www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2025.3.2

УДК 004.056.5(470+571)
ББК 32.972.53(2Рос)

# ОБЗОР УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭКОСИСТЕМЕ УМНОГО ГОРОДА И ИХ МИНИМАЛИЗАЦИИ

**Олеся Александровна Какорина**

Кандидат физико-математических наук,
заведующий кафедрой информационной безопасности,
Волгоградский государственный университет
kakorina@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

**Александра Николаевна Панченко**

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
IBm-241_744165@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

**Надежда Ильинична Хлыбова**

Студент, кафедра педагогики, психологии и социальной работы,
Волгоградский государственный университет
povb-251_342398@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

**Аннотация.** Умные города представляют собой сложную экосистему, где цифровые технологии глубоко интегрированы в городскую инфраструктуру для повышения эффективности управления и улучшения качества жизни граждан. Однако такая цифровизация приводит к возникновению новых киберугроз и уязвимостей, способных нарушить работу критически важных городских служб и поставить под угрозу безопасность жителей. В данной научно-обзорной статье проведен анализ технических угроз информационной безопасности, присущих инфраструктуре умного города, с акцентом на реалии Российской Федерации. Приводятся современные примеры киберинцидентов в России, затрагивающих элементы экосистемы умного города, и оцениваются их последствия. Особое внимание уделено методам минимизации рисков и защиты: рассматриваются технические подходы и нормативные меры, принимаемые в РФ (законодательные акты, стандарты и инициативы регуляторов). Сделан вывод о необходимости комплексного подхода, сочетающего передовые технологии кибербезопасности и строгое выполнение требований отечественного законодательства, для обеспечения устойчивой и безопасной цифровой городской среды.

**Ключевые слова:** умный город, информационная безопасность, киберугрозы, критическая информационная инфраструктура, интернет вещей, кибербезопасность, минимизация рисков, нормативное регулирование.

© Какорина О.А., Панченко А.Н., Хлыбова Н.И., 2025

## Введение

Концепция «умного города» предполагает эффективную интеграцию физических, цифровых и человеческих систем городской среды для обеспечения устойчивого и благополучного будущего граждан [3]. В России проект «Умный город», курируемый Министерством строительства и ЖКХ (Минстрой), направлен на цифровую модернизацию городского хозяйства, повышение конкурентоспособности городов и создание безопасных и комфортных условий для жизни горожан [2]. Реализация подобных проектов сопровождается масштабным внедрением интернета вещей (IoT), облачных сервисов, больших данных и других передовых технологий во все сферы городской инфраструктуры – от энергетики и транспорта до систем безопасности и коммунальных услуг.

При этом обеспечение информационной безопасности становится критически важной задачей для устойчивого функционирования умного города. Как отмечают эксперты, проблемы кибербезопасности городских систем нередко остаются на втором плане, уступая приоритет развитию сервисов [3]. Если не заложить механизмы защиты заблаговременно, городская инфраструктура может оказаться уязвимой для кибератак, что чревато серьезными последствиями – от сбоя работы служб до прямой угрозы жизни и здоровью людей. В последние годы значимость этой проблемы возросла многократно, особенно в контексте России, активно реализующей программы цифровой трансформации и сталкивающейся с новым витком киберактивности. В данной работе мы рассмотрим основные технические угрозы информационной безопасности в экосистеме умного города, проанализируем реальные инциденты, произошедшие в России, и обсудим методы снижения рисков – как технологические, так и нормативно-правовые, применяемые в российской практике.

## Технические угрозы информационной безопасности в инфраструктуре умного города (в контексте России)

Инфраструктура умного города включает широкий спектр систем: датчики и устройства IoT (интернет вещей) для мониторинга транспорта, окружающей среды, ЖКХ; городские информационные системы и базы данных (например, порталы госуслуг, системы учета); промышленные системы управления (АСУ ТП) городских объектов – энергооборудования, сетей водо- и теплоснабжения; системы общественной безопасности (камеры видеонаблюдения, системы оповещения и управления дорожным движением) и др. Каждая из этих подсистем подвержена специфическим техническим угрозам, а их высокая взаимосвязанность увеличивает потенциальный масштаб ущерба.

Многие IoT-устройства, на которых строятся решения умного города, имеют ограниченные вычислительные ресурсы и упрощенные механизмы безопасности [3]. Компрометация таких устройств позволяет проводить несанкционированное наблюдение, нарушает приватность граждан и открывает путь для дальнейших атак.

Критически важные сервисы города – энергоснабжение, водоканалы, системы отопления, транспортные узлы – управляются программно-аппаратными комплексами, зачастую относящимися к критической информационной инфраструктуре (КИИ) [3]. Злоумышленники, получив доступ к АСУ ТП городского объекта, способны манипулировать технологическими процессами – например, отключить электроподстанцию, загрязнить систему водоснабжения, дезактивировать насосное оборудование и т. п.

Киберпреступники могут нацеливаться на цифровые платформы с целью кражи конфиденциальной информации, нарушения работы электронных сервисов или подрыва доверия к ним [3; 7]. В случае успеха вредоносное ПО способно парализовать системы администрации, центры управления трафиком, биллинговые сервисы ЖКХ.

Городские сети передачи данных служат связующей основой для всех компонентов умного города. Их компрометация грозит перехватом управления устройствами и сервисами [8].

Целенаправленные сложные атаки (APT) со стороны квалифицированных групп и фишинг остаются самыми распространенными векторами проникновения – до 70 % всех

атак начиналось с фишинговых рассылок или компрометации учетных записей [5].

### Современные примеры угроз и инцидентов (российские кейсы)

В июле 2020 г. получила огласку продажа несанкционированного доступа к сети камер видеонаблюдения Москвы [6]. Продавец утверждал, что некоторые камеры доступны не только для просмотра, но и для поворота и масштабирования. Департамент ИТ подтвердил факт инцидента, назвав предоставление доступа противоправным действием.

В октябре 2023 г. «Росводоканал» подвергся масштабной кибератаке, которая привела к сбоям в веб-сайтах, системах оплаты, мобильных приложениях и телефонии [1]. Аналитики связывают атаку с действиями хактивистов, а также указывают на устаревшую и уязвимую инфраструктуру предприятия.

На учениях The Standoff 2020 были смоделированы атаки на цифровую инфраструктуру города, включая транспорт, энергетику и телекоммуникации [5]. Хакерам удалось реализовать почти половину предусмотренных сценариев, включая подмену контента на экранах, остановку добычи нефти и деструкцию оборудования.

### Методы минимизации рисков и защиты (технические и нормативные подходы в РФ)

Обеспечение кибербезопасности умного города требует комплексного подхода. Необходимо изначально планировать сегментацию сети, внедрять шифрование, средства мониторинга и реагирования, применять доверенные платформы [3; 4].

В РФ действует закон №187-ФЗ «О безопасности КИИ», обязательное категорирование, и рекомендации от ФСТЭК по защите АСУ ТП [8]. Кроме того, указ Президента РФ № 250 от 01.05.2022 г. требует перехода всех субъектов КИИ на отечественные решения в ИБ до 2025 г. [8].

Создаются SOC и региональные центры мониторинга, проводится обучение персонала, включаются механизмы ГосСОПКА [2]. Особое внимание уделяется киберустойчивости – способности систем быстро восстанавливаться после атак [4].

### Заключение

Цифровая трансформация городского хозяйства неизбежно сопровождается появлением новых вызовов в сфере информационной безопасности. Проведенный обзор показывает, что умный город становится привлекательной целью для различного рода злоумышленников – от любителей, ищущих уязвимые камеры наблюдения, до организованных хакерских группировок и государственных структур, способных парализовать ключевые сервисы. Технические угрозы охватывают весь спектр городской экосистемы: IoT-устройства, промышленные системы, коммуникационные сети, базы данных. Реальные инциденты в России, такие как утечки доступа к городским камерам или атаки на компании коммунального сектора, подтверждают высокую степень риска. В то же время они дают ценный опыт и стимулируют развитие защитных мер.

Для построения безопасной цифровой городской среды необходим проактивный и системный подход. Со технической стороны – это внедрение надежных средств защиты (шифрование, аутентификация, мониторинг), архитектурное выделение критических компонентов, регулярные аудиты и учения, развитие компетенций специалистов. С нормативной стороны – актуальная законодательная база и стандарты, которые учитывают особенности умных городов, а также строгий надзор за их исполнением. Российская практика движется именно в этом направлении: усиливается регулирование безопасности критической инфраструктуры, вводятся требования по импортозамещению и централизации защиты, распространяются лучшие практики кибербезопасности на уровень городов и регионов.

Важно подчеркнуть, что информационная безопасность умного города – не разовая задача, а непрерывный процесс. По мере развития технологий (5G, искусственный интеллект, автономный транспорт и др.) будут появляться и новые типы угроз, способные обходить прежние меры защиты. Поэтому муниципальным властям и ответственным службам следует планировать безопасность

«на вырост», закладывать механизмы быстрого обновления и адаптации систем безопасности. Не менее значима и просветительская работа с жителями умных городов: информирование граждан о правилах цифровой гигиены, о безопасном использовании городских электронных сервисов также снижает вероятность успеха атак (например, фишинга).

В заключение, устойчивость умного города к киберугрозам становится одним из ключевых факторов его успешного развития. Без надежной защиты любых преимуществ «умности» может оказаться недостаточно: единая уязвимость способна свести на нет эффекты многолетней цифровизации. Поэтому инвестировать необходимо не только в новые технологии для городов, но и в их защищенность. Совместными усилиями государства, бизнеса и научного сообщества возможно создать в России такие умные города, которые будут не только эффективными и комфортными, но и безопасными в информационном отношении – что, в конечном счете, служит интересам каждого гражданина.

### *СПИСОК ЛИТЕРАТУРЫ*

1. «Росводоканал» вновь оказался под атакой хакеров // CISOCLUB. – 2023. – 21 окт. – Электрон. текстовые дан. – Режим доступа: https://cisoclub.ru/rosvodokanal-vnov-okazalsja-pod-atakoj-hakerov/

2. «Умный» город и безопасность – аналитический обзор // FSA3D (ФСА). – 2020. – 19 марта. – Электрон. текстовые дан. – Режим доступа: https://fsa3d.com/2020/03/19/smart-city-and-safety-19/

3. Иванов, О. Умные города – новые угрозы и возможности / О. Иванов // Anti-Malware.ru. – 2018. – 21 июня. – Электрон. текстовые дан. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/smart-cities-threats-opportunities

4. Киберустойчивость вместо «бетонной» защиты // IT-World.ru. – 2025. – Электрон. текстовые дан. – Режим доступа: https://www.it-world.ru/security/frm037qukxs0wk 40k0owsws80ggsg8g.html

5. Макарова, Ю. Атака на «умный» город: как прошли киберучения по защите инфраструктуры / Ю. Макарова // РБК Тренды. – 2020. – 10 дек. – Электрон. текстовые дан. – Режим доступа: https://trends.rbc.ru/trends/industry/cmrm/5fd1dc729a7947 a505d40c26

6. Морозова, О. В даркнете продают доступ ко всем камерам наблюдения в Москве. Власти города напомнили, что это противоправное действие / О. В. Морозова // Сноб. – 2020. – 8 июля. – Электрон. текстовые дан. – Режим доступа: https://snob.ru/science/v-darknete-prodayut-dostup-ko-vsem-kameram-nablyudeniya-v-moskve-vlasti-goroda-napomnili-chto-eto-protivopravnoe-dejstvie/

7. О'Двойт, С. Моделирование угроз в условиях методической неопределенности / С. О'Двойт, А. Шлейфер // Kaspersky ICS CERT (блог). – 2018. – 11 дек. – Электрон. текстовые дан. – Режим доступа: https://ics-cert.kaspersky.ru/publications/reports/2018/12/11/modelirovanie-ugroz-v-usloviyakh-metodichskoy-neopredelennosti/

8. С 1 января 2025 года объекты критической инфраструктуры должны перейти на отечественные решения для обеспечения информационной безопасности // Инфо-аналитический журнал «RUБЕЖ». – 2022. – 4 мая. – Электрон. текстовые дан. – Режим доступа: https://ru-bezh.ru/zakonodatelstvo-i-normativyi/news/22/05/04/s-1-yanvarya-2025-goda-obektyi-kriticheskoj-infrastruk turyi-dolz

### *REFERENCES*

1. «Rosvodokanal» vnov okazalsya pod atakoy khakerov ["Rosvodokanal" Was Attacked by Hackers Again]. *CISOCLUB*, 2023, Oct. 21. URL: https://cisoclub.ru/rosvodokanal-vnov-okazalsja-pod-atakoj-hakerov/

2. «Umnyy» gorod i bezopasnost – analiticheskiy obzor ["Smart" City and Security – an Analytical Review]. *FSA3D (FSA)*, 2020, Mar. 19. URL: https://fsa3d.com/2020/03/19/smart-city-and-safety-19/

3. Ivanov O. Umnye goroda – novye ugrozy i vozmozhnosti [Smart Cities – New Threats and Opportunities]. *Anti-Malware.ru*, 2018, June 21. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/smart-cities-threats-opportunities

4. Kiberustoychivost vmesto «betonnoy» zashchity [Cyber Resilience Instead of "Concrete" Protection]. *IT-World.ru*, 2025. URL: https://www.it-world.ru/security/frm037qukxs0wk40k0owsws80ggsg8g.html

5. Makarova Yu. Ataka na «umnyy» gorod: kak proshli kiberucheniya po zashchite infrastruktury [Attack on a "Smart" City: How Cyber Exercises on Infrastructure Protection Were Conducted]. *RBK Trendy* [RBC Trends], 2020, Dec. 10. URL: https://trends.rbc.ru/trends/industry/cmrm/5fd1dc729a7947a505d40c26

6. Morozova O. V darknete prodajut dostup ko vsem kameram nablyudeniya v Moskve. Vlasti goroda napomnili, chto eto protivopravnoe dejstvie [Darknet Sells Access to All Surveillance Cameras in Moscow. City Authorities Reminded That This is an Illegal Act].

*Snob*, 2020, July 8. URL: https://snob.ru/science/v-darknete-prodayut-dostup-ko-vsem-kameram-nablyudeniya-v-moskve-vlasti-goroda-napomnili-chto-eto-protivopravnoe-dejstvie/

7. O'Dvoit S., Shleyfer A. Modelirovanie ugroz v usloviyakh metodicheskoy neopredelennosti [Threat Modeling Under Methodological Uncertainty]. *Kaspersky ICS CERT (blog)*, 2018, Dec 11. URL: https://ics-cert.kaspersky.ru/publications/reports/2018/12/11/modelirovanie-ugroz-v-usloviyakh-metodichskoy-neopredelennosti/

8. S 1 yanvarya 2025 goda obyekty kriticheskoy infrastruktury dolzhny pereyti na otechestvennye resheniya dlya obespecheniya informatsionnoy bezopasnosti [From January 1, 2025, Critical Infrastructure Facilities Must Switch to Domestic Solutions for Ensuring Information Security]. *Info-analiticheskiy zhurnal «RUBEZh»* [Info-Analytical Journal "RUBEZh"], 2022, May 4. URL: https://rubezh.ru/zakonodatelstvo-i-normativyi/news/22/05/04/s-1-yanvarya-2025-goda-obektyi-kriticheskoj-infrastrukturyi-dolz

# OVERVIEW OF INFORMATION SECURITY THREATS IN THE SMART CITY ECOSYSTEM AND THEIR MINIMIZATION

**Olesya A. Kakorina**

Candidate of Sciences (Physics and Mathematics),
Head of the Department of Information Security,
Volgograd State University
kakorina@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

**Alexandra N. Panchenko**

Student, Department of Information Security,
Volgograd State University
IBm-241_744165@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

**Nadezhda I. Khlybova**

Student, Department of Pedagogy, Psychology and Social Work,
Volgograd State University
povb-251_342398@volsu.ru
Prosp. Universitetsky, 100, 400062, Volgograd, Russian Federation

**Abstract**. This scientific review analyzes information security threats within the smart city ecosystem, with a specific focus on the context of the Russian Federation. Smart cities, characterized by the deep integration of digital technologies like the Internet of Things (IoT), big data, and cloud services into urban infrastructure, significantly enhance management efficiency and citizen quality of life. However, this digital transformation introduces severe cybersecurity vulnerabilities that can disrupt critical services such as energy, water supply, and public safety systems and endanger residents. The article systematically examines the technical threats targeting key components, including vulnerable IoT devices, industrial control systems (ICS), communication networks, and city data platforms. It further provides contemporary Russian case studies, such as unauthorized access to Moscow surveillance cameras and cyberattacks on utility companies, to illustrate real-world risks and consequences. In response, the work explores a dual approach to risk minimization. It reviews essential technical measures like network segmentation, encryption, and continuous monitoring. Simultaneously, it outlines the evolving Russian regulatory framework, including laws on Critical

Information Infrastructure (CII) security and mandates for import substitution in cybersecurity solutions. The conclusion emphasizes that ensuring a resilient smart city requires a proactive, comprehensive strategy that integrates advanced technological protections with strict adherence to and development of national regulatory standards.

**Key words:** smart city, information security, cybersecurity vulnerabilities, critical information infrastructure, Internet of Things, cybersecurity, risk minimization, regulatory control.