Научная статья
УДК 001.891.57

СПОСОБЫ ПРОТИВОДЕЙСТВИЯ НЕСАНКЦИОНИРОВАННОМУ ВОЗДЕЙСТВИЮ НА ЭЛЕКТРОМАГНИТНЫЕ ПОЛЯ

Павел Олегович Гончаров[1], Александр Витальевич Лубенцов[2]
[1, 2] Воронежский институт ФСИН России, Воронеж, Россия
[1] pavi992@yandex.ru
[2] lubensov@mail.ru

Аннотация. В данной статье были рассмотрены способы противодействия несанкционированному воздействию на электромагнитные поля. Также были рассмотрены основные способы противодействия проникновению в радиоэфир.

Ключевые слова: воздействие, противодействие, радиосигнал, радиоэфир

Для цитирования: Гончаров П. О., Лубенцов А. В. Способы противодействия несанкционированному воздействию на электромагнитные поля // Научное творчество молодежи – лесному комплексу России = Scientific creativity of youth to the forest complex of Russia : материалы XXI Всероссийской (национальной) научно-технической конференции студентов и аспирантов. Екатеринбург : УГЛТУ, 2025. С. 553−557.

Original article

METHODS OF COUNTERING UNAUTHORIZED EXPOSURE TO ELECTROMAGNETIC FIELDS

Pavel O. Goncharov[1], Alexander V. Lubentsov[2]
[1, 2] Voronezh Institute of the Federal Penitentiary Service of Russia, Voronezh, Russia
[1] pavi992@yandex.ru
[2] lubensov@mail.ru

Abstract. We have considered ways to counteract unauthorized exposure to electromagnetic fields in this article. The main ways to counteract penetration into the radio airwaves were also considered.

Keywords: impact, counteraction, radio signal, radio broadcast

***For citation**:* Goncharov P. O., Lubentsov A. V. (2025) Sposoby protivodejstviya nesankcionirovannomu vozdejstviyu na elektromagnitnye polya [Methods of countering unauthorized exposure to electromagnetic fields]. Nauchnoe tvorchestvo molodezhi – lesnomu kompleksu Rossii [Scientific creativity of youth to the forest complex of Russia] : proceedings of the XXI All-Russian (national) Scientific and Technical Conference of undergraduate and postgraduate students. Ekaterinburg : USFEU, 2025. Pp. 553–557. (In Russ).

Радиотехнические системы в настоящее время занимают важное место в обеспечении надежности и эффективного функционирования различного рода предприятий. Эти системы применяются для организации связи между сотрудниками, а также для контроля управления доступом. На сегодняшний день внедрение радиотехнических систем может столкнуться с рядом проблем, связанных с несанкционированным воздействием на электромагнитные поля. Такое воздействие способно повредить работу систем, привести к утечкам конфиденциальной информации и даже создать угрозу для безопасности всей уголовно-исполнительной системы.

Существует множество методов незаконного воздействия на радиосистемы учреждений и предприятий. Одним из этих методов является перехват радиосигнала, при этом злоумышленники могут попытаться получить информацию, передающуюся через радиоканалы, с целью доступа к конфиденциальным данным или удаленного управления системами обеспечения связи или интегрированными системами безопасности.

Введение помех в радиоэфир способно нарушить функционирование систем связи, слежения и управления, снижая их эффективность. Важно помнить, что злоумышленники могут пытаться фальсифицировать сигналы, чтобы обойти системы безопасности, проникнуть в охраняемые зоны или взять под контроль устройства удаленно. Незаконное вмешательство в программное обеспечение РТС может использоваться для изменения его работы, кражи конфиденциальных данных или несанкционированного управления системами, минуя установленные протоколы. Наиболее серьезным риском остается прямое физическое воздействие на оборудование РТС (радиотехническая станция), которое может привести к его поломке или полной утрате работоспособности [1].

Для противодействия всем этим угрозам необходимо применять комплексный подход, который включает в себя:

1. Физическую защиту, которая состоит в защите оборудования РТС посредством монтажа охранных ограждений, установки камер видеонаблюдения, систем контроля доступа, а также размещения оборудования в специально защищенных помещениях.

2. Криптография, т. е. применение современных алгоритмов шифрования для защиты передаваемой информации от перехвата и дешифровки.

3. Специальные виды антенн. Использование антенн с узкой диаграммой направленности (рис. 1), направленных только на приемники, чтобы минимизировать возможность перехвата сигнала и снизить уязвимость систем к помехам [2].

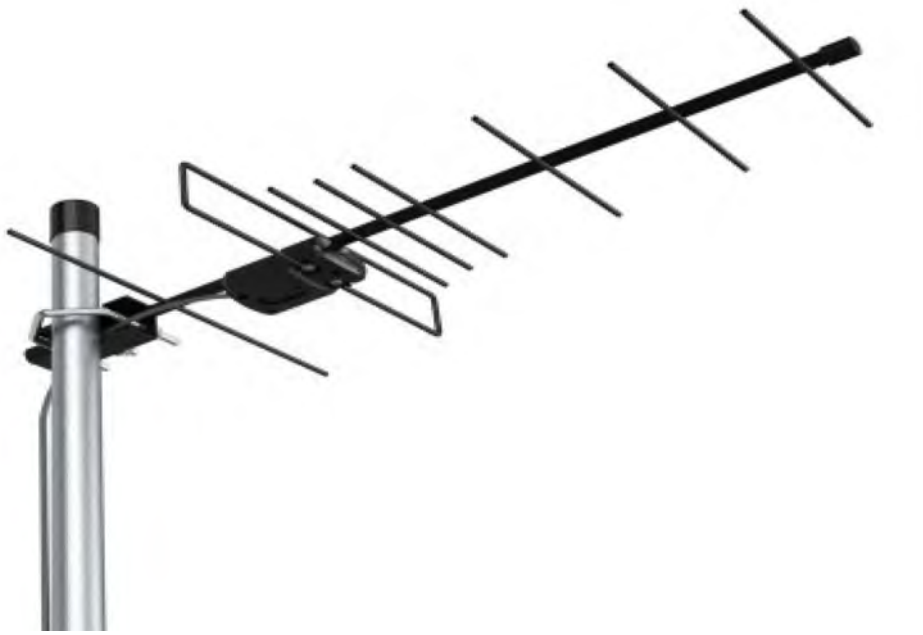

Рис. 1. Узконаправленная антенна

4. Подавление помех, т. е. применение специальных фильтров (рис. 2) и систем подавления помех для минимизации влияния внешних источников помех на работу РТС [2].

Рис. 2. Фильтр фм помех

5. Обнаружение и предотвращение атак. Использование систем обнаружения и предотвращения атак, которые способны идентифицировать несанкционированные попытки доступа к системам и блокировать их, а также анализировать трафик и выявлять подозрительные действия.

6. Обучение персонала и проведение систематических курсов по вопросам безопасности и защиты РТС для персонала, чтобы повысить осведомленность о существующих угрозах и правилах безопасной эксплуатации систем.

7. Проведение регулярных аудитов безопасности РТС для выявления уязвимостей и слабых мест системы, а также для своевременного внедрения необходимых мер по их устранению.

8. Применение технологий «интернета вещей» (IoT). Использование IoT для создания более защищенных и интеллектуальных систем, которые способны отслеживать свое состояние, обнаруживать аномалии и взаимодействовать с другими системами для улучшения безопасности.

9. Создание единой системы защиты РТС, которая включает в себя все вышеперечисленные элементы и обеспечивает комплексный подход к обеспечению безопасности систем на предприятии.

Защита от несанкционированного воздействия на РТС является одной из самых важных задач, требующей комплексного подхода, с учетом особенностей среды и угроз, с которыми она сталкивается. Применение современных технологий, системных решений и своевременное переобучение персонала позволит обеспечить надежную работу радиотехнических станций в УИС и создать более безопасную среду для сотрудников, осужденных и остальных людей.

В настоящее время необходимо уделить внимание разработке и внедрению единых стандартов безопасности для радиотехнических систем [3–7], которые будут учитывать специфику эксплуатации систем в данной среде. Своевременное внедрение современных систем мониторинга и анализа данных необходимо для обнаружения и предотвращения несанкционированного воздействия на РТС. Также необходимо создать специальное подразделение по защите РТС с высокой квалификацией и практическим опытом в области кибербезопасности и радиотехники. Постоянное обучение и повышение квалификации персонала в области безопасности РТС с использованием современных методов и технологий. Не стоит забывать о сотрудничестве с университетами и научными центрами для проведения исследований в области защиты РТС и разработки новых технологий и методов защиты.

Список источников

1. Струк П. В. Комплекс мер защиты от утечки по техническим каналам при обеспечении режима коммерческой тайны // Форум молодых ученых. 2019. №4 (32). URL: https://cyberleninka.ru/article/n/kompleks-mer-zaschity-ot-utechki-po-tehnicheskim-kanalam-pri-obespechenii-rezhima-kommercheskoy-tayny (дата обращения: 09.11.2024).

2. Ворона В. А. Способы и средства защиты информации от утечки по техническим каналам // Computational nanotechnology. URL: https://cyberleninka.ru/article/n/sposoby-i-sredstva-zaschity-informatsii-ot-utechki-po-tehnicheskim-kanalam (дата обращения: 22.09.2024).

3. Лубенцов А. В., Душкин А. В. Комплексные системы безопасности: системный анализ, архитектура, управление жизненным циклом. Воронеж: «Научная книга», 2022, 254 с.

4. Ворона В. А., Костенко В. О. Способы и средства защиты информации от утечки по техническим каналам // Computational nanotechnology. 2016. № 3. URL: https://cyberleninka.ru/article/n/sposoby-i-sredstva-zaschity-informatsii-ot-utechki-po-tehnicheskim-kanalam (дата обращения: 09.11.2024)

5. Лубенцов А. В., Власова А. И. Модель подавления канала мобильной связи шумоподобным сигналом // Молодежь и научно-технический прогресс : сборник докладов XVII Международной научно-практической конференции студентов, аспирантов и молодых ученых. В 2 т. Т. 1. Старый Оскол : Ассистент плюс, 2024. С. 103–108.