Интернет вещей и его влияние на безопасность сетей: новые угрозы и решения

The internet of things and its impact on network security: new threats and solutions

УДК 004.056.5, 004.42, 004.9
Получено: 18.01.2026 Одобрено: 21.02.2026 Опубликовано: 25.03.2026

Лоскутов И.А.
Канд. техн. наук, преподаватель, Колледж телекоммуникаций ордена Трудового красного знамени ФГБОУ ВО «Московский технический университет связи и информатики», доцент кафедры ИП, Институт перспективных технологий и индустриального программирования структурное подразделение ФГБОУ ВО «МИРЭА-Российский технологический университет», г. Москва
e-mail: faxvex@ya.ru

Loskutov I.A.
Candidate of Technical Sciences, lecturer, College of Telecommunications of the Order of the Red Banner of Labor Moscow Technical University of Communications and Informatics, associate professor of the Department of IP, Institute of Advanced Technologies and Industrial Programming, structural division of MIREA-Russian Technological University, Moscow
e-mail: faxvex@ya.ru

Ярусова С.Д.
Студент, Колледж телекоммуникаций ордена Трудового красного знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Москва

Yarusova S.D.
Student, College of Telecommunications of the Order of the Red Banner of Labor Moscow Technical University of Communications and Informatics, Moscow

Аннотация
В статье проводится анализ влияния технологий Интернета вещей на информационную безопасность сетей. В работе рассматривается традиционная и расширенная многоуровневая архитектура ИВ, основные угрозы, распределённые по уровням архитектуры, а также новые их виды, направленные на компоненты искусственного интеллекта. Обзор научной литературы показал высокую актуальность проблемы в условиях быстрого роста количества подключённых устройств и их ограниченных ресурсов. В связи с этим предложены практические рекомендации по минимизации рисков, включающие использование лёгкой криптографии, блокчейн-технологий, многоуровневой защиты по принципу security-by-design и соблюдения регуляторных требований. Особое внимание уделено математическому моделированию рисков и эффективности защитных механизмов для ресурсоограниченных ИВ-систем.
Ключевые слова: Интернет вещей, информационная безопасность, киберугрозы, архитектура, оценка рисков.

Abstract
The article analyzes the impact of Internet of Things technologies on the information security of networks. The study examines traditional and extended multi-level IoT security architectures, the main threats distributed across architectural levels, as well as new types of threats targeting artificial intelligence components. A review of the scientific literature highlights the high relevance of the problem in the context of the rapid growth in the number of connected devices and their limited resources. In this regard, practical recommendations for risk mitigation are proposed, including the use of lightweight cryptography, blockchain technologies, multi-level security based on the security-by-design principle, and compliance with regulatory requirements. Special attention is paid to mathematical modeling of risks and the effectiveness of protection mechanisms for resource-constrained IoT systems.
Keywords: Internet of Things, information security, cyber threats, architecture, risk assessment.

Введение

XXI век уже невозможно представить без устройств Интернета вещей (ИВ), и именно поэтому современность называют веком цифровизации. Действительно, вся наша жизнь постепенно и неумолимо связывается во едино с Интернетом, становится полностью зависимой от так называемых «умных» устройств.

Стоит отметить, что данная тенденция свойственна не только повседневной жизни человека, она в полной мере применима и к местам работы индивидуумов – т.е. производствам, а потому становится очевидно, что обозревание столь важной технологии до сих пор остаётся крайне актуальным деянием.

По многим интернет прогнозам, уже к концу третьего десятилетия, количество активных ИВ-устройств превысит десятки миллиардов, тем самым подтверждая ранее отмеченные доводы о неотъемлемости их как в быту, промышленности, так и в городской инфраструктуре [1]. Однако, развитие любой технологии всегда совмещено с рисками и угрозами. В цифровом мире такие вопросы возложены на понятия информационной безопасности (ИБ). Как показывают прошлогодние отчеты [2], ежедневно фиксируется порядка 820 тысяч киреатак (КА) на ИВ-устройства, число киберинцидентов (КИ) с использованием тех же ботнетов ежегодно растет на десятки процентов.

Особая проблема ИВ-устройств в части ИБ нередко связана с банальными ограничениями вычислительных ресурсов. Такие механизмы работают автономно и нередко используют устаревшее ПО, что приводит к утечкам персональных данных (ПД), нарушениям работы предприятий, в том числе относящихся к объектам критической информационной инфраструктуры (КИИ). Т.о. необходимо проанализировать архитектуру ИВ, выявить основные киберугрозы (КУ) и предложить практические решения по защите.

Архитектура ИВ

Очевидно, что ИВ представляет собой сложную экосистему, которая объединяет самые разные физические объекты, будь то всевозможные датчики, некоторые «прогрессивные» бытовые приборы, промышленное оборудование и конечно системы управления, содержащие в себе логику замкнутого контура в части обмена данными по локальной и глобальной сетям. Ключевыми компонентами здесь, как известно, выступают сенсорные сети (USN) и технологии радиочастотной идентификации (RFID), без которых трудно представить полноценное функционирование любой ИВ-системы.

Традиционно архитектуру ИВ принято описывать в виде относительно простых моделей, не более 5 уровней, включающих уровень восприятия, непосредственно связующую сеть, приложение и т.п. Однако, в настоящее время для действительно сложных решений, особенно на объектах КИИ, немного реже в обычной промышленности, всё чаще используют значительно более развёрнутые многоуровневые архитектуры. Т.о., в работе акцент будет делаться именно на расширенную многоуровневую модель, которая позволит учесть, во-первых, специфику периферийных устройств, во-вторых, особенности функционирования

облачных сервисов и в-третьих, но не менее важных, промежуточных звеньев обработки данных [3].

Недаром современные подходы к архитектуре ИВ всё чаще включают следующие основные уровни:

- Физический;
- периферийных вычислений;
- сети и шлюзов;
- ИБ.

На первом происходит сбор первичной информации из окружающей среды при помощи датчиков, актуаторов, некоторых исполнительных механизмов. Именно тут устройства напрямую взаимодействуют с реальным физическим миром, преобразуя физические параметры в цифровые сигналы. На втором уровне осуществляется первичная обработка данных. Она происходит в непосредственной близости с источником. Это позволяет существенно снизить задержки и уменьшить нагрузку на центральные серверные компоненты (СК). На третьем уровне полученные ранее данные передаются через локальные сети шлюзы. Важно отметить, что в качестве первых вполне могут выступать беспроводные самоорганизующиеся Ad Hoc и Mesh-сети. В шлюзовой же зоне выполняются так называемые функции ETL: извлечение, преобразование и загрузка информации. И наконец на последнем, уровне ИБ, проводится аутентификация устройств и пользователей, шифрование передаваемых данных, особенно это важно для ПД вследствие законодательных требований, в частности 152-ФЗ и предотвращение несанкционированного доступа (НСД).

В дополнение к ранее названным четырем уровням существуют еще уровень обработки и облачных сервисов, на которых происходит именно та логика, что заложена в названии, включая аналитику, маршрутизацию, обработку больших данных и т.п.

Конечно, представленная модель, состоящая из 4-6 уровней это лишь одна из версий, если брать тот же промышленной ИВ, то там уровневая градация может дойти и до 12 уровней, что значительно отличается от классической архитектуры семи уровневой модели ЭМВОС. Связано это с акцентированием на периферийные вычисления, необходимостью обеспечения ИБ непосредственно на уровне устройств и учёта ограниченных ресурсов большинства ИВ-узлов.

Т.о. уже становится очевидно, что правильный выбор архитектуры ИВ напрямую влияет на ИБ, производительность и стоимость подобных решений. Именно поэтому необходимо далее подробнее рассмотреть какие КУ наиболее значимы для системы.

Новые КУ безопасности ИВ

Как уже указали ранее, возможность НСД к экосистеме ИВ обусловлена не только архитектурной сложностью, но особенностью связанных элементов, а точнее их физическими ограничениями. На основании анализа современных КИ и отчётных материалов [2, 4], а также рассмотренной ранее архитектуре, КУ ИБ ИВ распределим по соответствующим уровням и характеру воздействия.

На физическом и периферийном уровнях цель большинства КА связано с компрометацией датчиков и исполнительных механизмов. Среди популярных методов отмечают перехват телеметрии, спуфинг и конечно несанкционированное вмешательство в работу микроконтроллерной техники. Наибольшую опасность представляют КА на физический уровень, т.е. на аппаратное обеспечение. Его реализация связана с внедрением вредоносных программных продуктов (ВПП) и использованием архитектурных уязвимостей в интерфейсах отладки, таких как JTAG, UART, SWD и т.п. Успешная реализация подобных КА позволяет злоумышленникам получить полный контроль над устройством, в т.ч. на этапе его производства, про эксплуатацию – очевидно. В условиях, когда многие узлы функционируют автономно и не обладают встроенными механизмами самопроверки, подобные атаки ВПП остаются наименее заметными, устройства не могут реализовать защитные деяния и способны далее заражать связанные механизмы.

Сетевой и шлюзовый уровни подвергаются масштабным распределённым КА типа DDoS. В результате формирования ботнетов из миллионов скомпрометированных ИВ-узлов генерируется трафик, способный вывести из строя КИИ объекты, что крайне опасно для поддержания стабильности работы атакуемой экономической отрасли государства. В 2024–2025 гг. зафиксировано увеличение интенсивности подобных КА на 20–35%, средний уровень риска заражения устройств ВПП вырос на 15–33%. Наиболее подверженными секторами является здравоохранение, промышленная автоматизация и системы, реализующие технологии умных городов [4]. Эксплуатация уязвимостей, подобных React2Shell и аналогичных RCE-багов, позволяет удалённо выполнять произвольный код без предварительной аутентификации, превращая штатные устройства в элементы распределённых вычислительных сетей злоумышленников, что крайне опасно при их обнаружении на поздних стадиях и может парализовать огромное количество сфер.

На уровне облачных сервисов и обработки данных, возрастает угроза утечек конфиденциальной информации и ПД, так как ИВ-системы собирают и агрегируют значительные их объёмы, то при отсутствии должного уровня шифрования или при применении устаревших протоколов возникает высокий шанс нарушения целостности и конфиденциальности данных.

Все перечисленные КУ уже не раз упоминались в научной литературе, но в последнее время появился еще один вид, который называют часто «emerging threats» и «adversarial threats», по сути, это новый вид КУ. Их цель – КА на компоненты искусственного интеллекта (ИИ), интегрированные в ИВ-системы, предназначенные для предиктивной аналитики и организации автономного управления, а также на модели машинного обучения [5]. В результате внедрения такого рода ВПП, происходит искажение входных данных, из-за чего система начинает принимать ошибочные решения. Такие ошибки критичны в промышленном, медицинском секторам, так как способны привести в лучшем случае к аварийным ситуациям, а в худшем – стать причиной массовой гибели и травматизма людей.

Отдельным дополнением к новым КУ следует также отнести виды ВПП, связанные с цепочками поставок, выраженные в компрометации сторонних библиотек, модификации прошивок при сборке или интеграция недоверенных компонентов. Все это создает новые скрытые векторы КА, обнаружение которых сложная задача, поскольку требует глубокого аудита кода и верификации аппаратного обеспечения.

Стоит отметить, что для количественной оценки таких КУ часто применяется рисковая матмодель, которая позволяет формализовать вероятность и последствия КА. В общем виде риск для ИВ-системы можно представить следующим образом:

$$R=P\times I\times V$$

Где:

R – общий уровень риска;

P – вероятность реализации КУ, с учетом ограничения ресурсов устройства;

I – потенциальный ущерб: финансовый, репутационный, связанный с безопасностью КИИ и т.п.;

V – коэффициент уязвимости устройства, что зависит от уровня архитектуры и наличия обновлений.

Недаром в условиях автономной работы ИВ-узлов данный показатель часто корректируется дополнительным коэффициентом утомляемости системы или коэффициентом ресурсоограниченности kr, находящемся в диапазоне $0 < kr < 1$:

$$R_{ИВ} = P \times I \times V \times (1 + kr)$$

Т.о., чем выше ограниченность ресурсов, тем выше становится реальный риск, даже при средней вероятности КА.

Определив комплекс угроз, необходимо перейти к мерам профилактики и решения.

Меры профилактики и решения по защите

Традиционные методы ИБ, такие как шифрование и аутентификация, безусловно важны, однако они требуют серьёзной адаптации под жёсткие ограничения вычислительных ресурсов большинства ИВ-устройств. Стоит особо отметить, что в условиях, когда устройства работают автономно, без постоянного контроля оператора и часто на устаревшем программном обеспечении, применение классических тяжёлых криптографических алгоритмов становится практически невозможным. В связи с этим рекомендуемые подходы включают, прежде всего, сильную аутентификацию с обязательным использованием двухфакторной или многофакторной верификации, присвоение жёстко заданных уникальных идентификационных данных, а также переход на современные облегчённые протоколы, такие как LwM2M [6].

Недаром в последние годы всё большее внимание уделяется так называемой лёгкой криптографии (ЛК). В частности, алгоритмы семейства Ascon, которые были официально стандартизированы NIST в период 2023–2025 гг. [7], уже доказали свою эффективность для ресурсоограниченных устройств ИВ. Такие алгоритмы позволяют обеспечить необходимый уровень конфиденциальности и целостности данных при минимальных затратах на вычисления и энергопотребление.

Кроме того, стоит отметить растущую роль блокчейн-технологий (БТ) в облегчённом (lightweight) исполнении. Они обеспечивают не только целостность передаваемых данных, но и децентрализованную аутентификацию устройств, а также возможность traceability всей цепочки операций. В промышленных и критически важных системах такие решения позволяют существенно снизить риски компрометации отдельных узлов и предотвратить каскадное распространение КУ.

Многоуровневая защита по принципу security-by-design сегодня признаётся одним из наиболее эффективных подходов. Это означает, что механизмы безопасности должны быть встроены на каждом уровне архитектуры ИВ – начиная от физического и периферийного и заканчивая облачным. В частности, на периферии активно применяется edge-анализ аномалий, позволяющий выявлять подозрительное поведение устройств в режиме реального времени, без необходимости постоянной передачи больших объёмов данных в облако. Не менее важным остаётся регулярное обновление прошивок и программного обеспечения, хотя, как известно, именно этот процесс до сих пор остаётся одной из самых слабых сторон большинства ИВ-решений.

Отдельное внимание следует уделить физической защите устройств. Оборудование специальными защитными кейсами, ограничение физического доступа к интерфейсам отладки, такие как JTAG, UART, SWD, и сегментация сетей позволяют значительно снизить риск атак на аппаратном уровне. В дополнение к техническим мерам ИБ, большую роль играют регуляторные требования. В частности, самым свежим примером может вступивший в силу законодательный акт Евросоюза EU Cyber Resilience Act 2024 [8], который устанавливает строгие требования к жизненному циклу ИБ подключённых устройств, включая обязательную CE-маркировку и ответственность производителей за весь период эксплуатации изделия.

Стоит особо отметить, что выбор оптимальных механизмов защиты также можно формализовать математически. Один из подходов – модель ранжирования механизмов защиты по двум критериям: сложности реализации (C) и универсальности (U). Интегральный показатель эффективности защиты E для механизма i рассчитывается по формуле:

$$E_i = \alpha \cdot U_i - \beta \cdot C_i$$

Где:

α и β – весовые коэффициенты, определяемые экспертно или на основе политики ИБ организации. Как правило $\alpha + \beta = 1$;

Ui – степень универсальности механизма, т.е. применимость его к разным уровням архитектуры ИВ);

C_i – сложность реализации, в том числе вычислительные затраты, энергопотребление, стоимость внедрения и т.п.

Т.о., задача сводится к максимизации E_i при ограничениях на ресурсы устройства. Недаром ЛК и БТ в облегчённом исполнении показывают высокие значения данного показателя для большинства ИВ-узлов.

Подытоживая – минимизация рисков в экосистеме ИВ требует комплексного подхода в виде сочетания ЛК, современных протоколов, блокчейн-решений, встроенной многоуровневой защиты и строгого соблюдения нормативных требований. В связи с этим становится очевидно, что только security-by-design, реализованный на всех уровнях архитектуры и подкреплённый матмоделированием рисков и эффективности ИБ, способен обеспечить приемлемый уровень защищённости в условиях стремительного роста количества ИВ-устройств и усложнения КУ.

Заключение

Проведённый анализ показал, что ИВ, несмотря на все свои очевидные преимущества и широкие перспективы применения, создаёт значительное количество новых векторов КУ, которые в условиях ограниченных ресурсов устройств и их массового внедрения представляют серьёзную опасность как для отдельных предприятий, так и для объектов критической информационной инфраструктуры в целом.

Стоит отметить, что традиционная архитектура ИВ с её многоуровневой структурой, с одной стороны, обеспечивает необходимую гибкость и масштабируемость, а с другой – открывает дополнительные возможности для злоумышленников. Особенно опасными остаются атаки на физический и периферийный уровни, масштабные DDoS-атаки через ботнеты, утечки ПД и emerging threats, направленные на компоненты ИИ и моделей машинного обучения.

Недаром эффективная защита ИВ-систем требует принципиально нового подхода – отказа от устаревших тяжёлых методов в пользу ЛК, встроенной безопасности на всех уровнях архитектуры, использования БТ и современных протоколов. Только комплексное применение мер технического, организационного и регуляторного характера способно существенно снизить существующие риски и повысить доверие к технологиям ИВ.

В заключение следует подчеркнуть, что дальнейшие исследования в данной области должны быть направлены на разработку адаптивных моделей безопасности для ресурсоограниченных устройств, совершенствование методов обнаружения аномалий в режиме реального времени и интеграцию ИИ не только для функциональности, но и для обеспечения ИБ ИВ-систем. Реализация предложенных в работе рекомендаций позволит не только минимизировать угрозы, но и способствовать более безопасному и устойчивому развитию технологий ИВ в ближайшие годы.

Литература

1. S. Saravana Kumar, Balaji Kannan, "Enhancing Industrial IoT Security with AI and Cloud Computing: A Review of Threats and Solutions", 2025 International Conference on Modern Sustainable Systems (CMSS), pp.1082-1089, 2025.
2. DDoS-атаки в 2025 году: цифры, тренды, аналитика // StormWall. – 2026. – 23 января. – URL: https://stormwall.pro/resources/blog/ddos-trendy-2025 (дата обращения: 09.03.2026).
3. 12 уровней IIoT-архитектуры: от периферийных датчиков до аналитики Big Data // BigDataSchool. – 2019. – 10 ноября. – URL: https://bigdataschool.ru/blog/iiot-architecture-levels-and-tools/ (дата обращения: 07.04.2026).
4. Атаки на Android и IoT выросли в несколько раз в 2025 году // SecPost. – 2025. – 6 ноября. – URL: https://secpost.ru/mobilnye-i-iot-ugrozy-2025-42-milliona-skachivanij-vredonosov-i-rost-atak-na-promyshlennost (дата обращения: 05.04.2026).
5. Emerging Threats & Vulnerabilities to Prepare for in 2025 // Dark Reading. – 2024. – 26 декабря. – URL: https://www.darkreading.com/vulnerabilities-threats/emerging-threats-vulnerabilities-prepare-2025 (дата обращения: 30.03.2026).
6. NIST утвердил стандарт быстрой криптографии Ascon для защиты IoT-устройств // Anti-Malware.ru. – 2025. – 15 августа. – URL: https://www.anti-malware.ru/news/2025-08-15-111332/47003 (дата обращения: 25.03.2026).
7. Asma Lahbib, Khalifa Toumi, Anis Laouiti, Steven Martin. Blockchain based distributed trust management in IoT and IIoT: a survey. Journal of Supercomputing, 2024, 80 (15), pp.21867-21919.
8. Cyber Resilience Act // European Commission. Shaping Europe’s digital future. – 2025. – URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (дата обращения: 10.04.2026).