DOI 10.37882/2223-2966.2025.02.33

ОБЗОР КИБЕРУГРОЗ ДЛЯ «УМНЫХ ДОМОВ» И «УМНЫХ ГОРОДОВ»: СИСТЕМНАЯ КЛАССИФИКАЦИЯ И АНАЛИЗ ТЕНДЕНЦИЙ

OVERVIEW OF CYBER THREATS TO SMART HOMES AND SMART CITIES: SYSTEMATIC CLASSIFICATION AND TREND ANALYSIS

S. Fedorov
D. Drilenko
A. Drilenko

Summary. In recent years, smart home and smart city solutions based on the Internet of Things, computer vision, and artificial intelligence have been rapidly evolving. The massive connectivity and lack of unified cybersecurity standards lead to an expanded attack surface and the emergence of new vulnerabilities. Cybercriminals exploit default configurations and insufficient network segmentation to compromise both individual devices and large-scale urban systems. Targeted attacks can disrupt transportation infrastructure, surveillance services, and resource management systems. The prevalence of DDoS attacks and IoT botnets creates conditions for service failures in critical sectors. Combined (hybrid) attacks, merging network intrusions, social engineering, and physical penetration, pose a particular danger. This article offers a systematic classification and trend analysis of current threats, as well as identifies gaps in existing cybersecurity measures. The findings outline directions for the development of system-analytical methods of cyber risk management.

Keywords: smart home, smart city, cybersecurity, IoT, vulnerabilities.

Федоров Сергей Юрьевич
старший преподаватель, Кубанский государственный технологический университет
Дриленко Даниил Владимирович
Кубанский государственный технологический университет
dv@russia.ms
Дриленко Александра Александровна
заместитель директора, Кубанский государственный технологический университет
a.drilenko@russia.ms

Аннотация. В последние годы стремительно развиваются системы «умных домов» и «умных городов», базирующиеся на технологиях интернет-вещей, машинном зрении и искусственном интеллекте. Массовая подключенность и отсутствие единых стандартов кибербезопасности приводят к расширению поверхности атаки и появлению новых уязвимостей. Киберпреступники активно используют слабые настройки по умолчанию и недостаток сетевой сегментации, чтобы компрометировать как отдельные устройства, так и крупные городские системы. Таргетированные атаки могут нарушать транспортную инфраструктуру, службы видеонаблюдения и системы управления ресурсами. Широкая распространенность DDoS-атак и IoT-ботнетов создает предпосылки для сбоев в обслуживании критических сервисов. Особую опасность представляют комбинированные (гибридные) векторы атак, совмещающие сетевые вторжения, социальную инженерию и физический доступ. Исследование предлагает системную классификацию и анализ тенденций, а также выявляет пробелы в существующих мерах киберзащиты. Полученные результаты позволяют определить направления развития системно-аналитических методов управления киберрисками.

Ключевые слова: умный дом, умный город, кибербезопасность, IoT, уязвимости.

Введение

Инфраструктуры «умных домов» и «умных городов» — это сложные, многокомпонентные системы, ориентированные на повышение качества жизни населения, оптимизацию потребления ресурсов и обеспечение устойчивого развития городских пространств. Благодаря интеграции датчиков различного типа, систем машинного зрения, искусственного интеллекта и автоматизированного управления, данные экосистемы могут адаптироваться к меняющимся условиям [1, с. 23], предоставлять пользователям новые сервисы, повышать эффективность городских служб и снижать операционные затраты.

Однако, растущая масштабируемость таких систем создает комплексные проблемы кибербезопасности. Интернет вещей (IoT), обеспечивающий взаимодействие между интеллектуальными устройствами, датчиками и системами управления, неизбежно расширяет поверхность атаки. Массовая подключенность, разнообразие технологий, протоколов и производителей, отсутствие единых стандартов и регламентов — все это открывает возможности для злоумышленников [2, с.3].

Цель данного исследования — систематизировать существующие киберугрозы для «умных домов» и «умных городов», проанализировать характерные атаки на IoT-устройства в городской среде, выделить основные векторы угроз [4, с.63], уязвимости и пробелы в контрме-

рах. Полученные результаты позволят не только понять текущее состояние проблемы, но и наметить направления для дальнейшей разработки системно-аналитических методов предотвращения, обнаружения и снижения киберрисков.

Методология исследования

Настоящее исследование основано на комплексном подходе, включающем:

1. Контент-анализ научных публикаций и отраслевых отчетов: были изучены работы, опубликованные в ведущих журналах по кибербезопасности, а также отчеты исследовательских лабораторий и компаний, специализирующихся на безопасности IoT [6, с. 36–38].
2. Исследование инцидентов из практики: рассмотрение ряда реальных случаев компрометации «умных» устройств, систем видеонаблюдения, городских систем управления дорожным движением и др.
3. Системно-аналитический подход к классификации: разработана структура классификации угроз [8, с.122], включающая типы атак, векторы проникновения, эксплуатируемые уязвимости, а также выделение отдельных тенденций и срезов по отраслям, типам устройств и уровням городской инфраструктуры.

Основываясь на данном подходе, исследование предлагает систематизированный обзор угроз и анализирует их эволюцию, связав результаты с существующими и перспективными методами защиты.

Особенности «умных домов» и «умных городов» как цели кибератак

«Умные дома» (Smart Homes) представляют собой технологически насыщенные жилые пространства, где устройства умного освещения, интеллектуальных систем отопления, голосовых помощников, камер видеонаблюдения и бытовой техники подключены к единой сети управления. «Умные города» (Smart Cities), в свою очередь, — это масштабная экосистема, включающая умные системы управления ресурсами (энергией, водой), уличное освещение, транспортную инфраструктуру, услуги городского видеонаблюдения, системы мониторинга качества воздуха, общественной безопасности и др. [6, с. 42]

Важная особенность этих систем — высокая степень интеграции между физической и цифровой средой. Взлом или саботаж отдельного IoT-устройства может привести к каскадным последствиям [5, с. 346], влияющим на целые сектора городской жизни. Кроме того, подчиненность систем центральным платформам управления влечет риски от компрометации единой точки контроля, что является крайне привлекательной целью для хакеров.

Классификация актуальных кибератак на IoT-устройства

Кибератаки на IoT-устройства в контексте «умных домов» и «умных городов» можно классифицировать по ряду критериев.

По целям атак:

— Атаки с целью нарушения работоспособности: DDoS (распределённые атаки отказа в обслуживании), физическое разрушение устройств через их перегрузку, вывод из строя сетевой инфраструктуры.
— Атаки на конфиденциальность: перехват и анализ данных с датчиков (температура, присутствие людей, видеоданные), кража личной информации (идентификационные данные жильцов, пароли доступа к системам).
— Атаки с целью экономической выгоды: вымогательство, блокировка систем «умного дома» или городских сервисов с требованием выкупа; использование скомпрометированных устройств для майнинга криптовалют, кража платежных данных.
— Атаки на целостность инфраструктуры: подмена показаний датчиков, изменение параметров «умных» светофоров или систем снабжения ресурсами, чтобы вызвать сбои или перенаправить потоки данных и ресурсов.

По используемым средствам и методам:

— Вредоносное ПО, ориентированное на IoT: специализированные вредоносные программы, трояны, черви, руткиты, эксплуатирующие слабые места прошивок и протоколов.
— Эксплуатация уязвимостей в протоколах связи: атаки типа «man-in-the-middle», подмена сертификатов, подделка пакетов данных.
— Физический доступ и атаки на периферийные узлы: подмена устройств, использование скрытых устройств-паразитов (например, поддельных датчиков), атаки на несегментированные сети.
— Социальная инженерия и фишинг: компрометация учетных данных пользователей или операторов систем, ввод в заблуждение обслуживающего персонала.

По уровню инфраструктуры:

— Домашний уровень: атаки на домашние хабы, голосовых помощников, камеры видеонаблюдения, системы безопасности дверей.
— Городской уровень: атаки на интеллектуальные системы управления транспортом, городской

инфраструктурой, системами электроснабжения, видеонаблюдения, системами управления уличным освещением.
— Интеграционные платформы: атаки на облачные сервисы, серверы обработки данных, центральные платформы аналитики и машинного зрения.

Таким образом, классификация атак формирует многоуровневую матрицу, отражающую сложность и разнообразие угроз для «умных» экосистем.

Анализ современных векторов угроз и уязвимостей

Современные тенденции развития киберугроз для «умных домов» и «умных городов» можно охарактеризовать следующими направлениями (Таблица 1).

С увеличением числа IoT-устройств возрастает вероятность наличия плохо защищенных узлов. Некоторые производители экономят на встроенных средствах безопасности, используя слабые или устаревшие протоколы шифрования, тривиальные пароли по умолчанию. Это облегчает компрометацию устройств на уровне прошивки [4, с. 91–93], подмену данных о среде, внедрение бэкдоров.

Системы машинного зрения, применяемые для распознавания лиц, номеров автомобилей, анализа потоков людей, становятся объектом таргетированных атак. Злоумышленники могут подменять видеопоток, искажать или подделывать данные для обхода систем аутентификации или дезинформации оператора.

Широкое применение Wi-Fi, ZigBee, Bluetooth LE, LoRaWAN создает новые возможности для атак. Недостатки в протоколах шифрования, наличие небезопасных каналов передачи данных позволяет злоумышленникам перехватывать трафик, изменять команды управления.

Распространение IoT-ботнетов, таких как Mirai, стало одной из ключевых тенденций последних лет. Компрометированные устройства формируют распределенную сеть для осуществления массовых DDoS-атак, внедрения вредоносного кода и предоставления услуг киберпреступникам.

Наблюдается все более частое комбинирование традиционных сетевых атак [7, с. 43] с физическим проникновением, социальной инженерией и целенаправленными манипуляциями с данными. Такие гибридные атаки требуют комплексного подхода к защите.

Выявление пробелов в существующих контрмерах

1. Отсутствие единых глобальных стандартов кибербезопасности для IoT-устройств и распылённая ответственность производителей

Ключевой проблемой является отсутствие четко регламентированных требований к уровню кибербезопасности IoT-продукции. В отличие от традиционных сфер (например, производства медицинского оборудования или автомобилей), где существуют строгие сертификаты и стандарты качества, в области умных домов и городов подобный комплексный, юридически закреплённый и общепризнанный норматив отсутствует. Производи-

Таблица 1.

Классификация атак

Тип атаки	Сложность реализации	Необходимый уровень компетенций	Потенциальный ущерб	Примерные сценарии
DDoS (отказ в обслуживании)	Средняя	Средний	Высокий (массовые сбои)	Масштабное отключение городских сервисов, перегрузка «умных» светофоров и датчиков освещения
Атаки на конфиденциальность (перехват данных)	Низкая–Средняя	Средний	Средний (утечка данных пользователей)	Кража видеопотока с камер в доме, сбор личных данных о жителях через датчики присутствия
Подмена данных датчиков/систем машинного зрения	Высокая	Высокий	Высокий (искажение управленческих решений)	Манипуляции с показаниями «умных» светофоров, подделка видеопотоков систем безопасности
Заражение устройств ботнетом IoT	Низкая–Средняя	Низкий–Средний	Высокий (массовое использование для атак)	Формирование ботнетов для дальнейших DDoS-атак, несанкционированный майнинг криптовалют
Комбинированные (гибридные) атаки	Высокая	Высокий (комплексные навыки)	Чрезвычайно высокий (многоуровневые сбои)	Совмещение сетевых атак с физическим проникновением и социальной инженерией, вывод из строя критически важных городских систем

тели часто стремятся к быстрому выходу на рынок, сосредотачиваясь на функциональности, удобстве и стоимости продукта [8, с. 19], а вопросы безопасности могут восприниматься ими как второстепенные. В результате:

— Одни и те же уязвимости могут многократно повторяться в продуктах разных брендов.
— Отсутствие чёткого правового поля приводит к дефициту ответственности: компании не обязаны оперативно исправлять обнаруженные уязвимости, а потребители зачастую не имеют механизмов принуждения к обновлению [9, с. 114].
— Нет единых руководств по базовой защищённости (например, обязательных требований к шифрованию, механизмам аутентификации и обновлениям).

Решение могло бы заключаться в разработке и принятии международных стандартов, поддержанных на уровне государств и отраслевых ассоциаций, с чёткими минимальными требованиями к шифрованию, контролю целостности прошивок, политике обновления и аудитам сторонними экспертными организациями. Это создаст равные условия для производителей, стимулируя их поднимать качество защиты устройств.

2. Недостаток сетевой сегментации и отсутствие «принципа нулевого доверия» (Zero Trust)

В современных «умных» экосистемах (домашних или городских) множество устройств часто подключаются к одной логической сети, не имея строгого разделения на сегменты по уровню важности, типам данных и функциям. В такой среде, если злоумышленник компрометирует одно устройство, то он может потенциально получить доступ к другим, возможно, более критическим узлам. Это похоже на незащищённый дом: проникнув в любую дверь, злоумышленник может перемещаться по всей внутренней структуре.

Отсутствие сегментации означает также, что системы жизнеобеспечения, камеры наблюдения, интеллектуальные счетчики ресурсов и развлекательные устройства могут находиться в одном пространстве адресов [11, с. 54]. Это упрощает проведение атак, эскалацию прав и доступ к управлению критическими сервисами.

Более глубокий подход к решению заключается в применении «принципа нулевого доверия», где ни одному устройству по умолчанию не доверяется, и каждое взаимодействие требует аутентификации и авторизации. Также необходима микросегментация сетей на уровне виртуальных подсетей, VLAN, VPN или использования software-defined networking (SDN) для управления доступом по принципу «минимальных привилегий». Это снизит риск распространения атаки и повысит устойчивость инфраструктуры.

3. Отсутствие безопасных и автоматизированных механизмов обновления и патчинга прошивок IoT-устройств

Многие IoT-устройства разрабатываются с упором на минимизацию себестоимости и сокращение сроков вывода на рынок. Это нередко приводит к упрощённым [12, с. 84] или вовсе отсутствующим механизмам обновления прошивок. Как следствие:

— Устройства с устаревшими версиями ПО остаются уязвимыми к уже известным атакам и эксплойтам.
— Владельцы, не имеющие технических навыков или контроля над устройствами, не могут самостоятельно и оперативно обновить ПО.
— Злоумышленники годами могут эксплуатировать известные уязвимости из-за отсутствия эффективных механизмов доставки патчей.

Глубина проблемы проявляется ещё и в том, что во многих случаях устройства используются в критических городских сервисах, где недоступность или сбой обновления может нарушить работу инфраструктуры. Решение предполагает разработку безопасной и стандартизированной системы обновлений [13, с. 56], включающей подписанную производителем прошивку, проверку целостности, автоматические уведомления о доступности патчей и внедрение процедур «мягкого» обновления (rolling updates), чтобы минимизировать риск одновременного выхода из строя всех устройств при неудачном обновлении.

4. Фрагментарное внедрение системно-аналитических методов, машинного обучения и машинного зрения

На сегодняшний день существуют отдельные решения для обнаружения аномалий в сетевом трафике и поведения устройств, но их применение носит точечный характер и не представляет собой стройной системы [14, с. 67]. Проблемы в том, что:

— Разработчики и операторы часто используют несогласованные методики, алгоритмы и инструменты.
— Нет единых протоколов для обмена данными между различными аналитическими подсистемами, что затрудняет создание комплексных моделей угроз.
— Системы машинного обучения могут страдать от недостатка разнообразных и репрезентативных данных, а также от отсутствия механизмов контекстного анализа [15, с. 24], позволяющего отличать допустимые отклонения (например, связанные с сезонными изменениями в потреблении ресурсов) от реальных признаков атаки.

Глубинное решение предполагает интеграцию аналитических платформ с системами машинного зрения,

IoT-датчиками и данными от внешних источников (например, информацию о глобальных угрозах от CERT-центров). Применение контекстно-зависимого анализа позволит точнее идентифицировать угрозы. Необходима стандартизация интерфейсов и протоколов, использование унифицированных форматов данных, чтобы различные модули аналитики могли «общаться» на одном языке.

5. Ориентация существующих решений на точечную защиту отдельных компонентов, а не на системное управление киберрисками

Текущие практики [1, с. 37] часто представляют собой набор разрозненных инструментов (фаерволы, системы обнаружения вторжений, шифрование каналов связи), не связанных в единую стратегию защиты. Это приводит к тому, что:

— Без системного подхода сложно увидеть картину целиком: на уровне «умного дома» не учитывается влияние городской инфраструктуры, а на уровне «умного города» не учитываются особенности сегментов отдельных зданий.
— Затруднено приоритизирование рисков: без интегрированных инструментов анализа сложно определить, какие уязвимости действительно критичны и требуют немедленного исправления.
— Информационная перегрузка операторов систем кибербезопасности, которым приходится анализировать многократные сигналы и алармы от разных систем, не имея средств автоматического коррелирования событий.

Глубинный системно-аналитический подход должен включать создание комплексных платформ управления киберрисками, способных в реальном времени:

— Интегрировать данные о состоянии всех уровней инфраструктуры (дом, микрорайон, город).
— Проводить корреляционный анализ инцидентов с использованием машинного обучения и контекстно-зависимых датчиков.
— Автоматически формировать рекомендации по смягчению угроз, приоритизировать патчи, выделять ресурсы на защиту наиболее уязвимых и критичных узлов.

Таким образом, рассмотренные пробелы представляют собой сложный комплекс технических, организационных и регуляторных проблем. Их решение требует системного и стандартизированного подхода, направленного на формирование единой нормативно-правовой базы, сегментацию сетей и внедрение «нулевого доверия», создание безопасных и автоматизированных систем обновления, массовую интеграцию аналитических методов и машинного обучения, а также переход от разрозненных мер защиты к полноценному системно-аналитическому управлению киберрисками. Только при таком многопрофильном и скоординированном подходе возможно обеспечить устойчивую безопасность развивающихся «умных» экосистем.

Полученные результаты

В ходе анализа было показано, что киберугрозы для «умных домов» и «умных городов» носят многоуровневый характер, охватывают широкий спектр устройств и систем, используют различные методы — от простой эксплуатации слабых паролей до сложных таргетированных атак с применением машинного обучения. Выделены актуальные векторы угроз, связанные с уязвимостями периферийных устройств, протоколов связи, систем машинного зрения, а также с недостатками в регламентации и интеграции мер защиты.

Выявленные пробелы указывают на необходимость системного подхода к снижению киберрисков, включающего разработку единых стандартов безопасности, внедрение комплексных аналитических платформ, ориентированных на контекстуальный анализ угроз в реальном времени. Предлагаемый путь — применение машинного обучения, контекстно-зависимых датчиков и методов машинного зрения для динамической оценки рисков, выявления аномалий и автоматизации процессов принятия решений.

Заключение

«Умные дома» и «умные города» — это технологический вектор развития, призванный повысить качество жизни людей, улучшить использование ресурсов, снизить издержки и оптимизировать функционирование общественных сервисов. Однако параллельно с этими преимуществами растут и киберриски. Изложенный обзор показал, что современные киберугрозы отличаются сложностью, многообразием и постоянной эволюцией.

Чтобы противостоять этим вызовам, необходим системный, аналитический подход к оценке киберрисков, а также использование инновационных инструментов — от машинного обучения и машинного зрения до контекстно-зависимых датчиков. Только комплексный подход, основанный на стандартизации, развитии аналитических методик и интеграции разнообразных технических и организационных мер, позволит обеспечить устойчивую кибербезопасность для будущих «умных» экосистем.

ЛИТЕРАТУРА

1. Weber R.H. Internet of Things — New security and privacy challenges // Computer Law & Security Review. — 2010. — Т. 26, № 1. — С. 23–30.
2. Stojmenovic I., Wen S. The fog computing paradigm: Scenarios and security issues // 2014 Federated Conference on Computer Science and Information Systems: сб. тр. — IEEE, 2014. — С. 1–8.
3. Kolias C., Kambourakis G., Stavrou A., Voas J., Bojanova I. DDoS in the IoT: Mirai and other botnets // Computer. — 2017. — Т. 50, № 7. — С. 80–84.
4. Lee J., Lee H. Security and privacy challenges in the IoT-based smart home // 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things: сб. тр. — IEEE, 2015. — С. 63–67.
5. Yang P., Wu G., Li G.Y., et al. A survey on smart city infrastructures: Objectives, applications, and research challenges // IEEE Communications Surveys & Tutorials. — 2018. — Т. 20, № 4. — С. 3463–3494.
6. Лапин Б.Н., Кузнецов В.И., Малышев А.Н. Безопасность «умных городов»: анализ рисков и методы снижения уязвимостей // Информационная безопасность систем. — 2019. — № 2. — С. 34–45.
7. Сидоров П.А., Крамаров А.С. Применение IoT-технологий в городских системах: проблемы стандартизации и безопасности // Вестник компьютерных и информационных технологий. — 2020. — № 5. — С. 56–62.
8. Ильинский А.Ю., Васильев В.П., Горохов В.И. Аналитические методы обнаружения аномалий в IoT-сетях умных домов // Управление большими системами. — 2021. — № 14. — С. 122–133.
9. Поляков И.Е. Обеспечение кибербезопасности систем машинного зрения в умных городах // Современные информационные технологии и ИТ-образование. — 2020. — № 1. — С. 89–97.
10. ГОСТ Р 58639–2019 «Интернет вещей. Требования к информационной безопасности». — Введ. 01.01.2021. — М.: Стандартинформ, 2019. — 25 с.
11. European Union Agency for Cybersecurity (ENISA). Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures [Электронный ресурс]. — 2017. — URL: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (дата обращения: 14.12.2024).
12. The National Institute of Standards and Technology (NIST). NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers [Электронный ресурс]. — 2020. — URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf (дата обращения: 14.12.2024).
13. Chen H., Chiang R.H.L., Storey V.C. Business Intelligence and Analytics: From Big Data to Big Impact // MIS Quarterly. — 2012. — Т. 36, № 4. — С. 1165–1188.
14. Medina E., Gamundani A.M., Niekerk J.V. Security in IoT: A Survey on Challenges and Solutions // 2020 IEEE 15th International Conference on Industrial and Information Systems (ICIIS): сб. тр. — IEEE, 2020. — С. 1–6.
15. Серов С.В., Минаев В.В. Выявление и предотвращение DDoS-атак в сетях интернета вещей // Проблемы информационной безопасности. Компьютерные системы. — 2018. — № 1. — С. 77–85.

Журнал «Современная наука: актуальные проблемы теории и практики»