Журнал зарегистрирован 01.03.2021 Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Свидетельство о регистрации ПИ № ФС 77-80320

Адрес издателя и редакции: 630073, г. Новосибирск, пр. К. Маркса, 20.
E-mail: office@publish.nstu.ru и digital-tech-security@mail.ru
Web site: http://publish.nstu.ru и http://journals.nstu.ru/digital-tech-security/

Publisher and editorial office adress: 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation

До номера 1 (100) 2021 г. включительно журнал выходил под названием «Сборник научных трудов НГТУ» (ISSN 2307-6879)

16+

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ

ISSN 2782-2230

№ 2 (121) **2026**

СОДЕРЖАНИЕ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Выпускающий редактор *И.П. Брованова*
Корректор *Л.Н. Киншт*
Компьютерная верстка *С.И. Ткачева*

Лицензия № ИД 04303 от 20.03.01. Подписано в печать 19.06.2026. Выход в свет 25.06.2026
Формат 60×84 1/16. Бумага офсетная. Тираж 300 экз. Уч.-изд. л. 6,51
Печ. л. 7,0. Изд. № 93. Заказ № 138. Цена свободная

Отпечатано в типографии
Новосибирского государственного технического университета
630073, г. Новосибирск, пр. К. Маркса, 20

Publisher and editorial adress: 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation
E-mail: office@publish.nstu.ru, digital-tech-security@mail.ru
Web site: http://publish.nstu.ru, http://journals.nstu.ru/digital-tech-security/

DIGITAL TECHNOLOGY SECURITY

ISSN 2782-2230

№ 2 (121) **2026**

CONTENTS

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

Publishing Editor *I.P. Brovanova*
Editor *L.N. Kinsht*
Computer imposition *S.I. Tkacheva*

License № ID 04303 from 20.03.01. Signed in print June 19, 2026
Date of publication June 25, 2026. Format 60 × 84 1/16
Offset Paper. Circulation is 300 copies. Educational-ed. liter. 6,51. printed pages 7,0
Publishing number 93. Order number 138

It is printed in printing house of Novosibirsk State Technical University
630073, Novosibirsk, 20 K. Marx Prospekt

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2026. – № 2 (121). – 9–36

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 338.2:005.922.1:004 DOI: 10.17212/2782-2230-2026-2-9-36

ФАКТОРЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В СФЕРЕ СТРОИТЕЛЬНОГО ДЕВЕЛОПМЕНТА*

И.А. ПЛОТНИКОВ[1], В.Д. КОЛЫЧЕВ[2]

[1] *РФ, 115409, г. Москва, Каширское шоссе, 31, Национальный исследовательский ядерный университет «МИФИ», студент 2-го курса магистратуры кафедры управления бизнес-проектами (№ 72) факультета бизнес-информатики и управления комплексными системами. E-mail: megavanek18@list.ru*

[2] *РФ, 115409, г. Москва, Каширское шоссе, 31, Национальный исследовательский ядерный университет «МИФИ», кандидат технических наук, доцент кафедры финансового мониторинга (№ 75) Института финансовых технологий и экономической безопасности. E-mail: kolychev@mephi.ru*

Исследование посвящено проблемам информационной безопасности в сфере строительного девелопмента в условиях цифровизации отрасли. Цель работы – систематизировать факторы информационной безопасности для строительного девелопмента, выявить основные угрозы и разработать рекомендации по защите информационных активов. Методология включает анализ нормативно-правовой базы (ФЗ-152 «О защите персональных данных», ГОСТ Р 58439.1-2019, ГОСТ Р 71452-2024), оценку актуальных киберугроз, изучение специфики информационных систем девелоперских компаний (в том числе с применением BIM-технологий), а также разработку системы ключевых показателей эффективности (KPI) и алгоритма их мониторинга. Выявлены основные угрозы: инсайдерские атаки, компрометация цепочки поставок, уязвимости облачной инфраструктуры, фишинг. Разработана методология обеспечения информационной безопасности, адаптированная к отраслевым особенностям (долгосрочность проектов, множественность участников, объемные BIM-модели). Сформирована система KPI, охватывающая технические (время обнаружения инцидентов, процент защищенных систем), организационные (обучение персонала, выполнение плана мероприятий) и нормативные показатели (соответствие ФЗ и ГОСТ). Предложен интегральный показатель результативности информационной безопасности и концепция панели мониторинга (дашборда) для визуализации данных. Результаты могут использоваться девелоперскими компаниями для построения и оценки систем защиты информации, принятия управленческих решений, прогнозирования рисков и минимизации ущерба от кибератак. Комплексный подход, сочетающий технические меры (DLP, IDS, шифрование), организационные мероприятия (обучение, аудит партнеров) и непрерывный мониторинг KPI,

* Статья получена 14 апреля 2026 г.

позволяет обеспечить устойчивую защиту информационных активов и превратить безопасность в конкурентное преимущество.

Ключевые слова: панель индикаторов безопасности, строительный девелопмент, киберугрозы, управление доступом, защита данных, информационные системы, ключевые показатели эффективности

ВВЕДЕНИЕ

Сфера строительного девелопмента, являющаяся важной экономической отраслью, активно изменяется в условиях повсеместного внедрения цифровых технологий в бизнес-процессы. Компании-девелоперы в настоящее время применяют интегрированные программные решения (экосистемы) для контроля реализации инвестиционно-строительных проектов и оперируют обширными массивами данных, включающими конфиденциальные материалы по объектам, финансовую отчетность, а также персональные данные заказчиков и контрагентов.

Как показывают статистические данные, в 2024 году в России было зарегистрировано 765,4 тыс. киберпреступлений, что на 13,1 % больше, чем годом ранее [1]. На долю организаций из стран СНГ в период с июля 2024 года по сентябрь 2025 года пришлось от 14 до 18 % всех результативных кибератак в мире, при этом процент успешных вторжений, завершившихся утечкой данных, возрос с 41 до 54 % [1]. Для девелоперской отрасли эти цифры особенно значимы, поскольку компании аккумулируют стратегически важные активы: архитектурные чертежи, сметную документацию, договоры, информацию о клиентах и инвестиционных планах.

Настоящая статья ставит своей целью обобщение сведений о значимых для строительного девелопмента факторах информационной безопасности, определение ключевых направлений угроз и формулировку предложений по созданию эффективной системы защиты информационных ресурсов.

Практическая значимость настоящей работы заключается в выработке предложений по разработке отраслевой методологии анализа проблем и направлений совершенствования деятельности в области информационной безопасности для компаний в сфере строительного девелопмента. Предлагаемая методология учитывает специфику сектора (применение BIM-технологий, продолжительный цикл реализации проектов, разветвленную сеть поставщиков) и современный ландшафт киберугроз.

В основе исследования лежит изучение действующей российской нормативно-правовой базы, международных стандартов и актуальных тенденций в области кибербезопасности.

1. ОСОБЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ В СФЕРЕ СТРОИТЕЛЬНОГО ДЕВЕЛОПМЕНТА

1.1. НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ И ТРЕБОВАНИЯ К ПРОЦЕССАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРОИТЕЛЬНОЙ ОТРАСЛИ

Российские правовые нормативно-технические акты в сфере информационной защиты направлены на создание многоуровневой системы требований к безопасности и хранению коммерческих данных, а также к сохранению ценной информации в момент их создания и к последующему практическому использованию для организаций в сфере строительного девелопмента.

- Федеральный закон № 152-ФЗ «О персональных данных». Этот закон вводит обязательные нормы по обработке и защите персональной информации, которую компании-девелоперы получают от своих клиентов. От организаций требуется внедрение комплекса технических и административных мер, таких как системы разграничения доступа, использование шифрования и непрерывное отслеживание инцидентов. Несоблюдение этих предписаний влечет за собой применение финансовых взысканий и может серьезно повлиять на деловую репутацию.
- ГОСТ Р 58439.1–2019. Указанный государственный стандарт регламентирует основные термины и принципы построения информационной среды при строительстве с применением BIM-технологий. Документ определяет порядок управления данными на всех этапах существования объекта – от проектирования до эксплуатации, уделяя особое внимание вопросам минимизации рисков и обеспечения защиты информации. Требования стандарта:

– формирование и фиксация в документах политики обращения с информацией;

– установление критериев информационной безопасности для каждой фазы реализации проекта;

– внедрение процедур, регулирующих доступ к данным;

– проведение регулярных проверок документированной оценки рисков, связанных с передачей информации.

- ГОСТ Р 71452–2024. Этот стандарт, действующий с 1 июля 2025 года, закрепляет принципы совмещения функциональной безопасности и киберзащиты на протяжении полного жизненного цикла систем промышленной автоматики (IACS). Несмотря на первостепенную направленность на промышленный сектор, его положения могут быть распространены и на системы управления зданиями и сооружениями. Стандарт обязывает использовать механизмы

контроля привилегий, защищенные криптографией каналы обмена данными, средства для управления уязвимостями и платформы для наблюдения за событиями безопасности.

1.2. УГРОЗЫ, ВЛИЯЮЩИЕ НА ЦИФРОВУЮ ТРАНСФОРМАЦИЮ СТРОИТЕЛЬНОЙ СФЕРЫ

Цифровизация строительной отрасли затрагивает все уровни – от проектирования до эксплуатации. Информационные технологии обеспечивают целостность данных, увеличивают производительность труда, выстраивают новые командные формы и упрощают взаимодействие участников сложных отраслевых строительных инвестиционных проектов, повышая гибкость и управляемость процессов на основе массивов данных, формируемых в режиме реального времени.

Современные IT-инструменты позволяют создавать строительные объекты быстрее и безопаснее, поскольку в цифровых процессах появляются механизмы автоматического контроля, прогнозирования и документирования. На уровне компаний образуется эффект, заключающийся в снижении издержек, ускорении выполнения работ, возрастании доли заимствований до 80 % за счет формирования документации в электронном виде; появляются возможности масштабирования проектов без увеличения числа ошибок за счет сокращения продолжительности жизненного цикла.

Информационные системы девелоперских компаний характеризуются специфическим набором функций и особенностями архитектуры. Современные корпоративные системы управления проектами (Project Management Information Systems), особенно в инвестиционно-строительной сфере, включают модули планирования, финансирования, контроля качества, управления человеческими ресурсами и логистики [14]. Кроме того, широкое внедрение технологии информационного моделирования (BIM – Building Information Modeling) создает сложные распределенные информационные среды, посредством которых множество участников цепочек поставок взаимодействуют через общие платформы хранения данных [2, 12].

Ниже перечислены специфические характеристики ИС в сфере девелопмента.

1. Множественность участников. В реализации проекта участвуют заказчики, проектировщики, подрядчики, субподрядчики, поставщики материалов, органы государственного контроля. Каждый участник требует дифференцированного доступа к информации, что существенно усложняет систему управления доступом.

2. Объемные графические данные. BIM-модели содержат большие объемы трехмерных чертежей, спецификаций и расчетов, требующих защиты от несанкционированного копирования.

3. Долгосрочность проектов. Жизненный цикл строительного проекта может составлять от нескольких лет до десятилетий, что подразумевает длительное хранение и управление конфиденциальной информацией [1].

4. Интеграция с облачными сервисами. Внедрение облачных решений для совместной работы команд в формате BaaS (Backend as a Service) создает новые векторы атак через ошибки в конфигурации облачной инфраструктуры [1].

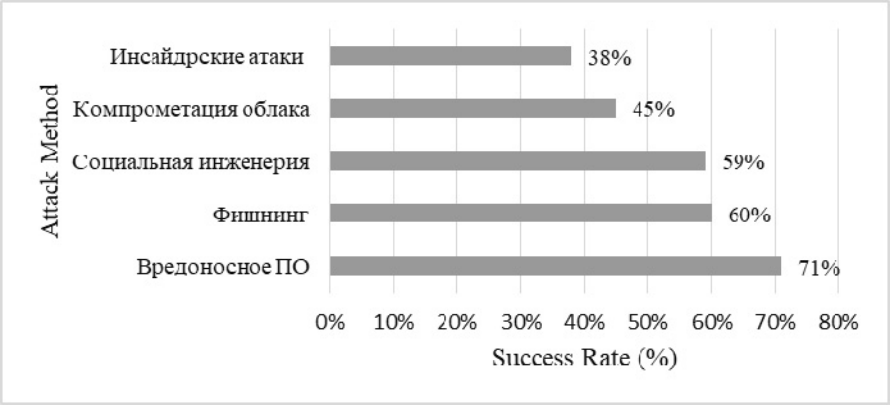


Рис. 1. Основные методы кибератак и процент успешных атак на организации СНГ в 2024–2025 годах

Fig. 1. Main methods of cyberattacks and the percentage of successful attacks on CIS organizations in 2024–2025

Ключевыми факторами, формирующими картину киберугроз в период 2025–2026 гг., остаются скорость цифровой трансформации и состояние международных отношений. Злоумышленники нацелены на нарушение функционирования стратегических цифровых активов предприятий, кражу и уничтожение информационных ресурсов, а также на подрыв деловой репутации организации.

Защита экономических интересов компании в строительной отрасли характеризуется сочетанием универсальных и отраслевых особенностей. Сравнительный анализ специфики обеспечения процессов экономической безопасности строительного сектора и практик, распространенных в смежных областях экономики, представлен в табл. 1.

Таблица 1

Table 1

Особенности обеспечения процессов экономической безопасности для строительных организаций [2, 8]

Features of ensuring economic security of construction organizations [2, 8]

Универсальные практики (сходства)	Отраслевые практики (различия)
1. Финансовый контроль и мониторинг вложений, расходов и доходов, сокращение финансовых рисков и оптимизация издержек	1. Особенности реализации инвестиционно-строительного проекта, имеющего ряд специфических характеристик: выбор площадки и месторасположение, рельеф местности, специальные требования к материалам или технологиям строительных работ
2. Управление, идентификация, анализ и моделирование рисков компании	2. Длительный инвестиционно-экономический цикл. Вопросы экономической безопасности при реализации длительного проекта становятся наиболее актуальными, поскольку наблюдается увеличение продолжительности жизненного цикла строительного проекта
3. Анализ законодательных норм и стандартов, включая налоговое законодательство, правила безопасности и трудовое право	3. Лицензирование и сертификации для реализации условий проведения высотных работ в замкнутых пространствах, включая необходимость получения лицензий для работы со специальным техническим оборудованием
4. Кадровая безопасность. Необходимость привлечения новых трудовых ресурсов и обеспечения их безопасности	4. Промышленная безопасность производства. Наличие высокого риска травматизма обусловливает необходимость обеспечения требований охраны труда одним из наиболее важных аспектов экономической безопасности

В сфере строительного бизнеса существуют универсальные проблемы, связанные с защитой финансовых интересов, но отраслевая специфика требует повышенного внимания к следующим аспектам: к организации инвестиционно-строительных процессов, минимизации рисков в рамках долгосрочных капитальных вложений и неукоснительному следованию жестким нормативам безопасности [3].

При оценке степени воздействия различных угроз на экономическую стабильность, безопасность и устойчивость строительной компании оказывается

важным распределить их по источнику возникновения: внешние или внутренние. Такая классификация позволяет четко определить, на каких группах рисков следует сконцентрировать дополнительные усилия, чтобы сократить возможность негативного воздействия на операционную, финансовую и инвестиционную деятельность, а также спрогнозировать потенциальный масштаб ущерба.

Визуализация угроз экономической безопасности в инвестиционно-строительной сфере представлена на рис. 2.

Рис. 2. Угрозы экономической безопасности строительных организаций

Fig. 2. Threats to the economic security of construction organizations

Очевидно, что уровень экономического ущерба, связанный с различными факторами и угрозами экономической безопасности в строительной сфере, может разниться и зависеть от горизонта планирования и оценки показателей

эффективности деятельности строительной компании, рыночной конъюнктуры, технологической развитости и уровня цифровизации.

Однако в последнее время наиболее очевидным является соотнесение угроз экономической безопасности, связанных с нарушением целостности объектов цифровой инфраструктуры строительной компании, с критическим или катастрофическим уровнем, поскольку проявление перечисленных угроз в практической деятельности компании приводит к частичной или полной приостановке процессов функционирования.

1.3. ОСОБЕННОСТИ ПРОЦЕССОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВНЕДРЕНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ СОЗДАНИЯ ЦИФРОВЫХ ДВОЙНИКОВ СТРОИТЕЛЬНЫХ ОБЪЕКТОВ

Внедрение автоматизированных систем создания цифровых двойников объектов в сфере строительного девелопмента инициирует разработку многоуровневой модели с регулярным изменением и возможной перестройкой необходимых для повышения информационной безопасности процессов.

1. В рамках анализа процессов информационной безопасности при внедрении цифровой системы класса BIM на предприятии необходимо предусмотреть следующее:

– дифференцированное предоставление прав доступа на основе функциональных ролей;

– двухфакторную аутентификацию для доступа к критичным данным и подсистемам цифровых двойников строительных объектов;

– логирование всех операций по работе с конфиденциальной информацией и данными, содержащими сведения контрактации или коммерческого характера;

– автоматизацию выявления и отзыва избыточных прав доступа [5].

2. Управление рисками инсайдерских атак требует разработки комплексной программы внутренней безопасности, включающей следующие действия:

– проведение регулярного обучения персонала основам информационной безопасности и социальной инженерии;

– проверку биографических данных при найме, особенно для должностей с доступом к критичной информации;

– мониторинг подозрительной активности пользователей в корпоративной сети;

– четкое определение классификации информации и правил работы с ней [7].

3. Технологии аудита и управление безопасностью логистических цепочек поставок в рамках внедрения BIM-системы подразумевают уменьшение

рисков компрометации посредством сети партнерств или контрагентов, при этом необходимо:

– проведение регулярных аудитов безопасности подрядчиков и субподрядчиков;

– включение требований информационной безопасности в контрактную документацию;

– использование контроля целостности кода и цифровых подписей для проверки обновлений программного обеспечения;

– разграничение доступа партнеров только к необходимому объему информации [2].

4. Для защиты облачной инфраструктуры в современных условиях работы цифровых сервисов и автоматизированной системы создания цифровых двойников необходимы следующие шаги:

– регулярный аудит конфигураций облачных сервисов для выявления некорректных настроек;

– внедрение систем управления конфигурациями (Configuration Management);

– непрерывный мониторинг облачной инфраструктуры и событий доступа;

– использование шифрования для защиты данных в облачном сервисе [2].

5. Применение современных технологий защиты данных в условиях создания цифровых моделей сложных строительных объектов подразумевает необходимость внедрения:

– систем контроля доступа к файловым хранилищам (Data Loss Prevention);

– антивирусной защиты и систем обнаружения вторжений;

– инструментов для управления уязвимостями и анализа безопасности;

– систем резервного копирования и аварийного восстановления [2].

6. Для непрерывного мониторинга и реагирования на инциденты в сфере информационной безопасности в современных условиях необходимы дополнительные усилия:

– организация центров управления безопасностью (Security Operations Center) или привлечение услуг управляемых поставщиков безопасности (Managed Security Service Provider);

– разработка регламентов и процедур реагирования на инциденты;

– проведение регулярных модельных сценарных экспериментов кибератак;

– постоянный анализ событий безопасности и уязвимостей [2].

На основе перечисленных выше направлений совершенствования процессов управления информационной безопасностью при внедрении автоматизи-

рованных систем создания цифровых двойников сложных объектов необходима разработка продуманной системы ключевых показателей эффективности для взвешенной и обоснованной оценки угроз и анализа рисков деятельности предприятий сферы строительного девелопмента.

2. СИСТЕМА КЛЮЧЕВЫХ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ДЛЯ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРОИТЕЛЬНОМ ДЕВЕЛОПМЕНТЕ

2.1. РАЗРАБОТКА НАБОРА ПОКАЗАТЕЛЕЙ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Эффективность системы информационной безопасности строительного предприятия представляет собой сложный комплексный показатель. Его формирование зависит от нескольких ключевых направлений деятельности компании: во-первых, от способности технических средств противостоять кибератакам и утечкам данных, во-вторых, от качества внутренних регламентов и действий сотрудников, направленных на защиту информации, и, в-третьих, от полноты соблюдения отраслевых стандартов и законодательства в данной сфере.

Для объективной оценки и дальнейшего развития системы безопасности необходима тщательно разработанная система ключевых показателей эффективности (KPI). Такой набор KPI должен быть сбалансированным, охватывать как операционные, так и стратегические цели и отражать специфику строительной отрасли.

Ключевые показатели эффективности для оценки информационной безопасности строительных компаний можно разделить на несколько основных групп. Технические KPI, такие как количество успешно отраженных атак, время обнаружения инцидентов, процент защищенных систем, являются основой для оценки технической защищенности. Организационные KPI, в свою очередь, фокусируются на эффективности процессов управления безопасностью: соблюдение сроков проведения аудитов, выполнение плана мероприятий по безопасности и процент сотрудников, прошедших обучение по ИБ [6].

Также значимыми являются и показатели, связанные с необходимостью выполнения нормативных требований и управлением рисками. Сюда относятся такие метрики, как количество нарушений законодательства, процент выполненных требований стандартов, уровень покрытия рисков мерами защиты,

а также показатели эффективности системы управления инцидентами. Кроме того, современные строительные компании всё чаще включают в свои системы оценки KPI, связанные с безопасностью цепочки поставок и защитой BIM-данных (например, уровень безопасности партнеров, степень защиты BIM-моделей, контроль доступа к проектной документации).

Таблица 2

Table 2

Технические показатели информационной безопасности

Technical indicators of information security

Показатель	Формула / методика расчета	Источник данных	Периодичность	Целевое значение
Количество успешно отраженных атак	Абсолютное число за период	Системы обнаружения вторжений, журналы безопасности	Ежемесячно	100 % критичных атак
Среднее время обнаружения инцидента	∑ (время обнаружения) / количество инцидентов	SIEM-системы, системы мониторинга	Ежемесячно	< 1 часа
Процент защищенных систем	Защищенные системы / все системы × 100 %	Инвентаризация ИТ-активов, системы защиты	Ежеквартально	≥ 95 %
Количество выявленных уязвимостей	Абсолютное число за период	Сканеры уязвимостей, системы управления уязвимостями	Ежемесячно	Ежегодное снижение
Процент устраненных уязвимостей	Устраненные уязвимости / выявленные уязвимости × 100 %	Системы управления уязвимостями, отчеты	Ежемесячно	≥ 90 % критичных

Набор представленных показателей может быть использован для повышения уровня безопасности цифровых систем класса BIM, в которых сохраняется актуальная информация о цифровых двойниках строительных объектов. Организационные показатели, представленные в табл. 3, применяются с целью улучшения организации процессов информационного аудита и повышения устойчивости цифровой инфраструктуры.

Таблица 3

Table 3

Организационные показатели информационной безопасности

Organizational indicators of information security

Показатель	Формула / методика расчета	Источник данных	Периодичность	Целевое значение
Процент сотрудников, прошедших обучение	Обученные сотрудники / все сотрудники × 100 %	Системы обучения, журналы инструктажей	Ежеквартально	100 %
Соблюдение сроков аудитов безопасности	Аудиты в срок / все аудиты × 100 %	План аудитов, отчеты	Ежеквартально	≥ 95 %
Выполнение плана мероприятий	Выполненные мероприятия / все мероприятия × 100 %	План мероприятий, отчеты	Ежемесячно	≥ 90 %
Количество инсайдерских инцидентов	Абсолютное число за период	Системы мониторинга, отчеты	Ежемесячно	0
Эффективность управления доступом	Нарушения доступа / все операции доступа × 100 %	Системы управления доступом, журналы	Ежемесячно	≤ 0,1 %

Набор показателей управления рисками и инцидентами, а также методики расчета достигнутых значений показателей эффективности процессов информационной безопасности для предприятия в сфере строительного девелопмента представлены в табл. 4.

Показатели эффективности процессов безопасности цепочки поставок и хранения данных, накапливаемых в цифровых системах, представлены в табл. 5.

Таблица 4

Table 4

Показатели соответствия и управления рисками

Compliance and Risk Management Indicators

Показатель	Формула / методика расчета	Источник данных	Периодичность	Целевое значение
Соответствие требованиям ФЗ-152	Выполненные требования / все требования × 100 %	Аудит соответствия, отчеты	Ежеквартально	100 %
Соответствие ГОСТ Р 58439.1–2019	Выполненные требования / все требования × 100 %	Аудит соответствия, отчеты	Ежеквартально	≥ 95 %
Уровень покрытия рисков	Риски с мерами / все риски × 100 %	Реестр рисков, план мероприятий	Ежеквартально	≥ 90 %
Среднее время реагирования на инцидент	∑ (время реагирования) / количество инцидентов	Системы управления инцидентами	Ежемесячно	Менее 4 часов
Эффективность восстановления	Успешные восстановления / все восстановления × 100 %	Системы резервного копирования, тесты	Ежеквартально	100 %

Таблица 5

Table 5

Показатели безопасности цепочки поставок и BIM-данных

Supply chain and BIM data security indicators

Показатель	Формула / методика расчета	Источник данных	Периодичность	Целевое значение
Уровень безопасности партнеров	Партнеры с аудитом / все партнеры × 100 %	База партнеров, отчеты аудитов	Ежеквартально	100 % ключевых партнеров
Защита BIM-моделей	Защищенные модели / все модели × 100 %	Системы управления BIM, системы защиты	Ежемесячно	100 %

Окончание табл. 5

End of the tab. 5

Показатель	Формула / методика расчета	Источник данных	Периодичность	Целевое значение
Контроль доступа к проектной документации	Нарушения доступа / все операции × 100 %	Системы управления документами, журналы	Ежемесячно	≤ 0,05 %
Безопасность облачной инфраструктуры	Аудит конфигураций / все конфигурации × 100 %	Системы управления облаком, отчеты	Ежемесячно	100 % критичных
Защита персональных данных	Нарушения защиты персональных данных / все операции × 100 %	Системы защиты персональных данных, отчеты	Ежемесячно	

Анализ предложенного набора показателей оценки эффективности процессов информационной безопасности предприятия в сфере строительного девелопмента позволяет обоснованно подойти к задаче формирования информационной панели индикаторов.

2.2. ФОРМИРОВАНИЕ ПАНЕЛИ МОНИТОРИНГА ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Создание эффективной панели мониторинга (дашборда) для оценки информационной безопасности строительной компании является стратегически важным шагом, направленным на повышение управляемости, прозрачности и, как следствие, защищенности информационных активов. В основе этой инициативы лежит четкое понимание основных целей, визуализацию которых выполняет дашборд, обеспечивающий мониторинг и оперативный контроль достижения установленных на этапах предварительного планирования ключевых показателей эффективности [8, 10] в сфере информационной безопасности в режиме реального времени. Это означает, что руководители и специалисты по ИБ должны иметь возможность в любой момент времени видеть актуальное состояние индикаторов по всем критически важным аспектам защиты информации.

Вторая ключевая цель – визуальные модели принятия управленческих решений в сфере информационной безопасности. Сложные массивы инфор-

мации, собранные из различных источников, зачастую трудно воспринимаются в виде таблиц или сырых данных. Дашборд трансформирует эти данные в наглядные графические модели [9], диаграммы и индикаторы, оперативно выявляя закономерности, сравнивая показатели и, самое главное, принимая обоснованные и своевременные управленческие решения, основанные на фактических достижениях измеряемых показателей эффективности деятельности [6, 9].

Не менее важной задачей является выявление проблемных зон и трендов в области информационной безопасности. Панель мониторинга должна отображать текущие значения, демонстрируя динамику изменения показателей эффективности, указывая на негативные тренды, отклонения от плановых значений показателей, отображая потенциальные риски [4]. Предлагаемый подход позволяет менеджменту компании оперативно реагировать на возникающие проблемы, прежде чем они преобразуются в угрозы различных уровней (см. рис. 2).

Система дашбордов [9] способствует повышению прозрачности процессов информационной безопасности, делая информацию о состоянии защиты доступной для всех заинтересованных сторон [15] на соответствующих уровнях управления [5].

Для достижения перечисленных выше целей система мониторинга должна решать немало задач, включая автоматизацию сбора данных из разнородных источников. В деятельности строительного предприятия используется широкий спектр инструментов обеспечения информационной безопасности, включая персонифицированные средства защиты данных, системы мониторинга событий (SIEM), решения для анализа уязвимостей, механизмы контроля доступа и регистрационные журналы. Объединение перечисленных компонентов в единую инфраструктуру для централизованной обработки данных – первостепенная задача, решение которой позволит сформировать и представить унифицированные отчеты из разных источников в едином стандартизированном формате [14], обеспечивая при этом настройку системы оповещений о критических отклонениях, уведомляя ответственных лиц о выходе показателей безопасности за допустимые пределы и гарантируя, что ни одна выявленная угроза не останется незамеченной.

При этом критически важной задачей остаётся и формирование обоснованной системы разграничения доступа для разных уровней управления. Дашборд должен быть адаптирован [9, 10] под потребности различных категорий пользователей – от топ-менеджеров, которым нужны обобщенные стратегические показатели, до специалистов по ИБ, которым необходима детальная техническая информация [13, 14].

2.3. АЛГОРИТМ ФОРМИРОВАНИЯ СИСТЕМЫ ИЗМЕРИТЕЛЕЙ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

Создаваемый алгоритм формирования системы показателей результативности информационной безопасности [8] включает четыре укрупненных этапа.

Первый этап заключается в составлении перечня показателей, которые отражают различные стороны процессов управления информационной безопасностью предприятия и являются значимыми для оценки.

Второй этап направлен на формирование обоснованной структуры системы показателей эффективности. На этом этапе устанавливаются цели процессов защиты информации, выявляются препятствия (ограничения), мешающие их достижению, проводится анализ этих препятствий и оценивается их степень влияния. Для количественного измерения предлагается использовать средневзвешенную оценку по формуле

$$P_i = \left(\sum R_{ij} V_{ij}\right) \Big/ n_i \ , \qquad (1)$$

где P_i – итоговая значимость *i*-го препятствия (в баллах), принимающая значения от 0 до 25; R_{ij} – оценка вероятности возникновения *i*-го препятствия, данная *j*-м экспертом (от 0 до 5 баллов). Оценка выставляется по шкале, где 0 баллов соответствует 0 % вероятности, а 5 баллов – 100 % вероятности; V_{ij} – оценка серьезности последствий *i*-го препятствия, данная *j*-м экспертом (от 0 до 5 баллов). Шкала серьезности построена следующим образом: 0 – последствия отсутствуют; 1 – незначительные последствия; 2 – последствия слабой значимости, способные повлиять на вспомогательные процессы; 3 – существенные последствия, затрагивающие основные процессы, снижающие конкурентоспособность и незначительно ухудшающие экономические показатели; 4 – серьезные последствия, ведущие к заметному ухудшению рыночных позиций и экономических результатов; 5 – критические последствия, способные привести к ликвидации организации; n_i – общее количество экспертных оценок, полученных для *i*-го препятствия.

Для отбора наиболее значимых препятствий применяется правило Парето: из всего множества выявленных проблем для дальнейшего анализа оставляют 20 % проблем, получивших наивысшие значения P_i. Второй этап завершается соответствием отобранных препятствий показателям из перечня, сформированного на первом этапе.

Третий этап включает непосредственно расчет показателей. На этом этапе определяют периодичность их измерения, фиксируют текущие значения, устанавливают целевые ориентиры и пороговые границы, а также вычисляют интегральный показатель результативности и разрабатывают план мероприятий, необходимых для достижения намеченных целей.

Четвертый этап предполагает разработку документа, регламентирующего функционирование системы, ввод ее в действие, проведение аудита и последующую эксплуатацию в установленном порядке.

Графическая модель предложенной последовательности действий представлена на рис. 3.

2.4. ИНТЕГРАЛЬНЫЙ ПОКАЗАТЕЛЬ РЕЗУЛЬТАТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для расчета интегрального показателя результативности информационной безопасности предложена следующая формула:

$$R = \frac{\sum_{i=1}^{n} P_i B_i f(\mathrm{KPI}_i)}{n}, \qquad (2)$$

где R – интегральный показатель результативности информационной безопасности; P_i – значимость (вес) i-го показателя панели индикаторов в баллах; B_i – балл в выбранной шкале, соответствующий достигнутому значению i-го показателя в одной из трех выделенных зон (измеренное достигнутое значение показателя ниже критического уровня соответствует зоне «1», или «красной зоне»; если значение выше критического, но ниже установленного целевого (нормативного) уровня – соответствие зоне «2», или «желтой зоне»; если достигнутое значение превосходит целевой уровень – соответствие зоне «3», или «зеленой зоне»); n – число показателей в сформированной информационной панели мониторинга.

С целью оценки достигнутых значений показателей будем использовать $f(\mathrm{KPI}_i)$ – функцию корректировки по конкретному значению KPI, при этом для маркировки сведений о наличии критических отклонений в значениях показателей введем следующую шкалу:

$$f(\mathrm{KPI}_i) = \begin{cases} 0{,}5, & \text{если в «красной зоне» (рискованно),} \\ 1{,}0, & \text{если в «желтой зоне» (умеренный риск),} \\ 1{,}5, & \text{если в «зеленой зоне» (идеально).} \end{cases} \qquad (3)$$

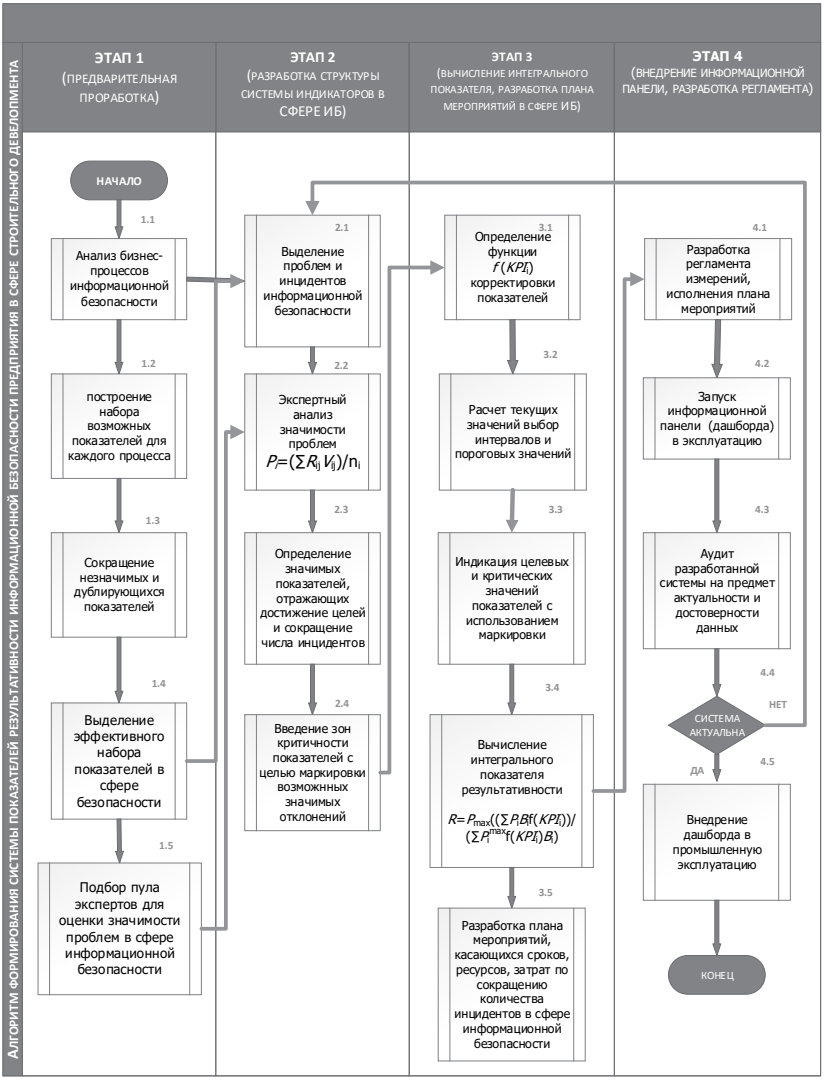


Рис. 3. Алгоритм формирования системы показателей результативности информационной безопасности предприятия в сфере строительного девелопмента

Fig. 3. Algorithm for forming a system of performance indicators for information security of an enterprise in the field of construction development

Модифицированная формула для определения интегрального показателя результативности приобретает следующий вид:

$$R = P_{\max}\left(\frac{\sum_{i=1}^{n} P_i B_i f(\mathrm{KPI}_i)}{\sum_{i=1}^{n} P_i^{\max} \max f(\mathrm{KPI}_i) \max B_i}\right), \quad (4)$$

где $P_i^{\max}$ – максимальный вес *i*-го показателя, $\max B_i$ – максимальный балл зоны (B_i), $f(\mathrm{KPI}_i)$ – коэффициент достижения значения показателя эффективности, при этом множитель $P_{\max}$ выступает в качестве нормировочного в установленном диапазоне значения показателя эффективности.

На рис. 4 представлена цветовая визуальная панель [9] для анализа ключевых показателей результативности процессов информационной безопасности предприятия [8] в сфере строительного девелопмента.

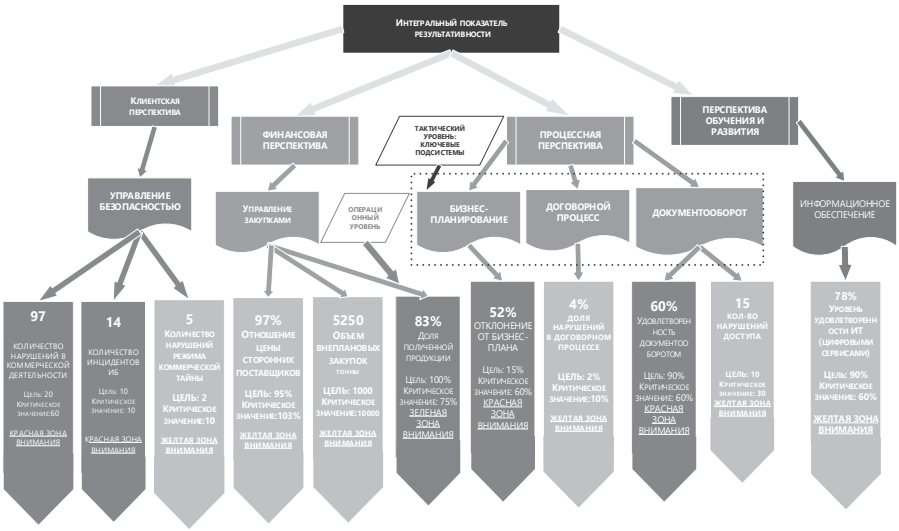


Рис. 4. Цветовая панель [9] отслеживания ключевых показателей результативности строительного предприятия

Fig. 4. Color panel [9] for tracking key performance indicators of a construction company

В соответствии с предлагаемым подходом каждый показатель в системе оценки результативности по итогам проведенных измерений может находиться в одном из трех состояний. Первое состояние фиксируется, когда фактическое значение оказывается ниже установленного критического порога (эта область обозначается как зона 1 либо «красная зона»). Второе состояние соответствует значениям, превышающим критический уровень, но еще не достигшим запланированного целевого ориентира (зона 2 или «желтая зона»). Третье состояние наступает при превышении целевого значения (зона 3, или «зеленая зона»). Для обеспечения возможности последующих вычислений каждому из указанных состояний может быть поставлен в соответствие числовой коэффициент. С целью индикации «красной зоны», как было отмечено ранее, предусматривается значение «–1», для индикации «желтой зоны» – «0», для индикации зеленой зоны – «+1».

Внедрение системы ключевых показателей эффективности для оценки информационной безопасности в строительном девелопменте [11] позволяет не только контролировать текущее состояние защиты информационных активов, но и создавать основу для их непрерывного совершенствования. Предложенная система KPI охватывает все ключевые аспекты информационной безопасности: техническую защищенность, организационные меры, соответствие нормативным требованиям, управление рисками, безопасность цепочки поставок и защиту BIM-данных [12].

Панели индикаторов (*dashboards*) представляют собой мощный инструмент управления информационной безопасностью, который демонстрирует свою высокую эффективность в условиях турбулентной экономической среды и растущих киберугроз [9]. Они способны оперативно удовлетворять трансформирующиеся потребности менеджмента [14], предоставляя наглядную и структурированную информацию о ключевых аспектах защиты информационных активов [13].

Эффективность внедрения системы KPI в сфере информационной безопасности в значительной степени обусловлена процессом выбора набора показателей. Качество и релевантность выбранных индикаторов обеспечивает информационную наполненность, содержательность и полезность систем мониторинга. В системе должны присутствовать показатели, отражающие различные перспективы информационной безопасности, что обеспечивает комплексное видение ситуации.

На рис. 5 представлена модель отображения отобранных значений показателей результативности в формате диаграммы, которая может быть использована в качестве панели мониторинга (дашборда) для повышения эффективности принимаемых решений [8, 9] в сфере информационной безопасности.

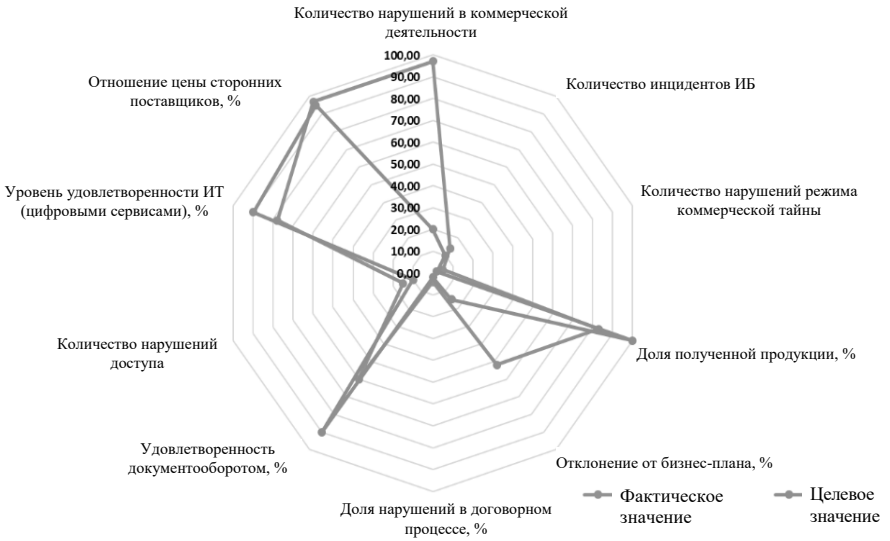


Рис. 5. Модель визуализации показателей эффективности информационной безопасности предприятия в сфере строительного девелопмента

Fig. 5. Model for visualizing the performance indicators of information security of an enterprise in the field of construction development

Таким образом, оказывается возможным формировать и анализировать новые формы и методы развития технологий информационной безопасности, защиты данных и связанной с ними процессной деятельности на предприятии [11], прикладывая дополнительные усилия по поддержанию устойчивого уровня роста, развитию организации на основе полученных значений показателей эффективности, сопоставляя их с установленными на этапах предварительного планирования целевыми значениями [13].

По мнению авторов, предложенная методика позволяет строительным компаниям [10, 11] не только оценивать текущее состояние информационной безопасности, но и прогнозировать будущие риски, принимать обоснованные управленческие решения и обеспечивать устойчивое развитие системы защиты информационных активов в условиях цифровой трансформации строительной отрасли [13, 15].

ЗАКЛЮЧЕНИЕ

В ходе проведенного исследования систематизированы и проанализированы ключевые факторы информационной безопасности, актуальные при внедрении и использовании автоматизированных систем в сфере строительного девелопмента в условиях активной цифровизации отрасли.

Специфика информационных систем в строительном девелопменте предопределяет специфический набор требований для организации процессов информационной безопасности. Множественность участников инвестиционно-строительных проектов, работа с объемными BIM-моделями и цифровыми двойниками строительных объектов, долгосрочность жизненного цикла объектов и интеграция с облачными сервисами создают сложную инфраструктуру и архитектуру информационных активов, требующую дифференцированного подхода, в частности, к правилам и регламентам управления доступом. Предложения по организации процессов информационной безопасности на предприятиях в сфере строительного девелопмента разработана с учетом анализа отраслевых особенностей и их влияния на формирование рисков и выполнения условий безопасной эксплуатации объектов на основе технологий цифровизации.

Как показал анализ нормативно-правовой базы, включая Федеральный закон № 152-ФЗ и стандарты серии ГОСТ Р (58439.1–2019, 71452–2024), устанавливаются обязательные условия защиты персональных данных и информации на протяжении всего жизненного цикла строительного объекта, что является не только юридической необходимостью, но и основой для выстраивания доверительных отношений с клиентами, партнерами и контрагентами и обеспечивает экономическую безопасность и снижение рисков возможной компрометации деятельности компании.

Проведенный анализ ландшафта угроз показывает, что строительные компании сталкиваются как с распространенными киберугрозами (фишинг, ransomware), так и со специфическими рисками, такими как компрометация цепочки поставок через субподрядчиков, инсайдерские атаки со стороны сотрудников и уязвимости в конфигурации облачной инфраструктуры. Набор мер по организации эффективной системы защиты должен быть комплексным и включать не только технические меры (DLP, IDS, шифрование), но и организационные – регулярное обучение персонала, аудит партнеров и разработку согласованных и непротиворечивых регламентов работы с конфиденциальной информацией.

Предложенная в статье методика построения системы показателей результативности на основе панелей мониторинга (dashboards) позволяет интегрировать показатели результативности управления процессами информаци-

онной безопасности в общую систему управления компанией [8]. В частности, включение таких индикаторов, как количество инцидентов информационной безопасности или степень соблюдения режима коммерческой тайны, в единую панель KPI делает безопасность измеримым и управляемым бизнес-процессом [9], а не обособленной технической функцией.

Реализация предложенных мер – от внедрения систем управления цифровыми двойниками сложных строительных объектов, разработки многоуровневой системы управления доступом и повышения информационной безопасности до создания центра мониторинга и реагирования на инциденты (SOC) – требует существенных инвестиционных вложений и проведения серии организационных изменений. Однако такого рода затраты следует рассматривать как стратегические инвестиции в устойчивость бизнеса и повышение капитализации, поскольку ущерб от успешной кибератаки может многократно превысить расходы на превентивную защиту, приводя не только к прямым финансовым потерям, но и к репутационному дефолту, срыву сроков реализации проектов и кратному превышению первоначальных плановых смет.

Внедрение цифровых технологий в сфере девелопмента направлено на формирование новой автоматизированной среды взаимодействия стейкхолдеров в цепочках поставок и создает виртуальную среду, включая системы класса BIM – цифровых двойников сложных строительных объектов.

Эффект от цифровизации заключается в повышении синхронности работы над проектом, сокращении числа ошибок, увеличении количества заимствований при создании модели объекта на основе типовых проработанных решений или лучших отраслевых практик и способствует непрерывному обмену цифровыми ресурсами.

Обеспечение информационной безопасности в строительном девелопменте представляет собой непрерывный и динамичный процесс, требующий адаптации к меняющимся цифровым технологиям с учетом изменения нормативных требований и к новым, всё более развитым методам кибератак, взломов и действий злоумышленников.

Таким образом, информационная безопасность в сфере строительного девелопмента достигается за счет синергетического эффекта внедряемых технологических решений, рационально выстроенных процессов и осознания важности защиты конфиденциальных данных на всех уровнях управления компанией, комплексного подхода при защите информационных активов и цепочек создания стоимости, превращения безопасности в конкурентное преимущество, повышения доверия инвесторов, заказчиков, регуляторов и контрагентов.

СПИСОК ЛИТЕРАТУРЫ

1. *Клименко К.Е., Котляревский А.А.* Информационные системы как основа современного строительства // Инновации и инвестиции. – 2023. – № 5. – URL: https://cyberleninka.ru/article/n/informatsionnye-sistemy-kak-osnova-sovremennogo-stroitelstva (дата обращения: 25.02.2026). – EDN: WNCLGR.

2. *Норец Н.К.* Обеспечение кибербезопасности в строительной отрасли // Проблемы информационной безопасности социально-экономических систем: труды IX Международной научно-практической конференции, Гурзуф, 02–04 марта 2023 г. – Симферополь, 2023. – С. 148–150. – EDN: UXMDRS.

3. *Стрункина М.С., Воробьева А.В.* Разработка системы информационной безопасности для строительной компании // Международный научно-исследовательский журнал. – 2016. – № 10-2 (52). – URL: https://cyberleninka.ru/article/n/razrabotka-sistemy-informatsionnoy-bezopasnosti-dlya-stroitelnoy-kompanii (дата обращения: 25.02.2026). – EDN: WWSDEF.

4. *Цыпылова Р.Н.* Цифровая трансформация строительной отрасли: преимущества и вызовы // Научный аспект. – 2024. – Т. 55, № 6. – С. 7107–7114. – EDN: YGOCEB.

5. *Шевко Н.Р., Коростиева В.С.* Кибербезопасность в строительстве // Информационные технологии в строительных, социальных и экономических системах. – 2025. – № 2 (36). – С. 172–175. – EDN: KCNVJX.

6. *Щепкина Н.Н.* Оценка рисков информационной безопасности строительных предприятий // Вестник МГСУ. – 2022. – Т. 17, № 11. – URL: https://cyberleninka.ru/article/n/otsenka-riskov-informatsionnoy-bezopasnosti-stroitelnyh-predpriyatiy (дата обращения: 25.02.2026). – EDN: RQDDOZ.

7. *Ovsiannikova T.Yu., Patsukov A.A.* Building information modelling systems: strategic objectives and realities of digital transformation in construction // Недвижимость: экономика, управление. – 2022. – № 1. – С. 13–18. – DOI: 10.22337/2073-8412-2022-1-13-18. – EDN: VJSJCW.

8. *Колычев В.Д., Буданов Н.А.* Комплексная методика оценки рисков информационной безопасности в коммерческом банке // Безопасность информационных технологий. – 2021. – Т. 28, № 2. – С. 83–97. – DOI: 10.26583/bit.2021.2.08. – EDN: MHMRJK.

9. *Kolychev V.D., Shebotinov A.A.* Application of business intelligence instrumental tools for visualization of key performance indicators of an enterprise in telecommunications // Научная визуализация. – 2019. – Т. 11, № 1. – С. 20–37. – DOI: 10.26583/sv.11.1.03. – EDN: CZNAPN.

10. *Копалеишвили М.Д.* Цифровая трансформация девелопмента: инновационные технологии и маркетинговые стратегии как фактор устойчивости в условиях экономической нестабильности // Актуальные проблемы экономики и управления в строительстве: материалы III Национальной (Всероссийской) научно-практической конференции с международным участием. – СПб., 2025. – С. 368–375. – EDN: CGAKZG.

11. *Кисель Т.Н., Прохорова Ю.С.* Исследование уровня цифровизации на российских предприятиях инвестиционно-строительной сферы: монография. – М.: Изд-во МИСИ – МГСУ, 2023. – DOI: 10.22227/978-5-7264-3243-4.2023.53.

12. *Субботина Н.А., Нам Г.Е., Георгиади В.В.* BIM-моделирование как инструмент внедрения принципов OH&S в строительство // BIM-моделирование в задачах строительства и архитектуры: материалы II Международной научно-практической конференции. – СПб., 2019. – С. 91–95. – DOI: 10.23968/BIMAC.2019.016.

13. *Сулимова Е.А., Новицкая Д.А.* Развитие цифровой экономики в сфере строительства // Экономика строительства. – 2022. – № 10. – С. 89–95. – EDN: JIFDVM.

14. *Куровский С.В., Мишин Д.А., Самойленко А.В.* Методические и системные решения управления строительными проектами: проблемы их практического применения и направления их предотвращения // Экономика и управление: проблемы, решения. – 2025. – Т. 10, № 6 (159). – С. 42–54. – DOI: 10.36871/ek.up.p.r.2025.06.10.005.

15. *Рябоконь А.И., Черканов Н.С.* Особенности цифровизации процессов девелопмента недвижимости // Передовые технологии и инновации в образовании и науке для улучшения качества жизни и стимулирования устойчивого экономического роста: сборник статей VIII Международной научно-технической конференции. В 3-х томах. Минск, 2025. – Т. 2. – С. 327–330. – EDN: XZKHJW.

DOI: 10.17212/2782-2230-2026-2-9-36

Security factors of information systems in the construction development sphere*

I.A. Plotnikov[1], V.D. Kolychev [2]

[1] *National Research Nuclear University MEPhI, 31 Kashirskoye Shosse, Moscow, 115409, Russian Federation, second-year Master's student of the Department of Business Project Management (No. 72), Faculty of Business Informatics and Integrated Systems Management. E-mail: megavanek18@list.ru*
[2] *National Research Nuclear University MEPhI, 31 Kashirskoye Shosse, Moscow, 115409, Russian Federation, Candidate of Technical Sciences, Associate Professor of the Department of Financial Monitoring (No. 75), Institute of Financial Technologies and Economic Security. E-mail: kolychev@mephi.ru*

The research is devoted to the problems of information security in the field of construction development in the context of digitalization of the industry. The purpose of the work is to systematize information security factors for construction development, identify the main threats and develop recommendations for the protection of information assets. The methodology includes an analysis of the regulatory framework (FZ-152 "On Personal Data Protection", GOST R 58439.1–2019, GOST R 71452–2024), an assessment of current cyber threats, and a study of the specifics of information systems of development companies (including using BIM technologies), as well as the development of a system of key performance indicators (KPIs) and an algorithm for monitoring them. Results: the main threats have been identified: insider attacks, supply chain compromise, cloud infrastructure vulnerabilities, phishing; an information security methodology has been developed, adapted to industry specifics (long-term projects, multiple participants, voluminous BIM models); A KPI system has been formed, covering technical (incident detection time, percentage of protected systems), organizational (staff training, implementation of the action plan) and regulatory indicators (compliance with Federal Law and GOST); An integrated information security performance indicator and the concept of a dashboard for data visualization have been proposed. Scope of application: the results can be used by development companies to build and evaluate information security systems, make management decisions, predict risks and minimize damage from cyber attacks. Conclusions: an integrated approach combining technical measures (DLP, IDS, encryption), organizational measures (training, audit of partners) and continuous monitoring of KPIs allows for sustainable protection of information assets and turn security into a competitive advantage.

Keywords: security indicators panel, construction development, cyber threats, access control, data protection, information systems, key performance indicators

REFERENCES

1. Klimenko K.E., Kotlyarevskii A.A. Informatsionnye sistemy kak osnova sovremennogo stroitel'stva [Information systems as the backbone of modern construction]. *Innovacii i investicii*, 2023, no. 5. (In Russian). Available at:

* *Received 14 April 2026.*

https://cyberleninka.ru/article/n/informatsionnye-sistemy-kak-osnova-sovremennogo-stroitelstva (accessed 25.02.2026).

2. Norets N.K. [Ensuring cybersecurity in the construction industry]. *Problemy informatsionnoi bezopasnosti sotsial'no-ekonomicheskikh sistem* [Problems of information security of socio-economic systems]. Proceedings of the IX International Scientific and Practical Conference, Gurzuf, March 02–04, 2023. Simferopo, 2023, pp. 148–150. (In Russian).

3. Strunkina M.S., Vorobyeva A.V. Razrabotka sistemy informatsionnoi bezopasnosti dlya stroitel'noi kompanii [Development of an information security system for a construction company]. *Mezhdunarodnyi nauchno-issledovatel'skii zhurnal = International Research Journal*, 2016, no. 10-2 (52). Available at: https://cyberleninka.ru/article/n/razrabotka-sistemy-informatsionnoy-bezopasnosti-dlya-stroitelnoy-kompanii (accessed 25.02.2026).

4. Tsypylova R.N. Tsifrovaya transformatsiya stroitel'noi otrasli: preimushchestva i vyzovy [Digital transformation of the construction industry: advantages and challenges]. *Nauchnyi aspect*, 2024, vol. 55, no. 6, pp. 7107–7114. (In Russian).

5. Shevko N.R., Korostieva V.S. Kiberbezopasnost' v stroitel'stve [Cybersecurity in construction]. *Informatsionnye tekhnologii v stroitel'nykh, sotsial'nykh i ekonomicheskikh sistemakh*, 2025, no. 2 (36), pp. 172–175.

6. Shchepkina N.N. Otsenka riskov informatsionnoi bezopasnosti stroitel'nykh predpriyatii [Assessment of information security risks for construction enterprises]. *Vestnik MGSU = Monthly Journal on Construction and Architecture*, 2022, vol. 17, no. 11. Available at: https://cyberleninka.ru/article/n/otsenka-riskov-informatsionnoy-bezopasnosti-stroitelnyh-predpriyatiy (accessed 25.02.2026).

7. Ovsiannikova T.Yu., Patsukov A.A. Building information modelling systems: strategic objectives and realities of digital transformation in construction. *Nedvizhimost': ekonomika, upravlenie = Real Estate: Economics, Management*, 2022, no. 1, pp. 13–18. DOI: 10.22337/2073-8412-2022-1-13-18.

8. Kolychev V.D., Budanov N.A. Kompleksnaya metodika otsenki riskov informatsionnoi bezopasnosti v kommercheskom banke [Development of a comprehensive methodology for assessing information security risks in a commercial bank]. *Bezopasnost' informatsionnykh tekhnologii = IT Security*, 2021, vol. 28, no. 2, pp. 83–97. DOI: 10.26583/bit.2021.2.08

9. Kolychev V.D., Shebotinov A.A. Application of business intelligence instrumental tools for visualization of key performance indicators of an enterprise in telecommunications. *Nauchnaya vizualizatsiya = Scientific Visualization*, 2019, vol. 11, no. 1, pp. 20–37.

10. Kopaleishvili M.D. [Digital transformation of real estate development: innovative technologies and marketing strategies as a factor of sustainability in conditions of economic instability]. *Aktual'nye problemy ekonomiki i upravleniya v*

stroitel'stve [Current Issues in Economics and Management in Construction]. Materials of the III National (All-Russian) Scientific and Practical Conference with International Participation, St. Petersburg, 2025, pp. 368–375. (In Russian).

11. Kisel' T.N., Prokhorova Yu.S. *Issledovanie urovnya tsifrovizatsii na rossiiskikh predpriyatiyakh investitsionno-stroitel'noi sfery* [A study of the level of digitalization in Russian enterprises of the investment and construction sector]. Moscow, MISI – MGSU Publ., 2023. DOI: 10.22227/978-5-7264-3243-4.2023.53.

12. Subbotina N.A., Nam G.E., Georgiadi V.V. [BIM-modeling as a tool for the implementation of OH&S principles in construction]. *BIM-modelirovanie v zadachakh stroitel'stva i arkhitektury* [BIM in construction & architecture]. Materials of the II International Scientific and Practical Conference, St. Prtrsburg, 2019, pp. 91–95. DOI: 10.23968/BIMAC.2019.016. (In Russian).

13. Sulimova E.A., Novitskaya D.A. Razvitie tsifrovoi ekonomiki v sfere stroitel'stva. [Development of the digital economy in the construction industry]. *Ekonomika stroitel'stva = Economics of Construction*, 2022, no. 10, pp. 89–95.

14. Kurovsky S.V., Mishin D.A., Samoylenko A.V. Metodicheskie i sistemnye resheniya upravleniya stroitel'nymi proektami: problemy ikh prakticheskogo primeneniya i napravleniya ikh predotvrashcheniya [Methodological and system solutions for managing construction projects: problems of their practical application and directions for their prevention]. *Ekonomika i upravlenie: problemy, resheniya = Economics and Management: Problems, Solutions*, 2025, vol. 10, no. 6 (159), pp. 42–54. DOI: 10.36871/ek.up.p.r.2025.06.10.005.

15. Ryabokon A.I., Cherkanov N.S. [Features of digitalization in real estate development processes]. *Peredovye tekhnologii i innovatsii v obrazovanii i nauke dlya uluchsheniya kachestva zhizni i stimulirovaniya ustoichivogo ekonomicheskogo rosta* [Advanced technologies and innovations in education and science for improving the quality of life and stimulating sustainable economic growth]. Collection of Articles of the VIII International Scientific and Technical Conference. Minsk, 2025, vol. 2, pp. 327–330.

Для цитирования:

Плотников И.А., Колычев В.Д. Факторы безопасности информационных систем в сфере строительного девелопмента // Безопасность цифровых технологий. – 2026. – № 2 (121). – С. 9–36. – DOI: 10.17212/2782-2230-2026-2-9-36.

For citation:

Plotnikov I.A., Kolychev V.D. Faktory bezopasnosti informatsionnykh sistem v sfere stroitel'nogo developmenta [Security factors of information systems in the construction development sphere]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2026, no. 2 (121), pp. 9–36. DOI: 10.17212/2782-2230-2026-2-9-36.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2026. – № 2 (121). – 37–49

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.93 DOI: 10.17212/2782-2230-2026-2-37-49

ИССЛЕДОВАНИЕ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ И РАЗРАБОТКА ВЕБ-ПРИЛОЖЕНИЯ ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПО ЛИЦУ С ИСПОЛЬЗОВАНИЕМ БИБЛИОТЕК МАШИННОГО ОБУЧЕНИЯ*

В.В. ПЕРЕВОЗНИКОВ[1], К.Д. ГАРБУЛИН[2]

[1] *РФ, 614030, г. Пермь, ул. Гремячий лог, 1, Пермский военный институт Войск национальной гвардии Российской Федерации, доцент кафедры автоматизации управления войсками и информационной безопасности. E-mail: perevoznikovvv@rosgvard.ru*
[2] *РФ, 614030, г. Пермь, ул. Гремячий лог, 1, Пермский военный институт Войск национальной гвардии Российской Федерации, курсант факультета связи и автоматизированного управления войсками. E-mail: garbulinkd@rosgvard.ru*

В настоящей работе рассматриваются методы биометрической аутентификации в целях минимизации несанкционированного доступа к конфиденциальной информации. Осуществлен сравнительный анализ подходов к детекции и верификации личности с акцентом на технологию распознавания лиц на основе глубоких нейронных сетей. Практической составляющей исследования является разработка веб-приложения, реализующего аутентификацию пользователя по лицу. В работе описана архитектура программной системы, этапы обработки изображений (детекция, выравнивание, экстракция признаков) и интеграция обученных моделей машинного в бэкенд на языке Python с использованием фреймворков Django и библиотеки DeepFace. Приведены результаты экспериментальной оценки точности и производительности предложенного решения.

Ключевые слова: биометрическая аутентификация, распознавание лиц, машинное обучение, сверточные нейронные сети, веб-разработка, DeepFace, Django, информационная безопасность

* Статья получена 17 апреля 2026 г.

ВВЕДЕНИЕ

С непрерывным совершенствованием цифровых сервисов и одновременным повышением уровня требований к информационной безопасности информационных ресурсов ограниченного доступа автоматизированные системы доступа, использующие традиционные методы аутентификации на основе пароля или PIN-кода, физического носителя в виде ключа-карты, демонстрируют свою недостаточную эффективность [1]. К основным проблемам таких методов можно отнести низкую устойчивость парольной защиты от фишинга, возможность перехвата ключевой информации, а также неудобство запоминания сложных парольных комбинаций. Уязвимостями физических носителей может быть их повреждение, утеря или похищение злоумышленником [1, 3].

В связи с достаточным количеством перечисленных негативных факторов, присущих классическим методам аутентификации, возникает вполне обоснованная причина для разработки и внедрения биометрических систем доступа к защищаемым ресурсам. Биометрическая аутентификация, основанная на верифицировании уникальных физических характеристик человека, лишена подобных недостатков, поскольку подделывание подобных атрибутов является максимально трудоемкой технической задачей.

Цель настоящей работы – на основе существующих методов биометрической аутентификации осуществить исследование эффективных методов машинного обучения для задачи верификации личности, разработать архитектуру и прототип программного решения, обеспечивающего безопасный вход в систему посредством анализа видеопотока с камеры пользователя.

ОБЗОР МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Среди основных методов биометрической аутентификации выделяют два основных: статические методы (физиологические) и динамические методы (поведенческие) [4, 5].

Кратко рассмотрим наиболее популярные статические методы, использующие уникальные анатомические характеристики, которые остаются продолжительно неизменными в течение жизни.

1. Сканирование отпечатков пальцев. Этот метод основан на считывании уникального папиллярного узора пальца. Отпечаток, полученный с помощью сканера, преобразуется в цифровой код, а затем сравнивается с ранее введенными в базу данных наборами эталонов.

2. Распознавание лица. Такой метод использует 2D-/3D-технологии фиксации черт лица в виде цифровой модели (дескрипторы лица) с последующим сравнением с эталонами.

3. Сканирование радужной оболочки или сетчатки глаза. Является высокоточным методом, основанным на уникальном рисунке глаза.

4. Геометрия руки. Принцип работы этого метода заложен в измерении и анализе формы и размера кисти.

Динамические методы основаны на анализе привычек и особенностей поведения человека, проявляемых при его деятельности.

1. Голосовая аутентификация. Этот метод основывается на использовании данных анализа тембра, частоты и ритма речи.

2. Клавиатурный почерк. Принцип работы этого метода заключается в измерении и анализе ритма и скорости набора текста.

3. Анализ подписи. Основан на детекции особенностей почерка в динамике (учитывает не только начертание, но и скорость и нажим).

4. Анализ походки. Такой метод основывается на распознавании человека по манере движения.

В настоящей работе мы уделим внимание аутентификации на основе метода распознавания лица, которое человек всегда «носит с собой». Этот метод имеет ключевое преимущество: он не требует прямого физического контакта со сканирующим устройством и может быть реализован с использованием стандартных веб-камер, что делает его идеальным для интеграции в веб-приложения. Благодаря технологическому прорыву в области глубокого обучения искусственных нейронных сетей и появлению специализированных программных библиотек можно достичь точности распознавания объектов, сопоставимой с человеческим зрением.

1. ЭТАПЫ ПРОЦЕССА РАСПОЗНАВАНИЯ ЛИЦ

Процесс автоматического программного распознавания лиц состоит из нескольких этапов, к каждому из которых предъявляются высокие требования к точности и скорости работы [2].

1. Детекция лица. Первичный этап, на котором необходимо выделить контуры лица на фотографии или в видеопотоке. Классические методы, такие как каскады Хаара, хорошо работают лишь на фронтальных положениях лица, так как чувствительны к поворотам головы и яркости освещения. Современные подходы базируются на использовании многослойных нейросетей. Так, нейросетевая архитектура MTCNN (Multi-Task Cascaded Convolutional Networks) является одним из наиболее популярных решений, поскольку не только обнаруживает лицо, но и определяет ключевые точки (глаза, нос, уголки рта) для последующего выравнивания.

2. Нормализация и выравнивание. Для инвариантности к поворотам изображение лица приводится к стандартному виду на основе найденных ключевых точек.

3. Извлечение признаков и верификация. На этом этапе лицо преобразуется в числовое векторное представление – эмбеддинг (embedding). Здесь задача дифференциации изображений состоит в том, чтобы «сжатые» лица одного человека в векторном пространстве находились близко друг к другу, а нескольких – далеко.

3. Выбор метрического подхода к глубокому обучению. Чаще используется архитектура на основе сверточной нейронной сети (CNN) и специальные функции потерь (Triplet Loss, Additive Angular Margin Loss), которые напрямую оптимизируют расстояние между векторами признаков. Также используются предобученные модели на огромных датасетах с человеческими лицами (например, VGGFace2, MS-Celeb-1M).

4. Сравнение. Полученный эмбеддинг сравнивается с эмбеддингами, хранящимися в базе данных. Обычно используется вычисление косинусного расстояния или евклидовой метрики. Порог принятия решения определяется экспериментально для баланса между ложными срабатываниями (FAR) и ложными отказами (FRR).

2. АРХИТЕКТУРА И РЕАЛИЗАЦИЯ ВЕБ-ПРИЛОЖЕНИЯ

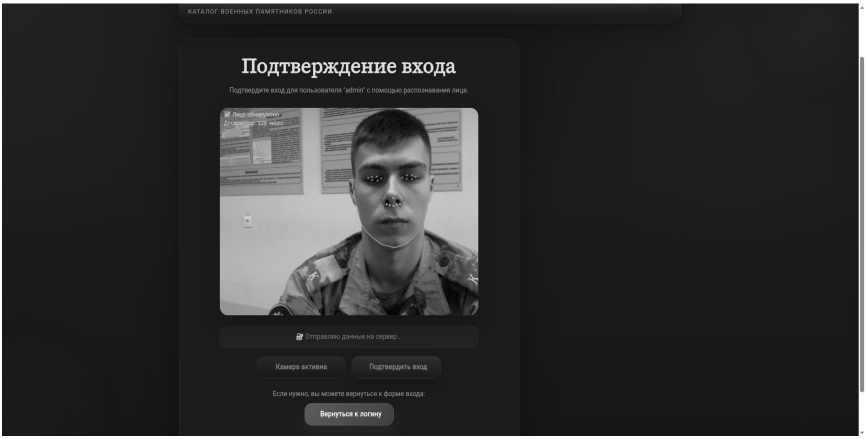
Разработанное нами веб-приложение построено по классической клиент-серверной архитектуре. Основная логика обработки данных вынесена на удаленный сервер для обеспечения безопасности и возможности использования тяжелых вычислительных моделей.

В качестве серверного языка программирования выбран Python. Основой веб-приложения стал фреймворк Django, имеющий встроенную админ-панель, ORM для работы с базой данных, систему парольной аутентификации и защиту от типовых уязвимостей (CSRF, XSS-атак).

Базовой библиотекой для распознавания лиц выбрана библиотека DeepFace [6], являющаяся оберткой над несколькими популярными моделями глубокого обучения. Она включает встроенные функции детекции, выравнивания и извлечения эмбеддингов. Для обнаружения лиц DeepFace требует наличия библиотеки компьютерного зрения OpenCV для работы с видеопотоком и базовой обработки изображений, а также модели машинного обучения TensorFlow или PyTorch для детекции лиц на основе MTCNN.

Распознавание лиц осуществляется на основе предобученной модели Inception ResNet, обученной на датасете VGGFace2 с использованием подходов системы FaceNet [7] для создания эмбеддингов с функцией потерь Triplet Loss.

Клиентская часть веб-приложения реализована на HTML5, CSS3 и JavaScript. Интерфейс входа пользователя в систему представлен на рисунке.



Страница входа в систему

Login page

JavaScript использует API getUserMedia для захвата видеопотока с веб-камеры пользователя и отправки кадров на сервер для дальнейшей обработки и хранения.

Для хранения профилей пользователей и соответствующих им векторов эмбеддингов может использоваться реляционная база данных PostgreSQL или MySQL. В прототипе нами реализовано хранение эмбеддингов в SQLite в виде поля JSONField. Так, в файле models.py создана модель данных FaceProfile, которая через ключевое поле связана со стандартной моделью User фреймворка Django. Эмбеддинг вычисляется при регистрации и сохраняется в поле embedding в виде списка чисел.

3. ФУНКЦИОНАЛЬНОСТЬ И АЛГОРИТМ РАБОТЫ

Приложение реализует два основных режима: регистрацию и аутентификацию (логирование).

Процесс регистрации включает следующие процедуры:

1) пользователь через веб-интерфейс загружает несколько фотографий лица с веб-камеры и отправляет их на сервер;

2) контроллер (View) Django получает изображение;

3) вызывается функция DeepFace.represent() для обработки и создания эмбеддинга;

4) эмбеддинг сохраняется в базе данных в виде строки (сериализация numpy.array в байты/JSON).

Аутентификация включает следующие шаги:

1) страница входа предлагает пользователю сделать снимок с камеры или загрузить файл, при этом запрашивает доступ к камере;

2) снимок отправляется на сервер через AJAX с CSRF-токеном;

3) контроллер Django получает изображение и выполняет верификацию с помощью функции DeepFace.verify(). Полученный эмбеддинг сравнивается со всеми эмбеддингами в базе данных. Если найден пользователь с косинусным расстоянием меньше заданного порога (например, 0.6), сервер возвращает успешный ответ и создает сессию пользователя. Если лицо не найдено или сходство недостаточно высокое, пользователь получает сообщение об ошибке.

4. ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА

Для объективной оценки разработанной настоящей системы аутентификации был проведен комплекс экспериментов:

– измерение точности распознавания (метрики FAR, FRR, Accuracy, EER);

– сравнение различных моделей распознавания, доступных в DeepFace;

– анализ производительности (время обработки одного запроса) в зависимости от аппаратного обеспечения и параметров детекции;

– тестирование устойчивости к вариациям освещения, угла поворота и к эмоциональному состоянию.

4.1. ДАТАСЕТ И УСЛОВИЯ ЭКСПЕРИМЕНТА

В эксперименте участвовали 50 добровольцев. Для каждого пользователя было собрано 20 изображений в различных условиях:

– 5 изображений при нормальном фронтальном освещении (лабораторные условия);

– 5 изображений при слабом освещении (50…100 люкс);

– 5 изображений с поворотом головы до ±25°;

– 5 изображений с изменением эмоций (улыбка, удивление, нейтральное выражение).

Итоговый размер датасета составил 1000 изображений (50 × 20). Из них 700 использовались для регистрации эталонных значений эмбеддингов, 300 – для тестирования верификации. Дополнительно в тестовую выборку было включено 100 изображений посторонних лиц (не зарегистрированных в системе) для оценки ложного пропуска (FAR).

Оборудование

Серверная часть: Intel Core i7-11800H (8 ядер, 2.3 ГГц), 32 Гб RAM, NVIDIA GeForce RTX 3060 (6 Гб VRAM).

Клиентская часть: веб-камера Logitech C920 (разрешение 1280 × 720, частота 30 кадров/с).

Сетевое окружение: локальная сеть 1 Гбит/с, с задержкой менее 5 мс.

Параметры DeepFace

1. Модели распознавания: FaceNet, ArcFace, VGGFace, OpenFace.
2. Бэкенд детекции: MTCNN (по умолчанию) и OpenCV.
3. Метрика расстояния: косинусное расстояние (Cosine Distance).
4. Порог принятия решения подбирался для каждой модели отдельно по Equal Error Rate (EER).

4.2. МЕТРИКИ И ПРОЦЕДУРА ТЕСТИРОВАНИЯ ДЛЯ КАЖДОЙ МОДЕЛИ

- **Accuracy (A)**: доля верно классифицированных попыток аутентификации (истинно положительные и истинно отрицательные).
- **FAR (False Acceptance Rate)**: вероятность того, что злоумышленник будет ошибочно принят за авторизованного пользователя.
- **FRR (False Rejection Rate)**: вероятность того, что авторизованный пользователь будет ошибочно отклонен.
- **EER (Equal Error Rate)**: значение FAR=FRR при оптимальном пороге.
- **AUC (Area Under Curve) ROC-кривой**: метрика качества модели по разделению классов.

4.3. РЕЗУЛЬТАТЫ РАСПОЗНАВАНИЯ

Таблица 1

Table 1

Сравнение моделей распознавания лиц в составе DeepFace (порог подобран по EER)

Comparison of facial recognition models in DeepFace (threshold selected based on EER)

Модель	Точность (Accuracy), %	FAR, %	FRR, %	EER, %	AUC	Размер эмбеддинга
FaceNet	98,7	0,4	0,9	0,65	0,997	512
ArcFace	99,2	0,3	0,5	0,40	0,999	512
VGGFace	96,8	1,2	2,0	1,60	0,985	4096
OpenFace	93,5	2,5	4,0	3,25	0,962	128

Анализ результатов

Модель ArcFace показала наилучшую точность (99,2 %) и минимальные значения FAR/FRR. Таким образом, она обеспечивает увеличение разделимости классов в пространстве эмбеддингов.

Модель FaceNet также демонстрировала высокие показатели (98,7 %), что делает ее предпочтительной при необходимости баланса между точностью и вычислительной сложностью.

OpenFace уступает современным моделям, но может быть приемлема для маломощных устройств из-за низкой размерности эмбеддинга.

Кроме этого, использование MTCNN (вместо OpenCV) повысило точность на 1,2 % для всех моделей за счет более точного выравнивания, но увеличило время обработки на 35 %.

4.4. ПРОИЗВОДИТЕЛЬНОСТЬ И ВРЕМЯ ОТКЛИКА

Измерялось среднее время выполнения одного запроса аутентификации (включая детекцию, извлечение признаков и сравнение с 50 эталонами). Результаты анализа представлены в табл. 2.

Таблица 2

Table 2

Время аутентификации (в миллисекундах)

Authentication time (in milliseconds)

Модель	CPU (без кэша)	CPU (с кэшем модели)	GPU (RTX 3060)
FaceNet	1250 ± 150	620 ± 50	210 ± 30
ArcFace	1420 ± 180	710 ± 60	240 ± 35
VGGFace	2350 ± 200	980 ± 90	410 ± 50
OpenFace	480 ± 40	290 ± 30	150 ± 20

Кэширование модели достигается однократной загрузкой модели в память при запуске Django-приложения. Это сокращает время доступа примерно вдвое.

Вывод по производительности: для аутентификации в режиме реального времени целесообразно использовать GPU и модель FaceNet или ArcFace. На CPU при кэшировании модели время 600…700 мс является приемлемым для большинства веб-приложений.

4.5. ИТОГИ ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ

Лучшая модель по точности: ArcFace (Accuracy 99,2 %, EER 0,40 %).

Лучшая модель по скорости на CPU: OpenFace (290 мс).

Рекомендуемая компромиссная модель: FaceNet (98,7 % при 620 мс на CPU).

Критичным фактором является детекция MTCNN: она повышает точность, но замедляет работу приложения.

Предложенная система на основе библиотеки DeepFace может быть использована в реальных веб-приложениях с невысокой нагрузкой (до 5–10 запросов в секунду на GPU).

ЗАКЛЮЧЕНИЕ

В ходе исследования был проведен анализ современных методов биометрической аутентификации. Разработанное веб-приложение на фреймворке Django с интеграцией библиотеки DeepFace доказало свою эффективность как

с точки зрения точности распознавания (до 99,2 % на модели ArcFace), так и с позиции разработчика – низкий порог входа, высокая абстракция. Экспериментальная оценка показала, что выбор модели влияет на баланс быстродействия и точности решения. Для критически важных систем рекомендуется использовать модели ArcFace или FaceNet с использованием GPU, для систем общего назначения – OpenFace на CPU.

Эксперименты подтвердили высокую точность работы системы в контролируемых условиях. Интеграция предобученных моделей глубокого обучения в веб-стек на Python позволяет создавать надежные и относительно простые в реализации системы аутентификации. Дальнейшие направления работы включают улучшение алгоритмов детекции «живости» (liveness detection) для защиты от дипфейков и атак с использованием фотографий, а также оптимизацию времени отклика для использования в высоконагруженных системах.

СПИСОК ЛИТЕРАТУРЫ

1. *Абселямов А.А., Лагуткина Т.В.* Исследование методов аутентификации на веб-сервисах. Текущие тенденции и перспективы развития // Научный результат. Информационные технологии. – 2024. – Т. 9, № 2. – URL: https://cyberleninka.ru/article/n/issledovanie-metodov-autentifikatsii-na-veb-servisah-tekuschie-tendentsii-i-perspektivy-razvitiya (дата обращения: 20.03.2026).

2. *Безгачев Ф.В.* Распознавание лиц на основе нейронных сетей: современные технологии // Научный компонент. – 2021. – № 4 (12). – URL: https://cyberleninka.ru/article/n/raspoznavanie-lits-na-osnove-neyronnyh-seteysovremennye-tehnologii (дата обращения: 22.03.2026).

3. *Иванов М.С.* Анализ уязвимостей и актуальных биометрических методов аутентификации в системах безопасности // Молодой ученый. – 2023. – № 20 (467). – С. 4–7. – URL: https://moluch.ru/archive/467/103000 (дата обращения: 20.03.2026).

4. *Корнев Л.В.* Методы биометрии при обеспечении информационной безопасности // Молодой ученый. – 2022. – № 17 (412). – С. 358–361. – URL: https://moluch.ru/archive/412/90789 (дата обращения: 21.03.2026).

5. *Сьянов С.Л., Ланцов В.М.* Применение технологий биометрической идентификации для систем контроля управления доступом на объектах уголовно-исполнительной системы // Техника и безопасность объектов уголовно-исполнительной системы: сборник материалов Международной научно-практической конференции, Воронеж, 22–23 мая 2024 г. – Воронеж, 2024. – С. 150–153. – EDN: DJEWYX.

6. *Serengil S.I., Ozpinar A.* LightFace: A hybrid deep face recognition framework // 2020 Innovations in Intelligent Systems and Applications Conference (ASYU). – Istanbul, Turkey, 2020. – P. 1–5. – DOI: 10.1109/ASYU50717.2020.9259802.

7. *Schroff F., Kalenichenko D., Philbin J.* FaceNet: A unified embedding for face recognition and clustering // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. – Boston, 2015. – P. 815–823. – DOI: 10.1109/CVPR.2015.7298682.

Перевозников Владислав Владимирович, доцент кафедры автоматизации управления войсками и информационной безопасности Пермского военного института Войск национальной гвардии Российской Федерации. E-mail: perevoznikovvv@rosgvard.ru

Гарбулин Кирилл Дмитриевич, курсант факультета связи и автоматизированного управления войсками Пермского военного института Войск национальной гвардии Российской Федерации. E-mail: garbulinkd@rosgvard.ru

DOI: 10.17212/2782-2230-2026-2-37-49

Research of biometric authentication methods and development of a web application for facial user identification using machine learning libraries*

V.V. Perevoznikov[1], K.D. Garbulin[2]

[1] *Perm Military Institute of the Russian National Guard Troops, 1 Gremyachiy Log Street, Perm, 614030, Russian Federation, associate Professor of the Department of Troop Command and Information Security Automation. E-mail: perevoznikovvv@rosgvard.ru*

[2] *Perm Military Institute of the Russian National Guard Troops, 1 Gremyachiy Log Street, Perm, 614030, Russian Federation, cadet of the Faculty of Communications and Automated Troop Command. E-mail: garbulinkd@rosgvard.ru*

This paper examines biometric authentication methods for minimizing unauthorized access to confidential information. A comparative analysis of approaches to identity detection and verification is conducted, with a focus on facial recognition technology based on deep neural networks. The practical component of the study is the development of a web application implementing user facial authentication. The paper describes the software system architecture,

* *Received 17 April 2026.*

image processing stages (detection, alignment, feature extraction), and the integration of trained machine learning models into a Python backend using the Django framework and the DeepFace library. The results of an experimental evaluation of the accuracy and performance of the proposed solution are presented.

Keywords: biometric authentication, facial recognition, machine learning, convolutional neural networks, web development, DeepFace, Django, information security

REFERENCES

1. Abselyamov A.A., Lagutkina T.V. Issledovanie metodov autentifikatsii na veb-servisakh. Tekushchie tendentsii i perspektivy razvitiya [Investigation of authentication methods on web services. current trends and development prospects]. *Nauchnyi rezul'tat. Informatsionnye tekhnologii = Research Result. Information Technologies*, 2024, vol. 9, no. 2. Available at: https://cyberleninka.ru/article/n/issledovanie-metodov-autentifikatsii-na-veb-servisah-tekuschie-tendentsii-i-perspektivy-razvitiya (accessed 20.03.2026).

2. Bezgachev F.V. Raspoznavanie lits na osnove neironnykh setei: sovremennye tekhnologii [Face recognition based on neural networks: modern technologies]. *Nauchnyi komponent*, 2021, no. 4 (12). (In Russian). Available at: https://cyberleninka.ru/article/n/raspoznavanie-lits-na-osnove-neyronnyh-seteysovremennye-tehnologii (accessed 22.03.2026).

3. Ivanov M.S. Analiz uyazvimostei i aktual'nykh biometricheskikh metodov auten-tifikatsii v sistemakh bezopasnosti [Analysis of vulnerabilities and current biometric authentication methods in security systems]. *Molodoi uchenyi = Young Scientist*, 2023, vol. 20, no. 467, pp. 4–7. Available at: https://moluch.ru/archive/467/103000 (accessed 20.03.2026).

4. Kornev L.V. Metody biometrii pri obespechenii informatsionnoi bezopasnosti [Biometric methods in information security]. *Molodoi uchenyi = Young Scientist*, 2022, vol. 17, no. 412, pp. 358–361. Available at: https://moluch.ru/archive/412/90789 (accessed 21.03.2026).

5. S'yanov S.L., Lantsov V.M. [Application of biometric identification technologies for access control systems in penal facilities]. *Tekhnika i bezopasnost' ob"ektov ugolovno-ispolnitel'noi sistemy* [Technology and safety of penal system facilities]. Collection of materials from the International scientific and practical conference. Voronezh, 2024, pp. 150–153. (In Russian).

6. Serengil S.I., Ozpinar A. LightFace: A hybrid deep face recognition framework. *2020 Innovations in Intelligent Systems and Applications Conference (ASYU)*, Istanbul, Turkey, 2020, pp. 1–5. DOI: 10.1109/ASYU50717.2020.9259802.

7. Schroff F., Kalenichenko D., Philbin J. FaceNet: A unified embedding for face recognition and clustering. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Boston, 2015, pp. 815–823. DOI: 10.1109/CVPR.2015.7298682.

Для цитирования:

Перевозников В.В., Гарбулин К.Д. Исследование методов биометрической аутентификации и разработка веб-приложения для идентификации пользователей по лицу с использованием библиотек машинного обучения // Безопасность цифровых технологий. – 2026. – № 2 (121). – С. 37–49. – DOI: 10.17212/2782-2230-2026-2-37-49.

For citation:

Perevoznikov V.V., Garbulin K.D. Issledovanie metodov biometricheskoi autentifikatsii i razrabotka veb-prilozheniya dlya identifikatsii pol'zovatelei po litsu s ispol'zovaniem bibliotek mashinnogo obucheniya [Research of biometric authentication methods and development of a web application for facial user identification using machine learning libraries]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2026, no. 2 (121), pp. 37–49. DOI: 10.17212/2782-2230-2026-2-37-49.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2026. – № 2 (121). – 50–67

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2026-2-50-67

РАЗРАБОТКА ПОДХОДА К АВТОМАТИЗАЦИИ ВЫБОРА МЕР ЗАЩИТЫ ГИС В ПЕРЕХОДНЫЙ ПЕРИОД*

Е.Е. КОРОТКОВА[1], В.В. СЕЛИФАНОВ[2]

[1] *РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: iza.korotkova@gmail.com*
[2] *РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E- mail: sfo1@mail.ru*

Статья посвящена проблеме проектирования систем защиты информации государственных информационных систем (ГИС) в условиях изменения нормативной базы. Проведен сравнительный анализ приказов ФСТЭК России № 17 и № 117, выявлены ключевые усложнения в части расширения области регулирования, появления новых категорий мер защиты и ужесточения требований к отчетности. Обосновывается необходимость перехода от экспертного проектирования к автоматизированному ввиду усложнения требований, динамичности угроз и дефицита квалифицированных кадров. Представлен алгоритм автоматизированного сопоставления параметров ГИС с базой данных угроз (БДУ) ФСТЭК, а также архитектурное решение сервиса для автоматической генерации проектной документации.

Ключевые слова: ГИС, Приказ ФСТЭК № 117, Приказ ФСТЭК № 17, защита информации, модель угроз, меры защиты, БДУ ФСТЭК, средства защиты информации

ВВЕДЕНИЕ

С вступлением в силу приказа ФСТЭК России № 117 смещается акцент со статичного проектирования систем защиты в сторону более динамичного управления безопасностью. Новые требования расширяют область действия, детализируют процессы и процедуры защиты информации, увеличивают объем используемых мер. Высокая детализация требований ведет к росту трудозатрат и повышает риск ошибок из-за человеческого фактора. В условиях дефицита кадров и необходимости оперативного реагирования на изменения обстановки вопрос автоматизации процессов выходит на передний план.

* Статья получена 27 апреля 2026 г.

В статье приводится анализ Приказа ФСТЭК № 117, а также уже действующих и проектируемых методических документов и предлагаются меры по автоматизации процессов моделирования угроз и подбору средств защиты информации (СЗИ) в условиях перехода на новые требования и постоянные изменения обстановки (от обновления техник и тактик атак до обновления реестров сертифицированных СЗИ).

1. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРИКАЗОВ ФСТЭК № 17 И № 117

Приказ № 117 сохраняет базовую структуру требований к защите информации, но существенно развивает их содержание, предлагая более детализированные и обширные меры безопасности. Проведенный анализ позволяет выделить несколько ключевых направлений изменений.

1.1. РАСШИРЕНИЕ ОБЛАСТИ ДЕЙСТВИЯ

Одним из ключевых изменений, вносимых Приказом № 117, является расширение круга информационных систем, на которые распространяются его требования. Если ранее Приказ № 17 регулировал вопросы создания и ввода в действие систем защиты информации преимущественно для ГИС [1–3], то новая редакция охватывает более широкий перечень объектов.

Действие Приказа № 117 распространяется:

– на государственные информационные системы, обрабатывающие информацию ограниченного доступа;

– иные информационные системы государственных органов;

– информационные системы государственных унитарных предприятий и государственных учреждений;

– муниципальные информационные системы.

Для некоторых указанных систем ранее уже существовали отдельные требования по аттестации. При этом Приказ № 117 впервые устанавливает унифицированный подход к их защите, предъявляя единые, более детализированные и строгие требования.

Расширение области действия напрямую повлияло на состав применяемых мер защиты и порядок их реализации.

1.2. ЭВОЛЮЦИЯ МЕР ЗАЩИТЫ И ПОЯВЛЕНИЕ НОВЫХ КАТЕГОРИЙ

Изменение круга регулируемых систем повлекло за собой пересмотр подходов к регламентации стадий и этапов ввода СЗИ в эксплуатацию. Ранее Приказ ФСТЭК № 17 содержал требования к стадиям и этапам работ по вводу

в действие СЗИ информационных систем. Приказ ФСТЭК № 117 таких требований не содержит, а ссылается на другие нормативные акты: для ГИС применяются требования ПП РФ № 676, к иным ИС применяется ГОСТ Р 51583–2014 [4–7]. Ниже представлена таблица сравнения.

Таблица 1

Table 1

Сравнение стадий и этапов работ по вводу в действие СЗИ ИС

Comparison of stages and phases of work on the commissioning of information security systems

Группа этапов	ПП РФ 676	ГОСТ Р 51583	Приказ ФСТЭК № 17
Подготовка и установка	Этап отсутствует	Комплектация АС	Установка и настройка средств ЗИ ИС
	Этап отсутствует	Строительно-монтажные работы	
Настройка и внедрение	Пусконаладочные работы	Пусконаладочные работы	Этап отсутствует
	Этап отсутствует	Подготовка объекта автоматизации к вводу АС в действие	Разработка организационно-распорядительных документов по ЗИ
			Внедрение организационных мер ЗИ
	Этап отсутствует	Подготовка персонала	Этап отсутствует
Испытания	Проведение предварительных испытаний	Проведение предварительных испытаний	Предварительные испытания системы ЗИ ИС
	Проведение опытной эксплуатации	Проведение опытной эксплуатации	Опытная эксплуатация системы ЗИ ИС
	Этап отсутствует	Этап отсутствует	Анализ уязвимостей ИС и принятие мер ЗИ по их устранению
Завершающие мероприятия	Проведение приемочных испытаний	Проведение приемочных испытаний	Приемочные испытания системы ЗИ ИС

Применение различных нормативных актов для регламентации стадий и этапов ввода СЗИ в эксплуатацию в зависимости от типа системы усложняет

процесс проектирования и внедрения. Введенное разделение на государственные и иные информационные системы, а также отсутствие жесткой регламентации этапов для последних создает риск возникновения ошибок.

Другим важным изменением, вносимым Приказом № 117, является введение требований к организационной структуре системы защиты информации. Ключевым последствием стало расширение сферы действия ПП РФ № 1272. Если ранее документ распространялся только на субъекты критической информационной инфраструктуры (КИИ), то теперь Приказ № 117 делает его требования обязательными для более широкого круга организаций, подпадающих под действие приказа [8–10]. Это обязывает такие организации привести свои системы защиты в соответствие с ПП РФ № 1272 (рис. 1), что унифицирует и ужесточает требования к информационной безопасности для многих субъектов, ранее не охваченных регулированием.

Рис. 1. Организационная структура в Приказе ФСТЭК № 117 [11]

Fig. 1. Organizational structure in the FSTEC order № 117 [11]

Что касается состава мер и мероприятий защиты, то в Приказе № 117 отсутствует их полный перечень. Однако даже базовый набор претерпел существенные изменения. Появились следующие группы мер:

- защита виртуализации и облачных вычислений;
- защита технологий контейнерных сред и их оркестрации;
- защита сервисов электронной почты;
- защита веб-технологий;

– защита программных интерфейсов взаимодействия приложений;
– защита конечных устройств;
– защита мобильных устройств;
– защита технологий интернета вещей;
– защита точек беспроводного доступа;
– обнаружение и предотвращение вторжений на сетевом уровне;
– сегментация и межсетевое экранирование;
– защита каналов передачи данных и сетевого взаимодействия.

Сравнение базового перечня мероприятий представлено в табл. 2.

Таблица 2
Table 2

Сравнение мероприятий защиты информации в приказах № 17 и № 117
Comparison of information security measures in orders № 17 and № 117

Приказ ФСТЭК России № 17 (было)	Приказ ФСТЭК России № 117 (стало)
Выявление и оценка угроз безопасности информации (УБИ)	Обеспечение разработки безопасного ПО
Контроль конфигураций ИС	Обеспечение физической защиты ИС
Управление уязвимостями	Обеспечение непрерывности функционирования ИС при возникновении нештатных ситуаций
Управление обновлениями	Повышение уровня знаний и информированности пользователей по вопросам ЗИ
Обеспечение ЗИ при обработке, хранении и обращении с информацией ограниченного доступа	Обеспечение ЗИ при взаимодействии с подрядными организациями
Обеспечение ЗИ при применении конечных устройств	Обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании
Обеспечение ЗИ при применении мобильных устройств	Обеспечение ЗИ при использовании искусственного интеллекта
Обеспечение ЗИ при удаленном доступе пользователей к ИС	Реализация в ИС мер по их защите и защите содержащейся в них информации
Обеспечение ЗИ при беспроводном доступе пользователей к ИС	Проведение контроля уровня защищенности информации, содержащейся в ИС
Обеспечение ЗИ при предоставлении пользователям привилегированного доступа	Обеспечение непрерывного взаимодействия с ГосСОПКА на информационные ресурсы РФ
Обеспечение мониторинга ИБ	–

Исчерпывающий перечень мер и мероприятий содержится в соответствующем методическом документе. В нем описано 96 мер и 18 мероприятий, из них для 42 и 15 соответственно установлены требования к документированию.

Для реализации этих мер требуется применение различных сертифицированных средств защиты информации. По состоянию на май 2026 года в реестре ФСТЭК России зарегистрировано 1919 СЗИ, в реестре ФСБ России – 833 СЗИ, в реестре Минцифры России – 30 313 единиц отечественного программного обеспечения (ПО). При этом СЗИ и ПО должны корректно функционировать совместно.

В настоящее время существует широкий спектр требований к СЗИ. В рамках системы сертификации ФСТЭК России действует 13 типов требований, которые не охватывают все необходимые виды средств. Например, отсутствуют требования к средствам идентификации и аутентификации, анализа уязвимостей, SIEM-системам и другим классам. Такие средства сертифицируются на соответствие уровню доверия, что не отражает их функциональные возможности и дополнительно усложняет выбор и обоснование применения средств защиты.

При выборе СЗИ также необходимо учитывать возможности нарушителя. Соответствующие требования приведены в табл. 3.

Таблица 3

Table 3

Требования к средствам защиты информации

Requirements for information security tools

Вид требования	Класс 1	Класс 2	Класс 3
СВТ (средства вычислительной техники)	5-й уровень доверия	5-й уровень доверия	5-й уровень доверия
СЗИ	4-й уровень доверия	5-й уровень доверия	6-й уровень доверия
УД (устройства доверенной загрузки)	4-й уровень доверия	5-й уровень доверия	6-й уровень доверия
Уровень возможностей нарушителя (Приказ № 117)	Высокий	Повышенный	Базовый
Уровень возможностей нарушителя (Приказ № 17)	Высокий	Усиленный базовый	Базовый

Кроме того, в Приказе № 117 установлены меры по обязательному выполнению требований эксплуатационной документации и организации технической поддержки. В этой части Приказ № 117 полностью совпадает с Приказом ФСТЭК № 239, устанавливающим требования к защите значимых объектов КИИ [12–15].

Увеличение числа критериев выбора средств, а также отсутствие четких требований к реализуемому функционалу значительно повышает трудоемкость проектирования систем защиты информации. Это требует внедрения процессов автоматизации фильтрации применяемых мер.

Помимо изменений в составе мер и процедур их внедрения, Приказ № 117 вводит новые подходы к оценке состояния защиты информации.

1.3. ОЦЕНКА СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Приказ № 117 вводит два ключевых показателя оценки соответствия: уровень защищенности (количественная оценка, выражаемая коэффициентом защищенности, $К_{зи}$) и уровень зрелости (качественная оценка процессов обеспечения защиты информации, $П_{зи}$). Первый контролируется не реже одного раза в полгода с обязательной отчетностью во ФСТЭК России. Второй проверяется не реже одного раза в два года.

Приказ устанавливает требования к регулярной отчетности. Необходимо проводить контроль уровня защищенности, мониторинг безопасности и иные мероприятия, перечисленные в табл. 4 [11, 16, 17]. В связи с этим возникает потребность в регулярной обработке больших объемов данных.

На май 2026 года в БДУ ФСТЭК России содержится 227 угроз и 83 991 уязвимость. Ожидается, что темпы роста этих показателей будут увеличиваться. В ходе проектирования системы защиты информации специалисты должны учитывать все возможные способы реализации угроз безопасности, что требует обработки огромного количества вариантов. При таком объеме данных традиционный «ручной» подход становится неэффективным.

Помимо увеличения количества отчетных документов новый приказ вводит нормативные сроки для ряда процессов. Стоит отметить, что для некоторых процессов, например устранения уязвимостей, установленные сроки могут потребовать привлечения сотрудников в нерабочее время.

Таблица 4
Table 4

Отчетность во ФСТЭК
Reporting to FSTEC

Пункт Приказа № 117	Что отправляется	Периодичность	Срок предоставления
32	Оценка показателя защищенности ($К_{зи}$)	Один раз в 6 месяцев	5 рабочих дней
32, 73	Оценка показателя уровня зрелости ($П_{зи}$)	Один раз в 2 года	5 рабочих дней
36	Модель угроз (техническое задание) со ссылкой на ПП РФ 676 (только для ГИС)	При создании	–
38	Информация о найденных уязвимостях, отсутствующих в БДУ	При обнаружении	5 рабочих дней
49	Последний в текущем году отчет по результатам мониторинга либо итоговый отчет за текущий год	Ежегодно	–
65, 73	Аттестационные материалы (Приказ ФСТЭК России № 77)	При аттестации	5 рабочих дней
65, 73	Протоколы контроля защиты информации (Приказ ФСТЭК России № 77)	Один раз в 2 года (для аттестованных ИС)	–
67	Отчет по результатам проведения контроля уровня защищенности	Один раз в 3 года или после инцидента	5 рабочих дней

Таблица 5
Table 5

Сроки выполнения процессов
Process execution times

Пункт Приказа № 117	Процесс	Срок выполнения
38	Устранение уязвимостей	От 24 часов до 7 календарных дней
53	Восстановление функционирования	От 24 часов до 4 недель
55	Проверка возможности восстановления выполнения значимых функций с использованием резервных копий	Один раз в 2 года
57	Оценка уровня знаний	Один раз в 3 года или после контрольных испытаний

1.4. СИНТЕЗ ПРОБЛЕМАТИКИ

Проведенный сравнительный анализ приказов № 17 и № 117 демонстрирует существенное увеличение объема и детализации требований к защите ГИС. Переход к динамическому управлению безопасностью, расширение круга регулируемых систем и значительное увеличение объема отчетности создают условия, в которых автоматизация процессов становится критически важной.

Количество актуальных угроз и выявляемых уязвимостей исключает возможность их качественной «ручной» обработки. Автоматизация в этом сегменте должна быть направлена на непрерывное сопоставление архитектурных и технологических параметров ГИС с актуальными данными об угрозах.

С учетом появления новых мер и мероприятий, а также изменения подходов к их группировке процесс их выбора значительно усложнился. Автоматизация позволяет перейти от субъективных экспертных оценок к формализованному алгоритмическому сопоставлению.

Анализ реестров Минцифры, ФСТЭК и ФСБ выявил наличие тысяч наименований ПО и СЗИ при отсутствии единых функциональных требований к ряду их классов. В этих условиях автоматизированная система должна выступать в роли фильтра, сопоставляющего функциональные возможности средств защиты с требованиями к уровням доверия и спецификой архитектуры ГИС.

Таким образом, выявленное усложнение нормативных требований, рост числа угроз и многообразие средств защиты обосновывают необходимость перехода от экспертного проектирования к формализованному алгоритмическому подходу. Описание структуры и логики такого алгоритма приведено в следующем разделе.

2. АЛГОРИТМ АВТОМАТИЗИРОВАННОГО СОПОСТАВЛЕНИЯ ПАРАМЕТРОВ ГИС И МЕР ЗАЩИТЫ

С учетом выявленных ранее проблем разработан общий алгоритм работы сервиса проектирования систем защиты информации ГИС. Алгоритм включает пять основных этапов: 1) сбор общей информации, 2) построение модели угроз, 3) определение мер защиты, 4) выбор СЗИ и 5) генерация отчета. При реализации в виде программного обеспечения каждый этап выполняется отдельным одноименным модулем (рис. 2).

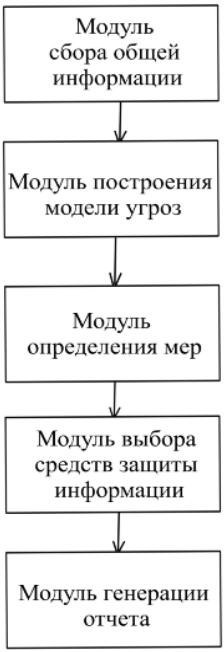


Рис. 2. Структура программы

Fig. 2. Program structure

2.1. ЭТАП СБОРА ОБЩЕЙ ИНФОРМАЦИИ

Первый этап предназначен для формирования цифрового паспорта ГИС, а также определения ее класса защищенности. На основе входных параметров автоматически определяется требуемый класс защищенности ГИС (К1, К2 или К3). Сформированные на этом этапе данные служат основой для всех последующих шагов.

2.2. ЭТАП ФОРМИРОВАНИЯ МОДЕЛИ УГРОЗ

Этот этап представляет собой центральный аналитический блок, интегрированный с актуальными базами данных угроз. Его цель – из всего множества УБИ выделить только те, которые актуальны для конкретной ГИС с заданными архитектурными, технологическими и режимными характеристиками.

На основе класса защищенности и ценности информации система автоматически назначает потенциал нарушителя: базовый, повышенный или высокий. Дополнительно учитываются особенности архитектуры – они могут повышать уровень нарушителя. Модель нарушителя включает его предполагаемые навыки, ресурсы, время, местонахождение (внешний/внутренний) и легальный статус доступа.

Выполняется импорт актуальной версии БДУ. Из общего перечня отбираются только те, которые удовлетворяют совокупности формальных критериев: соответствие типу нарушителя, технологическая совместимость, наличие канала реализации, ценность информации. Фильтрация выполняется по формализованным правилам, заданным в базе знаний системы. Это позволяет исключить заведомо неприменимые угрозы и сократить перечень с сотен до десятков релевантных записей. Для каждой отобранной угрозы из БДУ ФСТЭК система автоматически сопоставляет соответствующие техники и тактики.

Для каждой пары «угроза – техника» с учетом архитектуры ГИС и модели нарушителя автоматически генерируется типовой сценарий реализации в виде последовательности действий нарушителя. Сценарии не являются творческим описанием, а собираются из шаблонных фрагментов, что обеспечивает воспроизводимость и пригодность для последующей автоматической проверки мер защиты.

Полученная модель угроз передается на следующий этап для выбора соответствующих мер защиты.

2.3. ЭТАП ВЫБОРА И АДАПТАЦИИ МЕР ЗАЩИТЫ

На основе класса защищенности ГИС и требований Приказа № 117 автоматически формируется базовый перечень технических и организационных мер защиты.

Из этого перечня исключаются меры, которые неприменимы к данной ГИС. Каждое исключение сопровождается автоматически генерируемым обоснованием, что важно для последующей экспертной оценки.

Результатом этапа является комплексный перечень технических и организационных мер защиты информации, адаптированный под специфику ГИС, ее класс, актуальные угрозы и технологический стек. Перечень оформляется в виде требований технического задания на систему защиты информации.

Сформированный перечень мер служит основой для подбора конкретных средств защиты.

2.4. ЭТАП ПОДБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Входными параметрами для этого этапа являются перечень требуемых мер защиты и класс защищенности ГИС. Система обращается к внутренней базе знаний СЗИ, которая содержит актуальные сведения о продуктах, сертифицированных ФСТЭК России и ФСБ России: функциональные возможности, классы защиты, номера и сроки действия сертификатов, версии.

Каждая требуемая мера защиты сопоставляется с функциональными возможностями доступных СЗИ. Автоматически проверяются наличие и актуальность действующих сертификатов для предложенных средств, а также их соответствие требуемому классу защищенности ГИС.

Выходные данные этапа – спецификация оборудования и программного обеспечения, включающая наименования продуктов, их версии, сертификационные данные и обоснование выбора.

Сформированная спецификация вместе со всеми накопленными данными поступает на финальный этап.

2.5. ЭТАП ГЕНЕРАЦИИ ПРОЕКТНОЙ И ОТЧЕТНОЙ ДОКУМЕНТАЦИИ

Финальный этап обеспечивает формирование полного пакета документов. На этом шаге используются все данные, полученные на предыдущих этапах, и применяются предопределенные шаблоны, соответствующие требованиям ФСТЭК России. Кроме того, формируются отчеты, необходимые для предоставления во ФСТЭК России. Все сгенерированные документы экспортируются в форматах .docx и/или .pdf.

ЗАКЛЮЧЕНИЕ

Приведенный в первом разделе анализ положений Приказа ФСТЭК России № 117 в сравнении с Приказом № 17 демонстрирует значительное усложнение и расширение требований к защите государственных информационных систем. Эти изменения затрагивают все стадии жизненного цикла системы защиты информации – от проектирования до эксплуатации и контроля.

В условиях динамичного обновления нормативной базы, постоянного появления новых угроз и дефицита квалифицированных специалистов традиционные «ручные» подходы к проектированию систем защиты становятся неэффективными, трудозатратными и подверженными ошибкам.

Предложенный во втором разделе алгоритм позволяет автоматизировать построение актуальной модели угроз на основе БДУ ФСТЭК России, подбор мер защиты и сертифицированных средств защиты информации, а также генерацию необходимой проектной и отчетной документации.

Внедрение такого автоматизированного подхода даст организациям возможность снизить трудоемкость работ и минимизировать риски, связанные с человеческим фактором.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

2. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3. *Заугольков И.А., Исаева О.В., Рожнова Е.А.* Комплексное обеспечение защиты информации ограниченного доступа в мировом суде // Материалы пула научно-практических конференций, Сочи, 04–08 января 2025 г. – Керчь, 2025. – С. 154–159.

4. ГОСТ Р 51583–2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: дата введения 2014–09–01. – М.: Стандартинформ, 2014. – 13 с.

5. *Вялых С.А., Ульянов В.А.* Актуальные вопросы технической защиты информации в государственных информационных системах регионального уровня // Информатика: проблемы, методы, технологии: материалы XXV Международной научно-практической конференции им. Э.К. Алгазинова, Воронеж, 12–13 февраля 2025 г. – Воронеж, 2025. – С. 501–510.

6. *Киреева Н.В., Кузнецова Д.В., Шамина Ю.И.* Современные методы обеспечения информационной безопасности // Актуальные проблемы информатики, радиотехники и связи: материалы XXXI Российской научно-технической конференции, Самара, 01–02 февраля 2024 г. – Самара, 2024. – С. 101–103.

7. Постановление Правительства РФ от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

8. Постановление Правительства РФ от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».

9. *Попова В.В., Булаев В.Д., Галицкий П.А.* Системный подход к построению комплексной защиты информации на объектах критической информационной инфраструктуры. Создание Единой централизованной федеральной телекоммуникационной сети // Безопасность личности, общества и государства: теоретико-правовые аспекты: сборник научных статей XVII Международной научной конференции обучающихся образовательных организаций высшего образования, проводимой в рамках IV Санкт-Петербургского международного молодежного научного форума «Северная Пальмира: территория возможностей», Санкт-Петербург, 30 мая 2024 года. – СПб., 2024. – С. 1694–1703.

10. *Милько Д.С., Данеев А.В.* Множество вариантов решений для задачи выбора мер защиты объектов критической информационной инфраструктуры // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2023. – Т. 26, № 1. – С. 82–90. – DOI: 10.21293/1818-0442-2023-26-1-82-90.

11. *Селифанов В., Ситьков И.* Информационная безопасность 2.0: что изменится с новым приказом ФСТЭК России. – URL: https://infotecs.ru/press-center/events/informatsionnaya-bezopasnost-2-0-chto-izmenitsya-s-novym-prikazom-fstek-rossii/ (дата обращения: 15.12.2024).

12. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

13. *Павлов Е.О.* Подходы к обеспечению безопасности объектов критической информационной инфраструктуры // Журнал высоких гуманитарных технологий. – 2024. – № 3 (6). – С. 32–38.

14. Обеспечение безопасности государственных информационных систем как объектов критической информационной инфраструктуры / Г.П. Гавдан, А.А. Голубев, А.Г. Голубев, И.Ю. Жуков, Э.П. Рыбалко // Безопасность информационных технологий. – 2025. – Т. 32, № 3. – С. 26–43. – DOI: 10.26583/bit.2025.3.03.

15. *Гончаренко М.Д., Холкина К.С.* Безопасность критической информационной инфраструктуры // Научное и техническое творчество молодежи: материалы Всероссийской научно-практической конференции с международным участием, Новосибирск, 19–20 апреля 2023 г. Ч. 5 (дополнительная). – Новосибирск, 2023. – С. 200–208.

16. *Михиенко О.В., Ламонина Л.В., Смирнова О.Б.* К вопросу о кибербезопасности критической информационной инфраструктуры // Инновационные технологии в АПК как фактор развития науки в современных условиях: сборник XIV Международной научно-практической конференции, посвященной 75-летию факультета Технического сервиса в АПК (факультет механиза-

ции сельского хозяйства Омского сельскохозяйственного института им. С.М. Кирова), Омск, 27 ноября 2025 г. – Омск, 2025. – С. 787–791.

17. *Замилов А.Р.* Автоматизация контроля состояния безопасности объектов критической информационной инфраструктуры // Радиоэлектроника, электротехника и энергетика: тезисы докладов Тридцатой Международной научно-технической конференции студентов и аспирантов. – М., 2024. – С. 344.

Короткова Елизавета Евгеньевна, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – разработка систем автоматизации процессов. E-mail: iza.korotkova@gmail.com

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность. E-mail: sfo1@mail.ru

DOI: 10.17212/2782-2230-2026-2-50-67

Development of an approach to automating the selection of GIS protection measures during the transition period*

E.E. Korotkova[1], V.V. Selifanov[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: iza.korotkova@gmail.com*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Senior Lecturer at the Department of Information Security. E-mail: sfo1@mail.ru*

This article examines the design of information security systems for government information systems (GIS) in the context of changing regulatory frameworks. A comparative analysis of FSTEC of Russia Orders № 17 and № 117 is provided, identifying key challenges related to the expansion of the regulatory scope, the emergence of new categories of security measures, and stricter reporting requirements. The need for a transition from expert-based to automated design is substantiated in light of increasingly complex requirements, dynamic threats, and a shortage of qualified personnel. An algorithm for automated comparison of GIS parameters with the FSTEC Threat Database (TDB) and other sources

* *Received 27 April 2026.*

is presented, along with an architectural solution for a service for the automatic generation of design documentation.

Keywords: GIS, FSTEC order №117, FSTEC order № 17, information protection, threat model, protective measures, FSTEC TDB, information security tools

REFERENCES

1. Order of the FSTEC of Russia of 04.11.2025, N 117 "On approval of requirements for the protection of information contained in state information systems, other information systems of state bodies, state unitary enterprises, and state institutions". (In Russian).

2. Order of the FSTEC of Russia of 11.02.2013, N 17 "On approval of requirements for the protection of information not constituting state secrets contained in state information systems". (In Russian).

3. Zaugolkov I.A., Isaeva O.V., Rozhnova E.A. Kompleksnoe obespechenie zashchity informatsii ogranichennogo dostupa v mirovom sude [Comprehensive protection of restricted access information in the world court]. *Materialy pula nauchno-prakticheskikh konferentsii* [Proceedings of the pool of scientific and practical conferences], Sochi, January 04–08, 2025. Kerch, 2025, pp. 154–159.

4. GOST R 51583–2014. *Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii. Obshchie polozheniya* [State Standard R 51583–2014. Information protection. Sequence of protected operational system formation. General]. Moscow, Standartinform Publ., 2014. 13 p.

5. Vyalykh S.A., Ul'yanov V.A. [Actual issues of technical protection of information in state information systems at the regional level]. *Informatika: problemy, metody, tekhnologii* [Informatics: problems, methods, technologies]. Materials of the XXV International Scientific and Practical Conference named after E.K. Al-Gazinov, Voronezh, February 12–13, 2025, pp. 501–510. (In Russian).

6. Kireeva N.V., Kuznetsova D.V., Shamina Yu.I. [Modern methods of ensuring information security]. *Aktual'nye problemy informatiki, radiotekhniki i svyazi* [Actual problems of computer science, radio engineering and communications]. Proceedings of the XXXI Russian Scientific and Technical Conference, Samara, February 01–02, 2024, pp. 101–103. (In Russian).

7. Decree of the Government of the Russian Federation dated July 6, 2015 N 676 "On the requirements for the procedure for the creation, development, commissioning, operation and decommissioning of state information systems and the further storage of information contained in their databases". (In Russian).

8. Decree of the Government of the Russian Federation dated July 15, 2022 N 1272 "On approval of the model regulation on the deputy head of the body (organization) responsible for ensuring information security in the body (organization)

and the model regulation on the structural unit in the body (organization) ensuring information security of the body (organization)". (In Russian).

9. Popova V.V., Bulaev V.D., Galitskii P.A. [A systematic approach to building comprehensive information protection at critical information infrastructure facilities. Co-building of the Unified centralized Federal Telecommunication network]. *Bezopasnost' lichnosti, obshchestva i gosudarstva: teoretiko-pravovye aspekty* [Security of the individual, society and the state: theoretical and legal aspects]. Collection of scientific articles of the XVII International Scientific conference of students of educational institutions of higher education, St. etersburg, 2024, pp. 1694–1703. (In Russian).

10. Milko D.S., Daneev A.V. Mnozhestvo variantov reshenii dlya zadachi vybora mer zashchity ob"ektov kriticheskoi informatsionnoi infrastruktury [Multiple of solutions for the choosing measures task to cybersecurity of critical infrastructure]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki = Proceedings of Tomsk State University of Control Systems and Radioelectronics*, 2023, vol. 26, no. 1, pp. 82–90. DOI: 10.21293/1818-0442-2023-26-1-82-90.

11. Selifanov V., Sit'kov I. *Informatsionnaya bezopasnost' 2.0: chto izmenitsya s novym prikazom FSTEK Rossii* [Information security 2.0: what will change with the new order of the FSTEC of Russia. Available at: https://infotecs.ru/press-center/events/informatsionnaya-bezopasnost-2-0-chto-izmenitsya-s-novym-prikazom-fstek-rossii/ (accessed 15.12.2024).

12. Order of the FSTEC of Russia of 25.12.2017, N 239 "On approval of requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation". (In Russian).

13. Pavlov E.O. Podkhody k obespecheniyu bezopasnosti ob"ektov kriticheskoi in-formatsionnoi infrastruktury [Approaches to ensuring the security of critical information infrastructure facilities]. *Zhurnal vysokikh gumanitarnykh tekhnologii = Hi-Hume Journal*, 2024, no. 3 (6), pp. 32–38.

14. Gavdan G.P., Golubev A.A., Golubev A.G., Zhukov I.Y., Rybalko A.P. Obespechenie bezopasnosti gosudarstvennykh informatsionnykh sistem kak ob"ektov kriticheskoi informatsionnoi infrastruktury [Managing the security of government information systems as critical information infrastructure objects]. *Bezopasnost' informatsionnykh tekhnologii = IT Security (Russia)*, 2025, vol. 32, no. 3, pp. 26–43. DOI: 10.26583/bit.2025.3.03.

15. Goncharenko M.D., Kholkina K.S. [Safety of critical information infrastructure]. *Nauchnoe i tekhnicheskoe tvorchestvo molodezhi* [Scientific and technical creativity of youth]. Materials of the All-Russian Scientific and Practical Conference with international participation, Novosibirsk, April 19–20, 2023, pp. 200–208. (In Russian).

16. Mikhienko O.V., Lamonina L.V., Smirnova O.B. [On the issue of cybersecurity of critical information infrastructure]. *Innovatsionnye tekhnologii v APK, kak faktor razvitiya nauki v sovremennykh usloviyakh* [Innovative technologies in agriculture as a factor in the development of science in modern conditions]. Collection of the XIV International Scientific and Practical Conference, Omsk, 2025, pp. 787–791. (In Russian).

17. Zamilov A.R. [Automation of security monitoring of critical information infrastructure facilities]. *Radioelektronika, elektrotekhnika i energetika* [Radio electronics, electrical engineering and power engineering]. Abstracts of the Thirtieth International Scientific and Technical Conference of Students and Postgraduates, Moscow, 2024, p. 344. (In Russian).

Для цитирования:

Короткова Е.Е., *Селифанов В.В.* Разработка подхода к автоматизации выбора мер защиты ГИС в переходный период // Безопасность цифровых технологий. – 2026. – № 2 (121). – С. 50–67. – DOI: 10.17212/2782-2230-2026-2-50-67.

For citation:

Korotkova E.E., Selifanov V.V. Razrabotka podkhoda k avtomatizatsii vybora mer zashchity GIS v perekhodnyi period [Development of an approach to automating the selection of GIS protection measures during the transition period]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2026, no. 2 (121), pp. 50–67. DOI: 10.17212/2782-2230-2026-2-50-67.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2026. – № 2 (121). – 68–90

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2026-2-68-90

ВЛИЯНИЕ ГЕОМЕТРИЧЕСКИХ ПАРАМЕТРОВ АНТЕННЫХ СИСТЕМ НА ФОРМИРОВАНИЕ ГАРАНТИРОВАННЫХ ЗОН ПОДАВЛЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ*

И.В. ТРУБИН[1], И.В. ВОЖОВ[2], П.Р. ЧЕРНЫШЕВ[3]

[1] *РФ, 630087, г. Новосибирск, ул. Немировича-Данченко 138 офис 2/2, Общество с ограниченной ответственностью «КБ Автоматика», заместитель директора. E-mail: i.trubin@corp.nstu.ru*

[2] *РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: ilvozhov@mail.ru*

[3] *РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: p.chernyshev.2021@stud.nstu.ru*

Статья посвящена исследованию пространственно-энергетических характеристик систем активного радиоподавления и их влиянию на информационную безопасность объектов. В работе проводится детальный анализ формирования зон гарантированного подавления сигналов в диапазоне 2,4 ГГц в зависимости от геометрических параметров и типа применяемых антенных систем. На базе программно-аппаратного комплекса (nRF24L01+PA+LNA и ESP32) и векторного анализатора спектра LIG Nex1 NS-30A проведено экспериментальное сравнение эффективности полуволновых диполей и четвертьволновых монополей с целью выявления зависимости между геометрией излучателя и равномерностью пространственного распределения помехи. Особое внимание уделено выявлению «коридоров радиопрозрачности» – зон критического падения мощности помехи (до 12…20 дБ), обусловленных формой диаграммы направленности и поляризационным рассогласованием. Результаты исследования позволяют количественно оценить риски утечки информации и сформулировать рекомендации по оптимизации пространственной конфигурации средств РЭБ для обеспечения непрерывного защитного поля.

Ключевые слова: информационная безопасность, диаграмма направленности, зона подавления, поляризация, полуволновой диполь, четвертьволновой монополь, техническая защита информации, nRF24L01, ESP32

* Статья получена 05 мая 2026 г.

ВВЕДЕНИЕ

Обеспечение информационной безопасности в современном мире неразрывно связано с контролем радиочастотного пространства. Широкое распространение протоколов Wi-Fi, Bluetooth и устройств интернета вещей (IoT), функционирующих в нелицензируемом ISM-диапазоне (2,4 ГГц), создает серьезные вызовы для технической защиты информации (ТЗИ), связанные с прозрачностью физических границ зданий для радиоизлучения, с доступностью аппаратных средств для перехвата данных и с высокой чувствительностью беспроводных интерфейсов к преднамеренному блокированию каналов связи. Одной из наиболее эффективных мер противодействия несанкционированному съему данных и деструктивным радиовоздействиям – преднамеренному блокированию каналов связи (DoS-атаки), подмене сигналов управления (спуфинг) или нарушению целостности передаваемой телеметрии – является применение систем активного радиоподавления.

Однако на практике эффективность защиты часто оценивается лишь по интегральной выходной мощности передатчика, без учета пространственной конфигурации электромагнитного поля. Подобный подход не охватывает всей специфики, так как любая реальная антенная система обладает неизотропной диаграммой направленности (ДН). Это приводит к возникновению «мертвых зон» и секторов с недостаточным энергетическим потенциалом помехи, через которые возможна скрытная передача данных злоумышленником.

Актуальность настоящей работы заключается в необходимости научного обоснования формирования «гарантированных зон подавления» с учетом геометрических параметров излучателей. Понимание физических процессов формирования ДН и специфики многолучевого распространения позволяет дополнить типовые методики размещения оборудования высокоточными данными о пространственных аномалиях поля, обеспечивая переход к адаптивному проектированию зон защиты в условиях сложных интерьеров.

Объектом исследования является структура электромагнитного помехового поля, формируемого в условиях реального интерьерного окружения (офисные/лабораторные помещения). В отличие от идеализированных измерений в дальней зоне, данный подход позволяет учесть влияние переотражений и интерференции на формирование зон подавления. В качестве генератора помех используется двухканальный модуль на базе микроконтроллера ESP32 и трансиверов nRF24L01+PA+LNA, функционирующий в режиме быстрого сканирования несущей VCO Sweep в полосе 2,4 ГГц.

Научная новизна исследования состоит в экспериментальной верификации зон радиопрозрачности, возникающих при различных комбинациях типов антенн (полуволновой диполь Е-3000 и четвертьволновой монополь штатная

штыревая антенна с коэффициентом усиления 2 дБи (децибел относительно изотропного излучателя) модели SMA-2.4G-2) и их пространственной ориентации. Методика измерений предполагает использование векторного анализатора спектра LIG Nex1 NS-30A на дистанциях 4…5 метров, что гарантирует работу в области полностью сформированного поля излучения.

Особое внимание уделено анализу наихудшего сценария – ситуации поляризационного и геометрического рассогласования антенн передатчика и приемника. Экспериментально доказывается, что некорректная пространственная ориентация антенн блокиратора может снижать эффективность защиты до 20…30 дБ, превращая систему активной защиты в «номинальную».

Реализация поставленной цели предполагает последовательное выполнение нескольких этапов эксперимента. На первом этапе проводится анализ характеристик сигнала при прямом кабельном соединении блокиратора с измерительным прибором. Это необходимо, чтобы зафиксировать точную мощность системы и оценить стабильность работы генератора без влияния внешних помех.

Дальнейшие исследования направлены на изучение сигнала уже в открытом пространстве. Это позволяет оценить реальную силу помехи в условиях помещения, где радиоволны отражаются от стен и препятствий. В рамках этого этапа сравниваются свойства полуволновых и четвертьволновых антенн, что помогает понять, как форма антенны влияет на надежность защиты.

1. ДИАПАЗОН 2,4 ГГц

Диапазон 2,4 ГГц занимает важное место в современных системах беспроводной связи, поскольку именно в нем реализуется работа большого числа распространенных технологий передачи данных. Его широкое применение связано не только с универсальностью, но и с доступностью элементной базы, используемой при построении радиосистем. В пределах этого диапазона одновременно функционируют такие стандарты, как Wi-Fi и Bluetooth, а также ряд других решений. Совместное использование одного и того же частотного ресурса различными технологиями неизбежно приводит к возникновению взаимных помех, что отрицательно сказывается на качестве и эффективности передачи данных [1]. Кроме того, специфика беспроводного радиоканала делает системы уязвимыми к воздействию внешних помех. При целенаправленном создании помехового сигнала возможно существенное нарушение или полное подавление работы технологии передачи данных [2].

1.1. ИНТЕРФЕЙСЫ ПЕРЕДАЧИ ДАННЫХ, ФУНКЦИОНИРУЮЩИЕ В ДИАПАЗОНЕ 2,4 ГГц

Одной из наиболее распространенных технологий беспроводной передачи данных является Wi-Fi, основанный на стандартах семейства IEEE 802.11 [3]. Согласно отчету WBA, в мире на 2023 год использовалось более 18 млрд Wi-Fi-устройств [4]. В диапазоне 2,4 ГГц сети Wi-Fi используют каналы шириной 20 или 40 МГц, при этом большинство каналов частично перекрываются по спектру. Технология Bluetooth, используемая для организации персональных беспроводных сетей, использует иной принцип организации передачи данных. Например, чтобы повысить устойчивость связи, используется механизм адаптивной перестройки частоты. Передача осуществляется посредством быстрого переключения между множеством узких каналов, что позволяет уменьшить влияние узкополосных помех и повысить надежность соединения [5].

Wi-Fi и Bluetooth функционируют в одном частотном диапазоне, что неизбежно приводит к взаимному влиянию этих технологий. Активность устройств Bluetooth может снижать пропускную способность устройств Wi-Fi и увеличивать задержки передачи данных, особенно в условиях высокой плотности спектра [6].

1.2. УЯЗВИМОСТИ БЕСПРОВОДНЫХ СЕТЕЙ К ПОМЕХОВОМУ ВОЗДЕЙСТВИЮ

Ключевой проблемой беспроводных систем связи является их высокая чувствительность к внешним электромагнитным воздействиям. В отличие от проводных каналов передачи данных, радиосигнал распространяется в открытой среде и может подвергаться воздействию различных источников помех. Помехи могут возникать как вследствие наложения сигналов устройств, работающих в одном диапазоне частот, так и в результате преднамеренных воздействий на радиоканал. Генерация радиочастотных помех может приводить к значительному снижению качества передачи данных. В исследовании «Against Jamming Attack in Wireless Communication Networks: A Reinforcement Learning Approach. Electronics» показано, что в условиях помехового воздействия успешность передачи пакетов снижалась до 0,5…0,7, тогда как применение специализированных алгоритмов позволяло повысить этот показатель до 0,84 при smart jamming и до 0,99 при sweep jamming [7].

Особую угрозу представляют атаки типа радиочастотного подавления, при которых злоумышленник намеренно формирует сигнал помехи для нарушения функционирования беспроводной сети. Такие воздействия способны

занимать радиочастотный спектр и препятствовать корректной передаче данных между легитимными устройствами [2].

Экспериментальные результаты показывают высокую эффективность подобных атак: в работе «Practical Realization of Reactive Jamming Attack on Long-Range Wide-Area Network» для пакетов с полезной нагрузкой 5 байт и более была зафиксирована полная потеря пакетов практически для всех исследованных режимов передачи, для некоторых конфигураций потери достигали 50…100 %. В каждом экспериментальном режиме оценка проводилась по серии из ста переданных пакетов [8].

В условиях развития беспроводных технологий и увеличения количества подключенных устройств задача обеспечения устойчивости радиосетей к подобным воздействиям приобретает особую актуальность. Поэтому исследование методов формирования помех, анализа их влияния на работу беспроводных интерфейсов и создание алгоритмов передачи данных, учитывающих наличие помех, является важным направлением современных исследований в области развития радиоэлектроники.

2. АРХИТЕКТУРА ЛАБОРАТОРНОГО СТЕНДА

Экспериментальный стенд представляет собой программно-аппаратный комплекс, предназначенный для формирования управляемых радиопомех и регистрации их пространственно-энергетических характеристик. Архитектура стенда разделена на три функциональных узла: 1) блок генерации помех, 2) сменный антенный комплекс и 3) измерительная система на базе анализатора спектра (рис. 1).

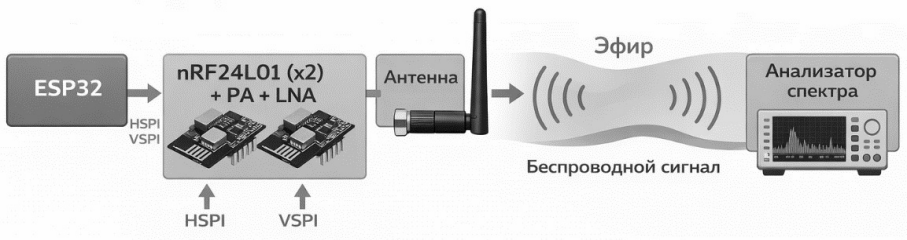


Рис. 1. Общая схема взаимодействия компонентов

Fig. 1. General diagram of component interactions

Блок генерации помех реализован на базе 38-пинового микроконтроллера ESP32 WROOM, который выступает в роли центрального узла управления.

Для создания помехового воздействия в диапазоне 2,4 ГГц используют два независимых радиомодуля nRF24L01+PA+LNA. Модули оснащены встроенными усилителями мощности (PA) и малошумящими усилителями (LNA), что критически важно для имитации высокомощных заградительных помех.

Для обеспечения максимальной скорости перестройки частоты модули подключены по раздельным аппаратным шинам: первый модуль подключен по интерфейсу HSPI (Hardware SPI), второй – по интерфейсу VSPI (Virtual SPI). В архитектуре микроконтроллера ESP32 эти интерфейсы представляют собой два независимых аппаратных блока (контроллера) стандартного протокола SPI. В отличие от традиционного последовательного подключения нескольких ведомых устройств к одной шине SPI (через выбор кристалла CS), использование двух раздельных шин позволяет осуществлять параллельную передачу данных. Это критически важно для реализации алгоритма VCO Sweep, так как минимизирует задержки на переключение между регистрами радиомодулей и позволяет в два раза увеличить скорость перестройки несущей частоты, обеспечивая формирование более плотного и непрерывного помехового спектра. Для стабилизации питания и компенсации пиковых токов потребления, возникающих в моменты активации выходных каскадов усилителей мощности (PA), в схему интегрированы электролитические конденсаторы емкостью 10 мкФ. Это позволяет минимизировать просадки напряжения на шине питания при высокой частоте переключения передатчиков в режиме сканирования диапазона (рис. 2).

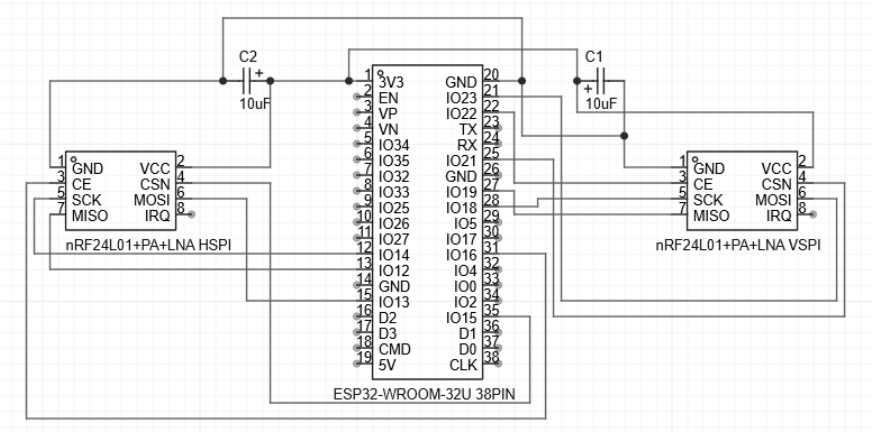


Рис. 2. Электрическая принципиальная схема

Fig. 2. Electrical schematic diagram

Важной особенностью эксплуатации стенда является обеспечение безопасности выходных каскадов радиомодулей. Поскольку архитектура предполагает одновременную работу двух передатчиков, а исследование проводится для одиночных антенных систем, ВЧ-выход неиспользуемого в конкретном замере модуля нагружался на согласованную величину номиналом 50 Ом. Это позволило избежать критического роста коэффициента стоячей волны (КСВ) и предотвратить выход из строя усилителя мощности из-за отраженной энергии.

Сменный антенный комплекс включает два типа излучателей с различными волновыми характеристиками. Основным объектом исследования является промышленная полуволновая дипольная антенна E-3000 (длина волны λ/2), обладающая выраженной тороидальной диаграммой направленности. В качестве альтернативной конфигурации используется четвертьволновой монополь (λ/4), работающий совместно с корпусом стенда как единой излучающей системой. Сравнение типов антенн (рис. 3) позволяет оценить влияние геометрических параметров на формирование зон безопасности.

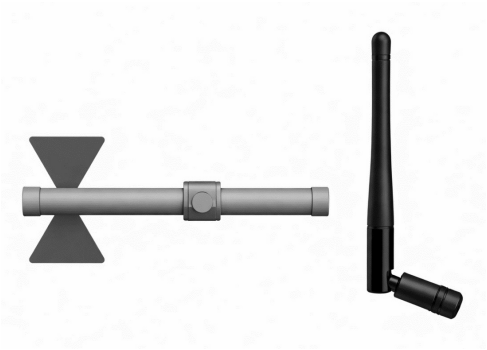


Рис. 3. Используемые антенны

Fig. 3. Antennas used

Измерительная система построена на базе векторного анализатора спектра LIG Nex1 NS-30A (рис. 4). Прибор обеспечивает фиксацию уровней мощности в режиме реального времени с высокой разрешающей способностью. Для калибровки источника использовалось прямое соединение через коаксиальный кабель с волновым сопротивлением 50 Ом, а для пространственных измерений применялась вертикально ориентированная широкополосная приемная антенна, установленная на штативе.

Рис. 4. Анализатор спектра LIG Nex1 NS-30A

Fig. 4. LIG Nex1 NS-30A Spectrum Analyzer

Такая архитектура стенда позволяет проводить комплексные испытания: от анализа «чистого» спектрального состава помехи внутри тракта до исследования сложных эффектов деполяризации и пространственного затухания в условиях реального интерьера.

Рис. 5. Общий вид стенда

Fig. 5. General view of the stand

Измерения проводились в условиях реального лабораторного помещения (рис. 5), что позволило оценить не только теоретическую форму лепестков диа-

граммы направленности, но и влияние переотражений от стен и мебели на общую устойчивость помехового поля.

3. МЕТОДИКА И РЕЗУЛЬТАТЫ ИСПЫТАНИЙ

Перед проведением испытаний были учтены действующие ограничения, связанные с использованием радиоэлектронных средств в полосе радиочастот 2400…2483,5 МГц. В соответствии с ФЗ 126 «О связи» использование радиочастотного спектра без соответствующего разрешения не допускается, если иное не предусмотрено законодательством [9]. Для ряда устройств малого радиуса действия в полосе 2400…2483,5 МГц допускается применение без оформления отдельных решений ГКРЧ и разрешений на использование радиочастот при соблюдении установленных условий, в том числе по параметрам излучения и режиму эксплуатации внутри закрытых помещений [10, 11].

В настоящей работе эксперимент проводился в пределах закрытого помещения на территории университета, а параметры стенда и схема размещения оборудования были выбраны таким образом, чтобы излучение не оказывало воздействия на сторонние радиоэлектронные средства за пределами лабораторной зоны. Следовательно, исследование является лабораторным моделированием помехового воздействия в контролируемых условиях.

В основу экспериментального исследования заложен принцип оценки эффективности активной радиоэлектронной защиты в условиях, максимально приближенных к реальной эксплуатации. Для получения достоверных данных о распределении электромагнитной энергии в пространстве измерения проводились в частотном диапазоне 2,4 ГГц, который является критически важным с точки зрения информационной безопасности (каналы Wi-Fi, Bluetooth).

Для изменения геометрических параметров антенных систем были выбраны два типа антенн (четвертьволновой монополь и полуволновой диполь).

Четвертьволновой монополь – это несимметричная антенна, представляющая собой один проводник длиной 1/4 длины волны, установленный над проводящей поверхностью. Такая антенна имеет конструкцию в виде одного штыря. В роли второго «плеча» выступает земля, металлический корпус прибора. Пространственная диаграмма направленности четвертьволнового монополя представляет собой тороидальную структуру, усеченную бесконечной проводящей плоскостью. Излучение сосредоточено исключительно в верхнем полупространстве и образует радиально-симметричную фигуру вращения относительно оси излучателя (рис. 6). Из-за отражения от земли энергия не уходит вниз, а концентрируется в верхнем полушарии.

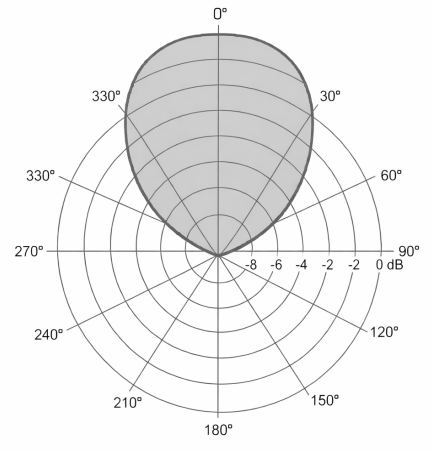


Рис. 6. Диаграмма направленности
четвертьволнового монополя

Fig. 6. Radiation pattern of
a quarter-wave monopole

Полуволновой диполь – это классическая симметричная антенна, состоящая из двух проводников длиной по 1/4 длины волны каждый. Общая длина антенны составляет примерно половину длины волны. Конструкция представляет собой два «плеча», запитанных посередине, и требует обязательного заземления для работы. Пространственная диаграмма направленности симметричного полуволнового вибратора представляет собой тороидальную структуру (тор), обладающую осевой симметрией относительно проводника. Максимум интенсивности излучения сосредоточен в плоскости, перпендикулярной геометрической оси антенны, при наличии глубоких минимумов (нулей излучения) вдоль самой оси (рис. 7).

Дистанция измерения от антенны до анализатора спектра была выбрана (4…5 метров), это обусловлено требованиями электродинамической корректности. При длине волны $\lambda \approx 12{,}3$ см для используемых типов антенн ($\lambda/2$ и $\lambda/4$) граница дальней зоны (зоны Фраунгофера) начинается на удалении 0,3…0,5 м. Таким образом, проведение замеров на дистанции 5 метров гарантирует работу измерительного комплекса в области полностью сформированной диаграммы направленности (ДН), исключая влияние реактивных компонентов ближнего поля и фазовых искажений.

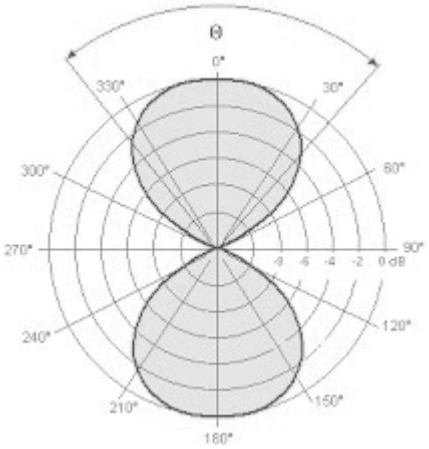


Рис. 7. Диаграмма направленности полуволнового диполя

Fig. 7. Radiation pattern of a half-wave dipole

С позиций информационной безопасности такой подход позволяет с высокой точностью верифицировать «зоны гарантированного подавления» и, что более важно, выявить «коридоры радиопрозрачности» – пространственные секторы, в которых энергетический потенциал помехи минимален. Исследование этих зон позволяет сформировать модель угроз, основанную на физических параметрах антенных систем, и разработать рекомендации по минимизации вероятности успешного перехвата данных в условиях активного радиопротиводействия.

3.1. КАЛИБРОВКА ИСТОЧНИКА И ОПРЕДЕЛЕНИЕ ЭНЕРГЕТИЧЕСКОГО ПОТЕНЦИАЛА

На первом этапе была произведена оценка спектральной плотности мощности генератора путем прямого подключения к анализатору спектра через коаксиальный кабель (рис. 8).

Анализ спектрограммы выявил «гребенчатую» структуру помехи, характерную для генераторов, управляемых напряжением (VCO). Было зафиксировано наличие амплитудной изрезанности (пик-фактор до 30…40 дБ), что свидетельствует о потенциальных временных лакунах в процессе сканирования диапазона, которыми могут воспользоваться адаптивные системы передачи данных.

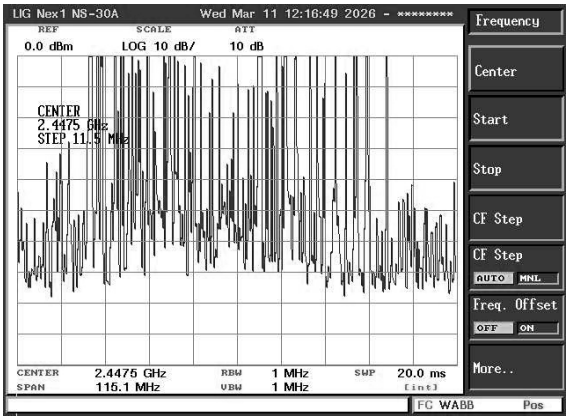


Рис. 8. Аппаратная спектрограмма выходного сигнала блокиратора при прямом соединении

Fig. 8. Hardware spectrogram of the blocker output signal with direct connection

3.2. ОЦЕНКА ЗАТУХАНИЯ В КАНАЛЕ И ВЛИЯНИЕ ДИСТАНЦИИ

Второй этап включал замеры уровня сигнала в эфире на дистанциях 1,5 и 5 м. Испытуемое устройство располагалось на фиксированной высоте (рис. 9).

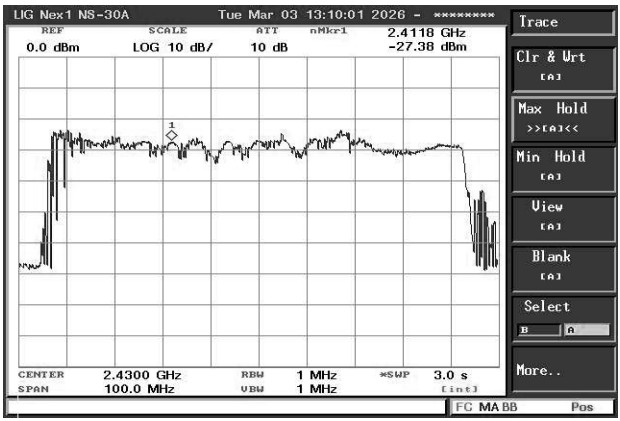


Рис. 9. Спектрограмма помехового поля на удалении 1,5 м

Fig. 9. Spectrogram of the interference field at a distance of 1,5 m

Сравнение результатов показало снижение уровня сигнала до –27,38 дБм на дистанции 1,5 м. Отмечено сглаживание спектральной «гребенки» за счет эффекта многолучевого распространения в закрытом помещении, что способствует более равномерному заполнению спектра шумом в точке приема.

3.3. ИССЛЕДОВАНИЕ ПРОСТРАНСТВЕННЫХ ХАРАКТЕРИСТИК (ДИАГРАММЫ НАПРАВЛЕННОСТИ)

Ключевой частью испытаний стало снятие сечений ДН. Испытуемая антенна вращалась относительно оси анализатора спектра с шагом 90° (рис. 10).

Рис. 10. Изменение мощности сигнала при различных угловых положениях полуволнового диполя (1-е положение)

Fig. 10. Change in signal power at different angular positions of the half-wave dipole (1th position)

При повороте на 90° (промежуточное положение) наблюдается начало спада амплитуды сигнала (рис. 11). Это демонстрирует постепенный выход приемника из основного лепестка диаграммы направленности.

Наиболее критическое падение мощности зафиксировано, когда антенна была направлена торцом к анализатору (рис. 12). Уровень сигнала снизился до –58,11…–60,97 дБм.

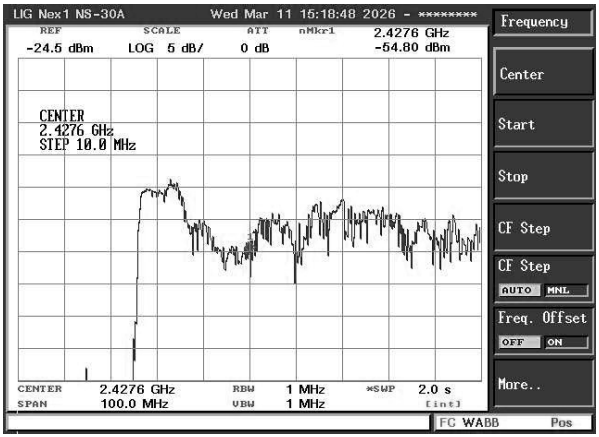


Рис. 11. Изменение мощности сигнала при различных угловых положениях полуволнового диполя (2-е положение)

Fig. 11. Change in signal power at different angular positions of the half-wave dipole (2th position)

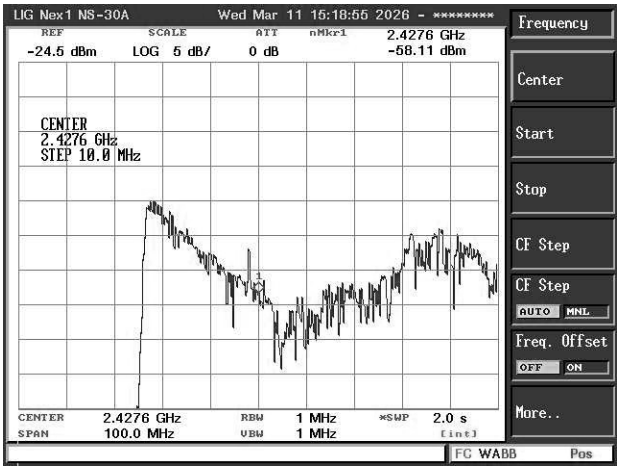


Рис. 12. Изменение мощности сигнала при различных угловых положениях полуволнового диполя (3-е положение)

Fig. 12. Change in signal power at different angular positions of the half-wave dipole (3th position)

Завершающий замер (рис. 13) подтвердил симметричность ДН диполя при возвращении в зону основного излучения.

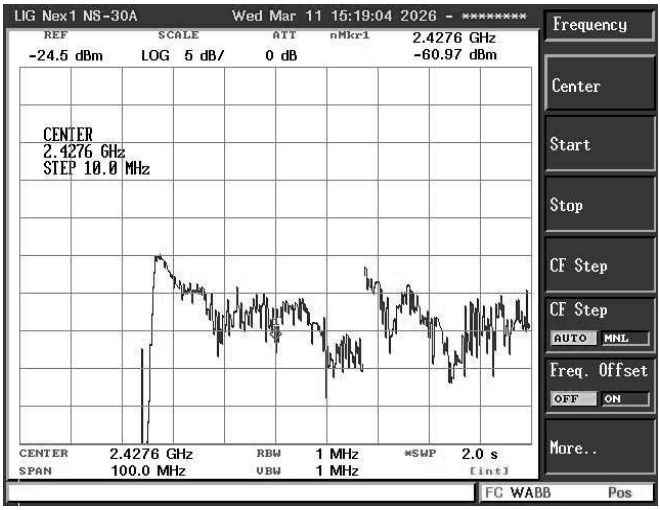


Рис. 13. Изменение мощности сигнала при различных угловых положениях полуволнового диполя (4-е положение)

Fig. 13. Change in signal power at different angular positions of the half-wave dipole (4th position)

Исходя из полученных данных можно сделать вывод, что при подключенном полуволновом диполе, при ориентации «широкой стороной» (broadside) зафиксирован максимум излучения (–48,83 дБм). При развороте антенны торцом (end-fire) к анализатору уровень сигнала снизился до –58,11...–60,97 дБм.

Зафиксированный провал мощности в 12,14 дБ (более чем в 16 раз) подтверждает наличие выраженных «мертвых зон» вдоль оси антенны. С точки зрения ИБ эти зоны являются критическими уязвимостями, позволяющими обходить систему защиты. В частности, наличие выявленных «коридоров радиопрозрачности» означает, что в определенных секторах пространства (вдоль геометрической оси антенны) отношение сигнал/помеха (SNR) остается достаточным для декодирования информации приемным устройством.

Поскольку мощность помехового поля в этих зонах падает более чем в 16 раз относительно максимума, эффективный радиус подавления сокращается пропорционально квадрату расстояния. Это создает условия, при которых в пределах одного помещения могут существовать локальные зоны,

где блокирование каналов связи фактически не осуществляется. Злоумышленник, обладающий информацией о пространственной ориентации антенн системы защиты, может физически разместить средства съема данных (например, Wi-Fi-микрофоны или скрытые камеры) именно в осевых «нулях» диаграммы направленности. В таком сценарии полезный сигнал будет успешно передаваться в обход основного лепестка помехового воздействия, что делает систему активной защиты номинальной и неэффективной против квалифицированной атаки

Далее были проведены испытания с четвертьволновой антенной. Уровень сигнала в основном сечении показан на рис. 14.

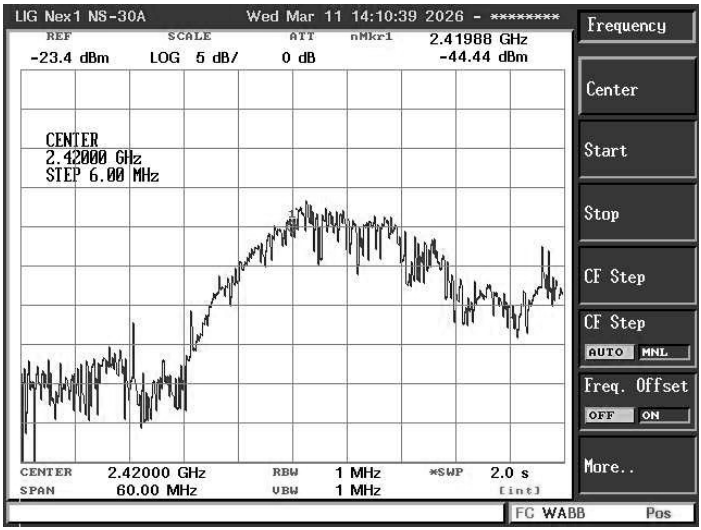


Рис. 14. Спектральные характеристики помехового поля при использовании четвертьволновой антенны (1-е положение)

Fig. 14. Spectral characteristics of the interference field when using a quarter-wave antenna (1th position)

При вращении монополя (рис. 15) уровень сигнала оставался стабильным (средний уровень – 44,44 дБм), что значительно выше, чем в «нулях» диполя.

Различное количество контрольных точек при снятии характеристик для полуволнового диполя и четвертьволнового монополя обусловлено фундаментальными различиями в их диаграммах направленности и результатами предварительного сканирования поля.

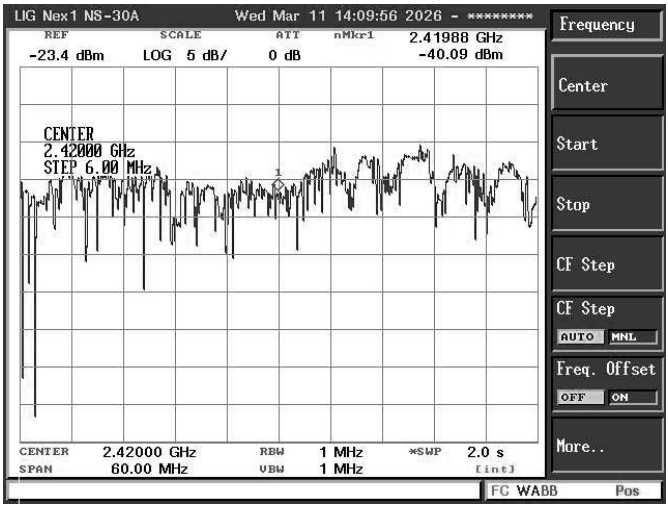


Рис. 15. Спектральные характеристики помехового поля при использовании четвертьволновой антенны (2-е положение)

Fig. 15. Spectral characteristics of the interference field when using a quarter-wave antenna (2th position)

Для полуволнового диполя было выбрано четырехточечное измерение (шаг 90°), так как теоретическая модель его излучения («тор») предполагает наличие выраженных экстремумов: двух максимумов в экваториальной плоскости и двух глубоких минимумов вдоль геометрической оси. Проведение четырех замеров позволило достоверно зафиксировать эти критические перепады мощности (до 12…20 дБ), которые являются ключевыми факторами риска в задачах ТЗИ.

Для четвертьволнового монополя количество контрольных точек было ограничено двумя диаметрально противоположными векторами (0° и 180°). Такое решение базируется на предварительной верификации стабильности помехового поля: в ходе первичного вращения было установлено, что отклонение уровня мощности не превышает 4,35 дБ. Высокая степень взаимодействия монополя с корпусом блокиратора, выполняющим роль противовеса, привела к «размытию» диаграммы направленности и формированию равномерного покрытия. В этих условиях увеличение числа измерительных позиций до четырех было признано избыточным, так как две контрольные точки уже подтвердили отсутствие глубоких осевых провалов, характерных для дипольной системы.

Зафиксированный максимум излучения для полуволнового диполя (–48,83 дБм) при номинальном кросс-поляризационном расположении антенн требует детального физического обоснования. В условиях идеального свободного пространства (отсутствие отражений) теоретические потери из-за несовпадения плоскостей поляризации могут составлять более 20…30 дБ, что привело бы к практически полному исчезновению помехового сигнала на входе приемника.

Однако в реальных условиях эксперимента (размещение на диэлектрической опоре в замкнутом пространстве) наблюдается эффект деполяризации и вращения вектора Е. Полученный уровень –48,83 дБм объясняется суммированием прямой волны и волн, отраженных от подстилающей поверхности (пола) и стен помещения. Отражение от диэлектрических и проводящих поверхностей приводит к «докручиванию» вектора поляризации до вертикальной составляющей, что и фиксируется анализатором спектра.

Этот факт имеет критическое значение для информационной безопасности: он доказывает, что в закрытых помещениях эффект многолучевого распространения частично компенсирует ошибки в ориентации антенн, «размазывая» энергию помехи по плоскостям поляризации.

3.4. РЕЗУЛЬТАТЫ ИСПЫТАНИЙ

Итоговым этапом стало моделирование условий эксплуатации, характеризующихся максимальным рассогласованием параметров (горизонтальное положение блокиратора при вертикальной поляризации приемника).

В ходе этого эксперимента было установлено катастрофическое снижение эффективности подавления: суммарные потери из-за кросс-поляризации и попадания в осевой «ноль» ДН превысили 20 дБ. В терминах практического применения это означает сокращение радиуса эффективного подавления в 10 раз (например, с 10 до 1 м).

Выводы по результатам испытаний

1. Экспериментально доказано, что при тестировании устройств на способность работать в условиях помех ключевым фактором является не только мощность генератора, но и пространственная ориентация антенн.

2. Обнаруженный эффект деполяризации в закрытом помещении частично компенсирует ошибки позиционирования за счет отражений, однако он не является достаточным для обеспечения гарантированной блокировки во всех ракурсах.

3. Для проведения корректных испытаний на помехоустойчивость рекомендуется использовать четвертьволновые антенны или антенные системы с круговой поляризацией, что минимизирует вероятность возникновения «ко-

ридоров радиопрозрачности», через которые испытуемое устройство может поддерживать связь в обход помехового воздействия.

4. Полученные количественные данные позволяют более точно рассчитывать необходимый энергетический запас (Safety Margin) при проектировании систем активной защиты информации.

ЗАКЛЮЧЕНИЕ

Проведенный сравнительный анализ экспериментальных данных показал, что переход от полуволнового диполя к четвертьволновому монополю привел к росту уровня сигнала в точке приема на 4,4 дБ. Этот эффект объясняется концентрацией излучаемой энергии в верхнюю полусферу относительно корпуса устройства, который в данном случае выполняет роль противовеса. Экспериментально подтверждено, что монополярная антенна в составе малогабаритного корпуса демонстрирует более высокую изотропность излучения, тогда как дипольная антенна показала глубокий провал мощности до 12 дБ вдоль собственной оси. Это свидетельствует о наличии выраженных пространственных зон радиопрозрачности, которыми могут воспользоваться сторонние устройства для поддержания связи в обход системы активной защиты.

При выборе типа антенной системы для конкретных прикладных задач необходимо учитывать их функциональные особенности и физические ограничения. Полуволновой диполь обладает преимуществом высокого усиления в плоскости, перпендикулярной оси антенны, что делает его эффективным инструментом для создания направленных радиочастотных барьеров (например, для защиты оконных проемов или периметра помещений). Однако наличие глубоких осевых минимумов требует строгого контроля пространственной ориентации излучателя. В свою очередь, четвертьволновой монополь отличается компактностью и обеспечивает более равномерное купольное покрытие пространства без критических осевых провалов. Это предпочтительное решение для портативных блокираторов и проведения лабораторных испытаний мобильных устройств на помехоустойчивость, так как в этом случае значительно снижается вероятность случайного попадания испытуемого прибора в мертвую зону диаграммы направленности.

В итоге для обеспечения гарантированного уровня технической защиты информации следует учитывать не только номинальную мощность передатчика, но и сложную геометрию формируемого поля с учетом поляризационных характеристик. Наиболее надежным подходом при тестировании систем на устойчивость к помехам является применение комбинированных антенных

решений, исключающих возникновение выявленных коридоров радиопрозрачности. Результаты выполненной работы могут служить методической базой для проектирования защищенных пространств внутри зданий и подготовки специалистов в области радиоэлектронной борьбы и информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Experimental Evaluation of Interference in 2.4 GHz Wireless Network / V. Agarwal, S. Mahmud, S. Kasera, M. Ji. – Office of Scientific and Technical Information, 2023. – DOI: 10.2172/2242485.

2. *Pirayesh H., Zeng H.* Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey // IEEE Communications Surveys & Tutorials. – 2022. – Vol. 24 (2). – P. 767–809. – DOI: 10.1109/COMST.2022.3159185.

3. A survey of IEEE 802.11ax WLAN temporal duty cycle for the assessment of RF electromagnetic exposure / Y. Yang, G. Vermeeren, L. Verloock, M. Guxens, W. Joseph // Applied Sciences. – 2025. – Vol. 15 (5). – P. 2858. – DOI: 10.3390/app15052858.

4. Wireless Broadband Alliance. WBA Annual Industry Report 2023.

5. *Subhagato Dutta*. The evolution of Bluetooth: A deep dive // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. – 2025. – Vol. 11 (1). – DOI: 10.32628/cseit251112261.

6. *Lim S.* IACR: An interference-aware channel reservation for wireless sensor networks // International Journal of Electrical and Computer Engineering. – 2019. – Vol. 9 (2). – DOI: 10.11591/ijece.v9i2.pp1220-1225.

7. *Ma D., Wang Y., Wu S.* Against jamming attack in wireless communication networks: A reinforcement learning approach // Electronics. – 2024. – Vol. 13 (7). – P. 1209. – DOI: 10.3390/electronics13071209.

8. Practical realization of reactive jamming attack on long-range wide-area network / J. Šabić, T. Perković, D. Begušić, P. Šolić // Sensors. – 2025. – Vol. 25 (8). – P. 2383. – DOI: 10.3390/s25082383.

9. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

10. Каков порядок использования радиочастотного спектра радиоэлектронными средствами беспроводного доступа в диапазоне радиочастот 2,4 ГГц? // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: сайт. – URL: https://digital.gov.ru/faq/kakov-poryadok-ispolzovaniya-radiochastotnogo-spektra-radioelektronnymi-sredstvami-besprovodnogo-dostupa-v-diapazone-radiochastot-24-ggcz (дата обращения: 26.05.2026).

11. Условия использования радиоэлектронных средств малого радиуса действия в полосе радиочастот 2400–2483,5 МГц // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: сайт. – URL: https://23.rkn.gov.ru/news/news114683.htm (дата обращения: 26.05.2026).

Трубин Игорь Витальевич, заместитель директора ООО «КБ “Автоматика”». Основное направление научных исследований – защита технических каналов утечки информации. E-mail: i.trubin@corp.nstu.ru

Вожов Илья Вадимович, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – разработка систем предотвращения утечки информации по техническим каналам. E-mail: ilvozhov@mail.ru

Чернышев Павел Романович, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – разработка систем обнаружения утечки информации по техническим каналам. E-mail: p.chernyshev.2021@stud.nstu.ru

DOI: 10.17212/2782-2230-2026-2-68-90

The influence of geometric parameters of antenna systems on the formation of guaranteed suppression zones for information leakage channels*

I.V. Trubin[1], I.V. Vozhov[2], P.R. Chernyshev[3]

[1] *«DB “AUTOMATION”» LTD, 138 Nemirovich-Danchenko Street, Novosibirsk, 630087, Russian Federation, associate director. E-mail: i.trubin@corp.nstu.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of Information Security Department. E-mail: ilvozhov@mail.ru*
[3] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of Information Security Department. E-mail: p.chernyshev.2021@stud.nstu.ru*

The article is devoted to the study of the spatial and energy characteristics of active radio suppression systems and their impact on the information security of facilities. The paper provides a detailed analysis of the formation of guaranteed signal suppression zones in the 2.4 GHz

* *Received 05 May 2026.*

band depending on geometric parameters and the type of antenna systems used. Based on a software and hardware complex consisting of nRF24L01+PA+LNA and ESP32 modules, as well as a LIG Nex1 NS-30A vector spectrum analyzer, an experimental comparison of the efficiency of half-wave dipoles and quarter-wave monopoles was conducted in order to identify the relationship between radiator geometry and the uniformity of the spatial distribution of interference.
Special attention is paid to identifying “radio-transparent corridors” – zones of critical interference power reduction of up to 12–20 dB, caused by the shape of the radiation pattern and polarization mismatch. The research results make it possible to quantitatively assess the risks of information leakage and to formulate recommendations for optimizing the spatial configuration of electronic warfare systems to ensure a continuous protective field.

Keywords: information security, radiation pattern, suppression zone, polarization, half-wave dipole, quarter-wave monopole, technical protection of information, nRF24L01, ESP32

REFERENCES

1. Agarwal V., Mahmud S., Kasera S., Ji M. *Experimental Evaluation of Interference in 2.4 GHz Wireless Network*. Office of Scientific and Technical Information, 2023. DOI: 10.2172/2242485.

2. Pirayesh H., Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2022, vol. 24 (2), pp. 767–809. DOI: 10.1109/COMST.2022.3159185.

3. Yang Y., Vermeeren G., Verloock L., Guxens M., Joseph W. A survey of IEEE 802.11ax WLAN temporal duty cycle for the assessment of RF electromagnetic exposure. *Applied Sciences*, 2025, vol. 15 (5), p. 2858. DOI: 10.3390/app15052858.

4. Wireless Broadband Alliance. *WBA Annual Industry Report 2023*.

5. Subhagato Dutta. The evolution of Bluetooth: A deep dive. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2025, vol. 11 (1). DOI: 10.32628/cseit251112261.

6. Lim S. IACR: An interference-aware channel reservation for wireless sensor networks. *International Journal of Electrical and Computer Engineering*, 2019, vol. 9 (2). DOI: 10.11591/ijece.v9i2.pp1220-1225.

7. Ma D., Wang Y., Wu S. Against jamming attack in wireless communication networks: A reinforcement learning approach. *Electronics*, 2024, vol. 13 (7), p. 1209. DOI: 10.3390/electronics13071209.

8. Šabić J., Perković T., Begušić D., Šolić P. Practical realization of reactive jamming attack on long-range wide-area network. *Sensors*, 2025, vol. 25 (8), p. 2383. DOI: 10.3390/s25082383.

9. Federal Law of July 7, 2003 N 126-FZ. "On Communications". (In Russian).

10. Kakov poryadok ispol'zovaniya radiochastotnogo spektra radioelektronnymi sredstvami besprovodnogo dostupa v diapazone radiochastot 2,4 GGts? [What is

the procedure for using the radio-frequency spectrum by radio-electronic equipment for wireless access in the 2.4 GHz radio-frequency band?]. *Ministerstvo tsifrovogo razvitiya, svyazi i massovykh kommunikatsii Rossiiskoi Federatsii* [Ministry of Digital Development, Communications and Mass Media of the Russian Federation]. Website. Available at: https://digital.gov.ru/faq/kakov-poryadok-ispolzovaniya-radiochastotnogo-spektra-radioelektronnymi-sredstvami-besprovodnogo-dostupa-v-diapazone-radiochastot-24-ggcz (accessed 26.05.2026).

11. Usloviya ispol'zovaniya radioelektronnykh sredstv malogo radiusa deistviya v polose radiochastot 2400–2483,5 MGts [Conditions for the Use of Short-Range Radio-Electronic Equipment in the 2400–2483.5 MHz Radio-Frequency Band]. *Federal'naya sluzhba po nadzoru v sfere svyazi, informatsionnykh tekhnologii i massovykh kommunikatsii* [Federal Service for Supervision of Communications, Information Technology and Mass Media]. Website. Available at: https://23.rkn.gov.ru/news/news114683.htm (accessed 26.05.2026).

Для цитирования:

Трубин И.В., Вожов И.В., Чернышев П.Р. Влияние геометрических параметров антенных систем на формирование гарантированных зон подавления каналов утечки информации // Безопасность цифровых технологий. – 2026. – № 2 (121). – С. 68–90. – DOI: 10.17212/2782-2230-2026-2-68-90.

For citation:

Trubin I.V., Vozhov I.V., Chernyshev P.R. Vliyanie geometricheskikh parametrov antennykh sistem na formiro-vanie garantirovannykh zon podavleniya kanalov utechki informatsii [The influence of geometric parameters of antenna systems on the formation of guaranteed suppression zones for information leakage channels]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2026, no. 2 (121), pp. 68–90. DOI: 10.17212/2782-2230-2026-2-68-90.

БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2026. – № 2 (121). – 91–106

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2026-2-91-106

РАЗРАБОТКА МЕТОДИКИ ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЯ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ*

К.А. БИРЮКОВ[1], А.В. ИВАНОВ[2]

[1] *РФ, 630047, г. Новосибирск, ул. Окружная, 29В, ООО «Предприятие “ЭЛТЕКС”», руководитель группы лицензирования сервисного центра ESR. E-mail: kirill.biryukov@eltex-co.ru*
[2] *РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент, заведующий кафедрой защиты информации. E-mail: andrej.ivanov@corp.nstu.ru*

В настоящей статье рассматривается разработка универсальной комплексной методики тестирования систем обнаружения и предотвращения вторжений для объективной оценки их эффективности в условиях роста сложности сетевых атак. Существующие подходы часто зависят от конкретного производителя, что затрудняет независимый сравнительный анализ. Методика основана на модульном подходе и реализуется на тестовом стенде с непосредственным включением системы на пути сетевого трафика. В рамках исследования сформулированы требования к методике, включая универсальность, воспроизводимость, простоту применения и прозрачность анализа результатов. В ходе функциональных тестов проверяется блокировка атак в реальном времени, корректность журналирования, обработка правил для различных протоколов, контентная фильтрация и поведение системы в режиме отказа. В статье предложена структура оценки, соответствующая рекомендациям стандартов ISO/IEC 27034-1 и NIST SP 800-94. Разработанное решение позволяет проводить независимый сравнительный анализ средств защиты независимо от вендора и сокращать затраты на тестирование, обеспечивает воспроизводимость тестов и повышает обоснованность выбора средств защиты для критической инфраструктуры.

Ключевые слова: система обнаружения вторжений, система предотвращения вторжений, методика тестирования, inline-режим, сигнатуры, фильтрация трафика

* Статья получена 12 мая 2026 г.

ВВЕДЕНИЕ

В условиях цифровой трансформации критической инфраструктуры системы обнаружения и предотвращения вторжений (Intrusion Detection and Prevention Systems, далее IDS/IPS) становятся неотъемлемым компонентом эшелонированной защиты, обеспечивая мониторинг и блокировку вредоносной активности [1]. Однако надежность периметра безопасности напрямую зависит от корректности конфигурации и действительной эффективности применяемых средств защиты.

Для подтверждения соответствия заявленных функций систем IDS/IPS их производители требуют проведения объективной оценки их характеристик [2]. Несмотря на наличие международных стандартов, практическая реализация тестирования часто сталкивается с ограничениями, связанными с отсутствием универсальных верификационных процедур. Большинство существующих подходов к оценке ориентированы на специфические программно-аппаратные комплексы, что затрудняет проведение независимого сравнительного анализа. Возникающее противоречие между необходимостью полноценного функционального и точечного тестирования имеющихся методик обусловливает актуальность разработки единого подхода к тестированию.

ПОСТАНОВКА ЗАДАЧИ

- Рассмотреть существующие методики тестирования систем IDS/IPS и выявить их слабые стороны.
- Сформировать критерии, которым должна соответствовать разрабатываемая методика тестирования.
- На основе критериев разработать методику тестирования систем IDS/IPS.

1. ПРОБЛЕМЫ СУЩЕСТВУЮЩИХ МЕТОДИК ТЕСТИРОВАНИЯ

В методиках тестирования систем IDS/IPS наблюдается следующая тенденция: процедуры оценки детально проработаны, но привязаны к конкретному продукту, так как большинство методик написаны непосредственно производителем этих систем и ориентированы на демонстрацию функционала конкретно их продукта [3]. Это не позволяет использовать данные методики в рамках тестирования различных продуктов класса IDS/IPS систем во время сравнительных тестов для выявления наиболее подходящего экземпляра под конкретные задачи.

Целью работы является разработка универсальной комплексной методики тестирования IDS/IPS, обеспечивающей объективную оценку эффективности средств защиты с возможностью полного понимания, контроля и воспроизведения тестов без необходимости обладания углубленными навыками работы с системами. Использование предложенного подхода позволит сократить затраты на тестирование, повысить объективность оценки и обеспечить более обоснованный выбор средств защиты для конкретных условий эксплуатации.

2. РАЗРАБОТКА МЕТОДИКИ ТЕСТИРОВАНИЯ

2.1. ТРЕБОВАНИЯ К МЕТОДИКЕ ТЕСТИРОВАНИЯ

Методика функционального тестирования должна соответствовать следующим критериям.

- Применимость к любой системе IDS/IPS независимо от производителя и ее типа (аппаратная/программная) [4].
- Стабильность воспроизведения тестов.
- Простота проведения тестов:
  - отсутствие необходимости использования сложного или платного программного обеспечения, предназначенного для тестирования [5];
  - легко воспроизводимые шаги методики тестирования и анализа результата для человека, не погруженного в специфику IDS/IPS систем.
- Описание назначения каждого тест-кейса, т. е. какой функционал проверяет конкретный тест-кейс и для чего этот функционал необходим в системе IDS/IPS.

В соответствии с указанными критериями была составлена методика тестирования системы IDS/IPS, включающая в себя тесты, отвечающие заданным критериям.

2.2. СХЕМА СТЕНДА ТЕСТИРОВАНИЯ

Для возможности проведения тестирования необходимо построить тестовый стенд.

Тестовый стенд для тестирования систем обнаружения и предотвращения вторжений реализует двунаправленную архитектуру с размещением IDS/IPS системы в режиме inline между внешним и внутренним сетевыми сегментами [6]. Inline-режим – это режим функционирования системы IPS, при котором

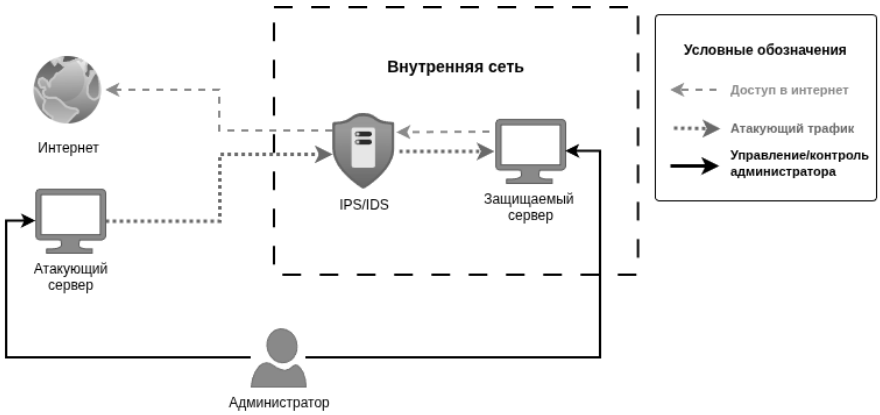


Схема стенда тестирования

Diagram of the test stand

устройство размещается непосредственно на пути сетевого трафика между внешней и защищаемой внутренней сетью, обеспечивая последовательную обработку всех проходящих пакетов [7]. Такая конфигурация соответствует рекомендациям NIST SP 800-94 и обеспечивает обязательную маршрутизацию всего трафика через систему, что критически важно для корректной оценки предотвращающих функций [8]. Стенд включает атакующую станцию с инструментами генерации эксплойтов и аномального трафика, защищаемый сервер с отключенными встроенными средствами защиты и доступом в интернет.

2.3. ПРОВЕРКА БЛОКИРОВАНИЯ АТАК В РЕЖИМЕ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Цель теста: подтвердить возможность системы IPS блокировать атаки в режиме реального времени [9].

Конфигурация стенда: IPS в режиме inline.

Конфигурация защищаемого сервера: сервисы с известными уязвимостями, для которых существуют готовые сигнатуры.

Конфигурация атакующей станции: утилита Metasploit Framework для эксплуатации уязвимостей, утилита iperf3 для генерации легитимного трафика в режиме фонового потока.

Методика тестирования: в рамках подготовки тестовой среды необходимо настроить IPS в inline-режиме с политикой блокирования для выбран-

ных сигнатур атак [10]; с помощью утилиты Metasploit выполнить последовательную генерацию атак с атакующей станции на защищаемый сервер [11], а также выполнить чередование атак с легитимным трафиком для проверки отсутствия влияния на легальный трафик.

Анализ результатов: сопоставить записи журнала IDS с фактическим состоянием защищаемого сервера, удостовериться в отсутствии вредоносной нагрузки при наличии события блокировки.

Ожидаемый результат: система должна выполнить полную блокировку атакующего трафика с генерацией события предотвращения в журнале и отсутствием признаков успешной эксплуатации уязвимости на защищаемом сервере [12].

Критерии успеха: полное блокирование всех проведенных атак при сохранении целостности легитимного трафика.

Критерии неуспеха: успешная эксплуатация уязвимости при наличии записи о блокировке в журнале (несоответствие лога реальному поведению) или блокирование легитимного трафика.

2.4. ПРОВЕРКА КОРРЕКТНОСТИ ЖУРНАЛИРОВАНИЯ И СООТВЕТСТВИЯ ЗАПИСЕЙ РЕАЛЬНЫМ СОБЫТИЯМ

Цель теста: подтвердить полноту, точность и целостность данных, фиксируемых системой в журналах событий.

Конфигурация стенда: развертывание IDS/IPS в режиме inline с настроенным полным журналированием событий в системе IDS.

Конфигурация защищаемого сервера: отключенные встроенные механизмы защиты хоста, настроенный сетевой интерфейс во внутреннем сегменте защищаемой сети.

Конфигурация атакующей станции: настроенный сетевой интерфейс во внешнем сегменте сети, утилита Scapy для генерации аномального трафика, утилита iperf3 для генерации легитимного трафика в режиме фонового потока.

Методика тестирования: развернуть IDS/IPS в режиме inline с настроенным полным журналированием событий; выполнить последовательную генерацию атак типа icmp-flood с помощью Scapy с одновременной генерацией легитимного фонового трафика через iperf3; провести атаку типа syn-flood путем генерации TCP-пакетов с флагом SYN через Scapy с интенсивностью, превышающей пороговое значение системы (например, 1500 соединений в секунду), с одновременной передачей легитимных установок соединений для проверки дифференциации атакующего и легитимного трафика [13]; дополнительно выполнить атаку типа UDP-flood с генерацией пакетов с произволь-

ными портами назначения через Scapy для имитации спуфинга и использованием iperf3 в режиме генерации UDP-трафика с пропускной способностью, превышающей лимит системы.

Анализ результатов: сравнить данные журнала событий с фактическими действиями, совершенными в ходе теста, а именно: временные метки событий, IP-адрес источника и цели, его порт, тип протокола, количество обработанных пакетов, действие системы обнаружения и предотвращения вторжений (блокировка, ограничение, журналирование).

Ожидаемый результат: система обеспечивает журналирование всех событий в соответствии с ее фактическими действиями.

Критерии успеха

- Разница во времени между реальным событием и тем, как оно записано, меньше одной секунды.
- Заявленное действие системы соответствует ее фактическому поведению.
- Отсутствуют ложные срабатывания на легитимном трафике.

Критерии неуспеха

- Разница во времени между реальным событием и тем, как оно записано, более одной секунды для более чем 5 % трафика.
- Заявленное действия системы не соответствует ее фактическому поведению.
- В журнале присутствуют ложные срабатывания на легитимном трафике (например, заявленная блокировка при прохождении пакетов).

2.5. ПРОВЕРКА СРАБАТЫВАНИЯ ПРАВИЛ ПО КОНКРЕТНЫМ ПРОТОКОЛАМ

Цель теста: проверить корректную отработку правила системы IDS/IPS по конкретным сетевым протоколам [14].

Конфигурация стенда: развертывание системы IPS в режиме с конфигурацией правил для протоколов TCP, UDP, ICMP, IP, HTTP.

Конфигурация защищаемого сервера: отключенные встроенные механизмы защиты хоста, настроенный сетевой интерфейс во внутреннем сегменте защищаемой сети.

Конфигурация атакующей станции: утилита Scapy для генерации трафика в формате конкретного протокола.

Методика тестирования: выполняем последовательную генерацию трафика по протоколам TCP, UDP, ICMP, IP, HTTP с помощью утилиты Scapy.

Анализ результатов: каждый тип протокола должен вызвать срабатывание правила, относящегося конкретно к его типу.

Ожидаемый результат: система должна обеспечить корректное детектирование и отработку правил для каждого протокола без взаимного влияния.

Критерии успеха

- Полное детектирование целевых аномалий для каждого протокола с корректной привязкой к соответствующему правилу.
- Отсутствие ложных срабатываний правил на легитимном трафике других протоколов.

Критерии неуспеха

- Отсутствие детектирования более чем 1 % аномальных пакетов для любого протокола.
- Ложное срабатывание правила для протокола, отличного от целевого.
- Расхождение между заявленным действием правила и фактическим поведением трафика (например, заявленная блокировка при прохождении пакетов).

2.6. ПРОВЕРКА НАСТРОЙКИ КАТЕГОРИЙ КОНТЕНТНОЙ ФИЛЬТРАЦИИ

Цель теста: подтвердить корректность и возможность фильтрации трафика по конкретным категориям контента [15].

Конфигурация стенда: развертывание системы IPS в режиме inline с установленными категориями для контентной фильтрации (например, Gambling, Social-media, Games).

Конфигурация защищаемого сервера: браузер или утилита wget для отправки запросов на ресурсы из сконфигурированных категорий.

Методика тестирования: выполнить генерацию трафика путем последовательной отправки запросов на сайты из категорий gambling, social-media и games, а также на любой другой сайт, не входящий в список настроенных категорий.

Анализ результатов: проверить срабатывание соответствующего правила на каждую категорию и удостовериться в отсутствии ложных срабатываний при отправке запросов на сайты, не входящие в список настроенных категорий.

Ожидаемый результат: система должна обеспечить корректную фильтрацию трафика согласно настроенным категориям контентной фильтрации.

Критерии успеха

- Полная сработка правил при попытках доступа к ресурсам, попадающим под настроенные категории.
- Отсутствие ложных срабатываний правил на легитимном трафике.

Критерии неуспеха

- Отсутствие детектирования более чем 1 % пакетов, подходящих под трафик указанных категорий.
- Ложное срабатывание правила для легитимного трафика при доступе к ресурсу, однозначно не относящемуся к указанной категории.

2.7. ВЕРИФИКАЦИЯ РЕЖИМА ОТКАЗА В БЕЗОПАСНОЕ СОСТОЯНИЕ (FAIL-CLOSE)

Цель теста: проверить корректную реализацию принципа «отказ в безопасное состояние» (fail-safe/fail-secure), при котором система IPS в условиях неготовности (отсутствие сигнатур, сбои обновления) [16] блокирует весь входящий трафик, предотвращая потенциальную эксплуатацию уязвимостей в период незащищенного состояния.

Конфигурация стенда: развертывание системы IPS в режиме inline в конфигурации режима отказа fail-close.

Конфигурация защищаемого хоста: наличие утилиты ping для генерации ICMP трафика.

Методика тестирования: необходимо прервать возможность обновления сигнатур путем отключения связи с сервером; удалить локально сохраненные сигнатуры; выполнить генерацию легитимного ICMP трафика с помощью утилиты ping; сравнить количество отправленных и полученных пакетов; вернуть связь системы IDS/IPS с сервером сигнатур и выполнить повторную генерацию аналогичного ICMP трафика; вновь сравнить количество отправленных и полученных пакетов.

Анализ результатов: при невозможности доступа к серверу сигнатур и отсутствии их в локальном кеше блокируется весь трафик. При подключении системы к серверу сигнатур и получении с него правил легитимный трафик свободно проходит через систему IPS/IDS.

Ожидаемый результат: при отсутствии сигнатур система блокирует прохождение всего трафика.

Критерии успеха

- Полное блокирование легитимного трафика при нулевом количестве загруженных сигнатур.
- Отсутствие потерь легитимного трафика после успешной загрузки сигнатур при отсутствии активных атак.

Критерии неуспеха

- Пропускание любого трафика при отсутствии загруженных сигнатур.
- Блокирование легитимного трафика после успешной загрузки сигнатур при отсутствии активных атак.

- Отсутствие системных событий, фиксирующих переходы между состояниями загрузки сигнатур.

2.8. ПРОВЕРКА ДОСТОВЕРНОСТИ ОПЕРАТИВНОЙ СТАТИСТИКИ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Цель теста: проверить возможность просмотра оперативной информации по сконфигурированным правилам и сигнатурам, а также корректность состояния счетчиков их срабатываний.

Конфигурация стенда: развертывание системы IPS в режиме inline с настроенными категориями и URL контентной фильтрации, скачанными и примененными сигнатурами. Для всех настроек установлены различные виды действия системы (оповещение, блокировка, пропуск).

Конфигурация защищаемого хоста: браузер или утилита wget для отправки запросов на ресурсы из списка сконфигурированных URL, утилита Scapy для генерации аномального трафика.

Методика тестирования: зафиксировать показатели статистики до загрузки базы сигнатур (количество правил, сигнатур, политик) и активировать загрузку сигнатур с мониторингом процесса через средство просмотра оперативной информации; выполнить генерацию трафика, подходящего под сигнатуры различных действий, а также генерацию легитимного трафика.

Анализ результатов: сопоставить количество срабатываний в интерфейсе статистики с фактическим количеством событий в трафике; проверить отсутствие инкрементации счетчиков ложных срабатываний при обработке легитимного трафика; проверить корректность агрегации данных (суммарное количество срабатываний по политике должно равняться сумме срабатываний всех входящих в нее правил); убедиться, что отображаемые метрики точно отражают текущее состояние системы и ее действий.

Ожидаемый результат: отображаемые метрики точно отражают текущее состояние системы и ее действий.

Критерии успеха

- Средняя задержка обновления оперативной статистики менее двух секунд при нагрузке до 90 % от номинальной пропускной способности системы.
- Полное соответствие агрегированных данных на уровне политик сумме данных по входящим в них правилам.
- Отсутствие ложной инкрементации счетчиков при обработке легитимного трафика.

Критерии неуспеха

- Относительная погрешность количественных метрик более 1 % для любого из проверяемых параметров.

- Отсутствие обновления статистики более 60 секунд после завершения операции загрузки сигнатур или после серии срабатываний.
- Несоответствие между заявленным количеством сработавших правил и фактическими действиями системы (например, блокирование трафика без инкрементации счётчика).
- Нарушение иерархической целостности данных (сумма срабатываний дочерних правил не равна количеству срабатываний родительской политики) для более чем 5 % проверенных политик.

3. СРАВНЕНИЕ РАЗРАБОТАННОЙ МЕТОДИКИ ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЯ С СУЩЕСТВУЮЩИМИ АНАЛОГАМИ

Для объективной оценки преимуществ и практической ценности разработанной методики функционального тестирования был проведен сравнительный анализ с существующими подходами к тестированию средств защиты информации. В качестве объектов сравнения выбраны методологии тестирования ведущих российских вендоров (Jet, Solar, Континент) [17–19], что обеспечивает репрезентативность выборки и позволяет выявить ключевые отличия предложенного подхода.

Разработанная методология функционального тестирования систем обнаружения и предотвращения вторжений представляет собой структурированный комплекс тест-кейсов, обеспечивающий проверку ключевых функциональных свойств средств защиты в соответствии с принципами объективности и воспроизводимости, рекомендованными в работах Национального института стандартов и технологий (NIST). Методика реализует системный подход к оценке, охватывающий критические аспекты функционирования IDS/IPS: эффективность предотвращения атак в реальном времени, достоверность журналирования, корректность обработки протокольно-специфичных правил и надежность механизмов отказоустойчивости.

Структурной основой методики выступает модульная организация тестовых сценариев, каждый из которых проверяет отдельный функциональный блок системы защиты IDS/IPS. Тестовый модуль верификации блокирования атак в режиме предотвращения обеспечивает оценку способности системы к детектированию и прерыванию эксплуатации уязвимостей на уровне прикладных протоколов. Эта методика позволяет выполнить проверку работы журнала событий для подтверждения соответствий записей реальному поведению системы. Такая проверка обеспечивает соответствие методики функционального тестирования стандарту ISO/IEC 27034-1.

Сравнительный анализ функциональных методик тестирования IDS/IPS

A comparative analysis of functional testing methods for IDS/IPS

Критерий сравнения	Авторская методика	Методика Jet	Методика Solar	Методика «Континент 4» (TS Solution)
Универсальность / независимость от вендора	Да	Частично	Нет	Нет
Воспроизводимость тестов	Да	Да	Частично	Нет
Использование только бесплатного / открытого ПО	Да	Нет	Нет	Да
Четкие критерии успеха и провала для каждого теста	Да	Частично	Частично	Нет
Соответствие международным стандартам	Да	Частично	Нет	Нет
Тестирование режима Fail-Close	Да	Нет	Нет	Нет
Проверка достоверности оперативной статистики	Да	Нет	Нет	Нет
Описание назначения каждого тест-кейса	Да	Частично	Частично	Нет

Важным отличием авторской методики является наличие проверки режима отказа. Такой сценарий проверяет работу системы при отсутствии сигнатур, что позволяет оценить поведение системы в нештатной ситуации при технических сбоях.

ЗАКЛЮЧЕНИЕ

Таким образом, разработанная методика функционального тестирования позволяет выполнять оценку функциональности систем обнаружения и предотвращения вторжений независимо от их производителя с возможностью воспроизведения тестовых сценариев, используя только открытые и бесплатные инструменты. Благодаря своей структуре методика может быть применена как для комплексной проверки функциональности систем IDS/IPS, так и для частичной проверки конкретных возможностей, что обеспечивает ее значительное преимущество относительно других методик функционального тестирования систем обнаружения и предотвращения вторжений.

СПИСОК ЛИТЕРАТУРЫ

1. *Mehta H., Nizama A., Subhashini K.* Comprehensive review of network intrusion detection and prevention systems // International Journal of Latest Technology in Engineering Management and Applied Science. – 2025. – Vol. 14 (6). – P. 804–807. – DOI: 10.51583/IJLTEMAS.2025.140600087.

2. *Bhadti A., Barthakur P.* A survey on next generation intrusion detection systems empowering advanced threat detection with generative AI // International Journal of Advanced Research in Computer and Communication Engineering. – 2024. – Vol. 13 (6). – DOI: 10.17148/IJARCCE.2024.13633.

3. ISO/IEC 27034-1:2011. Information technology – Security techniques – Application security – Part 1: Overview and concepts. – URL: https://www.iso.org/standard/44378.html (accessed: 03.02.2026).

4. *Tori A.R., Hasan K.F.* An evaluation framework for network IDS/IPS datasets: leveraging MITRE ATT&CK and industry relevance metrics // arXiv preprint. – 2025. – DOI: 10.48550/arXiv.2511.12743.

5. *Kott A.* Autonomous intelligent cyber-defense agent: Introduction and overview // Advances in Information Security. Vol. 87. – Cham: Springer, 2023. – DOI: 10.1007/978-3-031-29269-9_1.

6. PP-Module for intrusion prevention systems (IPS). Version: 1.0. – NIAP, 2021. – URL: https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/MOD_IPS_v1.0.pdf (accessed: 15.02.2026).

7. *Beale J.*, et al. Snort intrusion detection and prevention toolkit. – Syngress, 2021.

8. *Scarfone K.A., Mell P.M.* Guide to intrusion detection and prevention systems (IDPS). – URL: https://csrc.nist.gov/pubs/sp/800/94/r1/ipd (accessed: 22.02.2026).

9. *Vishrutha V., Nagaraja G.S.* Real-time intrusion detection system using scapy with hybrid machine and deep learning models and smart email alerting // SSRN Electronic Journal. – 2025. – URL: https://ssrn.com/abstract=5349776 (accessed: 07.02.2026).

10. *Alqahtani H., Kumar G.* A deep learning-based intrusion detection system for in-vehicle networks with knowledge graph and statistical methods // International Journal of Machine Learning and Cybernetics. – 2024. – Vol. 16 (5–6). – P. 3539–3555. – DOI: 10.1007/s13042-024-02465-0.

11. *Tandon A., Pandey S.* A study on penetration testing using metasploit framework // International Journal of Research and Review in Applied Science, Humanities, and Technology. – 2025. – Spec. iss. – P. 83–87. – DOI: 10.71143/y4sten11.

12. *Bejtlich R.* The practice of network security monitoring. – Starch Press, 2022.

13. *Manzuik S., Gold A., Gatford C.* Network security assessment: From vulnerability to patch. – Syngress, 2006. – 372 p.

14. Fortinet. Intrusion prevention system (IPS) // Fortinet Documentation Library. – URL: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/48143/intrusion-prevention-system-ips (accessed: 07.02.2026).

15. *Sun Q.* Intrusion detection in high-performance computing. – 2024. – URL: https://hps.vi4io.org/_media/teaching/autumn_term_2023/stud/hpcsa_sun_qumeng.pdf (accessed: 05.02.2026).

16. *Аникин А.Д., Бирюков К.А., Архипова А.Б.* Анализ протоколов безопасности на базе системы распространения лицензируемого контента // Безопасность цифровых технологий. – 2023. – № 1 (108). – С. 26–35. – DOI: 10.17212/2782-2230-2023-1-26-35.

17. РТ-Солар. Solar Next Generation Firewall. Методика тестирования. Версия 1.2. – М.: ООО «РТ-Солар», 2024. – 24 с. – URL: https://rt-solar.ru/upload/docs/solar-ngfw--metodika-testirovaniya-v1.2.pdf (дата обращения: 26.03.2026).

18. Отчет о тестировании функций безопасности NGFW «Континент 4» / С.Х. Аббас, В.А. Насер, А.А. Кадим; TS Solution. – М.: ООО «Код Безопасности», 2024. – 16 с. – URL: https://www.securitycode.ru/upload/blog/Отчет%20о%20тестировании%20функций%20безопасности%20NGFW_Континент%204.pdf (дата обращения: 26.03.2026).

19. Методика функционального тестирования устройств класса NGFW/UTM: версия 2.0. – М.: Инфосистемы Джет, 2024. – 25 с. – URL: https://ngfw.jet.su/metodika_funkczionalnogo_testirovaniya_2_0.pdf (дата обращения: 26.03.2026).

Бирюков Кирилл Андреевич, руководитель группы лицензирования сервисного центра ESR компании «Элтекс». Область научных интересов: информационная безопасность, компьютерные сети. E-mail: kirill.biryukov@eltex-co.ru

Иванов Андрей Валерьевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации Новосибирского государственного технического университета. Область научных интересов: информационная безопасность, кибербезопасность. E-mail: andrej.ivanov@corp.nstu.ru

DOI: 10.17212/2782-2230-2026-2-91-106

Development of a methodology for functional testing of intrusion detection and prevention systems*

K.A. Biryukov[1], A.V. Ivanov[2]

[1] *Eltex, 29V, Okruzhnaya Street, Novosibirsk, Russian Federation, 630073, Russian Federation, head of the licensing group of the service center ESR. E-mail: kirill.biryukov@eltex-co.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, PhD in Technology, head of the Information Security Department. E-mail: andrej.ivanov@corp.nstu.ru.*

This article discusses the development of a universal, comprehensive testing methodology for intrusion detection and prevention systems, designed to objectively evaluate their effectiveness in the face of increasingly complex network attacks. Existing approaches are often vendor-specific, which hinders independent comparative analysis. The methodology is based on a modular approach and is implemented on a test bench with the system directly integrated into the network traffic path. The study formulates requirements for the methodology, including universality, reproducibility, ease of use, and transparency of results analysis. Functional tests verify real-time attack blocking, logging accuracy, rule processing for various protocols, content filtering, and system behavior in failure mode. The article proposes an evaluation framework consistent with the recommendations of ISO/IEC 27034-1 and NIST SP 800-94. The developed solution enables independent, vendor-neutral comparative analysis of security measures, reduces testing costs, ensures test reproducibility, and enhances the soundness of security measure selection for critical infrastructure.

Keywords: intrusion detection system, intrusion prevention system, testing methodology, inline mode, signatures, traffic filtering

REFERENCES

1. Mehta H., Nizama A., Subhashini K. Comprehensive review of network intrusion detection and prevention systems. *International Journal of Latest Tech-*

* *Received 12 May 2026.*

nology in Engineering Management and Applied Science, 2025, vol. 14 (6), pp. 804–807. DOI: 10.51583/IJLTEMAS.2025.140600087.

2. Bhadti A., Barthakur P. A survey on next generation intrusion detection systems empowering advanced threat detection with generative AI. *International Journal of Advanced Research in Computer and Communication Engineering*, 2024, vol. 13 (6). DOI: 10.17148/IJARCCE.2024.13633.

3. ISO/IEC 27034-1:2011. *Information technology – Security techniques – Application security* – Part 1: *Overview and concepts*. Available at: https://www.iso.org/standard/44378.html (accessed 12.02.2026).

4. Tori A.R., Hasan K.F. An evaluation framework for network IDS/IPS datasets: leveraging MITRE ATT&CK and industry relevance metrics. *arXiv preprint*, 2025. DOI: 10.48550/arXiv.2511.12743.

5. Kott A. Autonomous intelligent cyber-defense agent: Introduction and overview. *Advances in Information Security*. Vol. 87. Cham, Springer, 2023. DOI: 10.1007/978-3-031-29269-9_1.

6. *PP-Module for intrusion prevention systems (IPS)*. Version: 1.0. NIAP, 2021. Available at: https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/MOD_IPS_v1.0.pdf (accessed 15.02.2026).

7. Beale J., et al. *Snort intrusion detection and prevention toolkit*. Syngress, 2021.

8. Scarfone K.A., Mell P.M. *Guide to intrusion detection and prevention systems (IDPS)*. Available at: https://csrc.nist.gov/pubs/sp/800/94/r1/ipd (accessed 22.02.2026).

9. Vishrutha V., Nagaraja G.S. Real-time intrusion detection system using scapy with hybrid machine and deep learning models and smart email alerting. *SSRN Electronic Journal*, 2025. Available at: https://ssrn.com/abstract=5349776 (accessed 07.02.2026).

10. Alqahtani H., Kumar G. A deep learning-based intrusion detection system for in-vehicle networks with knowledge graph and statistical methods. *International Journal of Machine Learning and Cybernetics*, 2024, vol. 16 (5–6), pp. 3539–3555. DOI: 10.1007/s13042-024-02465-0.

11. Tandon A., Pandey S. A study on penetration testing using metasploit framework. *International Journal of Research and Review in Applied Science, Humanities, and Technology*. 2025, Spec. iss., pp. 83–87. DOI: 10.71143/y4sten11.

12. Bejtlich R. *The practice of network security monitoring*. Starch Press, 2022.

13. Manzuik S., Gold A., Gatford C. *Network security assessment: From vulnerability to patch*. Syngress, 2006. 372 p.

14. Fortinet. Intrusion prevention system (IPS). *Fortinet Documentation Library*. Available at: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/48143/intrusion-prevention-system-ips (accessed 07.02.2026).

15. Sun Q. *Intrusion detection in high-performance computing*. 2024. Available at: https://hps.vi4io.org/_media/teaching/autumn_term_2023/stud/hpcsa_sun_qumeng.pdf (accessed 05.02.2026).

16. Anikin A.D., Biryukov K.A., Arkhipova A.B. Analiz protokolov bezopasnosti na baze sistemy rasprostraneniya litsenziruemogo kontenta [Analysis of security protocols based on the licensed content distribution system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 1 (108), pp. 26–35. DOI: 10.17212/2782-2230-2023-1-26-35.

17. RT-Solar. *Solar Next Generation Firewall. Metodika testirovaniya*. Versiya 1.2 [NGFW Solar Testing Methodology. Version 1.2]. Moscow, RT-Solar LLC, 2024. 24 p. Available at: https://rt-solar.ru/upload/docs/solar-ngfw--metodika-testirovaniya-v1.2.pdf (accessed 26.03.2026).

18. Abbas S.Kh., Naser V.A., Kadim A.A. *Otchet o testirovanii funktsii bezopasnosti NGFW «Kontinent 4»* [Security function testing report for NGFW "Continent 4"]. TS Solution. Moscow, Security Code LLC Publ., 2024. 16 p. Available at: https://www.securitycode.ru/upload/blog/Отчет%20о%20тестировании%20функций%20безопасности%20NGFW_Континент%204.pdf (accessed 26.03.2026).

19. Jet Security Team. *Metodika funktsional'nogo testirovaniya ustroistv klassa NGFW/UTM*: versiya 2.0 [Functional testing methodology for NGFW/UTM devices. Version 2.0]. Moscow, 2024. 25 p. Available at: https://ngfw.jet.su/metodika_funkczionalnogo_testirovaniya_2_0.pdf (accessed 26.03.2026).

Для цитирования:

Бирюков К.А., Иванов А.В. Разработка методики функционального тестирования систем обнаружения и предотвращения вторжений // Безопасность цифровых технологий. – 2026. – № 2 (121). – С. 91–106. – DOI: 10.17212/2782-2230-2026-2-91-106.

For citation:

Biryukov K.A., Ivanov A.V. Razrabotka metodiki funktsional'nogo testirovaniya sistem obnaruzheniya i predotvrashcheniya vtorzhenii [Development of a methodology for functional testing of intrusion detection and prevention systems]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2026, no. 2 (121), pp. 91–106. DOI: 10.17212/2782-2230-2026-2-91-106.

ПРАВИЛА ДЛЯ АВТОРОВ

УСЛОВИЯ ПРИЕМА СТАТЕЙ

Все статьи и сопровождающие их материалы в журнал подаются через сайт журнала в электронном виде после регистрации всех авторов статьи. Регистрация обязывает каждого автора иметь международный идентификационный номер ORCID. Иные варианты подачи материалов не рассматриваются.

Автор (один из соавторов) в своем личном кабинете выбирает в меню пункт «Подать статью» и вводит все необходимые данные. Своих соавторов при этом он выбирает из списка зарегистрированных пользователей.

Рукопись статьи готовится в соответствии с правилами оформления в редакторе MS Word и прикрепляется в формате *.doc, *.docx.

Сканированные лицензионный договор с подписями авторов и экспертное заключение (цветной режим сканирования, разрешение не менее 600 dpi) необходимо также разместить на сайте журнала в разделе «Подать статью» в формате *.pdf, *.jpg, *.jpeg.

По окончании всех работ обязательно нажать кнопку «Отправить в редакцию».

В редакцию журнала представляются следующие материалы.

1. **Статья**, подготовленная в соответствии с правилами оформления, – печатная версия, 2 экземпляра, подписанных авторами.

2. **Контактная информация** (телефоны рабочий и сотовый, адрес электронной почты, место работы, адрес места работы, должность, ученая степень, ученое звание автора) – печатная версия, 2 экземпляра.

3. **Описание статьи для базы данных «Российский индекс научного цитирования (РИНЦ)»**, подготовленное в соответствии с правилами оформления, – печатная версия, один экземпляр.

4. **Лицензионный договор**, заполненный и подписанный.

5. **Электронная версия статьи, контактной информации, описания статьи для базы данных РИНЦ, сканированный лицензионный договор и экспертное заключение о возможности опубликования отправляются отдельными файлами на адрес редакции**.

6. **Согласие на публикацию, обработку и распространение персональных данных авторов статей**.

7. **Экспертное заключение о возможности опубликования**.

Редакцией рассматриваются только те материалы авторов, которые полностью соответствуют вышеобозначенным требованиям. Неполный пакет материалов редакцией не рассматривается.

Подготовленные материалы направляются на почтовый адрес редакции: 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет (НГТУ), корп. 7, ком. 606, в редакцию журнала «Безопасность цифровых технологий».

Все рукописи рецензируются, по результатам рецензирования редколлегия принимает решение о целесообразности опубликования материалов.

ВНИМАНИЕ!

Авторы несут ответственность за оформление, содержание и сам факт публикации статьи. Редакция журнала не несет ответственности за возможный ущерб, вызванный публикацией статьи. При наличии существенных недостатков в оформлении и содержании статьи редакция принимает решение об отклонении статьи без приведения полного перечня ошибок автора.

Ранее опубликованные материалы, а также материалы, представленные для публикации в других журналах, к рассмотрению не принимаются.

ПРАВИЛА ОФОРМЛЕНИЯ

При подготовке документов для отправки в редакцию журнала авторам рекомендуется внимательно прочитать правила и посмотреть примеры оформления статей и всех необходимых сопутствующих документов. Редакция рассматривает статьи, подготовленные как на русском, так и на английском языке. Для опубликования статьи на английском языке необходимо дополнительно предоставить ее русскоязычный вариант, оформленный по правилам журнала (кроме зарубежных авторов).

Перед отправкой рукописи в редакцию авторам необходимо проверить свою статью с помощью системы «Антиплагиат». Принятый редакционной коллегией уровень оригинальности статей должен составлять не менее 85 %.

Чтобы статья была направлена на рецензирование, необходимо подготовить следующее:

1) **статью** в соответствии с правилами оформления;

2) **контактную информацию** в одном файле предоставить по каждому автору: ФИО полностью, ученая степень, ученое звание, должность, место работы, адрес места работы, телефон рабочий и мобильный, адрес электронной почты;

3) **описание статьи для базы данных «Российский индекс научного цитирования (РИНЦ)»**;

4) **лицензионный договор** заполнить, бланк лицензионного договора должен быть подписан только авторами (он доступен авторам также в личном кабинете). Если авторов несколько, то необходимо добавить поля на всех авторов и подписать каждому из них;

5) **экспертное заключение** о возможности опубликования, принятое в вашей организации;

6) согласие на публикацию, обработку и распространение персональных данных авторов статей;

7) авторы, не являющиеся сотрудниками НГТУ, предоставляют **сопроводительное письмо** на имя проректора по научной работе НГТУ (ссылка на страницу сайта НГТУ). Письмо нужно подготовить на бланке организации с подписью и печатью руководителя.

ОСНОВНЫЕ РАЗДЕЛЫ ЖУРНАЛА

Автоматизация и управление технологическими процессами и производствами.

Управление в социальных и экономических системах.

Методы и системы защиты информации, информационная безопасность.

RULES FOR AUTHORS

CONDITIONS FOR ACCEPTANCE OF ARTICLES

All articles and their accompanying materials are submitted to the magazine through the magazine's website in electronic form after registration of all the authors of the article. Registration obliges each author to have an international ORCID. No other material supply options are considered.

The author (one of the co-authors) in his personal account selects the item "Submit article" in the menu and enters all the necessary data. At the same time, he selects his co-authors from the list of registered users.

The manuscript of the article is prepared in accordance with the design rules in the MS Word editor and attached in the format * .doc, * .docx.

Scanned license agreement with signatures of authors and expert opinion (color mode scanning, resolution not less than 600 dpi) can also be attached on the website of the magazine in the section "Submit article" in the format * .pdf, * .jpg, * .jpeg.

At the end of all works, be sure to click the "Send to Design" button.

The following materials are provided to the journal editor:

1. **The article**, prepared in accordance with the rules of design, is a private version, 2 copies signed by the authors.
2. **Contact information** (working and cellular phones, e-mail addresses, place of work, address of the place of work, position, scientific degree, academic title of the author) – printed version, 2 copies.
3. **The description of the article** for the database "**Russian Scientific Citation Index (RSCI)**", prepared in accordance with the rules of form-making, is a printed version, one copy.
4. **License agreement** completed and signed.
5. **Electronic version of the article**, contact information, description of the article for the RSCI database, scanned license agreement and expert opinion on the possibility of publication (in separate files to the editorial address).
6. **Consent to the publication, processing and dissemination of the personal data** of the authors of the articles.
7. **Expert opinion** on the possibility of publication.

The editors consider only those materials of the authors that fully meet the above requirements. Incomplete package of materials is not considered by the revision.

The prepared materials are sent to the postal address of the editorial office: 630073, Novosibirsk, Karl Marx Prospekt, 20, Novosibirsk State Technical University (NSTU), building 7, office 606, to the editors of the journal "Digital Technology Security".

All manuscripts were reviewed, and according to the results of the review, the editorial board decided on the appropriateness of publishing the materials.

ATTENTION!

The authors are responsible for the design, content and the fact of publication of the article. The editorial board of the journal is not responsible for possible damage caused by the publication of the article. If there are significant shortcomings in the design and content of the article, the editorial board decides to reject the article without giving a full list of the author's mistakes.

Previously published materials, as well as materials submitted for publication in other journals, are not accepted for consideration.

FORMATTING RULES

When preparing documents for submission to the journal editor, authors are advised to carefully read the rules and see examples of the design of articles and all necessary related documents. The Drafting Committee considered articles prepared in both Russian and English. To publish the article in English, it is necessary to additionally provide its Russian-language version, drawn up according to the rules of the magazine (except for foreign authors).

Before sending the manuscript to the editorial office, authors must check their article using the Antiplagiarism system. The level of originality of articles adopted by the Editorial Board should be at least 85 %.

For the article to be aimed at peer review, you need to prepare the following:

1) **the article** in accordance with the rules of design (volume from 7 to 30 pages);

2) **provide contact information** in one file for each author: full name, degree, academic title of the author, position, place of work, address of the place of work, telephone number of the worker and mobile, e-mail address;

3) **description of the article** for the database "Russian Scientific Citation Index (RSCI)";

4) fill out the **license agreement**, the form of the license agreement must be signed only by the authors (it is also available to the authors in the personal office), if there are several authors, then it is necessary to add fields on all authors and sign each of them;

5) **expert opinion** on the possibility of publication, adopted in your organization;

6) consent to the publication, processing and dissemination of the personal data of the authors of the articles;

7) authors who are not employees of the NSTU provide a **companion letter** addressed to the vice-rector for scientific work of the NSTU (link to the page of the NSTU website). The letter should be prepared on the form of the organization with the signature and seal of the manager.

JOURNAL SECTION

Automation and control of technological processes and productions.
Governance in social and economic systems.
Methods and systems of information protection, information security.