Ефимов Андрей Валерьевич, магистрант
ВАС им. С.М. Буденного

Федоров Вадим Геннадиевич
ВАС им. С.М. Буденного

Марусин Александр Сергеевич, магистрант
ВАС им. С.М. Буденного

Федорова Светлана Викторовна,
к.т.н., преподаватель
ВАС им. С.М. Буденного

ЗАЩИТА ОБЪЕКТОВ СВЯЗИ ОТ ИНОСТРАННОЙ РАДИОРАЗВЕДКИ

Аннотация. В данной статье рассматриваются варианты защиты объектов связи от иностранной радиоразведки в современных условиях

Ключевые слова: Радиоразведка, радиомаскировка, защита объектов связи, методы защиты

Защита объектов связи от иностранной радиоразведки требует комплексного подхода, сочетающего как организационные, так и технические мероприятия. Одним из важнейших аспектов является маскировка компонентов системы связи, что позволяет сокрыть информацию о действиях и группировках войск. Этот метод включает в себя использование различных способов, например, укрытие антенн и радиостанций под природными или искусственными укрытиями, что затрудняет их обнаружение.

Технические средства в этой области включают радиомаскировку, где используются различные технологии для дезориентации противника относительно реального положения войск. Это достигается посредством создания ложных радиосигналов или имитации работы радиосредств. Применение направленных антенн также значительно снижает радио заметность, направляя сигнал в заданный сектор. Кроме того, работа с минимальной мощностью позволяет уменьшить вероятность перехвата радиосигналов, делая их менее заметными для средств радиоразведки.

Шифрование информации остается одним из ключевых методов защиты. Использование современных алгоритмов шифрования и кодов переписки защищает передаваемую информацию от несанкционированного доступа и перехвата [1]. Важно отметить, что каждый из этих методов должен быть частью интегрированной модели защиты, которая включает как организационные, так и технические мероприятия.

Контроль соблюдения режимов связи и обучение личного состава играют важную роль в предотвращении утечек информации. Обучение и повышение квалификации офицеров и связистов способствует их готовности к нештатным ситуациям и повышает общую безопасность системы связи [2]. Выявление источников перехвата также позволяет оперативно устранять угрозы, обнаруживая и нейтрализуя устройства, применяемые противником.

Сокращение времени работы радиосредств на излучение является дополнительной стратегией, позволяющей минимизировать окно уязвимости. Создание ложных радиосетей может значительно дезориентировать противника, что может привести к ошибочным выводам о реальной активности группы. В итоге, одной из наиболее эффективных стратегий оказывается скоординированное применение этих подходов, что позволяет существенно повысить уровень защиты объектов связи от иностранной радиоразведки.

Недостатки существующих методов

Сложности в защите объектов связи от иностранной радиоразведки коренятся в недостатках существующих методов. Один из основных недостатков заключается в том, что абсолютная надежность систем защиты недостижима. Постоянное развитие технологий позволяет злоумышленникам находить уязвимости, которые могут привести к компрометации данных. Это требует регулярного обновления и улучшения защитных мер [2].

Также следует отметить, что ошибки персонала играют значительную роль в обеспечении безопасности. Даже самые современные и надежные системы защиты могут быть подвержены неосторожным действиям пользователей. Легкомысленное отношение к вопросам безопасности зачастую приводит к нарушениям, что существенно ухудшает общую надежность системы [2]. Отсутствие должной культуры безопасности среди персонала может стать причиной утечек информации и, как следствие, успешных атак со стороны злоумышленников.

Дополнительной проблемой является сложность реализации существующих методов защиты. Внедрение комплексных систем, таких как криптографические решения или программно-аппаратные средства, требует значительных финансовых, временных и человеческих ресурсов. Это делает такие методы менее доступными и их использование может быть ограничено для организаций с ограниченным бюджетом.

Технологические инновации создают зависимость от наиболее актуальных решений, которые могут быстро устаревать. На фоне быстрого прогресса в области радиоразведки это делает традиционные методы защиты менее эффективными. Важно осознавать, что новые угрозы возникают одновременно с появлением новых технологий, и для защиты необходимо постоянное обновление систем.

Проблемы с интеграцией различных методов защиты также снижают общую эффективность системы. Из-за разнообразия подходов и средств возникают трудности в их совместной реализации, что может привести к образованию слабых мест в инфраструктуре защиты [3].

Все эти недостатки демонстрируют необходимость в разработке новых решений, которые будут способствовать более комплексной защите объектов связи от иностранных угроз. Устранение существующих пробелов и недостатков поможет создать более устойчивую к атакам систему, что в конечном счете повысит уровень безопасности.

Рекомендации по маскировке компонентов

Маскировка компонентов систем связи является важным элементом защиты от иностранных средств радиоразведки. Для эффективной реализации маскировки предлагается ряд конкретных методов, которые могут интегрироваться в существующие системы защиты.

Одним из современных решений является комплекс маскировки «Павлин», который разработан российской оборонной промышленностью. Он позволяет скрыть реальное местоположение объектов связи, используя переносные терминалы и оптоволоконные соединения для размещения компонентов на безопасном расстоянии от уязвимых позиций. Прототипы комплекса успешно прошли испытания и получили положительные отзывы, что подтверждает его практическую эффективность [3]. Это решение не только маскирует объекты, но и дезинформирует противника при помощи перемещаемых терминалов, которые сложно обнаружить.

Кроме этого, для маскировки компонент можно использовать методы изменения структуры сетей, например, применение различных передатчиков и маршрутизаторов для повышения скрытости связи. Это включает создание модулированных сигналов, которые переносятся через несколько сетевых узлов, что затрудняет определение истинного местоположения и характера общения системы [2]. Высокий уровень профессиональной подготовки персонала, ответственного за реализацию данной технологии, также играет важную роль в успешности маскировки.

Особое внимание стоит уделить физической маскировке объектов инфраструктуры связи. Маскировка может включать использование элементов ландшафта, таких как деревья или скалы, для скрытия антенн и радиопередатчиков. Варианты маскировки могут варьироваться от простых до сложных конструкций, и применять такие элементы необходимо с учетом эстетики и окружающей среды [2].

Кроме того, подход к повышению скрытности может включать в себя перестройку конфигурации систем связи путем внедрения элементов, которые сложно идентифицировать. Например, создание «ложных» узлов, которые имитируют настоящие каналы, может запутать вражеские разведывательные средства и уменьшить шансы на успешное перехват.

Таким образом, реализация этих методов требует не только применения технических решений, но также участия квалифицированного персонала, который сможет обеспечить эффективность мероприятий по маскировке систем связи и адаптировать их под реальную оперативную обстановку.

Список литературы:

1. Пермяков А. С., Лепешкин О. М., Кудрявцев А. М., Остроумов О. А. Подход к повышению скрытности системы телекоммуникационной связи от технической компьютерной разведки – Известия Тульского государственного университета. Технические науки. 2021. №10. URL: https://cyberleninka.ru/article/n/podhod-k-povysheniyu-skrytnosti-sistemy-telekommunikatsionnoy-svyazi-ot-tehnicheskoy-kompyuternoy-razvedki.

2. Методы защиты радиосигналов от перехвата техническими.. [Электронный ресурс] – Режим доступа: https://spravochnick.ru/informacionnaya_bezopasnost/metody_zaschity_radiosignalov_ot_perehvata_tehnicheskimi_sredstvami_razvedok.

3. Стародубцев Ю. И., Липатников В. А., Парфиров В. А. Проблема повышения разведывательной защищенности элементов военной системы связи – Военная мысль. 2023. №7. URL: https://cyberleninka.ru/article/n/problema-povysheniya-razvedyvatelnoy-zaschischennosti-elementov-voennoy-sistemy-svyazi.