ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.53

DOI: 10.21822/2073-6185-2026-53-1-40-48 Оригинальная статья/ Original article

Классификация линий связи и аппаратных средств как основа для выявления несанкционированных подключений

С.С. Васичкин
Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
193232, г. Санкт-Петербург, пр. Большевиков, 22, к. 1, Россия

Резюме. Цель. В статье рассматривается задача автоматизированного выявления подключений к проводным линиям связи, что особенно актуально в условиях роста угроз скрытого доступа. **Метод.** Исследование основано на методах выявления, идентификации, классификации угроз нарушения информационной безопасности объектов. **Результат.** Предложена расширенная классификация линий связи и подключаемых устройств с учётом их сигнальных характеристик. Проанализированы ограничения существующих методов контроля, включая импульсную рефлектометрию и частотно-параметрические подходы. Разработана структура классификатора, позволяющая формировать эталонные сигнальные профили и выявлять отклонения от них в режиме реального времени. Подход повышает точность удалённой идентификации, снижает влияние человеческого фактора и создаёт основу для интеллектуальных систем мониторинга. Рассмотрена устойчивость классификации к внешним помехам и изменению параметров среды. **Вывод.** Результаты могут быть применены в системах автоматического контроля целостности каналов связи.

Ключевые слова: линии связи, классификация устройств, сигнальные характеристики, рефлектометрия, контроль подключений, информационная безопасность

Для цитирования: С.С. Васичкин. Классификация линий связи и аппаратных средств как основа для выявления несанкционированных подключений. Вестник Дагестанского государственного технического университета. Технические науки. 2026;53(1):40-48. DOI:10.21822/2073-6185-2026-53-1-40-48

Classification of communication lines and hardware devices as a basis for Detecting Unauthorized Connections

S.S.Vasichkin
M.A. Bonch-Bruevich Saint Petersburg State University of Telecommunications,
22 Bolshevikov Ave., build. 1, St Petersburg 193232, Russia

Abstract. Objective. This article addresses the problem of automated detection of connections to wired communication lines, which is relevant in the context of increasing threats of hidden access. **Method.** The study is based on methods of detection, identification, classification of threats to information security of objects. **Result.** An extended classification of communication lines and connected devices is proposed, taking into account signal characteristics. The limitations of control methods, pulse reflectometry and frequency-parametric approaches are analyzed. A classifier structure has been developed that allows for the formation of reference signal profiles and the identification of deviations in real time. The approach improves the accuracy of remote identification, reduces the influence of the human factor, and creates the basis for intelligent monitoring systems. The robustness of the classification against environmental changes and interference is also discussed. **Conclusion.** The results may be applied in automated control of communication line integrity.

Keywords: communication lines, device classification, signal characteristics, reflectometry, connection control, information security

For citation: S.S. Vasichkin. Classification of communication lines and hardware devices as a basis for Detecting Unauthorized Connections. Herald of Daghestan State Technical University. Technical Sciences. 2026;53(1):40-48. (In Russ) DOI:10.21822/2073-6185-2026-53-1-40-48

Введение. Современные информационные системы всё чаще сталкиваются с угрозами, направленными не только на программное обеспечение и каналы логического взаимодействия, но и на физическую инфраструктуру связи. В частности, проводные линии остаются уязвимыми элементами в архитектуре защищённых коммуникаций. Несмотря на распространённость средств криптографической защиты, факт физического подключения стороннего устройства способен обойти логические барьеры и скомпрометировать всю систему. Это особенно критично для объектов с высокими требованиями к информационной безопасности - от промышленных сетей и банковской инфраструктуры до систем государственной важности.

Проблема несанкционированных подключений остаётся одной из наименее автоматизированных задач в сфере обеспечения безопасности сетей. При этом изменения физических характеристик линии связи, вызванные появлением нового устройства, фиксируемы и могут служить признаком потенциального вторжения. Однако на практике применение традиционных методов анализа, таких как импульсная рефлектометрия или частотный контроль, сопряжено с рядом ограничений: низкой чувствительностью, зависимостью от длины линии, сложностью интерпретации и невозможностью классификации типа устройства без участия специалиста. В современных условиях становится актуальной задача создания интеллектуальных систем, способных в реальном времени обнаруживать факт подключения нового оборудования на основе анализа сигнальных характеристик линии [1]. Для построения таких систем необходима база знаний, в которую входят сигнальные «портреты» различных типов линий и устройств, а также алгоритмы сравнения и принятия решений. Центральным элементом выступает классификатор, способный дифференцировать состояния линии и формировать гипотезы об изменениях.

Подход, основанный на классификации типов линий и устройств, позволяет существенно повысить эффективность контроля. В первую очередь, за счёт перехода от ручной диагностики к автоматическому режиму принятия решений. Во вторую - за счёт способности выявлять даже минимальные отклонения в сигнальной среде, которые традиционные методы могли бы не зафиксировать. В отличие от методов, основанных на локальном контроле и периодическом измерении, классификационный подход предполагает непрерывный мониторинг и анализ сигналов в динамике.

Постановка задачи. Цель данной работы - разработать расширенную классификацию линий связи и подключаемых к ним устройств, способную служить основой для построения интеллектуального механизма детектирования несанкционированных вмешательств. В статье рассматриваются принципы формирования классификатора, структура сигнальных признаков, методы их извлечения и интерпретации [2].

Особое внимание уделяется универсальности предлагаемого решения - его применимости к различным типам инфраструктур и минимальной зависимости от конкретной топологии сети. Представленный в работе подход может быть интегрирован в системы технической защиты информации, использован в качестве основы для разработки аппаратных средств контроля или программных комплексов удалённого мониторинга [3]. Подход способствует не только усилению физической безопасности линий связи, но и повышению общей устойчивости информационной системы к внешним воздействиям. Задача обеспечения контроля целостности и защищённости проводных линий связи актуальна в контексте современных угроз информационной безопасности.

Несмотря на использование сертифицированных программных средств защиты, физический уровень передачи данных остаётся потенциальной зоной уязвимости. Это обусловлено тем, что несанкционированные подключения могут быть выполнены с соблюдением электрических параметров линии, не нарушая явно её работоспособность,

но обеспечивая возможность перехвата информации или внедрения неавторизованных устройств. Существующие методы технического контроля, включая импульсную рефлектометрию и методы спектрального анализа, не всегда позволяют точно идентифицировать факт подключения нового устройства, особенно в случае его согласования с параметрами линии. Большинство решений ориентированы на ручной или полуручной режим диагностики, что ограничивает их применение в задачах непрерывного мониторинга.

Таким образом, требуется разработка подхода, обеспечивающего:

- автоматическую идентификацию изменений в сигнальных характеристиках линии;
- формирование эталонного сигнального «портрета» линии и устройств;
- классификацию подключаемых устройств по степени соответствия допустимым и потенциально опасным типам;
- минимизацию ложных срабатываний при высокой чувствительности системы к физическим изменениям в канале.

Для реализации данного подхода необходимо:

- провести структурированную классификацию типов линий связи и характеристик устройств;
- определить сигнальные признаки, чувствительные к вмешательству;
- разработать архитектуру классификатора, пригодную для встраивания в систему удалённого контроля;
- оценить применимость предложенного решения для различных сценариев эксплуатации.

Решение поставленной задачи позволит создать интеллектуальный механизм обнаружения несанкционированных подключений, не зависящий от конкретной архитектуры защищаемой системы и пригодный для применения в условиях ограниченного доступа к линии.

Методы исследования. Предлагаемый метод идентификации подключаемых устройств к линиям связи основан на предпосылке, что каждое устройство, включаемое в физическую цепь, неизбежно оказывает влияние на сигнальные характеристики линии, даже при выполнении всех норм согласования [4]. Эти изменения проявляются в параметрах, таких как импеданс нагрузки, форма и спектр отражённого сигнала, амплитудно-частотная характеристика, фазовые искажения и уровень собственных шумов [5].

В отличие от логических методов обнаружения, которые опираются на анализ сетевого трафика или активность портов, предложенный подход позволяет зафиксировать факт физического подключения, независимо от поведения устройства на уровне протоколов. Воздействие устройств на линию может быть зафиксировано с помощью стандартных методов электрических измерений: импульсной диагностики, частотного сканирования и анализа коэффициента отражения [6, 23]. Полученные данные затем интерпретируются и сравниваются с эталонными характеристиками, соответствующими состоянию линии без постороннего вмешательства. Это делает возможным не только фиксацию отклонений, но и их классификацию по степени опасности и типу подключённого объекта [7, 8]. Совместная обработка фазовой и амплитудной информации позволяет задать норму для сигнального состояния линии и организовать её постоянный контроль, выявляя подозрительные изменения и определяя тип возможного подключения.

В рамках работы разработан комплексный подход, сочетающий структурную классификацию линий связи и типов устройств с анализом отражённого сигнала. Такой синтез обеспечивает высокую чувствительность к минимальным изменениям, а также позволяет интерпретировать полученные сигнальные данные в терминах функционального назначения или допустимости того или иного подключения (рис. 1). Методологически обоснованное включение параметров структуры линии позволяет повысить достоверность классификации и минимизировать количество ложных срабатываний.

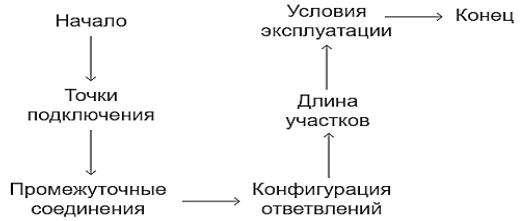

Рис. 1 – Учёт структуры подключения линии при построении сигнатуры
Fig. 1 – Accounting for Line Connection Structure in Signature Formation

Предложенный метод ориентирован на практическую реализацию в условиях реальной эксплуатации: он не требует внедрения в логическую структуру систем и может быть использован для непрерывного фоново-пассивного мониторинга состояния линии. Основой метода является анализ коэффициента отражения, который определяется как (1):

$$\Gamma = \frac{Z_H - Z_0}{Z_H + Z_0\mu} \tag{1}$$

Появление даже согласованной нагрузки способно изменить фазовые и амплитудные параметры сигнала, особенно при высокочастотной диагностике [7]. Таким образом, коэффициент отражения становится первичным маркером изменения состояния линии.

По времени задержки отражения Δt можно определить расстояние до места неоднородности (2).

$$L = \frac{v \times \Delta t}{2} \tag{2}$$

где L - расстояние до неоднородности, v - фазовая скорость распространения сигнала в линии (для витой пары примерно 0.6 от скорости света), Δt - временной интервал между посылкой и приёмом импульса.

На основании этой задержки вычислялось расстояние до точки потенциального подключения или нарушения. При $\Delta t = 20$ нс расстояние до точки вмешательства составило 2 метра. Для оценки влияния различных подключений на параметры линии проводился замер амплитудно-частотной характеристики (АЧХ). Этот параметр отражает зависимость уровня передаваемого сигнала от частоты и является одним из ключевых индикаторов состояния линии [9]. В процессе эксперимента для оценки характеристик линии связи использовался метод активного зондирования, при котором на вход подавался тестовый сигнал в виде линейно-частотно модулированной последовательности в диапазоне от 1 до 50 МГц. Регистрировался отклик линии, на основе которого формировалась передаточная функция (3):

$$H(f) = \frac{U_{\text{вых}}(f)}{U_{\text{вх}}(f)}, \tag{3}$$

где $U_{\text{вых}}(f)$ и $U_{\text{вх}}(f)$ - спектральные составляющие сигналов на входе и выходе линии соответственно.

АЧХ, являющаяся модулем передаточной функции, позволяла оценивать затухание сигнала в зависимости от частоты. При этом уровень затухания на участке линии длиной L вычислялся по формуле (4):

$$\alpha(\mathrm{f}) = 10 \cdot \log_{10}\left(\frac{\mathrm{P}_{\text{вых}}(\mathrm{f})}{\mathrm{P}_{\text{вх}}(\mathrm{f})}\right) \tag{4}$$

Для стандартной витой пары категории 5е в штатной конфигурации, без внешних подключений или структурных неоднородностей, измеренное затухание в диапазоне частот до 100 МГц составляло от 16 до 22 дБ на участке длиной 100 метров, в зависимости от наличия экранирования. Подключение устройств с реактивной нагрузкой вызывало дополнительные частотные и фазовые искажения, проявлявшиеся в виде резонансных

пиков и провалов на АЧХ, а также в виде нелинейных искажений фазово-частотной характеристики (ФЧХ). Изменения формы АЧХ и ФЧХ, особенно в диапазоне от 10 до 50 МГц, указывают на появление новых подключений и нарушения в топологии линии связи. Это связано с тем, что именно в этом частотном диапазоне наиболее ярко проявляются резонансные эффекты, вызванные изменениями нагрузки, неоднородностями или паразитными ответвлениями [21, 24]. Анализ зафиксированных амплитудных и фазовых характеристик позволяет выявлять не только сам факт вмешательства, но и делать выводы о его характере. При этом даже небольшие по уровню отклонения от эталонной характеристики могут свидетельствовать о подключении внешних устройств или изменении состояния линии. Сравнительный анализ АЧХ линии при штатной и нарушенной конфигурации позволил количественно оценить влияние подключений на затухание сигнала, а также определить частотные зоны, наиболее чувствительные к изменениям (табл. 1).

Таблица 1. Результаты анализа амплитудного отклика линии связи
Table 1. Results of Amplitude Response Analysis of the Communication Line

Частота (МГц) Frequency (MHz)	**Амплитуда без подключения (дБ) Amplitude without connection (dB)**	**Амплитуда с подключением (дБ) Amplitude with connection (dB)**
10	-1.2	-1.5
30	-2.5	-3.3
60	-4.8	-6.2

Наиболее чувствительным диапазоном к подключению нештатных устройств оказался интервал от 30 до 60 МГц, где наблюдались амплитудные отклонения более чем на 1 дБ. Для типовых линий связи, таких как витая пара категории 5e, затухание сигнала без нагрузки составляло в среднем 16-22 дБ на 100 м, тогда как вмешательства вызывали дополнительное ослабление на 0.6-1.4 дБ, а также фазовые сдвиги до 12° на частотах свыше 50 МГц. Эти изменения были выявлены с использованием расчёта передаточной функции $H(f)$ и коэффициента затухания $\alpha(f)$, описанных выше.

Полученные результаты подтверждают, что изменения формы АЧХ и ФЧХ линии в высокочастотном диапазоне являются надёжным индикатором появления новых подключений, даже в случае их согласованного импеданса. Это открывает возможность для применения фазово-амплитудного анализа в задачах удалённого контроля и классификации устройств [10, 22]. Одним из ключевых параметров, отражающих состояние линии связи, является ФЧХ, описывающая зависимость фазы выходного сигнала от частоты входного. При штатном (эталонном) подключении ФЧХ имеет близкую к линейной форму, что соответствует равномерному распространению сигнала по всем частотам спектра. В этом случае фазовый сдвиг $\varphi(f)$ описывается выражением (5):

$$\varphi(f) = argH(f) \tag{5}$$

При подключении внешнего устройства, особенно нештатного или паразитного, возникает нарушение линейности фазового отклика. Это связано с дополнительными отражениями, паразитной ёмкостью или индуктивностью на границе подключения [11]. В результате в спектре появляются частотные области с аномальным фазовым отклонением.
Для оценки таких искажений введён параметр максимального фазового отклонения (6):

$$\Delta\varphi = max\left|\varphi_{\text{измер}}(f) - \varphi_{\text{эталон}}(f)\right| \tag{6}$$

В рамках эксперимента зафиксировано, что при подключении устройств с несовпадающим импедансом ($Z_H \neq Z_0$), фазовый сдвиг на частотах 50-70 МГц возрастает в среднем на 12-18°. Установленный порог для допустимых фазовых искажений составляет 10°, что позволяет уверенно классифицировать подключение как нештатное [12, 16].

На рис. 2 представлена схема формирования сигнатуры линии, в которую включён фазовый отклик как один из ключевых компонентов. Совокупный анализ фазовых и амплитудных характеристик позволяет значительно повысить достоверность удалённой идентификации аппаратных средств.

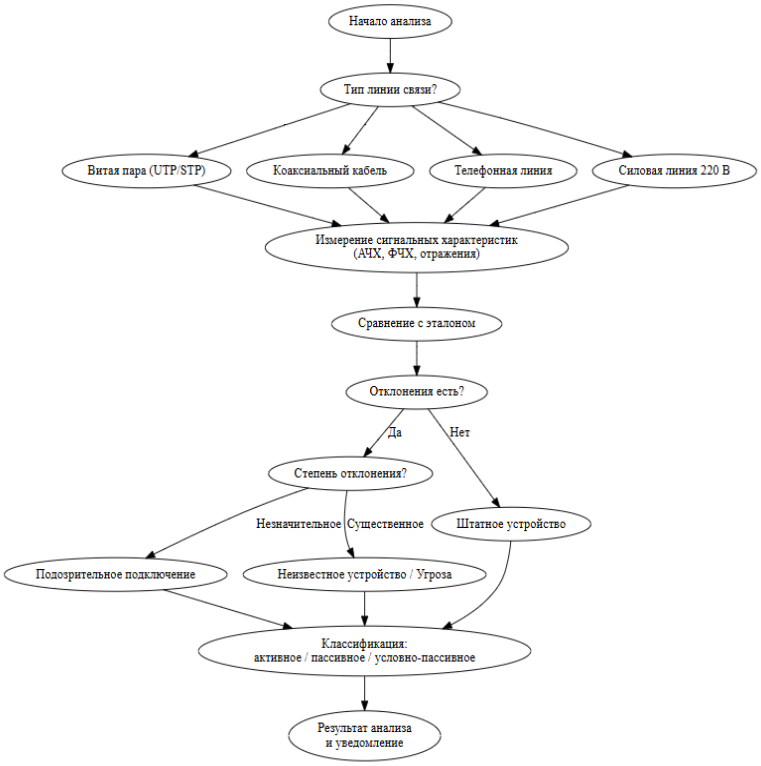

Рис. 2 – Структура классификации устройств по сигнатуре линии связи
Fig. 2 – Structure of device classification based on communication line signature

Полученные данные используются для формирования базы эталонных сигнальных «портретов» как для линий, так и для устройств. Эталон включает: амплитудно-частотную характеристику; коэффициент затухания на заданном участке; форму отражённого импульса; фазовые сдвиги. В процессе эксплуатации в линию вводится диагностический сигнал, измеряется текущий вектор характеристик и проводится сравнение с эталоном. Метод предполагает автоматическое вычисление отклонения в параметрах сигнала и принятие решения на основе допустимых пределов [13]. При этом классификация позволяет не только зафиксировать наличие вмешательства, но и провести идентификацию типа подключённого устройства. На основании сформированной сигнатуры осуществляется классификация подключения (рис. 2) и принятие соответствующего решения [17]. Отличительной чертой метода является возможность удалённой идентификации без необходимости физического доступа к линии или активного обмена данными с устройством. Это позволяет применять метод в фоновом режиме, снижая риск обнаружения со стороны нарушителя [14].

В отличие от существующих решений, ограниченных детекцией наличия нагрузки, предложенный подход обеспечивает детализированную идентификацию, с привязкой к типу линии и профилю устройства. Теоретическая значимость метода заключается в расширении представлений о взаимодействии физических линий связи с различными типами нагрузки и выявлении сигнальных признаков, пригодных для удалённой диагностики [18, 19]. Практическая значимость проявляется в возможности разработки модулей технического контроля и встроенных средств мониторинга защищаемых объектов, ориентированных на физический уровень передачи [20].

Обсуждение результатов. В ходе реализации предложенного подхода была сформирована классификационная модель, объединяющая сигнальные характеристики линий связи и аппаратных средств, подключаемых к ним. Основным результатом стало построение набора эталонных сигнатур, отражающих нормальное состояние линии в отсутствие нарушений, а также определение диапазонов допустимых отклонений, возникающих при различных типах подключений. Экспериментальное моделирование проводилось с целью выявления предельной чувствительности разработанного метода к различным

типам подключений, включая случаи подключения согласованных нагрузок, не нарушающих формально норму по импедансу. Устройства подключались к различным типам линий связи (витая пара, коаксиал, телефонная линия) с заранее известными параметрами. В линию вводился высокочастотный диагностический импульс с длительностью менее 10 нс, что соответствовало эффективной ширине спектра до 100 МГц [15]. Такое воздействие позволяет выделить даже минимальные неоднородности в тракте передачи за счёт высокой чувствительности к фазовым и частотным отклонениям. При включении даже номинально согласованной нагрузки (например, 100 Ом в линию с $Z_0 = 100$ Ом), наблюдались устойчивые изменения в форме отражённого сигнала. Они проявлялись как:

- небольшой фазовый сдвиг относительно эталона на частотах выше 40 МГц (до 7-12°);
- усиление затухания в полосе 50-70 МГц на 0.6-1.4 дБ;
- сдвиг по времени возврата отражённого импульса на 1.2-2.5 нс, обусловленный дополнительной нагрузочной ёмкостью.

Это подтверждает, что электрически «прозрачные» подключения всё же оказывают измеримое влияние на сигнальную картину линии, особенно при высокочастотном тестировании [15]. Подобный подход оказался особенно эффективным в условиях, когда физический доступ к линии отсутствует, а подключение выполняется скрытно. Именно это свойство делает метод перспективным для задач технической защиты информации, где требуется пассивный и фоновый контроль физического уровня соединений.

Проведённое сравнение с существующими методами, такими как импульсная рефлектометрия без последующей классификации, показало преимущество разработанного подхода по двум ключевым метрикам: точности идентификации и возможности дифференцировать штатные и нештатные подключения. Благодаря учёту структуры самой линии (рис. 1) и разнообразия откликов удалось минимизировать ложные срабатывания и увеличить чувствительность системы к скрытому вмешательству.

Особое внимание было уделено процедуре классификации устройств, представленному в виде логической схемы (рис. 2). Механизм позволяет формировать дерево решений, в котором сигнатурные признаки служат основанием для перехода по ветвям, заканчивающимся выводами о допустимости или недопустимости подключения. Такая реализация не только повышает автоматизм процесса, но и открывает возможность для дальнейшей интеграции элементов машинного обучения в классификатор.

Вывод. В рамках проведённого исследования решена задача выявления и идентификации подключений к проводным линиям связи на основе анализа их сигнальных характеристик. Предложенный подход ориентирован на физический уровень модели взаимодействия и обеспечивает возможность обнаружения несанкционированных или атипичных подключений без необходимости активного обмена данными с устройствами и без вмешательства в штатную топологию системы. Метод опирается на принцип отражения сигнала при нарушении согласования импеданса в линии и включает последовательную процедуру измерения, интерпретации и сравнения отражённого сигнала с эталонными характеристиками. Были использованы такие параметры, как коэффициент отражения, искажения амплитудных и фазово-частотных характеристик, а также время возврата импульса. Эти параметры формируют сигнатуру линии, позволяющую выполнять классификацию подключений по типу воздействия и потенциальной допустимости.

Разработанная классификационная модель была дополнена механизмом принятия решений, основанным на расчёте интегрального критерия отклонения. Это позволило провести сопоставление текущего состояния линии с базой эталонных профилей и выделить подключения, отличающиеся от штатных режимов эксплуатации. Результаты экспериментального моделирования подтвердили высокую чувствительность метода, в том числе к согласованным подключениям, ранее считавшимся малозаметными.

Теоретическая значимость предложенного подхода заключается в расширении представлений о взаимодействии сигнальных характеристик линии связи с различными типами

нагрузок. Практическая значимость выражается в возможности разработки автономных подсистем мониторинга, не требующих вмешательства оператора и способных функционировать в фоновом режиме. Методика может быть реализована в виде программно-аппаратного комплекса, встраиваемого в существующую инфраструктуру с минимальными затратами. Это создаёт предпосылки для использования предложенного решения в системах мониторинга инженерных сетей и в составе интеллектуальных платформ киберфизической безопасности. Сформулированные положения, теоретические и прикладные результаты подтверждены экспериментально и открывают перспективу для дальнейших разработок в области пассивного контроля и интеллектуального анализа физического уровня защищённых линий связи.

Библиографический список:

1. Алейников А.А., Билятдинов К.З., Красов А.В., Левин М.В. Контроль, измерение и интеллектуальное управление трафиком. – СПб.: Астерион, 2016. – 92с. ISBN 978-5-00045-385-8. EDN WLROTL.
2. Орлов Ю.Ф. Активная идентификация объектов управления.–М.:МГТУ им.Н.Э.Баумана, 2010.296 с.
3. Куклин А.А., Кукушкин А. В. Радиотехнические измерения: учеб. пособие. – М.: Радио и связь, 2006. – 284 с.
4. Поздняков С. А., Новиков Ю. А. Анализ электрических цепей. – М.: Высшая школа, 2008. – 368 с.
5. Гусев В. Е., Трифонов Ю. И. Импульсная рефлектометрия. – М.: Энергия, 1987. – 214 с.
6. Билятдинов К. З., Красов А. В., Меняйло В. В. Исследование систем и анализ результатов испытаний. – СПб.: Астерион, 2019. – 362 с. – ISBN 978-5-00045-813-6. – EDN OXKBZW.
7. Orfanidis S. J. Electromagnetic Waves and Antennas [El. resource]. – Rutgers University, 2016. – 954 p. – Режим доступа: https://eceweb1.rutgers.edu/~orfanidi/ewa/ (дата обращения: 14.04.2025).
8. Kurose J.F., Ross K.W. Computer Networking:A Top-Down Approach. 8th ed. Boston:Pearson, 2020;896.
9. Капралова И.А., Игнатьев М. С. Методы анализа сигналов в рефлектометрических системах // Вестник МГТУ им. Н. Э. Баумана. Сер. Радиоэлектроника. – 2019. – № 3. – С. 46–54.
10. Каменев М.И., Беляков Е.И. Сигналы и процессы в радиотехнических системах. – СПб.:Лань, 2004. – 432 с.
11. Чернов И.И., Корж В.Я. Электромагнитная совместимость: учебник. – М.: Горячая линия – Телеком, 2011. – 360 с.
12. Мухина И.А. Анализ методов защиты локальных вычислительных сетей от несанкционированного доступа // Информационные технологии и безопасность. – 2018. – № 1 (15). – С. 25–31.
13. Jones S.B., Wraith J.M., Or D. Time domain reflectometry measurement principles and applications // Soil Science Society of America Journal. – 2002. – Vol. 66, no. 5. – P. 1479–1486.
14. Хромов С.П. Основы анализа и синтеза электрических цепей. – М.: Энергоатомиздат, 2003. – 408 с.
15. Красильников В.И. Электромагнитные переходные процессы. – М.: Академия, 2012. – 304 с.
16. Петренко П.Б., Кривозубов П.А., Зайцев Д.И., Токарева А.С. Повышение точности рефлектометрии и достоверности идентификации устройств в проводных линиях связи//Труды СПИИРАН. – 2011. – № 6. – С. 126–148.
17. Словеснов Н.А., Мирсатов С.Ф., Светличный В.В. Исследование методов идентификации оборудования в системах защиты информации проводных сетей связи // Информационная безопасность телекоммуникационных систем. – 2014. – № 4. – С. 53–60.
18. Идентификация параметров источников побочных электромагнитных излучений по измерениям в ближней зоне [Электронный ресурс]. Режим доступа: https://mai.ru/upload/iblock/db3/db3e2997c3d7df16a90199a3df149a48.pdf (дата обращения: 14.04.2025).
19. Основы идентификационных измерений // Журнал радиоэлектроники [Электронный ресурс]. – Режим доступа: https://jre.cplire.ru/iso/nov06/2/text.html (дата обращения: 14.04.2025).
20. Методы и средства защиты телефонных аппаратов и линий связи/БНТИ [Электронный ресурс]. Режим доступа:https://www.bnti.ru/showart.asp?aid=68&lvl=04.03.02.&p=1(дата обращения: 14.04.2025).
21. Основные принципы измерений и анализа сигналов/KT-SPE Group[Электронный ресурс]. Режим доступа: https://kt-spegroup.ru/articles/osnovnye-printsipy-izmereniy-i-analiza-signalov/ (дата обращения: 16.04.2025).
22. Защита линий связи – обнаружение жучков [Электронный ресурс]. – Режим доступа: https://www.shpionam.net/zachita/zashhita-linij-svjazi (дата обращения: 16.04.2025).
23. Идентификация параметров источников побочных электромагнитных излучений:дис.. канд. техн. наук [Электрон. ресурс].Режим доступа:https://www.dissercat.com/content/identifikatsiya-parametrov-istochnikov-pobochnykh-elektromagnitnykh-izluchenii-po-izmereniya (дата обращения:16.04.2025).
24. Защита информации. Поисковая техника [Электронный ресурс]. – Режим доступа: https://bezar.ru/zaschita-informacii-poiskovaya-tehnika (дата обращения: 18.04.2025).

References:

1. Aleinikov A.A., Bilyatdinov K.Z., Krasov A.V., Levin M.V. Control, Measurement and Intelligent Traffic Management. St. Petersburg: Asterion, 2016; 92 p. ISBN 978-5-00045-385-8. – EDN WLROTL. (In Russ)
2. Orlov Yu.F. Active Identification of Control Objects. – Moscow: Bauman MSTU, 2010; 296 p. (In Russ)
3. Kuklin A.A., Kukushkin A.V. Radiotechnical Measurements:Textbook. Moscow: Radio i Svyaz, 2006;284 (In Russ)
4. Pozdnyakov S.A., Novikov Yu.A. Analysis of Electrical Circuits. Moscow: Vysshaya Shkola, 2008;368 p. (In Russ)
5. Gusev V.E., Trifonov Yu.I. Pulse Reflectometry. Moscow: Energiya, 1987; 214 p. (In Russ)
6. Bilyatdinov K.Z., Krasov A.V., Menyaylo V.V. Research of Systems and Analysis of Test Results. – St. Petersburg: Asterion, 2019; 362 p. – ISBN 978-5-00045-813-6. – EDN OXKBZW. (In Russ)
7. Orfanidis S.J. Electromagnetic Waves and Antennas [El. resource]. – Rutgers University, 2016; 954 p. – Available at: https://eceweb1.rutgers.edu/~orfanidi/ewa/ (accessed: 14.04.2025).
8. Kurose J.F., Ross K.W. Computer Networking:A Top-Down Approach. 8th ed. Boston:Pearson, 2020;896.
9. Kapralova I.A., Ignatiev M.S. Methods for Signal Analysis in Reflectometric Systems. *Bulletin of Bauman Moscow State Technical University. Series: Radioelectronics.* 2019;3:46–54. (In Russ)
10. Kamenev M.I., Belyakov E.I. Signals and Processes in Radiotechnical Systems. St. Petersburg: Lan', 2004; 432 p. (In Russ)
11. Chernov I.I., Korzh V.Ya. Electromagnetic Compatibility: Textbook. Moscow: Goryachaya Liniya – Telekom, 2011;360 p. (In Russ)
12. Mukhina I.A. Analysis of Methods for Protecting Local Area Networks from Unauthorized Access. *Information Technologies and Security*. 2018;1(15):25–31. (In Russ)
13. Jones S.B., Wraith J.M., Or D. Time Domain Reflectometry Measurement Principles and Applications. *Soil Science Society of America Journal*. 2002; 66(5):1479–1486.
14. Khromov S.P. Fundamentals of Analysis and Synthesis of Electrical Circuits. Moscow: Energoatomizdat, 2003; 408 p. (In Russ)
15. Krasilnikov V.I. Electromagnetic Transient Processes. Moscow: Akademiya, 2012; 304 p. (In Russ)
16. Petrenko P.B., Krivozubov P.A., Zaitsev D.I., Tokareva A.S. Improving the Accuracy of Reflectometry and Device Identification in Wired Communication Lines. *Proceedings of SPIIRAS.* 2011; 6:126–148. (In Russ)
17. Slovesnov N.A., Mirsatov S.F., Svetlichny V.V. Investigation of Equipment Identification Methods in Information Security Systems of Wired Communication Networks. *Information Security of Telecommunication Systems*. 2014; 4:53–60. (In Russ)
18. Identification of Parameters of Unintentional Electromagnetic Emission Sources in the Near Zone [El. resource].https://mai.ru/upload/iblock/db3/db3e2997c3d7df16a90199a3df149a48.pdf (accessed: 14.04.2025).
19. Fundamentals of Identification Measurements. *Journal of Radioelectronics* [Electronic resource]. – Available at: https://jre.cplire.ru/iso/nov06/2/text.html (accessed: 14.04.2025).
20. Methods and Means for Protecting Telephones and Communication Lines / BNTI [Electronic resource]. – Available at: https://www.bnti.ru/showart.asp?aid=68&lvl=04.03.02.&p=1 (accessed: 14.04.2025).
21. Basic Principles of Signal Measurement and Analysis / KT-SPE Group [Electronic resource]. – Available at: https://kt-spegroup.ru/articles/osnovnye-printsipy-izmereniy-i-analiza-signalov/ (accessed: 16.04.2025).
22. Communication Line Protection – Bug Detection [Electronic resource]. – Available at: https://www.shpionam.net/zachita/zashhita-linij-svjazi (accessed: 16.04.2025). (In Russ)
23. Identification of Parameters of Unintentional Electromagnetic Emission Sources: Cand. tech. sci. diss. [El. resource]. https://www.dissercat.com/content/identifikatsiya-parametrov-istochnikov-pobochnykh-elektromagnitnykh-izluchenii-po-izmereniya (accessed: 16.04.2025). (In Russ)
24. Information Security. Search Equipment [El.resource]. https://bezar.ru/zaschita-informacii-poiskovaya-tehnika (accessed: 18.04.2025). (In Russ)

Сведения об авторе:
Сергей Сергевич Васичкин, аспирант, кафедра защищенных систем связи, sergey_vasichkin@bk.ru
Information about authors:
Sergey S. Vasichkin, Postgraduate Student, Department of Secure Communication Systems, sergey_vasichkin@bk.ru

Конфликт интересов/Conflict of interest.
Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.
Поступила в редакцию/Received 10.08.2025**.**
Одобрена после рецензирования/Reviced 30.09.2025.
Принята в печать/Accepted for publication 26.01.2026.