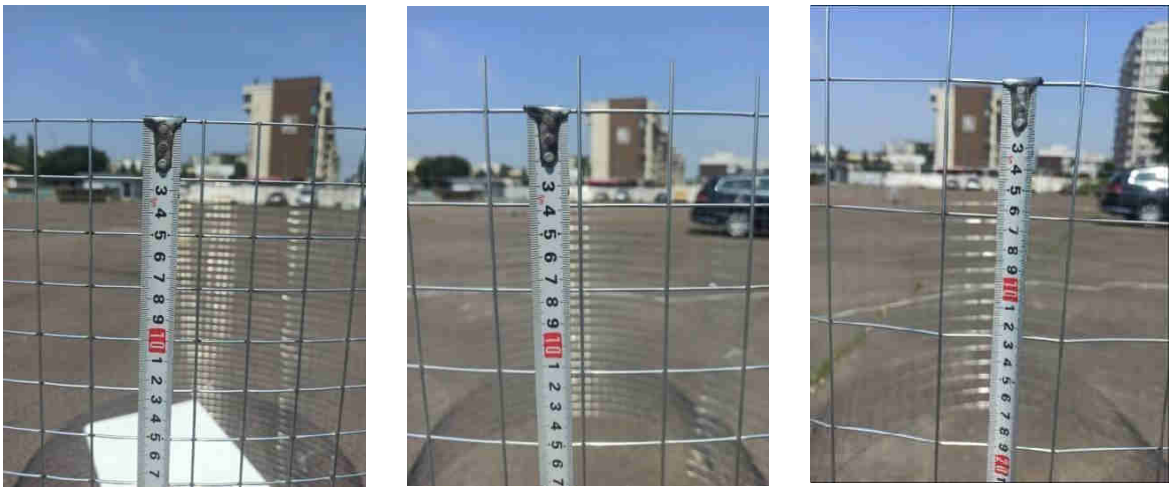

Рисунок 2.12 - Пример сетки с размером глазка 2.5х2.5 см, 3.5х3.5 см и 6х6 см

Рекомендуемые размеры «Клетки Фарадея» с диаметром окружности от 110 см до 120 см, высота - 120 см (пример приведен на рис. 2.13).

Рисунок 2.13 - Пример «клетки Фарадея» с диаметром окружности от 110 см до 120 см

2.4.1. Внешний вид терминалов спутниковой связи Starlink защищенных «клетками Фарадея» в один слой сеткой для армирования с размером ячейки 2.5х2.5, 3.5х3.5 и 6х6 см, приведен на рис. 2.14.

Рисунок 2.14 - Терминалы спутниковой связи Starlink защищенных «клетками Фарадея» в один слой сеткой для армирования с размером ячейки 2.5х2.5, 3.5х3.5 и 6х6 см

После осуществления защиты, следует настроить терминалы и проверить их работоспособность по приведенному выше порядку. Примеры результатов измерений приведены на рис. 2.14.

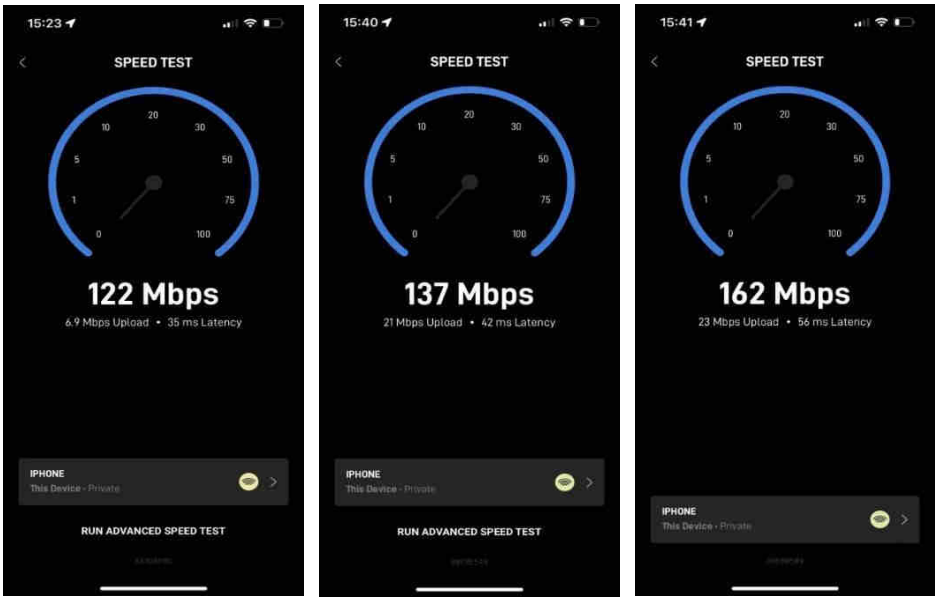

Рисунок 2.14 - Пример показателей скорости передачи данных терминалов спутниковой связи Starlink при настройке защищенных «клеткой Фарадея» с размером ячейки 2.5х2.5, 3.5х3.5 и 6х6 см под воздействием средств РЭБ

2.4.2. Терминалы спутниковой связи Starlink защищены «клеткой Фарадея» в три слоя сеткой для армирования, приведены на рис. 2.15.

Рисунок 2.15 - Терминал спутниковой связи Starlink защищен "клеткой Фарадея" в три слоя

После осуществления защиты, следует настроить терминалы и проверить их работоспособность по приведенному выше порядку. Примеры результатов измерений приведены на рис. 2.16.

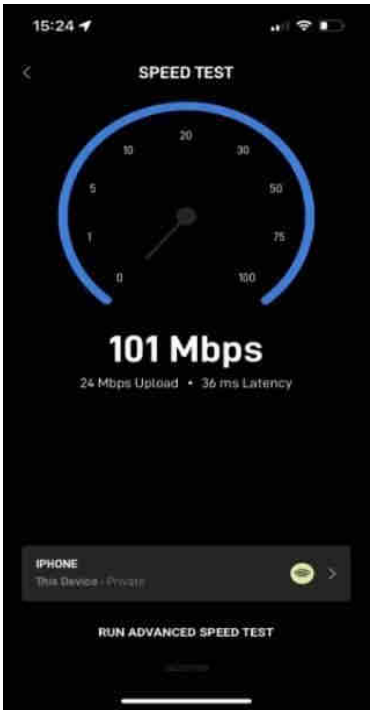

Рисунок 2.16 - Пример показателей скорости передачи данных терминалов спутниковой связи Starlink защищенных «клеткой Фарадея» в три слоя под воздействием средств РЭБ

Вывод: В условиях успешного соединения и установления доступа к сети Интернет терминалов спутниковой связи Starlink защищенных методом «клетки Фарадея» (сеткой в один слой с разными размерами ячейки 2.5х2.5, 3.5х3.5, 6х6 см и в три слоя клетки) под воздействием средств РЭБ время настройка увеличилась, что указано в таблице 2.4.

Таблица 2.4

Результаты проверки функционирования терминалов спутниковой связи Starlink под воздействием средствами РЭБ защищенных методом «клетки Фарадея»

№ з/п	Размер ячейки клетки Фарадея	Время настройки	Скорость нисходящая (Download), Мбит/сек	Скорость выходная (Upload), Мбит/сек	Время задержки (Ping), мсек
1.	2.5х2.5 см	32 мин.	122 Мбит/сек	6.9 Мбит/сек	35 мсек
2.	3.5х3.5 см	35 мин.	137 Мбит/сек	21 Мбит/сек	42 мсек
3.	6х6 см	39 мин.	162 Мбит/сек	23 Мбит/сек	56 мсек
4.	три слоя клетки	12 мин.	101 Мбит/сек	24 Мбит/сек	36 мсек

2.5. Практические рекомендации по защите терминалов спутниковой связи Starlink от воздействия средств РЭБ программным методом (выключение приемника GPS)

Для выключения приемника GPS в терминалах спутниковой связи Starlink необходимо обновить прошивку до версии **560a41f3-aa2d-4337-aef7-deb503a48130/uterm.release** (обновляется автоматически при каждом новом подключении к сети Интернет); в настройках терминала зайти на вкладу **DEBUG DATA** и в разделе **starlink location** выключить вкладку **Use Starlink**

Positioning Exclusively, которая выключает работу модуля GPS программным методом (рис. 2.18).

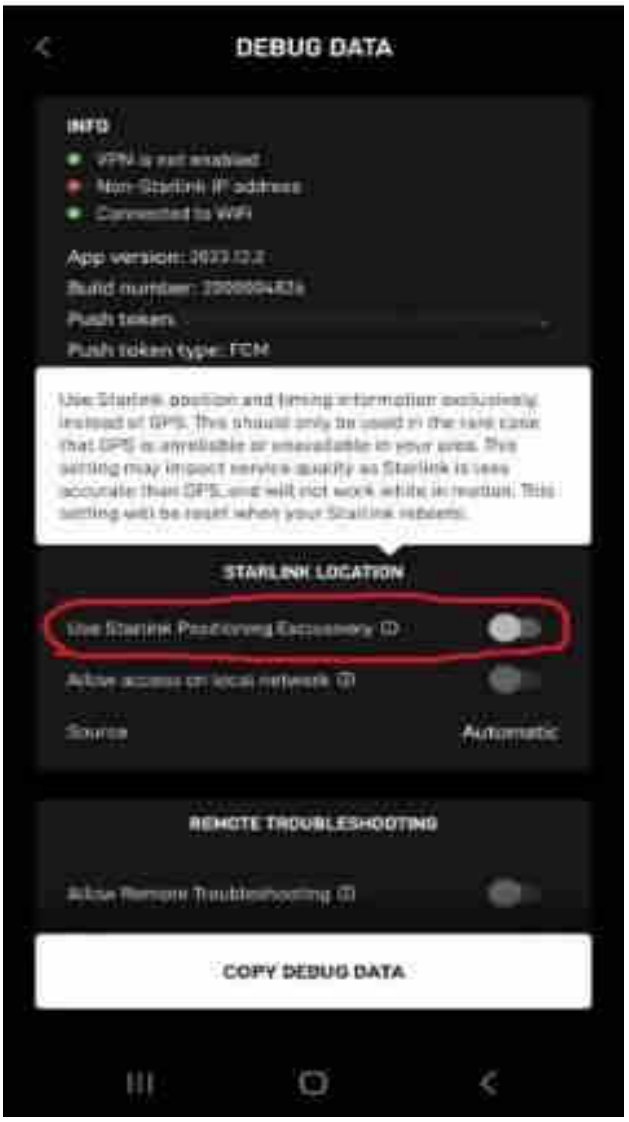

Рисунок 2.18 - Вкладка отключения модуля GPS программным методом

Для практической проверки указанного метода следует настроить терминал по приведенной выше методике и оценить скорость передачи данных терминалов спутниковой связи Starlink с использованием веб-интерфейса «**Speedtest**» в программном обеспечении Starlink (пример приведен на рис. 2.19).

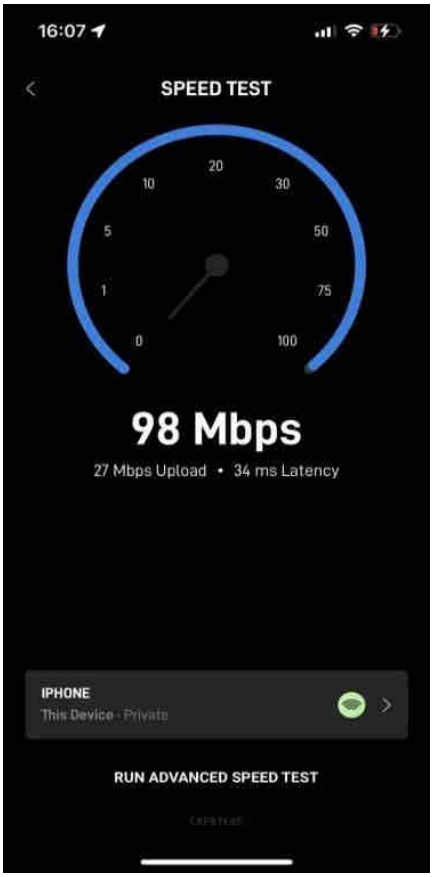

Рисунок 2.19 - Показатели передачи данных терминалов спутниковой связи Starlink с выключенным модулем GPS программным методом под воздействием средств РЭБ

Вывод: В условиях успешного соединения и установления доступа к сети Интернет терминалов под влиянием средств РЭБ, отключение модуля GPS программным методом позволяет эффективно защищать терминалы спутниковой связи Starlink (результаты измерений приведены в таблице 2.4).

Таблица 2.4

Результаты проверки функционирования терминалов спутниковой связи Starlink под воздействием средств РЭБ с выключенным модулем GPS программным методом

Время настройки	Скорость нисходящая (Download), Мбит/сек	Скорость выходная (Upload), Мбит/сек	Время задержки (Ping), мсек
2 мин.	98 Мбит/сек	27 Мбит/сек	34 мсек

3. ВЫВОДЫ И РЕКОМЕНДАЦИИ

По результатам практической апробации организационно-технических мероприятий по защите терминалов спутниковой связи Starlink от воздействия средств РЭБ следует отметить следующее.

Максимально негативно (до отсутствия связи) средства РЭБ влияют на спутниковые терминалы Starlink только во время настройки и подготовки к работе с производного положения (в том числе при первой настройке и развертывании).

Использование основных методов защиты, таких как углубление в землю, использование «клетки Фарадея» и отключением модуля GPS программным способом в качестве защиты от воздействия средств РЭБ оказалось эффективным.

Таким образом, для обеспечения эффективного противодействия средствам РЭБ, с целью минимизации радиоэлектронного воздействия на терминалы Starlink, **рекомендуется** использовать**:**

метод программного отключения модуля GPS, в соответствии с пунктом 2.5 раздела 2 этих Методических рекомендаций;

метод углубления терминалов спутниковой связи Starlink в землю на глубину от поверхности земли на 1 метр и диаметром ямы 1,5 м, в соответствии с пунктом 2.3 раздела 2 этих Методических рекомендации. Также целесообразным является использование природных укрытий - низины, ямы, котловины, оврага, воронки и т.д.;

метод «клетки Фарадея» с размером глазка от 2 до 6 см, диаметром в окружности от 110 до 120 см и высотой сетки 120 см. При этом для более действенной защиты рекомендуется использовать клетку в 3-4 слоя, в соответствии с пунктом 2.4 раздела 2 этих Методических рекомендации.

В то же время не следует недооценивать противника, который в перспективе будет искать новые организационные и технические способы эффективно воздействовать средствами РЭБ на терминалы спутниковой связи. Поэтому полученный практический опыт, а также теоретическое понимание физических явлений воздействия средств РЭБ противника, является основой для постоянного совершенствования известных и поиска новых методов защиты средств спутниковой связи от негативного радиоэлектронного воздействия.

Следует также отметить, что защита от РЭБ противника не является «чисто проблемой связистов». С использованием приведенных Методических рекомендаций, в случае выявления значительного ухудшения качества связи (уменьшения скорости передачи данных), специалистам подразделения связи следует не только принять меры по защите от негативного воздействия, но и немедленно доложить о выявленном факте возможного использования средств РЭБ противника. Предоставление такого доклада позволит своевременно обнаружить и обезвредить средства РЭБ противника, а в будущем - уменьшить вероятность их использования в районе выполнения задач по связи.