



ЭФФЕКТИВНЫЕ МЕТОДЫ ДЛЯ ОБНАРУЖЕНИЯ И ПОДАВЛЕНИЯ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ

В данной статье приводится анализ технологии радиозакладного устройства, представляющей устройство, эмулирующее их деятельность. Это устройство работает в диапазоне частот от 88 до 108 МГц, используя биполярный транзистор и электретный микрофон для амплитудной и частотной модуляции звуковых сигналов. Также производится разбор радиоподавляющего устройства, блокирующего радиосигналы и делающего радиозакладные устройства недоступными для прослушивания. Дополнительно в контексте современных требований безопасности рассмотрено устройство «индикатор поля» для обнаружения радиозакладных устройств в помещениях с оперативностью, высокой чувствительностью и способностью предупредить о потенциальных угрозах. Данные устройства были созданы и испытаны в реальных условиях. Приведенные графики и технические детали визуализируют разницу в мощности между сигналами радиоподавляющего и радиозакладного устройств, делая последнее недоступным для прослушивания.

Ключевые слова: индикатор поля, обнаружение радиозакладного устройства, подавление радиосигналов, радиоподавляющее устройство, радиопомехи, электромагнитное поле, эмуляция радиозакладного устройства.

Barankova I.I., Kuzmina U.V., Fedorova A.R., Kulevich Yu.Ya., Kazakov O.A.

EFFECTIVE METHODS FOR DETECTING AND SUPPRESSING RADIO- LAYING DEVICES

This article provides an analysis of the technology of a radio-laying device, representing a device that emulates their activities. This device operates in the frequency range from 88 to 108 MHz, using a bipolar transistor and an electret microphone for amplitude and frequency modu-

lation of audio signals. A radio suppression device is also being disassembled, blocking radio signals and making radio billboards inaccessible to listening. Additionally, in the context of modern security requirements, the device «field indicator» for detecting radio-laying devices in rooms with operability, high sensitivity and the ability to warn of potential threats is considered. These devices were created and tested in real conditions. The graphs and technical details below visualize the difference in power between the signals of a radio suppression and a radio alarm device, making the latter inaccessible to listening.

Keywords: field indicator, detection of a radio laying device, suppression of radio signals, radio suppressing device, radio interference, electromagnetic field, emulation of a radio laying device.

Введение

Радиосигналы представляют собой фундаментальный элемент для развертывания беспроводных коммуникаций, радиовещания и различных приложений в области связи. Однако, возникает также значимость их блокирования в ситуациях, требующих ограничения или прекращения их распространения. В данной статье рассматриваются три аспекта для повышения уровень безопасности в использовании беспроводных технологий: создание устройства, эмулирующего деятельность радиозакладного устройства (далее – ЭДРЗУ), радиоподавляющего устройства (далее – РПУ), а также устройства «индикатор поля».

Основной целью разработки ЭДРЗУ, является изучение способов эффективной защиты от подобного рода технических устройств. Для этого часто применяются два основных метода: подавление сигнала и обнаружение источника сигнала. Ниже описаны преимущества и недостатки каждого из этих методов.

Подавление сигнала представляет собой эффективный метод борьбы с РЗУ, так как он способен мгновенно мешать их работе, предотвращая передачу информации. Быстрая реакция делает этот метод подходящим для ситуаций, требующих моментального противодействия угрозе. Однако, использование средств подавления может нарушать законодательство о связи, а также вызывать коллатеральные повреждения, воздействуя на другие беспроводные устройства в районе применения.

С другой стороны, обнаружение источника сигнала обладает преимуществами точности и пассивности. Такие системы способны точно локализовывать и идентифицировать источники радиосигналов, а пассивный режим работы позволяет избежать создания дополнительных помех. Однако, этот метод имеет свои недостатки, такие как сложность

обнаружения, особенно если РЗУ скрыты или используют технические средства для избегания обнаружения. Кроме того, обнаружение может потребовать времени, что создает риск того, что злоумышленники успеют выполнить свои задачи до выявления [1].

Выбор между представленными методами зависит от конкретных условий и требований безопасности. В ряде случаев может быть эффективным использование комбинации обоих методов для обеспечения комплексной защиты от РЗУ.

Устройство, эмулирующее деятельность РЗУ

Для создания устройства, способного генерировать радиосигналы в середине УКВ ЧМ диапазона был выбран диапазон частот равный 88-108 МГц, так как сигналы данного диапазона можно поймать обычным радиоприемником, что в свою очередь облегчит этап тестирования устройств.

Принципиальная схема ЭДРЗУ на одном транзисторе представлена на рис. 1.

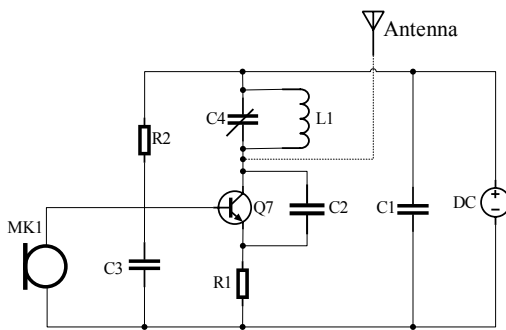


Рис. 1. Принципиальная схема ЭДРЗУ на одном транзисторе

Учитывая компоненты схемы, были использованы LC-генератор (L1, C4), построенный на основе биполярного транзистора Q7 типа 2N3904 и схема «ёмкостной, трёхточки». Данный генератор имеет возможность точечной настройки частоты вещания ЭДРЗУ с помощью переменной ёмкости конденсатора. В

то время как транзистор Q7 генерирует сигнал с заданной частотой.

Для достижения амплитудной и частотной модуляции сигнала звуковой информацией в создаваемом сигнале, использовался электретный микрофон МК1.

Резистор R2 и конденсатор C3, соединенные последовательно, выполняют роль RC-фильтра, который позволяет снизить уровень шума, поступающего с микрофона. Резистор R1 ограничивает ток, поступающий на транзистор Q7, обеспечивая его стабильную работу. Конденсатор C1, подключенный параллельно, способствует сглаживанию импульсов от источника питания, что также способствует повышению качества сигнала [2-3].

Перед сборкой схемы необходимо рассчитать мощность РЗУ, чтобы понимать эффективную дальность передачи, а также, чтобы оценить, насколько долго устройство может работать от автономного источника питания.

Номиналы компонентов выбираются таким образом, чтобы частота генерации составила около 90-100 МГц. Ниже представлены формулы для подбора номиналов компонентов.

Мощность рассчитывается по закону Ома для цепи постоянного тока:

$$P = V * I,$$

где P – мощность, V – напряжение, I – ток.

В соответствии с формулой приближительная мощность данного передатчика при питании от батарейки 9 В составляет примерно 0.27 Вт. Данную мощность необходимо перевести в децибел-милливатт:

$$dBm = 10 * \log_{10} \left(\frac{P}{1 \text{ мВт}} \right) = 24.31$$

Для правильной работы данной схемы требуется подключение антенны длиной 5-7 см, представленной в виде медной проволоки.

Катушка индуктивности в данной схеме состоит из 8 витков провода диаметром 0,5 мм, намотанных на оправке диаметром 6 мм.

Номиналы всех остальных элементов на схеме, следующие: C1 = 22 нФ, C2 = 4,7 пФ, C3 = 1 нФ, C4 = 10-40 пФ, R1 = 330 Ом, R2 = 4,7 кОм, DC = 3-9 В.

Все элементы кроме выключателя и батареи питания, монтируются на макетной плате. Смонтированная плата ЭДРЗУ показана на рис. 2.

ЭДРЗУ, собранное по схеме рисунка 1,

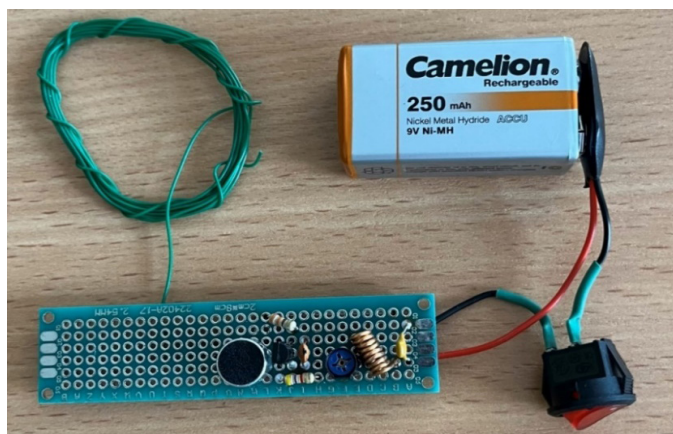


Рис. 2. Смонтированная плата ЭДРЗУ

должно вещать в FM диапазоне. Для определения частоты вещания радиопередатчика необходимо воспользоваться программно-аппаратным комплексом радиоконтроля «Кассандра С6» [4]. Для этого диапазон сканирования выставляется 90 – 100 МГц и фиксируется представленный результат (рис. 3).

В процессе использования ЭДРЗУ, все аудиосигналы, которые попадают на микрофон, автоматически транслируются на предварительно установленную частоту, как показано на представленном выше графике сканиро-

вания.

По результатам сканирования, представленного на рисунке 3, видно, что ЭДРЗУ передает информацию на частоте около 94,5 МГц. Радиус действия, равный 12 м, был определен экспериментальным путем. Иными словами, при отдалении ЭДРЗУ от приемника больше чем на 12 м мощность сигнала была сравнима с радиошумом.

Для того, чтобы обеспечить защиту от РЗУ, рассмотрим для начала случай, когда есть возможность определить частоту на котором

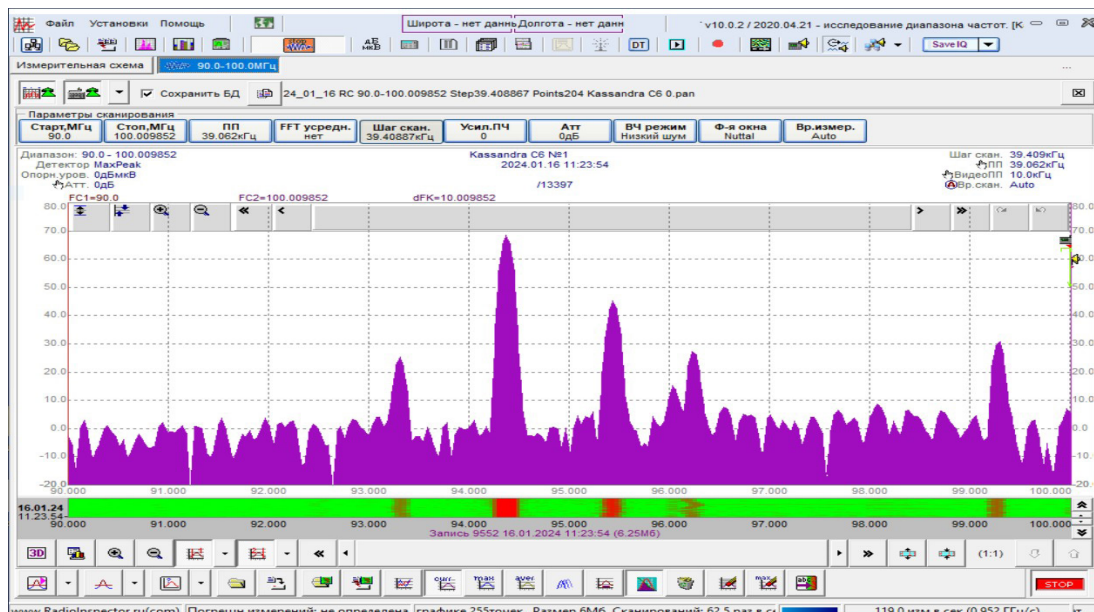


Рис. 3. Сканирование радиоэфира с включенным ЭДРЗУ

работает РЗУ. Для этого случая используют метод подавления сигнала.

Радиоподавляющее устройство

В ряде ситуаций возникает потребность в подавлении нежелательных радиопередач, создаваемых РЗУ, которые вмешиваются в работу незаконным образом и могут нарушить нормальный ход работы. Для этой цели существуют специальные устройства РПУ.

Принципиальная схема РПУ на двух транзисторах представлена на рис. 4.

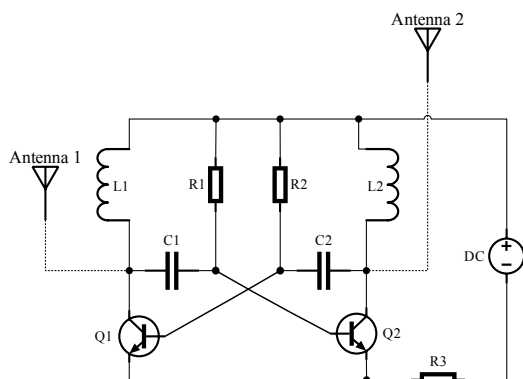


Рисунок 4. Принципиальная схема РПУ на двух транзисторах

Данная схема состоит из двух биполярных транзисторов Q1 и Q2 типа 2С53355, двух резисторов R1 и R2 и двух конденсаторов C1 и C2, и функционирует как мультивибратор, определяя необходимую выходную частоту. В нагрузке для каждого транзистора используются катушки индуктивности. Помимо этого, схема включает отдельный резистор R3 для

обратной связи питания эмиттеров транзисторов [5-6].

Перед сборкой схемы необходимо рассчитать несколько важных параметров, а именно резонансная частота, мощность и длина волны, на которой будет работать РПУ.

Резонансная частота для схемы рассчитывается следующим образом:

$$f = \frac{1}{2\pi \sqrt{L_1 C + L_2 C}}$$

Резонансная частота рассчитывается для понимания частоты устройства, а также для эффективной работы на настроенной частоте.

Расчет мощности передатчика можно выполнить с использованием закона Ома и закона электромагнитной совместимости (ЭМС).

Мощность рассчитывается по закону Ома для цепи постоянного тока:

$$P = V * I,$$

где P – мощность, V – напряжение, I – ток.

В соответствии с формулой приближительная мощность данного передатчика при питании от батарейки 9 В составляет примерно 0.45 Вт.

Мощность переводится в децибел-милливатт:

$$dBm = 10 * \log_{10} \left(\frac{P}{1 \text{ мВт}} \right) = 26.53$$

Мощность рассчитывается для понимания эффективной дальности передачи, а также, чтобы оценить, насколько долго устрой-

ство может работать от автономного источника питания.

Для расчета длин антенн для вещания в диапазоне 80-110 МГц, используется формула, связывающая частоту и длину волны:

$$\lambda = \frac{c}{f} = 3 \text{ м},$$

где λ – длина волны, c – скорость света, f – частота в герцах.

Длина волны рассчитывается для подбора антенн и подбора компонентов под конкретный диапазон.

Для правильной работы данной схемы требуется подключение двух антенн разной длины, представленных в виде медного провода. Первая антенна имеет длину 14 см, так как это $\frac{1}{16}$ длины волны нижнего диапазона. В то время как вторая антенна – 45 см, так как это $\frac{1}{8}$ длины волны верхнего диапазона.

Катушки индуктивности в данной схеме состоят из 7 витков провода диаметром 0,8 мм, намотанных на оправке диаметром 4 мм. Конденсаторы и резисторы и резистор R3 выполняют функцию сглаживания генерируемых импульсов, что способствует стабильности работы устройства.

Номиналы всех остальных элементов на схеме, следующие: C1, C2 = 1,0 мкФ, R1, R2 = 56 кОм, R3 = 100 кОм, DC = 9 В.

Все элементы монтировались на весу. Смонтированное РПУ на двух транзисторах представлено на рисунке 5.

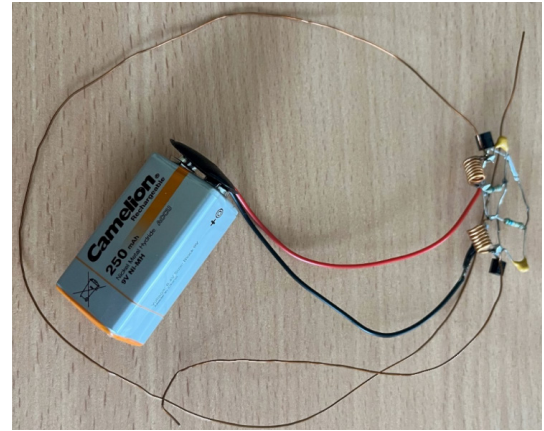


Рис. 5. Смонтированное РПУ на двух транзисторах

Определим диапазон работы схемы, для этого подключим антенну 0–600 МГц, подключим питание к устройству и запустим сканирование (рис. 6).

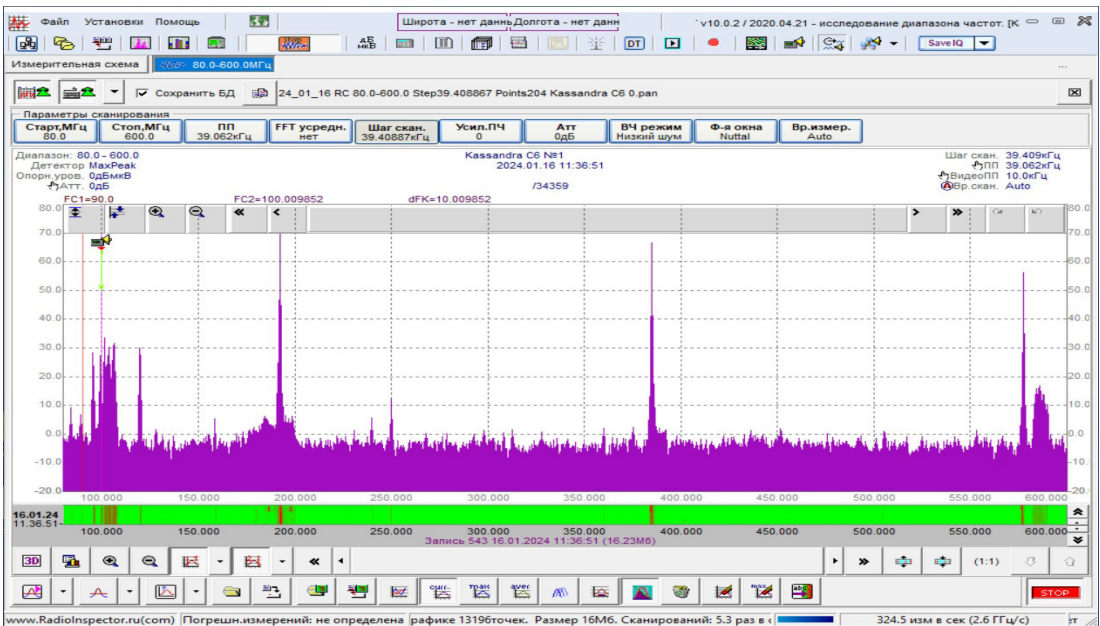


Рис. 6. Сканирование радиоэфира 80 – 600 МГц

При использовании РПУ возникают радиопомехи, которые начинают перекрывать и заглушать сигналы, передаваемые на определенных радиочастотах. РПУ обладает мощным сигналом, что позволяет успешно подавлять слабые радиопередачи, такие как РЗУ. Представленный выше график показывает,

что мощность сигнала от РПУ превышает мощность сигнала от РЗУ. Из-за этого, при попытке прослушивания частоты, на которой работает РЗУ, пользователь слышит только шум и помехи, не воспринимая информативный сигнал.

По результатам сканирования, представ-

ленного на рис. 6, видно, что устройство генерирует сигналы через каждые 100 – 110 МГц.

Диапазон работы данного устройства составляет примерно 4000 МГц, основная мощность приходит на первые 1000 МГц, далее постепенно уменьшается. Дальность работы сигнала составляет до 15 метров.

Рассмотрим случай, когда нет возможности определить частоту на котором работает РЗУ, для этого используют метод обнаружения источника сигнала.

Индикатор поля

Помимо того, что в ряде ситуаций можно

подавить нежелательные радиопередачи, создаваемые РЗУ. Также возникают ситуации с потребностью обнаружения. Для этой цели существуют устройства «индикаторы поля».

Рассмотрим схему индикатора радиоизлучений для регистрации напряженности электромагнитного поля в высокочастотном диапазоне 3-30 МГц длин волн со встроенным усилителем на транзисторах, позволяющем улучшить чувствительность (рис. 7).

Схема начинается с проволочной антенны длиной 20 см, скрученной в спираль. Длина антенны влияет на чувствительность к ча-

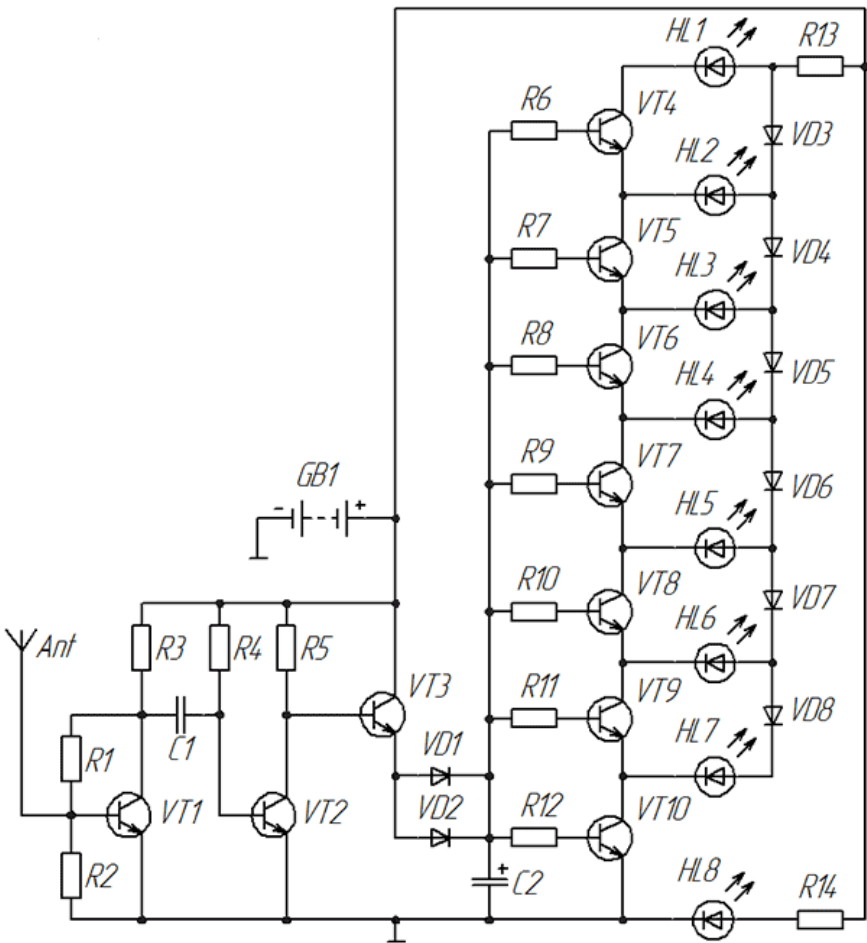


Рис. 7. Принципиальная схема индикатора ВЧ поля

стотам: короткая антенна лучше воспринимает высокие частоты, ориентируясь на четверть длины волны. Пойманный сигнал усиливается двумя NPN транзисторами, VT1, VT2 – KT3102ЕМ для хорошей чувствительности. Остальные транзисторы (VT3 – VT10) и диоды (VD1, VD2) – маломощные компоненты.

Индикация осуществляется линейкой светодиодов HL1 – HL7, при этом каждый све-

тодиод управляется своим транзистором. Используется пороговый диод (VD3 – VD8) для того, чтобы в каждый момент времени светился только один светодиод. Резистор R13 является токоограничителем для всей линейки, установлен с номиналом 680 Ом для яркости свечения светодиодов. Светодиоды для информативности оформлены в три цвета: зелёный в начале, оранжевый в середине и

красный в конце, предоставляя информацию о максимальном излучении. Схема питается от напряжения 9 В, при этом потребляемый ток не превышает 40 мА. В качестве источника питания используется крона, обеспечивающая несколько часов непрерывной работы. Конденсатор С2 (22 мкФ) вводится для поддержки гашения светодиодного столба, обеспечивая плавность в работе.

Номиналы всех остальных элементов на схеме, следующие: С1 = 10 нФ, R1, R4 = 1 МОм, R2 = 470 кОм, R3, R5 = 10 кОм, R6 – R12 = 1 кОм, R14 = 680 Ом.

Ввиду простоты схемы, индикатор собирается на макетной плате.

Учитывая вышеперечисленные условия, был изготовлен индикатора ВЧ поля (рисунок 9). Изготовленное устройство имеет чувствительность примерно от 20кГц до 2,45 ГГц. Светодиоды загораются снизу вверх, показывая уровень сигнала. Потому поиск скрытого РЗУ в исследуемом помещении осуществляется по нарастающей индикации светодиодов на устройстве.

При обнаружении РЗУ, сигнал будет слабым, так как частота РЗУ значительно меньше

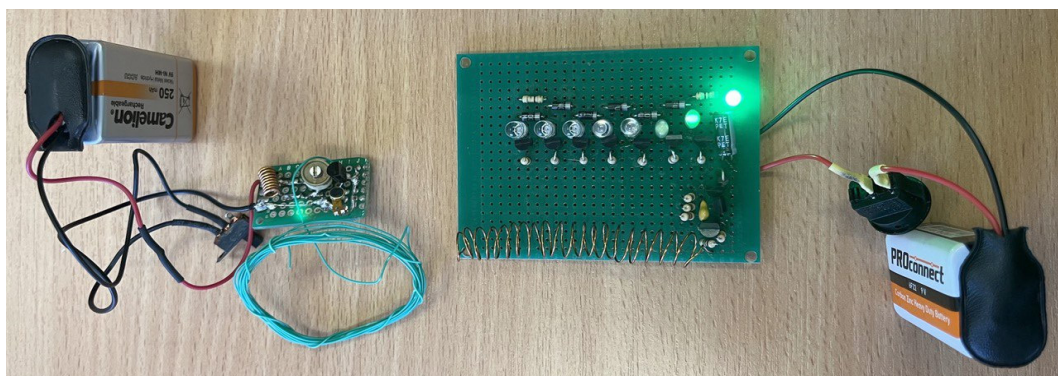


Рис. 9. Поиск РЗУ индикатором ВЧ поля

частоты на котором работает индикатор поля. В связи с этим загорится только нижний светодиод.

Заключение

В рамках данной работы были рассмотрены, проанализированы и разработаны три ключевых аспекта для повышения уровня безопасности в использовании беспроводных технологий: разработка устройства, эмулирующего работу РЗУ, применение РПУ, а также применение индикатора поля, предоставляющее возможность подавления и обнаружения РЗУ в исследуемом помещении.

Выбор между методами защиты от РЗУ – подавлением сигнала и обнаружением – зависит от конкретных требований и характера угрозы. Ниже описаны рекомендации для использования каждого метода.

Подавление сигнала является рекомендуемым методом в экстренных ситуациях, где требуется мгновенное прекращение связи с РЗУ из-за непосредственной опасности. Однако при использовании этого метода крайне

важно соблюдать законы и нормативы связи, чтобы избежать возможных юридических проблем, связанных с нарушением законодательства.

С другой стороны, обнаружение сигнала может быть предпочтительным в случае необходимости точной локализации и идентификации источника РЗУ. Этот метод также может быть более безопасным, минимизируя коллатеральные повреждения и избегая создания помех для других беспроводных устройств в окружающей среде.

Таким образом, данная статья подчеркивает эффективность методов обнаружения и подавления РЗУ в современном информационном обществе. Понимание их работы и принципов функционирования существенно для обеспечения эффективности и безопасности радиочастотных систем. Полученные результаты оказывают влияние на развитие технологий связи и повышение надежности работы радиочастотных систем в различных областях применения.

Литература

1. Бузов, Геннадий Алексеевич Защита информации ограниченного доступа от утечки по техническим каналам / Бузов Геннадий Алексеевич. – М.: Горячая линия – Телеком, 2016. – 909 с.

2. Малогабаритная радиоаппаратура. Вопросы конструирования, производства и эксплуатации. – М.: Издательство иностранной литературы, 2014. – 372 с.
3. Горшелев, В. Д. Основы проектирования радиоприемников / В.Д. Горшелев, З.Г. Красноцветова, Б.Ф. Федорцов. – Москва: СИНТЕГ, 2015. – 384 с.
4. Михайлова У.В., Фаткуллин А.Р. Использование возможностей комплекса радиомониторинга «Кассандра» для обнаружения современных технических средств с передачей информации по радиоканалу// Безопасность информационного пространства. Сборник трудов XVIII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. 2019. С. 124-127
5. Иванов-Цыганов, А. И. Электротехнические устройства радиосистем / А.И. Иванов-Цыганов. – М.: Высшая школа, 2019. – 490 с.
6. Фаткуллин А.Р., Михайлова У.В. Современные средства радиоразведки// Актуальные проблемы современной науки, техники и образования. Тезисы докладов 79-й международной научно-технической конференции. 2021. С. 402.

References

1. Buzov, Gennadiy Alekseyevich Zashchita informatsii ogranichennogo dostupa ot utehki po tekhnicheskim kanalam / Buzov Gennadiy Alekseyevich. – М.: Goryachaya liniya – Telekom, 2016. – 909 с.
2. Malogabaritnaya radioapparatura. Voprosy konstruirovaniya, proizvodstva i ekspluatatsii. – М.: Izdatel'stvo inostrannoy literatury, 2014. – 372 с.
3. Gorsheliev, V. D. Osnovy proyektirovaniya radiopriyemnikov / V.D. Gorsheliev, Z.G. Krasnotsvetova, B.F. Fedortsov. – Moskva: SINTEG, 2015. – 384 с.
4. Mikhaylova U.V., Fatkullin A.R. Ispol'zovaniye vozmozhnostey kompleksa radiomonitoringa «Kassandra» dlya obnaruzheniya sovremennykh tekhnicheskikh sredstv s peredachey informatsii po radiokanalu// Bezopasnost' informatsionnogo prostranstva. Sbornik trudov KHVIII Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uche-nykh. 2019. S. 124-127
5. Ivanov-Tsyganov, A. I. Elektrotekhnicheskiye ustroystva radiosistem / A.I. Ivanov-Tsyganov. – М.: Vysshaya shkola, 2019. – 490 с.
6. Fatkullin A.R., Mikhaylova U.V. Sovremennyye sredstva radio-razvedki// Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazova-niya. Tezisy dokladov 79-y mezhhdunarodnoy nauchno-tekhnicheskoy konferen-tsii. 2021. S. 402.

БАРАНКОВА Инна Ильинична, доктор технических наук, доцент, заведующая кафедрой информатики и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Associate Professor, Head of the Department of Computer Science and Information Security of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: inna_barankova@mail.ru

КУЗЬМИНА Ульяна Владимировна, кандидат технических наук, доцент по специальности «Информационная безопасность автоматизированных систем», доцент кафедры информатики и информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: u.mihaylova@magtu.ru

KUZMINA Ulyana Vladimirovna, Candidate of Technical Sciences, Associate Professor in the specialty «Information Security of automated systems», Associate Professor of the Department of Computer Science and Information Security of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: u.mihaylova@magtu.ru

ФЕДОРОВА Анастасия Романовна, студент федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: anastasia.43ag@yandex.ru

FEDOROVA Anastasia Romanovna, student of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: anastasia.43ag@yandex.ru

КУЛЬЕВИЧ Юрий Ярославович, студент федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: ykulevich01@mail.ru

KULEVICH Yuri Yaroslavovich, student of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: ykulevich01@mail.ru

КАЗАКОВ Олег Алексеевич, студент федерального государственного бюджетного образовательного учреждения высшего образования «Магнитогорский государственный технический университет им. Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: oleg.kazakov.2013@bk.ru

KAZAKOV Oleg Alekseevich, student of the Federal State Budgetary Educational Institution of Higher Education «Nosov Magnitogorsk State Technical University». 455000, Magnitogorsk, Lenin Ave., 38. E-mail: oleg.kazakov.2013@bk.ru