

ИМПУЛЬСНО-РЕФЛЕКТОРНЫЙ МЕТОД ОБНАРУЖЕНИЯ ЗАКЛАДНЫХ РАДИОУСТРОЙСТВ

И.С. Сурвило, С.Н. Петров

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Рассмотрены современные подходы к обнаружению закладных устройств, используемых для негласного получения информации. Описаны различные методы, основанные на регистрации физических явлений, таких как электромагнитные излучения, тепловые отклонения и гармонические искажения, каждый из которых имеет свои сильные и слабые стороны. Особое внимание уделено импульсно-рефлекторному методу, который выделяется своей универсальностью. Этот метод позволяет обнаруживать как активные, так и пассивные устройства за счет анализа отраженных сигналов и использования резонансных явлений, минимизируя при этом помехи для других систем. Несмотря на определенные ограничения, импульсно-рефлекторный метод рассматривается как перспективное решение для повышения точности и надежности обнаружения закладных устройств в условиях постоянно развивающихся технологий.

Ключевые слова: защита конфиденциальных данных; закладные устройства; обнаружение закладных устройств; электромагнитные излучения; резонансные характеристики; импульсно-рефлекторный метод; пассивные устройства; тепловые отклонения; гармонические искажения; системы защиты информации.

IMPULSE-REFLECTIVE METHOD FOR DETECTING HIDDEN RADIODEVICE

I.S. Survilo, S.N. Petrov

*Educational Institution "Belarusian State University of Informatics and Radioelectronics"
Minsk, Belarus*

Abstract. Modern approaches to detecting embedded devices used for unauthorized access to information were discusses. Various methods based on the registration of physical phenomena such as electromagnetic radiation, thermal deviations and harmonic distortions are described, each of which has its own strengths and weaknesses. Special attention is paid to the pulse-reflex method, which stands out for its versatility. This method makes it possible to detect both active and passive devices by analyzing reflected signals and using resonant phenomena, while minimizing interference to other systems. Despite certain limitations, the pulse-reflex method is considered as a promising solution for improving the accuracy and reliability of detecting embedded devices in conditions of constantly developing technologies.

Keywords: protection of confidential data; covert radio device; detection of covert radio device; electromagnetic radiation; resonant characteristics; impulse reflex method; passive devices; thermal deviations; harmonic distortion; information protection systems.

Введение

В современном мире, где информационные технологии чрезвычайно развиты, защита конфиденциальных данных становится одной из ключевых задач. Утечка информации может привести к серьезным последствиям, включая финансовые потери, репутационный ущерб и даже угрозу национальной безопасности. Одним из наиболее скрытных и опасных способов несанкционированного доступа к информации является использование закладных устройств. Эти устройства, часто миниатюрные и малозаметные, способны перехватывать, записывать и передавать данные на расстоянии, оставаясь незамеченными в течение длительного времени. Закладные устройства могут быть интегрированы в различные объекты инфраструктуры, включая офисные помещения, транспортные средства или бытовую технику. Их обнаружение представляет собой сложную техническую задачу, поскольку такие устройства часто работают в широком диапазоне частот, используют сложные методы модуляции сигналов и могут быть активированы только в определенных условиях. В связи с этим, разработка эффективных методов обнаружения закладных устройств является актуальной задачей в сфере обеспечения безопасности [1].

Основная часть

В условиях постоянного совершенствования элементной базы и структуры закладных устройств, методы их обнаружения также постоянно развиваются. Однако существующие подходы обладают определенными ограничениями и не могут считаться универсальными, что усложняет задачу обнаружения закладных устройств. Данные подходы обладают рядом особенностей, которые важно учитывать.

Линейный метод основывается на регистрации электромагнитных излучений, создаваемых активными электронными компонентами закладных устройств. Основная идея метода заключается в том, что многие электронные устройства, даже в режиме ожидания, могут излучать слабые сигналы в радиочастотном диапазоне, что позволяет их обнаружить с помощью специализированного оборудования. Линейный метод широко используется для поиска активных закладных устройств, работающих на различных радиочастотах. Однако данный метод имеет ряд ограничений. Прежде всего, метод эффективен только для устройств, находящихся в активном режиме и излучающих радиосигналы во время поиска. Если закладное устройство находится в пассивном режиме или использует сложные механизмы маскировки своих сигналов, линейный метод может оказаться недостаточно эффективным. Кроме того, данный метод требует точной настройки оборудования на конкретный диапазон частот, что может усложнить процесс поиска.

Нелинейный метод основан на обнаружении гармонических искажений, возникающих в электронных компонентах закладных устройств под воздействием мощного электромагнитного поля. При облучении таких устройств радиоволнами высокой мощности, полупроводниковые элементы начинают генерировать гармоники на кратных частотах. Именно эти гармоники и фиксируются оборудованием нелинейного радиолокатора, позволяя с высокой точностью обнаружить наличие электронных компонентов. Основное преимущество нелинейного метода заключается в возможности обнаружения закладных устройств, которые находятся в режиме ожидания и не излучают сигналы. Однако метод также имеет свои недостатки. Например, нелинейные радиолокаторы требуют значительной мощности излучения, что может создавать помехи для других электронных систем, находящихся в зоне

действия. Кроме того, работа в микроволновом диапазоне может оказать вредное воздействие на оператора при длительном использовании.

Тепловой метод обнаружения основан на фиксировании тепловых отклонений, возникающих в окружающей среде вследствие работы электронных компонентов закладных устройств. Любое электронное устройство при работе выделяет тепло, и это можно использовать для его обнаружения. Специальные тепловизоры способны фиксировать малейшие изменения температуры в окружающей среде, позволяя выявить активные закладные устройства по тепловым следам их работы. Однако тепловой метод также имеет свои ограничения. Во-первых, он может быть эффективен только в отношении устройств, которые выделяют достаточное количество тепла для регистрации. Во-вторых, тепловой метод требует использования высокочувствительных приборов, что увеличивает стоимость оборудования и сложность его эксплуатации.

Помимо перечисленных методов, существуют и другие подходы, такие как оптические, магнитные и рентгеновские, каждый из которых имеет свои области применения и ограничения. Однако ни один из этих методов не может гарантировать полного обнаружения всех типов закладных устройств, особенно с учетом их постоянного совершенствования и усложнения. Одним перспективных направлений является импульсно-рефлекторный метод, который сочетает в себе преимущества различных подходов и минимизирует их недостатки.

Импульсно-рефлекторный метод основывается на улавливании и анализе отраженных сигналов, возникающих в результате облучения исследуемой области зондирующими импульсами. Этот метод позволяет выявлять активные и пассивные элементы радиоустройств, такие как антенные системы и фильтрующие элементы, благодаря их резонансным характеристикам. Основная идея импульсно-рефлекторного метода заключается в следующем: с помощью специального лоатора исследуемое пространство облучается зондирующими импульсами в диапазоне частот, соответствующем возможным рабочим частотам закладных радиоустройств. Эти устройства, как правило, функционируют на фиксированной частоте или в узком диапазоне частот, что делает их уязвимыми для методов, основанных на резонансных явлениях. Антенные системы закладных устройств обычно имеют высокую добротность – параметр, характеризующий способность контура эффективно накапливать и отдавать энергию при резонансе. Когда устройство с высокодобротным контуром облучается зондирующим сигналом с частотой, равной резонансной частоте контура, амплитуда наведенных в контуре токов резко возрастает. Это приводит к значительному увеличению мощности отраженного сигнала, принимаемого лоатором [2].

Данный метод особенно эффективен при работе с закладными устройствами, чьи антенные системы работают в узком диапазоне частот и обладают выраженными резонансными характеристиками. В случае облучения устройств зондирующим сигналом на резонансной частоте происходит значительное усиление отклика, что позволяет надежно обнаруживать закладные устройства на фоне естественного электромагнитного шума и других помех.

Таким образом импульсно-рефлекторный метод обладает рядом ключевых преимуществ, которые делают его более эффективным и универсальным по сравнению с традиционными методами обнаружения закладных устройств:

- высокая чувствительность к резонансным элементам: антенные системы и другие высокодобротные компоненты закладных устройств создают четко выраженные резонансные отклики, которые легко обнаруживаются с помощью данного

метода. Это особенно важно при работе с устройствами, скрытыми в конструкциях или оборудовании;

- обнаружение устройств, работающих в пассивном режиме: в отличие от методов, требующих активного излучения от закладного устройства, импульсно-рефлекторный метод позволяет выявлять даже пассивные элементы, такие как антенные системы, которые не излучают сигналы, но откликаются на зондирующее воздействие;

- независимость результата от излучаемой мощности закладных устройств;

- низкая средняя мощность зондирующих сигналов позволяет минимизировать воздействие на окружающие системы связи и другое радиоэлектронное оборудование.

Несмотря на значительные преимущества, импульсно-рефлекторный метод не лишен недостатков. Одним из них является зависимость от наличия резонансных контуров в закладных устройствах. Если устройство использует нерезонансные схемы или имеет специальную экранировку, сигнал может быть ослаблен до такой степени, что его обнаружение станет затруднительным.

Реализация устройства, работающего на импульсно-рефлекторном методе, требует учета ряда особенностей, которые обеспечивают его эффективность и надежность. Центральным элементом системы является генератор, который создает короткие импульсы с заданной частотой и мощностью. В качестве зондирующего сигнала целесообразно использовать короткие импульсы с определенным периодом повторения [3]. Короткие импульсы позволяют достичь высокой пиковой мощности при относительно низкой средней мощности, что минимизирует энергопотребление. Кроме того, короткие импульсы обеспечивают высокую временную разрешающую способность.

Передающая антенна излучает зондирующие импульсы в окружающее пространство. Ее конструкция и характеристики должны обеспечивать эффективное распространение сигнала в заданном диапазоне частот. Антенна должна быть направленной, чтобы минимизировать рассеивание энергии и увеличить дальность действия системы. Приемная антенна должна обладать высокой чувствительностью, чтобы улавливать слабые отраженные сигналы, включая вторичное излучение от закладных устройств.

Полученные сигналы обрабатываются с использованием оптимальных алгоритмов. Это позволяет выделить характерные признаки отраженных сигналов, такие как резонансные частоты и амплитудные всплески, которые свидетельствуют о наличии закладного устройства.

Таким образом импульсно-рефлекторный метод предоставляет значительные возможности для улучшения систем обнаружения закладных устройств. Его использование позволяет объединить передовые технологии обработки сигналов и подходы к их передаче, создавая потенциал для повышения точности, дальности и надежности обнаружения, что делает данный метод перспективным для дальнейшего развития и применения в системах защиты информации.

Заключение

Существующие подходы к обнаружению закладных устройств имеют свои особенности и не всегда обеспечивают универсальное решение. Импульсно-рефлекторный метод, основанный на анализе отраженных сигналов и использовании резонансных явлений, предлагает более гибкий и универсальный подход. Он позволяет обнаруживать как активные, так и пассивные устройства, не создавая значительных помех для других систем. Однако его эффективность зависит от наличия резонансных

контуров в закладных устройствах, что в некоторых случаях может снизить его применимость.

Список использованных источников

1. Куприянов А. И., Петренко П. Б., Сычев М. П. (2010) *Теоретические основы радиоэлектронной разведки: учебное пособие*. Москва, МГТУ им. Баумана.
2. Буневич М. А., Майоров А. И., Врублевский И. А. (2022) Применение SDR-приемопередатчиков в системах для поиска закладных радиоустройств. *Цифровая трансформация*. 28 (4). 62-71.
3. Ворошень А. В., Ворошень В. И. (2015) Функциональные особенности резонансно-рефлектометрического локатора для обнаружения радиозакладных устройств. *Тезисы докладов XIII Белорусско-российской научно-технической конференции «Технические средства защиты информации»*. С 13-14.

References

1. Kupriyanov A. I., Petrenko P. B., Sychev M. P. (2010) *Theoretical Foundations of Electronic Intelligence: Textbook*. Moscow, Bauman Moscow State Technical University (in Russian).
2. Bunevich M. A., Mayorov A. I., Vrublevsky I. A. (2022) The Use of SDR Transceivers in Systems for Searching Covert Radiodevices. *Digital Transformation*. 28 (4). 62–71 (in Russian).
3. Voroshen A. V., Voroshen V. I. (2015) Functional Features of Resonance-Reflectometric Locator for Detection of Radio Bugs. *Proceedings of the XIII Belarusian-Russian Scientific and Technical Conference "Technical Means of Information Protection"*. P 13–14 (in Russian).

Сведения об авторах

Сурвило И.С., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ilya_survilo@mail.ru.
Петров С.Н., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», petrov@bsuir.by.

Information about the authors

Survilo I.S., Master's student of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", ilya_survilo@mail.ru.
Petrov S.N., Cand. of Sci., Associate Professor, Associate Professor of the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", petrov@bsuir.by.