DOI: 10.18137/RNU.V9187.26.01.P.89 УДК 004.056

**Красюк Полина Сергеевна**
студент, Кубанский государственный аграрный университет имени И.Т. Трубилина, город Краснодар.
Электронный адрес: pooliinaa.chkaa@gmail.com
**Polina S. Krasyuk**
Student, Kuban State Agrarian University, Krasnodar.
E-mail address: pooliinaa.chkaa@gmail.com

**Елецков Олег Сергеевич**
студент, Кубанский государственный аграрный университет имени И.Т. Трубилина, город Краснодар.
Электронный адрес: olegeleckov@mail.ru
**Oleg S. Eletskov**
Student, Kuban State Agrarian University, Krasnodar.
E-mail address: olegeleckov@mail.ru

**Алашеев Вадим Викторович**
кандидат технических наук, доцент, Кубанский государственный аграрный университет имени И.Т. Трубилина, город Краснодар.
SPIN-код: 8512-6963, AuthorID: 903223
Электронный адрес: alasheev.kub@mail.ru
**Vadim V. Alasheev**
Ph.D. of Engineering Sciences, Docent, Kuban State Agrarian University, Krasnodar.
SPIN-code: 8512-6963, AuthorID: 903223
E-mail address: alasheev.kub@mail.ru

# СТРАТЕГИИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННЫХ СЕТЯХ 5G ДЛЯ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

**Аннотация.** Статья посвящена решению актуальной научно-практической проблемы обеспечения комплексной кибербезопасности распределенных сетей пятого поколения (5G), используемых для объектов критической информационной инфраструктуры. Актуальность исследования обусловлена интенсивной цифровизацией ключевых отраслей экономики и одновременным ростом sophistication-кибератак на системы умных городов и объекты топливно-энергетического комплекса. В работе проведен системный анализ архитектурных уязвимостей и угроз безопасности, специфичных для технологии 5G. Детально исследованы риски, связанные с использованием программно определяемых сетей (SDN), виртуализации сетевых функций (NFV), периферийных вычислений (MEC) и сетевых срезов. Выявлено, что традиционные подходы к безопасности оказываются неэффективными в условиях распределенной динамической архитектуры сетей нового поколения. На основе проведенного анализа разработана интегрированная стратегия защиты, сочетающая принципы эшелонированной обороны, динамического контроля доступа по модели Zero Trust и изоляции критических компонентов. Предложена оригинальная архитектурная модель системы безопасности, обеспечивающая

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление». 2026. № 1

сквозную защиту данных на всех уровнях сетевой инфраструктуры. Особое внимание уделено механизмам изоляции сетевых срезов и защите периферийных вычислительных узлов. Практическая значимость исследования заключается в возможности непосредственного внедрения разработанных решений при проектировании и развертывании защищенных сетей 5G для объектов критической инфраструктуры. Реализация предложенной стратегии позволит существенно повысить устойчивость ключевых систем к современным киберугрозам за счет централизованного управления политиками безопасности, динамической сегментации сетевых компонентов и реализации системы непрерывного мониторинга угроз.

***Ключевые слова:*** кибербезопасность, критическая инфраструктура, сети 5G, распределенные сети, угрозы безопасности, стратегия защиты, сетевые срезы.

***Для цитирования:*** *Красюк П.С., Елецков О.С., Алашеев В.В.* Стратегии обеспечения кибербезопасности в распределенных сетях 5G для критической инфраструктуры // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ, управление. 2026. № 1. С. 89–98. DOI: 10.18137/RNU.V9187.26.01.P.89

## CYBERSECURITY STRATEGIES FOR 5G DISTRIBUTED NETWORKS IN CRITICAL INFRASTRUCTURE

**Abstract.** The article discusses the problems of 5G network architecture and their cybersecurity. *The purpose* of this article is to develop a strategy and a set of measures to ensure the cybersecurity of distributed 5G networks for critical infrastructure facilities. *The objectives* include analyzing key threats, proposing protection measures, and developing architectural diagrams that will visualize the approach to building a security system. The article proposes a comprehensive protection strategy based on the principles of layered defense, the Zero Trust model, and component isolation. It also develops an architectural model of a security system that provides end-to-end data protection. This strategy is being used to protect smart home and energy sector facilities from cyberattacks.

***Keywords:*** cybersecurity, critical infrastructure, 5G networks, distributed networks, security threats, protection strategy, network slices.

***For citation:*** Krasyuk P.S., Eletskov O.S., Alasheev V.V. (2026) Cybersecurity strategies for 5G distributed networks in critical infrastructure. *Vestnik of Russian New University. Series: Complex Systems: Models, analysis, management.* No. 1. Pp. **8**9–98. DOI: 10.18137/RNU.V9187.26.01.P.89 (In Russian).

### *Введение*

Стратегический курс на цифровую трансформацию ключевых отраслей экономики, закрепленный в национальных проектах Российской Федерации, напрямую связывает повышение эффективности и устойчивости критической инфраструктуры (далее – КИ) с внедрением передовых телекоммуникационных технологий. Сети 5G, обладающие ультранизкой задержкой, высокой пропускной способностью и поддержкой массового интернета вещей (IoT), становятся несущим каркасом для таких сложных систем, как «умный город» и объекты топливно-энергетического комплекса (далее – ТЭК) [1]. Внедрение 5G позволяет реализовать распределенное управление энергосетями, интеллектуальные транспортные потоки, автоматизированный мониторинг и контроль

объектов ЖКХ, что ведет к значительному экономическому и социальному эффекту [2].

*Актуальность исследования и постановка проблемы*

Актуальность работы обосновывается стремительной цифровой трансформацией ключевых отраслей экономики России. Внедрение концепций «умный город» и модернизация объектов ТЭК напрямую связаны с использованием передовых телекоммуникационных технологий.

Проблема заключается в том, что преимущества архитектуры 5G – распределенность, виртуализация и программная определяемость – одновременно формируют принципиально новую, расширенную поверхность для кибератак. Такие компоненты, как программно-определяемые сети (SDN), виртуализация сетевых функций (NFV), периферийные вычисления (MEC) и сетевые срезы, создают уникальные векторы угроз [3]. Кибервоздействие на эти системы перестает быть виртуальной угрозой, трансформируясь в риски физического разрушения, масштабных техногенных аварий и коллапса городской среды. При этом традиционные подходы к безопасности, ориентированные на защиту статичного сетевого периметра, оказываются неэффективными в высокодинамичной и гетерогенной среде 5G. Существует острая потребность в практических решениях, которые обеспечивали бы защиту на протяжении всего пути данных – от датчика до центра управления.

*Определение цели и постановка задачи*

*Целью* данной работы является разработка практической стратегии и комплекса мер по обеспечению кибербезопасности распределенных сетей 5G для объектов критической инфраструктуры.

Для достижения поставленной цели в работе ставятся следующие *задачи:*

1) провести анализ ключевых архитектурных угроз, специфичных для сетей 5G в контексте их использования в умном городе и ТЭК;

2) на основе лучших практик (Zero Trust, сегментация) предложить комплекс взаимосвязанных организационных и технических мер защиты;

3) разработать наглядные архитектурные схемы, визуализирующие предложенный подход к построению системы безопасности.

*Практическая значимость* работы заключается в том, что предложенные решения могут быть использованы операторами связи, системными интеграторами и службами информационной безопасности организаций для проектирования и развертывания защищенных сетей 5G, что будет способствовать повышению киберустойчивости критической инфраструктуры Российской Федерации.

*Обзор литературы*

В работе [4] авторами проведен анализ угроз безопасности информации в сетях передачи данных стандарта 5G. Описана модель наиболее опасной для сетей 5G DDoS-атаки на целевой сервер жертвы. В статье сформулированы общие рекомендации по нейтрализации угроз безопасности информации при строительстве сетей стандарта 5G без учета специфики КИ.

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление». 2026. № 1

В работе [5] анализируются основные уязвимости IoT-систем. Предложены комплексные решения по защите умных устройств, основанные на многофакторной аутентификации, шифровании данных и регулярном обновлении программного обеспечения. Особое внимание уделено вопросам безопасности промышленного интернета вещей (IIoT) и критической инфраструктуры. Данное исследование решает частную, но важную задачу в рамках общей проблемы безопасности 5G, но не охватывает угрозу для MEC (Multi-access Edge Computing) и SDN (Software-Defined Networking).

В статье [6] представлена методика мониторинга электромагнитных помех, что важно для обеспечения безопасности беспроводных каналов связи 5G. Авторами разработана методика решения проблемы отсутствия объективных данных об электромагнитной обстановке, а полученные результаты предлагается использовать для проектирования стратегий кибербезопасности сетей 5G.

Высокий уровень государственных угроз, в том числе в киберпространстве, – предмет рассмотрения в работе [7]. Как отмечают авторы, кибератаки в США считаются военными действиями, и чтобы им противостоять, необходимо безопасное обслуживание критически важных объектов. Это подчеркивает актуальность разработки стратегии защиты сетей 5G.

Авторами статьи [8] предлагаются обобщенные методы защиты беспроводной сети.

Настоящее исследование предлагает развитие и специализацию предложенных методов именно для оценки рисков в логической архитектуре сетевых срезов 5G.

### *Анализ ключевых угроз безопасности в распределенных сетях 5G*

Для системного выявления и оценки угроз безопасности в распределенных сетях 5G был применен комплексный подход, включающий два взаимодополняющих метода.

*Моделирование угроз с использованием методики STRIDE.* Данный метод позволяет классифицировать угрозы по шести ключевым типам: 1) Spoofing (подмена), 2) Tampering (несанкционированное изменение), 3) Repudiation (отказ от операций), 4) Information Disclosure (раскрытие информации), 5) Denial of Service (отказ в обслуживании), 6) Elevation of Privilege (повышение привилегий). Это позволит обеспечить структурный подход к анализу свойств безопасности каждого компонента архитектуры.

*Сопоставление с тактиками и техниками матрицы MITRE ATT&CK for ICS.* Данная база знаний используется для анализа поведения злоумышленников на протяжении всего жизненного цикла атаки именно против систем промышленной автоматики и критической инфраструктуры. Это позволяет перейти от абстрактных уязвимостей к конкретным сценариям атак, используемым современными APT-группами.

На основе применения указанных методик был проведен детальный анализ. Его результаты систематизированы в Таблице, где для каждого ключевого компонента 5G выделены соответствующие угрозы по методологии STRIDE, потенциальные сценарии атак на КИ в разрезе матрицы MITRE ATT&CK for ICS, а также качественная оценка уровня риска (высокий, средний, низкий).

*Таблица*

**Результаты анализа угроз безопасности для компонентов 5G в контексте критической инфраструктуры**

| Архитектурный компонент 5G | Угрозы (по методологии STRIDE) | Сценарий атаки на КИ / Тактика MITRE ATT&CK for ICS | Уровень риска |
|---|---|---|---|
| Программно-определяемые сети (SDN) и виртуализация сетевых функций (NFV) | S: Подмена контроллера SDN.<br>T: Изменение потоковых правил (Flow Rules).<br>I: Раскрытие топологии сети.<br>D: Отказ в обслуживании контроллера или гипервизора.<br>E: Получение привилегий администратора NFV-оркестратора | Сценарий: нарушение работы системы управления энергорайоном путем изменения сетевых маршрутов для данных АСУ ТП.<br>Тактика: MITRE T0830 - Network Denial of Service, T0807 - Manipulation of Control | Высокий |
| Периферийные вычисления (MEC) | S: Подмена легитимного edge-приложения.<br>T: Изменение логики или данных в edge-приложении.<br>I: Утечка данных с локального MEC-узла (например, видеопоток с камер).<br>D: DDoS-атака на MEC-сервис.<br>E: Выход из контейнера/виртуальной машины на уровень гипервизора | Сценарий: компрометация MEC-узла, обрабатывающего данные с датчиков трубопровода, с последующей модификацией параметров для скрытия аварии или ее провокации.<br>Тактика: MITRE T0896 - Modify Parameter, T0801 - Manipulation of Vie | Высокий |
| Сетевые срезы (Network Slicing) | S: Неавторизованный доступ к срезу.<br>T: Изменение политик изоляции среза.<br>I: Межсрезовый перехват трафика.<br>D: Исчерпание ресурсов, выделенных критическому срезу.<br>E: Привилегированный доступ к управлению жизненным циклом срезов | Сценарий: «побег» из среза общедоступного IoT (умные светофоры) в изолированный срез АСУ ТП энергосети за счет уязвимости в системе управления срезами.<br>Тактика: MITRE T0819 - Lateral Movement, T0873 - Exploit Public-Facing Application | Высокий |
| Радиоинтерфейс (Uu) | S: Атака «злоумышленник в середине» (MitM) между UE и базовой станцией (gNB).<br>I: Перехват пользовательского трафика.<br>D: Глушение радиосигнала (Jamming) | Сценарий: перехват данных телеметрии с беспилотного патруля в умном городе или создание помех для каналов связи аварийных служб.<br>Тактика: MITRE T0862 - Electronic Jamming, T0800 - Eavesdrop on Insecure Network Communication | Средний |
| Массовый IoT (mIoT) | S: Подмена легитимного IoT-устройства.<br>T: Прошивка вредоносного ПО в устройство.<br>D: Создание ботнета из IoT-устройств для DDoS-атак | Сценарий: массовая компрометация датчиков умного города с целью организации мощной DDoS-атаки на MEC-узлы или центр управления, приводящей к отказу в обслуживании критически важных систем.<br>Тактика: MITRE T0843 - Device Hijacking, T0839 - Theft of Operational Information | Средний |

*Источник:* таблица составлена авторами.

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление». 2026. № 1

Проведенный анализ позволил выявить следующие ключевые закономерности.

1. Наибольшую опасность представляют угрозы целостности (Tampering) и отказа в обслуживании (Denial of Service), направленные на компоненты управления сетью (SDN/NFV) и периферийные вычисления (MEC). Именно эти угрозы напрямую ведут к нарушению функционирования КИ и потенциальным физическим последствиям.

2. Архитектурная сложность 5G создает новые векторы атак, такие как межсрезовое перемещение, которое может быть использовано для преодоления логической изоляции между критическими и некритическими сервисами.

3. Массовый характер IoT-устройств, обладающих низким уровнем интернет-безопасности, формирует масштабируемую платформу для проведения координированных атак на сетевую инфраструктуру.

4. Проведенное сопоставление с матрицей MITRE ATT&CK for ICS наглядно демонстрирует, что угрозы в сетях 5G не являются гипотетическими, а соответствуют реальным тактикам злоумышленников, атакующих объекты энергетики и промышленности.

Полученные результаты систематизируют и детализируют угрозы, формируя основу для разработки целевой комплексной стратегии безопасности, представленной ниже.

### *Стратегия и практические меры защиты*

На основе проведенного анализа угроз предлагается комплексная стратегия безопасности, построенная на трех фундаментальных принципах: глубокая эшелонированная защита (Defense-in-Depth), динамический контроль доступа (Zero Trust) и изоляция с сегментацией. Реализация стратегии осуществляется через систему взаимосвязанных практических мер.

Рассмотрим подробно каждую парадигму безопасности.

*Глубокая эшелонированная защита.* Создание многоуровневой системы безопасности, где каждый уровень обеспечивает независимую защиту. Даже при компрометации одного барьера последующие уровни продолжают обеспечивать безопасность системы.

*Динамический контроль доступа (Zero Trust).* Реализация подхода «никому не доверяй, проверяй всё». Каждый запрос на доступ к ресурсам должен аутентифицироваться, авторизовываться и непрерывно проверяться независимо от источника запроса [9].

*Изоляция и сегментация.* Логическое разделение сети на минимально необходимые сегменты с гибким управлением политиками доступа между ними, что позволяет изолировать инциденты и предотвращать латеральное перемещение.

Взаимосвязь указанных принципов образует киберфизическую систему безопасности, где организационные меры интегрируются с техническими решениями, создавая адаптивную защитную среду. Такой подход позволяет реализовать компенсационную модель безопасности, где нарушение одного защитного механизма компенсируется действием других элементов системы. Далее подробно рассмотрим реализацию предлагаемой стратегии.

1. Реализация начинается с выделения защищенного сегмента управления, что является логическим продолжением принципа сегментации. Внедрение строгой аутентификации и сквозного шифрования трафика между контроллером и сетевыми элементами непосредственно поддерживает парадигму Zero Trust. Регулярный аудит конфигураций и автоматизированная проверка соответствия политикам безопасности обеспечивают соблюдение принципа Defense-in-Depth через многоуровневый контроль.

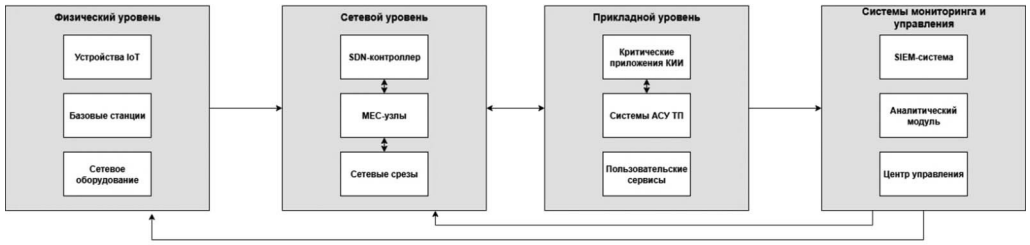


**Рисунок.** Архитектура интегрированной системы безопасности сетей 5G
*Источник:* рисунок выполнен авторами

2. Меры по упрощению операционных систем и гипервизоров на MEC-узлах логически вытекают из принципа Defense-in-Depth. Внедрение защищенных сред выполнения (TEE) для критических приложений является технологической реализацией изоляции. Установка межсетевых экранов нового поколения (NGFW) обеспечивает сегментацию на уровне периферийных узлов, создавая дополнительный эшелон обороны [10]. Научной основой данного подхода является теория графов безопасности, где каждый узел MEC представляет собой независимый домен безопасности с собственными политиками доступа.

3. Создание строго изолированных сетевых срезов для систем АСУ ТП является практической реализацией принципа сегментации. Настройка политик безопасности «запрещено по умолчанию» между разными срезами непосредственно поддерживает концепцию Zero Trust. Динамическая микросетевая сегментация на основе SDN обеспечивает гибкость системы защиты, позволяя адаптироваться к изменяющимся условиям.

4. Централизованный реестр IoT-устройств с присвоением уровня доверия является фундаментом для реализации Zero Trust. Сегментация IoT-устройств в отдельные VLAN-срезы по критичности продолжает принцип изоляции на уровне конечных устройств. Системы анализа сетевого трафика (NTA) обеспечивают мониторинг соблюдения политик безопасности на всех уровнях защиты.

Реализация многофакторной аутентификации образует базовый уровень системы Zero Trust. Атрибутное управление доступом (ABAC) на основе динамического контекста создает адаптивную систему авторизации. Непрерывная верификация активных сессий обеспечивает постоянство контроля, а принцип минимальных привилегий завершает построение системы динамического управления доступом.

Математической основой модели является теория конечных автоматов, где каждое состояние системы безопасности определяется совокупностью атрибутов доступа и контекстных параметров.

Разрабатываемая стратегия предполагает тесную интеграцию организационных и технических мер. Регламенты реагирования на инциденты формализуют процедуры управления безопасностью. Регулярные тренировки обеспечивают поддержание компетенций персонала. Система управления уязвимостями создает процессный фундамент для технических мер защиты. Обеспечение безопасности цепочки поставок расширяет периметр ответственности за пределы организации.

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление». 2026. № 1

Теоретической основой организационно-технической интеграции является системный подход, где технические решения и организационные процедуры рассматриваются как взаимосвязанные элементы единой системы безопасности.

Предложенная интегрированная стратегия обеспечивает комплексную защиту за счет синергетического эффекта от взаимодействия технологических решений и организационных мер, создавая адаптивную систему безопасности, способную противостоять современным киберугрозам для критической инфраструктуры.

### *Заключение*

Проведенное исследование подтвердило высокую актуальность разработки комплексных мер обеспечения кибербезопасности для распределенных сетей 5G, используемых в критической инфраструктуре. Анализ архитектурных особенностей сетей пятого поколения выявил наличие специфических векторов атак, требующих новых подходов к организации защиты.

Можно отметить следующие основные результаты работы.

1. Систематизация угроз безопасности, позволившая выделить критические зоны риска в архитектуре 5G, включая компоненты SDN/NFV, MEC-узлы и систему сетевых срезов. Установлено, что традиционные периметровые средства защиты неэффективны против современных угроз, направленных на распределенную инфраструктуру критически важных объектов.

2. Разработка интегрированной стратегии безопасности, основанной на принципах глубинной эшелонированной защиты, динамического контроля доступа (Zero Trust) и изоляции сетевых компонентов. Предложенная модель демонстрирует эффективность комбинированного применения организационных и технических мер защиты.

3. Создание архитектурной схемы, обеспечивающей визуализацию взаимодействия компонентов системы безопасности и позволяющей оптимизировать процессы управления защитой распределенной сетевой инфраструктуры.

Практическая значимость исследования заключается в том, что предложенные решения могут быть адаптированы для различных объектов критической инфраструктуры – от систем умного города до объектов топливно-энергетического комплекса.

Внедрение разработанной стратегии позволит существенно повысить устойчивость критически важных систем к кибератакам:

- за счет реализации централизованного управления политиками безопасности;
- обеспечения динамической изоляции сетевых срезов;
- внедрения системы непрерывного мониторинга и оперативного реагирования;
- снижения времени обнаружения и нейтрализации кибератак.

Перспективными направлениями дальнейших исследований являются: разработка адаптивных алгоритмов управления безопасностью на основе технологий ИИ, создание стандартизированных протоколов обмена информацией об угрозах между компонентами системы, а также развитие методов прогнозной аналитики для предиктивного предотвращения кибератак.

Внедрение предложенных решений будет способствовать обеспечению технологического суверенитета Российской Федерации в области защиты критической информационной инфраструктуры и созданию устойчивого фундамента для цифровой трансформации ключевых отраслей экономики.

**Литература**

1. *Пилипенко А.С., Маслова М.А.* Кибербезопасность в эпоху 5G – новые вызовы и стратегии защиты // Современные проблемы радиоэлектроники и телекоммуникаций. 2024. № 7. С. 212. EDN KEDVXT.
2. *Карпика А.Г.* Анализ рисков кибербезопасности в отношении объектов критической инфраструктуры // Юристъ-Правоведъ. 2022. № 3(102). С. 145–148. EDN RHOMZM.
3. *Акбарова А.Н., Ахунжанов И.Б.* Обзор новых угроз кибербезопасности и ее влияние на сеть пятого поколения (5G) // Известия Кыргызского государственного технического университета им. И. Раззакова. 2021. № 4(60). С. 96–101. EDN ZPAUNZ.
4. *Антонова В.М., Кондрашова Д.А., Сухорукова Н.А.* Угрозы безопасности сетей 5G // Colloquium-Journal. 2021. № 1-1(88). С. 57–60. DOI: 10.24412/2520-2480-2021-188-57-60. EDN BGEEJK.
5. *Ходжамаммедов М.М., Мухаммедов М.М., Рахымов К.Д., Рустамов Р.Р.* Безопасность интернета вещей (IOT) – защита умных устройств и сенсорных сетей от взлома // Символ науки: международный научный журнал. 2024. № 12-1-2. С. 157–158. EDN GQJIPA.
6. *Акишин А.В., Алашеев В.В., Стародубцев П.Ю.* Экспериментальная методика и результаты оценки уровня помех в ультракоротковолновом диапазоне // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) : Сборник научных статей : В 4 т. Санкт-Петербург, 28 февраля – 01 марта 2018 г. / Под ред. С.В. Бачевского. Т. 3. Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. С. 4–9. EDN VRUAGL.
7. *Алашеев В.В., Акишин А.В., Чеснаков М.Н.* Взгляды США на разработку доктрины информационного воздействия в киберпространстве // Проблемы технического обеспечения войск в современных условиях : Труды III Межвузовской научно-практической конференции, Санкт-Петербург, 16 февраля 2018 г. Т. 1. Санкт-Петербург : Военная академия связи имени Маршала Советского Союза С.М. Буденного, 2018. С. 67–71. EDN XMGZPF.
8. *Канатьев К.Н., Большаков В.Н., Куприков О.Д., Горошков Д.Б., Баулин Е.И.* Анализ угроз безопасности беспроводной сети и разработка оптимальных методов их предупреждения // Инновации и инвестиции. 2022. № 3. С. 116–123. EDN ZRTVQW.
9. *Сааков В.В., Кошиев К.Х., Боготов И.М., Агаджанян Э.Ю.* Концепция Zero Trust, или Что такое принцип нулевого доверия // Наука и образование: сохраняя прошлое, создаём будущее : Сборник статей XXXIX Международной научно-практической конференции, Пенза, 23 июня 2022 г. Пенза : Наука и Просвещение, 2022. С. 52–54. EDN JBSCIC.
10. *Тундайкин О.* Defense in Depth: военные принципы корпоративной безопасности // Системный администратор. 2018. № 12(193). С. 36–40. EDN YQJQXR.

**References**

1. Pilipenko A.S., Maslova M.A. (2024) Cybersecurity in the 5G Era – New Challenges and Protection Strategies. *Modern Issues in Radioelectronics and Telecommunications*. No. 7. P. 212. (In Russian).
2. Karpika A.G. (2022) Analysis of cybersecurity risks in relation to critical infrastructure facilities. *Jurist-Pravoved* [Lawyer-jurist]. No. 3(102). Pp. 145–148. (In Russian).
3. Akbarova A.N., Akhunzhanov I.B. (2021) Review of New Cybersecurity Threats and Their Impact on the Fifth Generation (5G) Network. *Izvestiya KSTU named after I. Razzakov*. No. 4(60). Pp. 96–101. (In Russian).
4. Antonova V.M., Kondrashova D.A., Sukhorukova N.A. (2021) Threats to 5g network security. *Colloquium-journal*. No. 1(88). Pp. 57–60. DOI: 10.24412/2520-2480-2021-188-57-60 (In Russian).

Вестник Российского нового университета
Серия «Сложные системы: модели, анализ и управление». 2026. № 1

5. Khodzamammedov M.M., Mukhammedov M.M., Rakhymov K.D., Rustamov R.R. (2024) Security of the internet of things (IOT) protecting smart devices and sensor networks from hacking. *Symbol of Science: International Scientific Journal*. No. 12-1-2. Pp. 157–158. (In Russian).
6. Akishin A.V., Alasheev V.V., Starodubtsev P.Yu. (2018) Experimental methodology and results of assessing the level of interference in the ultra-short-wave range. In: Bachevsky S.V. (Ed) *Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii (APINO 2018)* [Actual Problems of Infotelecommunications in Science and Education (APINO 2018)] : Collection of scientific articles : In 4 vols. St. Petersburg, February 28 – March 1, 2018. St. Petersburg : Bonch-Bruevich St. Petersburg State University of Telecommunications. Pp. 4–9. (In Russian).
7. Alasheev V.V., Akishin A.V., Chesnakov M.N. (2018) US views on the development of an information influence doctrine in cyberspace. In: Fedorova S.V. (Ed) *Problemy tekhnicheskogo obespecheniya voisk v sovremennykh usloviyakh* [Problems of Technical Support of Troops in Modern Conditions] : Proceedings of the III Interuniversity Scientific and Practical Conference. St. Petersburg, February 16, 2018. Vol. 1. St. Petersburg : Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny. Pp. 67–71. (In Russian).
8. Kanatyev K.N., Bolshakov V.N., Kuprikov O.D., Goroshkov D.B., Baulin E.I. (2022) Analysis of wireless network security threats and development of the best methods of their prevention. *Innovation and Investment*. No. 3. Pp. 116–123. (In Russian).
9. Saakov V.V., Koshiev K.Kh., Bogotov I.M., Agadzhanyan E.Yu. (2022) The Zero Trust Concept or What is the Zero Trust Principle. In: *Nauka i obrazovanie: sokhranyaya proshloe, sozdaem budushchee* [Science and education: Preserving the past, creating the future] : Proceedings of the XXXIX International Scientific and Practical Conference, Penza, June 23, 2022. Penza : Science and Education. Pp. 52–54. (In Russian).
10. Tundaykin O. (2018) Defense in Depth: Military Principles of Corporate Security. *System Administrator*. No. 12(193). Pp. 36–40. (In Russian).

Поступила в редакцию: 26.12.2025
Поступила после рецензирования: 24.01.2026
Принята к публикации: 12.02.2026

Received: 26.12.2025
Revised: 24.01.2026
Accepted: 12.02.2026