ИСПОЛЬЗОВАНИЕ БЕСПРОВОДНЫХ СЕТЕЙ В УСЛОВИЯХ ВОЕННЫХ КОНФЛИКТОВ

Бабич Н.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Вершило Д.Н. – старший преподаватель кафедры ТиОП

Аннотация. В статье рассматривается применение беспроводных сетей в военных конфликтах и связанные с этим проблемы безопасности. Обсуждаются меры по минимизации рисков обнаружения сетей противником, такие как контроль устройств, размещение роутеров в безопасных местах и использование специальных чехлов для защиты от радиоэлектронной разведки. Также предложены методы обеспечения безопасности передачи информации через беспроводные сети, включая использование нейтральных названий сетей, регулярную смену SSID и паролей. Обсуждаются различия между установлением соединения по Wi-Fi и обнаружением источника сигнала, а также эволюция технологий Wi-Fi и их применение в современных военных конфликтах.

В военных конфликтах тактические беспроводные сети широко используются для обмена информацией между развернутыми подразделениями.

Большинство беспроводных сетей работают в условиях возможного контроля противника. В связи с этим организации функционирования беспроводных сетей предъявляются повышенные требования к безопасности и возможности определения пользователей.

В данной статье приведены возникающие проблемы и основные тенденции развития беспроводных сетей на основе специальной военной операции проводимой Российской Федерацией.

Современные беспилотные летательные аппараты (БПЛА), оборудованные системами радиоэлектронной разведки, обнаруживают активный роутер на расстоянии, превышающем 10 000 метров. С поверхности земли терминалы спутниковой связи Starlink практически невозможно определить на расстоянии, превышающем 3000 метров [1].

Системы радиоэлектронной разведки противника может определить ваши позиции без БПЛА при помощи концентрации радиоэлектромагнитного излучения. Исключить данный фактор возможно при полном отказе от Wi-Fi.

В связи с этим необходимо минимизировать риски, а также уменьшить вероятность и расстояние обнаружения вашей Wi-Fi сети. Для этого необходимо соблюдать следующие правила:

контролируйте свои устройства и выключайте всё, что вы не можете контролировать. Каждый должен знать, как и выключить смартфон или смарт-часы (или хотя бы перевести их в режим «авиаполет»). Определите, какие устройства имеют неконтролируемый вами Wi-Fi модуль и выключайте их полностью при необходимости. Используйте чехлы для планшетов и телефонов с «сеткой Фарадея» (см. рисунок 1).

Рисунок 1 – Пример использования сетки Фарадея

- определите безопасные, закрытые места для размещения ваших роутеров, точек доступа и других передатчиков Wi-Fi, чтобы минимизировать возможность приема их сигналов в воздухе и на уровне земли. Рекомендуется выполнять установление соединения в непосредственной близости устройств. Поверхность земли – оптимальный экран для излучения. При возможности используйте проводное подключение вместо Wi-Fi.

- контролируйте с помощью специальных приборов излучения исходящие с ваших позиций. При отсутствии данной возможности применяйте простые Wi-Fi сканеры для смартфонов или ПК. Даже при использовании режима «скрытая сеть» (Hidden SSID) — это не уменьшает риск обнаружения системами радиоэлектронной разведки противника.

Также определим основные требования, обеспечивающие безопасность и надежность передачи информации посредством беспроводных сетей:

- применяйте название сетей не позволяющие вас идентифицировать, т.е. название (SSID), которое не содержащее специальной терминологии (АРТА, POST и т.д.), рекомендуется устанавливать нейтральные названия. Всегда используйте для Wi-Fi сети сложный пароль/ключ, что значительно усложнит возможность подбора пароля противником.

- установите правила переименования Wi-Fi сетей – по возможности меняйте название сети (SSID) и пароль при еженедельно, при смене позиций и т.д.

Основными ошибками, позволяющими противнику определять места расположения позиций, является, установление локаций любых источников Wi-Fi средствами радиоэлектронной разведки. Источниками сигнала Wi-Fi может быть не только точка доступа Wi-Fi (AP) или маршрутизатор Wi-Fi, но и компьютер, смартфон, умные часы, БПЛА, пульт управления БПЛА, умная колонка и другие устройства и т.д.

Существует большая разница между установлением соединения по Wi-Fi и обнаружением источника сигнала. Для установления соединения дистанция должна быть относительно незначительной. При незначительной мощности клиента, парный прибор определяет сигнал, но не может "дозвониться" до приемника точки доступа. Но это вовсе не означает, что сигнал источника невозможно "определить" на значительно большем расстоянии.

Технологии Wi-Fi прошли определенную эволюцию, и современные 802.11 ac/ax или даже 802.11 n имеют очень низкую мощность, а их сигналы на частоте 2,4 ГГц и тем более 5 ГГц затухают очень быстро на небольшом расстоянии. Необходимо учитывать, что большинство обычных БПЛА также работают по Wi-Fi данных стандартов. И они могут летать на довольно большое расстояние в условиях прямой видимости между антенной пульта и антенной БПЛА. Однако подавляющее большинство Wi-Fi модулей в современных устройствах имеет встроенную поддержку стандартов 802.11 a/b/g, которые предусматривают значительно большую мощность излучения, и данные режимы активируются автоматически.

В современных военных конфликтах практически невозможно исключить использование беспроводных сетей. В связи с этим возникает необходимость «культуры» применения систем таких как Wi- Fi, что позволит выполнить задачи подразделений, но и самое главное обезопасить личный состав подразделений [2].

С точки зрения безопасности данных, критическим моментом является защита информации от несанкционированного доступа. В контексте военных операций, утечка или перехват информации может иметь катастрофические последствия. Поэтому помимо технических мер безопасности, важно также обеспечить обучение и подготовку персонала к соблюдению правил безопасности информации.

Интеграция криптографических методов защиты данных может значительно усилить безопасность беспроводных сетей. Использование современных алгоритмов шифрования и протоколов аутентификации позволит обеспечить конфиденциальность и целостность передаваемой информации. Кроме того, регулярное обновление и адаптация защитных мер помогут противостоять появляющимся угрозам и уязвимостям.

С целью минимизации вероятности обнаружения сети противником, следует также уделить внимание использованию специализированных средств для скрытия и поддержания анонимности передаваемой информации. Применение технологий, основанных на принципах стеганографии и анонимизации данных, позволит сделать обнаружение сети более сложным для потенциального противника.

Таким образом, эффективное сочетание технических, организационных и криптографических мер безопасности позволит обеспечить защиту беспроводных сетей в условиях военных конфликтов и повысить уровень безопасности передаваемой информации.

Список использованных источников

1. Иванов, А.П. "Современные тенденции развития беспроводных сетей в военных операциях" // Вестник Военной Академии. - № 3 (2022). - с. 76-88. – *2016.*

2. Министерство обороны Российской Федерации. Официальный сайт.