БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2025. – № 2 (117). – 52–75

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2025-2-52-75

ИНТЕРНЕТ ВЕЩЕЙ (IOT): УГРОЗЫ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ*

А.А. КРАВЧЕНКО[1], Р.А. ПЕРМЯКОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: kravchenko.2020@stud.nstu.ru*

[2] *630090, РФ, г. Новосибирск, пр. Академика Лаврентьева, 6, Федеральное государственное бюджетное учреждение науки «Институт вычислительной математики и математической геофизики» Сибирского отделения Российской академии наук, ведущий инженер лаборатории искусственного интеллекта и информационных технологий. E-mail: pra@yandex.ru*

Развитие и распространение технологии Интернета вещей (IoT) привело к тому, что всё больше различных устройств объединяются в единые системы, подключаются к Интернету и передают различные данные без взаимодействия с человеком. При этом устройства, нацеленные на широкое потребление, зачастую не могут обеспечить безопасность и конфиденциальность передаваемых данных. Интернет вещей стал играть огромную роль в жизни обычных людей и организаций и предоставил новые возможности для злоумышленников. Включение миллионов устройств в DDoS-атаки, доступ к конфиденциальным данным пользователей, новые векторы атак на инфраструктуру и возможность обходить стандартные меры защиты превратили IoT в источник угроз. В статье представлен анализ ландшафта угроз, связанных с использованием устройств IoT в автоматизированных системах управления, основные сценарии развития и способы атаки на автоматизированные системы.

Ключевые слова: IoT, промышленный IoT, умный дом, кибербезопасность, протокол связи, ландшафт угроз, модель угроз, mitre att&ck

* Статья получена 14 мая 2025 г.

ВВЕДЕНИЕ

Развитие и распространение технологии Интернета вещей (IoT) привело к тому, что всё больше различных устройств объединяются в единые системы, подключаются к Интернету и передают различные данные без взаимодействия с человеком. В 2012 году в рекомендациях Сектора стандартизации электросвязи Международного союза электросвязи (МСЭ-Т) IoT был определен как «глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) сущностей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий». «Вещь» здесь «означает предмет физического мира (физические вещи) или информационного мира (виртуальные вещи), который может быть идентифицирован и интегрирован в сети связи» [1].

Сейчас IoT начинает играть ключевую роль в многих сферах жизни – от умных домов до промышленных автоматизированных систем. Ярким примером служит концепция умного предприятия (Smart Factory), которое контролирует промышленное оборудование и ищет проблемные места, а затем перестраивается так, чтобы не допустить поломок [2]. Бурный рост и развитие IoT создает не только новые возможности, но и новые угрозы безопасности, связанные с архитектурными особенностями IoT-инфраструктуры и свойствами объектов автоматизации.

1. АКТУАЛЬНОСТЬ

Современные автоматизированные системы на основе IoT широко распространены не только на производстве, но и в быту: система «умный дом» уже давно пользуется большим спросом и популярностью [3]. На конец 2024 года количество подключенных устройств оценивалось в 18,8 млрд с перспективой роста до 40 млрд к 2030 году [4]. К сожалению, уязвимость IoT-систем всё еще остается высокой [5], и злоумышленники активно этим пользуются: всем известен ботнет Mirai [6], чьи клоны повсеместно используются до сих пор [7]. Можно выделить следующие причины уязвимости IoT-систем (рис. 1).

Рассмотрим подробнее приведенные выше причины.

1. Ресурсы устройств

Большинство производителей, сокращая расходы производства, используют недорогие и маломощные компоненты, которые обеспечивают необходимый функционал для устройств и почти все ресурсы при работе, таким

образом, они не способны поддерживать должную защиту (надежные криптографические алгоритмы (SHA-256/512), фаерволы, продвинутые протоколы связи и т. д.).

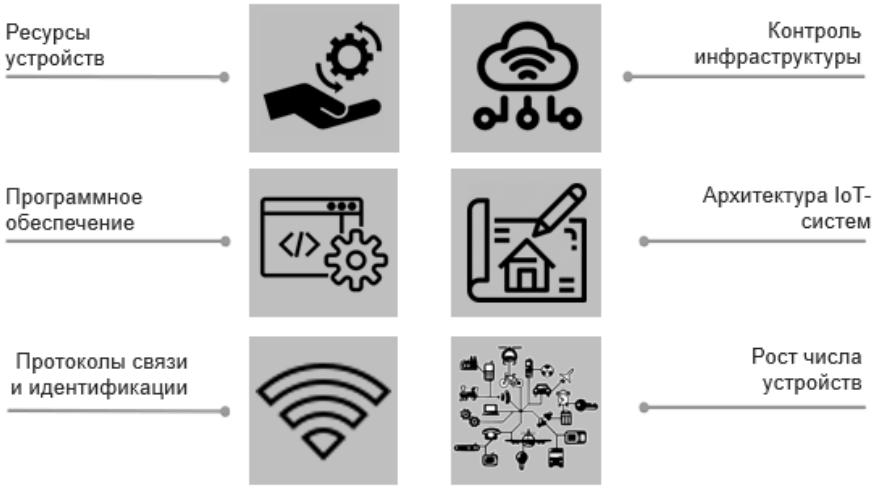

Рис. 1. Причины уязвимости IoT

2. Программное обеспечение

Устаревание программного обеспечения из-за блокировки сервисов IoT производителей внутри страны, игнорирование обновлений и патчей пользователями и администраторами систем с элементами IoT приводит к использованию устаревшего программного обеспечения, которое содержит критические уязвимости [8].

3. Устаревшие протоколы связи и идентификации

Современные системы IoT и IIoT проектируются для работы без участия человека, и из-за архитектурных ограничений устройств часто разработчики не применяют продвинутые протоколы идентификации, а ключи шифрования и пароли хранятся в незащищенных участках памяти, что в связке с ненадежными и устаревшими протоколами связи, такими как Telnet, создает угрозу перехвата и дешифровки либо подмены передаваемых данных [9].

4. Контроль инфраструктуры

Многие производители IoT-устройств предлагают облачные платформы для управления их девайсами и хранения пользовательских данных, однако это ведет к росту трансграничного трафика и делает системы IoT сложными для защиты и управления.

5. Архитектура IoT-систем

Системы IoT активно взаимодействуют с различными сервисами во внешней сети или сервисами поставщиков IoT-устройств, в том числе и с сервисами искусственного интеллекта [10]. Однако в промышленности, где изначально АСУТП является закрытой системой, функционал, обеспечивающий безопасность и целостность системы при взаимодействии с внешней сетью, слабо проработан и архитектура промышленной автоматики не предусматривает надлежащей защиты от современных внешних угроз.

6. Увеличение количества подключенных устройств

Рост количества активных IoT-устройств в информационных системах ведет к увеличению точек входа для атак не только на систему, но и на гражданскую инфраструктуру и на информационные системы, включенные в цепочку поставок, в том числе на промышленные объекты разных стран [11].

2. ЛАНДШАФТ УГРОЗ

Архитектура IoT, в том числе IIoT, основана на разработках автоматизированных систем управления технологическими процессами (АСУТП) и представляет собой трехуровневую модель (рис. 2).

Такой шаблон архитектуры сети IoT более характерен для промышленных сетей [12], так как для систем класса «умный дом» зачастую разделяют уровень периферии на уровень устройств (датчики, камеры, выключатели и т. д.) и сетевой уровень (коммутаторы, хабы беспроводных сетей, маршрутизаторы). Однако периферийные устройства могут сами выступать в роли точек доступа. Например, умные колонки могут предоставлять доступ к wi-fi, поэтому такое разделение не несет значительной практической пользы. Нацеленные на широкое потребление IoT-устройства зачастую не могут обеспечить высокий уровень безопасности и конфиденциальности передаваемых данных. Именно уровень периферии представляет основную опасность для IoT-систем.

Рис. 2. Архитектура сети IoT

Цель работы состоит в том, чтобы провести анализ ландшафта угроз и защищенности IoT-устройств и информационных систем, созданных на их основе либо использующих IoT-устройства. В настоящей работе мы не рассматриваем угрозы, связанные с катастрофическими воздействиями (стихийные бедствия, экологические катастрофы). Для достижения поставленной цели мы провели классификацию угроз в зависимости от уровня в архитектуре IoT-системы (рис. 2), используя общедоступные источники информации, такие как база данных БДУ, CVE, MITRE и др.

2.1. УГРОЗЫ ДЛЯ УРОВНЯ ПЕРИФЕРИИ

Уровень периферии – уровень сбора данных с датчиков и управления исполнительными устройствами, также на этом уровне осуществляется передача данных от устройств к центрам их обработки. Исходя из этого можно выделить следующие угрозы, которые представлены на рис. 3.

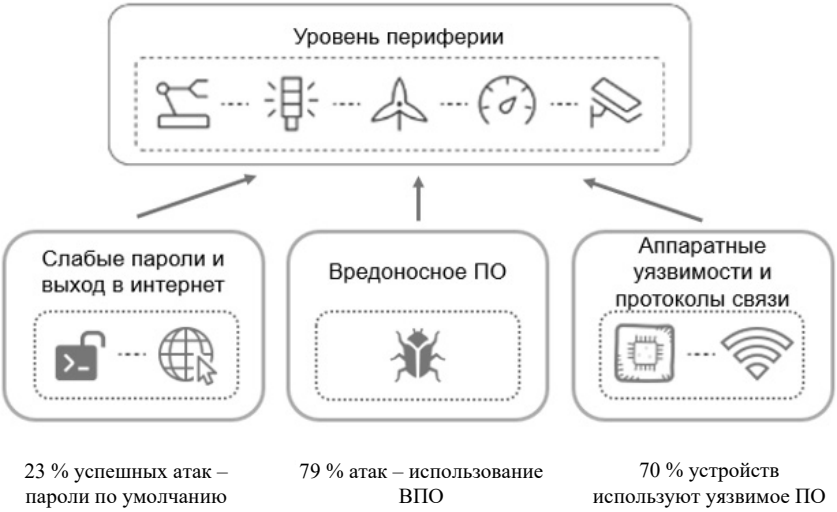

Рис. 3. Ландшафт угроз для уровня периферии

2.1.1. СЛАБЫЕ ПАРОЛИ И ВЫХОД В ИНТЕРНЕТ

Использование заданных паролей по умолчанию представляет собой распространенную уязвимость IoT-устройств. Стандартные пароли предпочтительнее их полного отсутствия, но это серьезная угроза безопасности системы. Например, маршрутизаторы NETGEAR XR1000 до версии 1.0.0.58 не позволяли изменить заданный по умолчанию пароль, что создавало угрозу несанкционированного доступа к устройству и компрометации сетевой инфраструктуры [13]. Кроме того, существует проблема инициализации IoT-устройств с беспроводным подключением к wi-fi, которая заключается в том, что при первоначальной активации или недоступности установленной сети устройство пытается подключиться к запрограммированному производителем сервису или само переходит в режим точки доступа (часто со стандартным несменяемым паролем). Таким образом, злоумышленники могут использовать данный функционал для получения доступа к устройству и последующей интеграции его в ботнет или проведения иных вредоносных действий.

2.1.2. ВРЕДОНОСНОЕ ПО

В отличие от глобальной сети, где периферийное устройство содержит, передает или обрабатывает информацию, на которую нацелен злоумышленник, в IoT-системе устройства могут свободно отправлять запросы другим устройствам, чем активно пользуются злоумышленники, проводя всё более серьезные DDoS-атаки [14]. Ботнеты стали широко известны в 2016 году, а сейчас почти половина их основана на самом первом ботнете Mirari (рис. 4) [7].

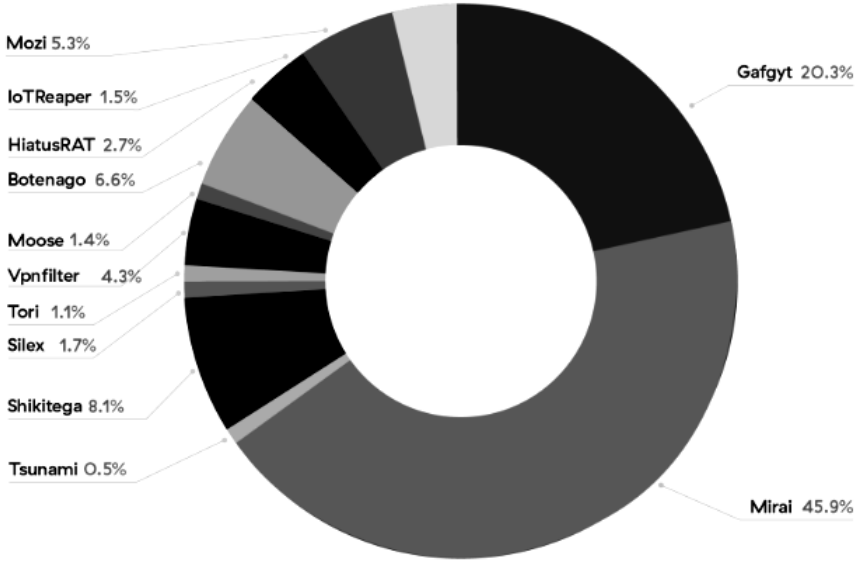

Рис. 4. Топ семейств ботнетов [7]

С другой стороны, периферийные устройства – это точки проникновения и закрепления в сети, которые взаимодействуют с центрами хранения данных – облачными платформами и дата-центрами поставщиков или организаций, использующих IoT-устройства. Именно ЦОДы являются целью атак для вымогателей и APT-группировок [15]. Эти особенности формируют уникальные свойства IoT-сетей, которые и отличают их от традиционных корпоративных, что отражается в используемом злоумышленниками ВПО (рис. 5).

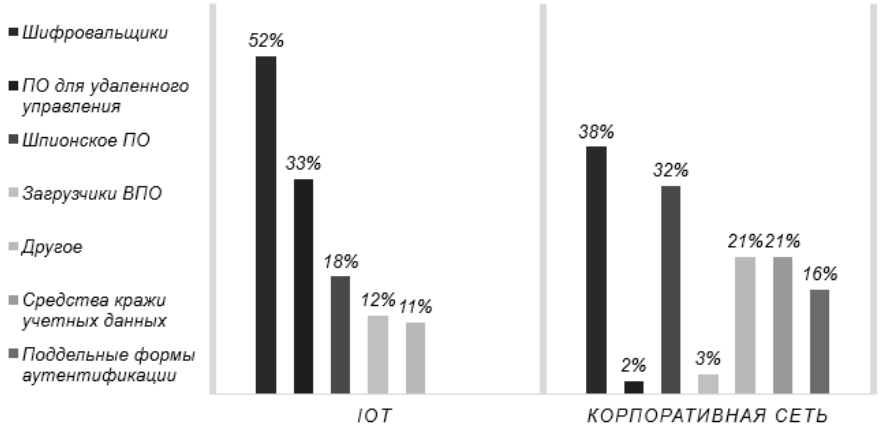

Рис. 5. Атаки на IoT и корпоративные сети организаций с использованием ВПО за 2024 год по данным Лаборатории Касперского и Positive Technologies [20]

Так, шифровальщики занимают первое место в списке используемого ВПО, на втором месте ПО для удаленного управления – ботнеты. Одним из ярких примеров IoT-шифровальщика является DeadBolt, поразивший тысячи устройств QNAP NAS в 2022 году. Для атаки использовалась уязвимость CVE-2022-27593, позволяющая злоумышленникам модифицировать системные файлы на устройстве [16].

2.1.3. ЭКСПЛУАТАЦИЯ АППАРАТНЫХ УЯЗВИМОСТЕЙ И НЕДОСТАТКОВ ПРОТОКОЛОВ СВЯЗИ

При построении современных систем с IoT-устройствами используются множество протоколов, которые можно классифицировать следующим образом.

1. Протоколы канального уровня

- Wi-Fi (802.11) – стандартный протокол для домашних и промышленных IoT.
- Bluetooth Low Energy (BLE) – энергоэффективный протокол для персональных устройств.
- Zigbee – сетевая mesh-связь для маломощных устройств.
- Z-Wave – альтернатива Zigbee, часто для умного дома.
- LoRaWAN – протокол для дальнобойных и энергоэффективных сетей.

- NB-IoT (Narrowband IoT) – стандартизованный протокол от мобильных операторов.
- 5G/6G – стандарты мобильной связи для массовых подключений IoT через сотовые сети.
- Ethernet – протокол для стационарных промышленных IoT-устройств.

2. Протоколы транспортного уровня

- MQTT (Message Queuing Telemetry Transport) – стандарт для легковесной передачи данных.
- CoAP (Constrained Application Protocol) – аналог HTTP для устройств с ограниченными ресурсами.
- AMQP (Advanced Message Queuing Protocol) – более тяжелый, промышленный стандарт обмена сообщениями.
- HTTP/HTTPS – протоколы передачи гипертекста. Используется там, где интеграция с веб- и облачными сервисами критична.
- Matter – новый открытый стандарт для умного дома.

3. Прикладные протоколы и стандарты интеграции

- DDS (Data Distribution Service) – протокол, использующийся в критичных к реальному времени системах (например, для автономных машин).
- LwM2M (Lightweight M2M) – протокол для удаленного управления и мониторинга IoT-устройств.
- XMPP (Extensible Messaging and Presence Protocol) – протокол для обмена сообщениями в умных устройствах.
- OPC UA – протокол для промышленной автоматизации (IIoT).

4. Протоколы безопасности

- DTLS (Datagram Transport Layer Security) – протокол защиты для CoAP.
- TLS – протокол защиты для MQTT, HTTP, AMQP.
- OSCORE (Object Security for Constrained RESTful Environments) – протокол для объектной безопасности в CoAP.

По данным IoT Analytics, из 16,6 млрд подключенных устройств IoT в 2023 году только 700 млн использовали проводную связь, а оставшиеся 15,9 млрд подключений были беспроводными [4]. Основываясь на данных этой статьи, мы можем выделить следующие ключевые технологии для беспроводных IoT-устройств:

1) wi-fi – 31 % всех подключений IoT;
2) bluetooth – 25 %;
3) мобильная связь (2G, 3G, 4G, 5G, LTE-M, and NB-IoT) – 21 %.

2.1.3.1. *Уязвимости протоколов передачи данных и IoT-шлюзов*

Протоколы, используемые в промышленных IoT-сетях, в первую очередь нацелены на обеспечение беспрерывного и надежного взаимодействия множества устройств, поэтому вопросам безопасности часто уделяется недостаточно внимания.

Modbus TCP – широко используемый в системах промышленной автоматизации на объектах критической инфраструктуры протокол. Используя его, злоумышленники могут напрямую взаимодействовать с промышленными системами управления, контролировать оконечные устройства и нарушать технологические процессы. Например, в апреле 2024 года Dragos обнаружил вредоносное ПО FrostyGoop, написанное на языке Go и напрямую взаимодействующее с промышленными системами управления с помощью Modbus TCP [17].

MQTT – протокол, специально разработанный для устройств с ограниченными ресурсами для передачи данных с минимальными задержками, но не имеющий встроенного шифрования; 56 % устройств промышленного IoT используют данный протокол [18], однако он уязвим для типа MitM, сниффинга, атак Pre-Shared Key и др. [19].

Большинство промышленных контроллеров и других физических систем всё еще используют устаревшие протоколы, и для доступа к таким сетям используются специальные IoT-шлюзы. Они также содержат уязвимости и становятся целью атак [20].

2.1.3.2. *Аппаратные уязвимости и недостатки прошивки*

Так как периферийные IoT-устройства – это товар широкого потребления, то производители стараются сделать его максимально дешевым и простым и только потом безопасным (с точки зрения информационной безопасности). Таким образом, в прошивках IoT-устройств появляются жестко запрограммированные пароли, незадекларированные функции, такие как удаленный доступ и активация самих устройств.

Так, в марте 2025 года была обнаружена ошибка в реализации стека чипов ESP32 компании Espressif, позволяющая злоумышленникам обходить системы безопасности, выдавать себя за доверенные устройства и красть данные [21].

С 2000 года работает международная программа CVE® Program Mission, в рамках которой ведется база данных уязвимостей [22]. На май 2025 года зарегистрировано 1298 уязвимостей IoT-устройств.

Следует отметить, что замена уязвимых устройств в IoT-системах – нетривиальная задача, а в системах городского масштаба это может стать еще сложнее (например, замена светофоров по всей стране может затянуться на несколько лет [23]).

Не следует забывать, что часть устройств предоставляет пользователям возможность самим прописывать их функционал, что дает злоумышленникам возможность изменять их при получении доступа к системе [6].

2.2. УГРОЗЫ ДЛЯ УРОВНЯ ПЛАТФОРМЫ

Уровень платформы – уровень обработки, фильтрации, агрегации и хранения данных. Следует учитывать, что он может быть представлен как в локальном виде, так и в облачных хранилищах. Именно этим обусловлены угрозы, которые представлены на рис. 6.

Рис. 6. Ландшафт угроз для уровня платформы

2.2.1. АТАКИ НА СПЕЦИАЛИЗИРОВАННОЕ ПРОМЫШЛЕННОЕ ПО

По данным аналитиков, 37 % успешных кибератак на промышленные предприятия за первые три квартала 2024 года были реализованы через эксплуатацию уязвимостей. В подавляющем большинстве случаев (71 %) зло-

умышленники эксплуатировали уязвимости программного обеспечения, в том числе в коде специфических промышленных систем управления, таких как SCADA [20].

2.2.2. АТАКИ НА ОБЛАЧНЫЕ РЕСУРСЫ И ДАТА-ЦЕНТРЫ

Атакуют преимущественно IoT-устройства, на которых есть пользовательские данные: NAS-хранилища, облачные среды. В сентябре исследователи Microsoft сообщили об атаке группировки Storm-0501, в ходе которой злоумышленникам удалось скомпрометировать гибридные облачные среды, что привело к эксфильтрации данных, постоянному доступу к целевой инфраструктуре, а также к развертыванию программ-вымогателей в локальной сети. Атака была нацелена на ряд организаций в США, включая правительственные органы, производство, транспорт [24].

2.2.3. АППАРАТНЫЕ УЯЗВИМОСТИ

Многие компании и поставщики IoT-устройств используют облачные хранилища для хранения и обработки данных или виртуализацию, чтобы не закупать дополнительное оборудование. Таким образом, эксплуатация уязвимостей в виртуализации для взлома IoT-устройств, работающих на виртуальных машинах (например, облачные IoT-платформы или промышленные контроллеры с виртуализацией), может быть реализована для выполнения вредоносного кода на виртуальных устройствах. Например, уязвимость гипервизоров VMware ESXi, VMware Fusion, VMware Fusion Pro, Vmware Workstation Player, Vmware Workstation Pro связана с переполнением буфера в SVGA-памяти и позволяет нарушителю, действующему локально, выполнить произвольный код в хостовой системе [25].

Уязвимости в процессорах или памяти серверного оборудования, а также открытые интерфейсы отладки/администрирования позволяют получить несанкционированный доступ к системе [26].

2.3. УГРОЗЫ ДЛЯ УРОВНЯ УПРАВЛЕНИЯ

Уровень управления – уровень визуализации, диспетчеризации (мониторинга) и обработки данных оператором через человеко-машинный интерфейс. Угрозы для этого уровня представлены на рис. 7.

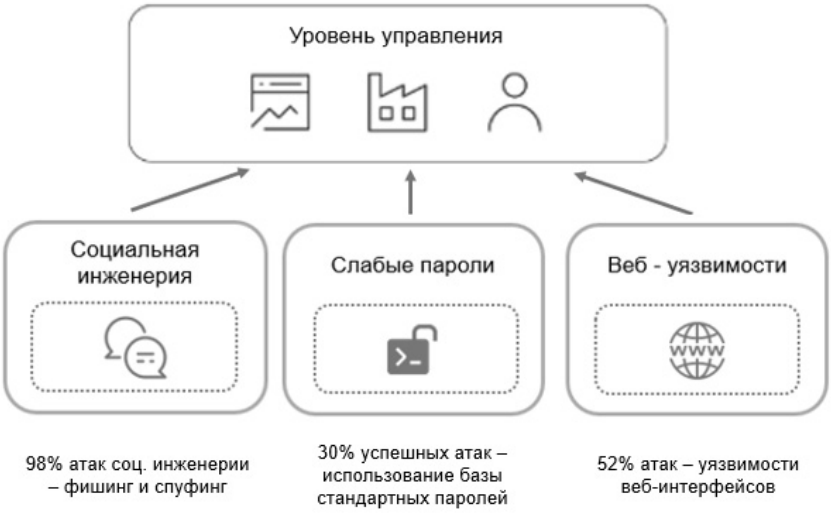

Рис. 7. Ландшафт угроз для уровня управления

2.3.1. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

На этом уровне самая уязвимая часть – это люди. Злоумышленники при помощи методов социальной инженерии (фишинг, претекстинг и т. п.) получают от пользователей доступ к системам управления и начинают свою деструктивную деятельность (рис. 8).

2.3.2. СЛАБЫЕ ПАРОЛИ

Большую опасность несут стандартные или слабые пароли, которые не меняются годами, а часть пользователей вообще используют один и тот же логин и пароль для нескольких сервисов, что упрощает их подбор.

2.3.3. ВЕБ-УЯЗВИМОСТИ

Пользовательские интерфейсы веб-приложений для управления IoT-устройствами также являются целью атак: уязвимости API, SQL-инъекции, командные инъекции, межсайтовый скриптинг XSS активно используются злоумышленниками для получения данных пользователей (логинов и паролей) или удаленного выполнения вредоносного кода.

3. МЕТОДЫ И ТРЕНДЫ АТАК НА IoT-СИСТЕМЫ

Учитывая специфику IoT, злоумышленники чаще используют ВПО, чем социальную инженерию, кроме того, преступники стали чаще использовать легитимное ПО производителей IoT для обнаружения устройств в сети, что значительно снизило эффективность обнаружения атак на начальных этапах (рис. 8) [18].

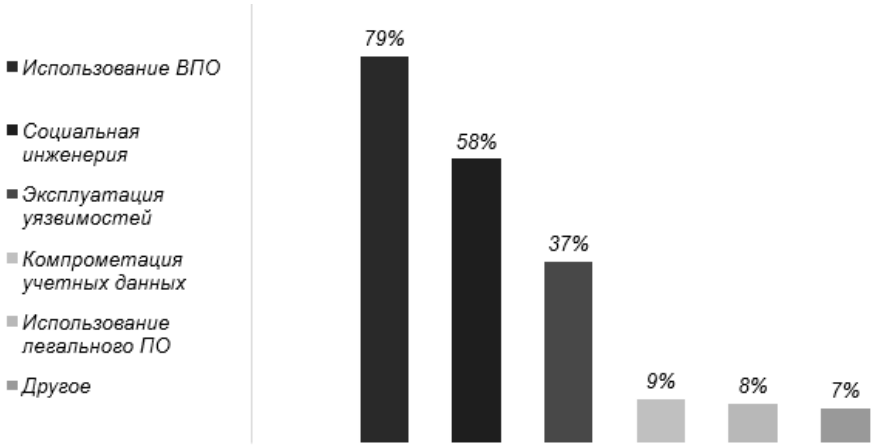

Рис. 8. Методы атак [20]

Не следует забывать и про ИИ. С его помощью написание ВПО становится легче и быстрее, а конечное качество возрастает, так как идет постоянное накопление знаний.

4. ПОСЛЕДСТВИЯ АТАК

Если для обычных пользователей основной угрозой является кража их конфиденциальных данных, то успешная атака на промышленную инфраструктуру может повлечь за собой более серьезные последствия: финансовые потери от полной или частичной остановки производства, физический вред из-за сбоев в работе оборудования, нарушение цепочек поставок и транспортировки сырья, негативное влияние на окружающую среду, нарушение основной деятельности и сбои в предоставлении услуг.

Чаще всего организации, подвергшиеся кибератакам, сталкиваются не с одним, а сразу с несколькими нежелательными последствиями (рис. 9).

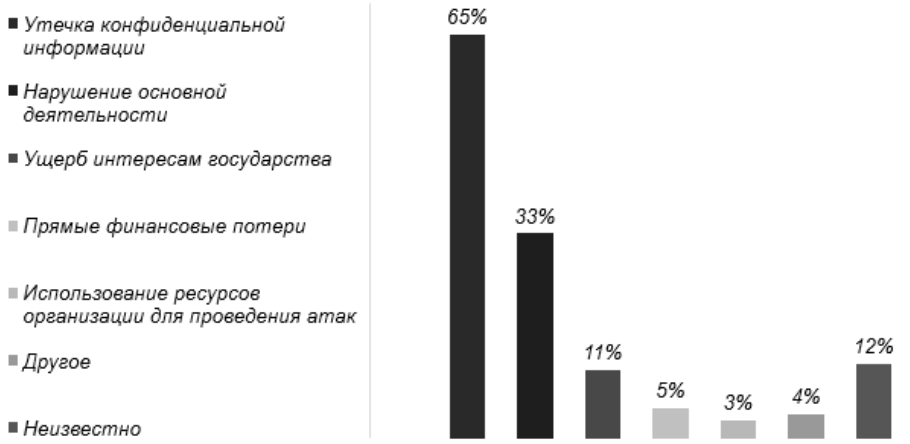

Рис. 9. Последствия атак [20]

5. МОДЕЛЬ УГРОЗ

После рассмотрения ландшафта угроз, методов и трендов, а также последствий атак была сформирована модель угроз для IoT-систем. Помимо основных угроз в модель включены основные техники, которые могут использовать злоумышленники для реализации атак. Техники взяты из таблицы MITRE ATT&CK [27]. Оценка рисков проводилась с помощью OWASP Risk Rating Calculator [28] на основе данных и статистики, полученных в ходе анализа открытых источников, и представлена в таблице.

Модель угроз IoT

Threat model of IoT

Уровень модели IoT	Угроза	Техника	Компонент	Риск
Периферия	Стандартные пароли	Метод перебора (T1110)	Веб-форма входа	Critical
		Поиск технической информации в общедоступных источниках (T1596)		
		Существующие учетные записи (T1078)		

Продолжение таблицы

Continuation of the Table

Уровень модели IoT	Угроза	Техника	Компонент	Риск
	Автоматическое подключение к доступной сети	Существующие учетные записи (T1078)	Датчик / выключатель / камера / др.	High
		Подключение к устройству с помощью инструментов поставщика		
	Вредоносное ПО	ПО для удаленного доступа (T1219)		High
		Несанкционированное использование ресурсов (T1496)		
		Точечный отказ в обслуживании (T1499)		
	Программные уязвимости	Эксплуатация уязвимостей в клиентском ПО (T1203)	ПО датчика / выключателя / камеры / др.	High
		Эксплуатация уязвимостей для повышения привилегий (T1068)		
	Аппаратные уязвимости	Межпроцессное взаимодействие (T1559)	Процессор	High
		Эксплуатация CVE уязвимостей	Процессор / память / чип связи / др.	
	Уязвимости в протоколе связи	Злоумышленник посередине (T1557)	Протокол связи	Critical
		Перехват вводимых данных (T1056)		
Платформа	Уязвимости специализированного ПО	Изучение установленного ПО (T1518)	Плата управления	High
		Эксплуатация уязвимостей в клиентском ПО (T1203)	ПО SCADA	
	Атака на облачное хранилище	Сетевой отказ в обслуживании (T1498)	Облачное хранилище	High
		Несанкционированное использование ресурсов (T1496)		

Окончание таблицы

End of the Table

Уровень модели IoT	Угроза	Техника	Компонент	Риск
		Средства администрирования облака (T1651)	Служба администрирования	
	Атака на центр хранения данных	Эксфильтрация через веб-службу (T1567)	База данных	High
		Шифрование данных (T1486)		
	Программные уязвимости	Эксплуатация уязвимостей в клиентском ПО (T1203)	ПО гипервизора	High
		Эксплуатация уязвимостей для повышения привилегий (T1068)		
	Аппаратные уязвимости	Межпроцессное взаимодействие (T1559)	Плата управления	High
		Эксплуатация CVE уязвимостей		
Управление	Социальная инженерия	Фишинг с целью сбора сведений (T1598)	Пользователь	Critical
		Фишинг (T1566)		
		Выполнение с участием пользователя (T1204)		
	Слабые пароли	Поиск на общедоступных сайтах (T1593)	Онлайн-ресурсы	Critical
		Метод перебора (T1110)	Веб-форма входа	
		Существующие учетные записи (T1078)		
	Веб-уязвимости	Теневая (drive-by) компрометация (T1189)	Веб-интерфейс	Medium
		Подделка учетных данных для веб-ресурсов (T1606)		

ЗАКЛЮЧЕНИЕ

Внедрение IoT в повседневную жизнь открывает новые возможности, но также создает значительные риски. Для их минимизации производителям IoT-устройств необходимо внедрять надежные алгоритмы шифрования,

использовать современные методы идентификации, продолжить и форсировать переход от «легких» небезопасных протоколов к их защищенным версиям (например, MQTTS, CoAPS) и использовать принципы Zero Trust при разработке устройств и развертывании систем с использованием IoT.

Пользователям рекомендуется регулярно обновлять программное обеспечение устройств, включить двухфакторную аутентификацию, использовать фаерволы, отключить неиспользуемые интеграции и расширения и отказаться от использования простых паролей.

Компаниям следует проводить регулярные аудиты безопасности, выделить IoT-устройства в отдельную сеть, использовать сертифицированное оборудование и использовать современные средства защиты от отечественных вендоров.

Как и в случае обеспечения информационной безопасности, одними техническими мерами не обойтись, необходимо обеспечить еще и нормативное (политики безопасности) и организационное сопровождение. Только комплексный подход обеспечит безопасность, надежность и устойчивость IoT-систем.

СПИСОК ЛИТЕРАТУРЫ

1. Рекомендация ITU-T Y.4000/Y.2060: Обзор Интернета. – Июнь, 2012. – URL: https://www.itu.int/rec/T-REC-Y.2060 (дата обращения: 10.06.2025).

2. *Hozdić E.* Smart factory for industry 4.0: a review // International Journal of Modern Manufacturing Technologies. – 2015. – Vol. 7 (1). – P. 28–35. – URL: https://www.researchgate.net/publication/282791888_Smart_factory_for_industry_40_A_review (accessed: 10.06.2025).

3. *Vaishnavi S. Gunge, Pratibha S. Yalagi*. Smart home automation: a literature review // International Journal of Computer Applications. National Seminar on Recent Trends in Data Mining (RTDM 2016). – P. 6–10. – URL: https://scispace.com/papers/smart-home-automation-a-literature-review-2bd4e0mlpp (accessed: 10.06.2025).

4. IoT Analytics. Number of connected IoT devices in 2024: 17 billion globally. – 2024, September 3. – URL: https://iot-analytics.com/number-connected-iot-devices/ (accessed: 10.06.2025).

5. OWASP Foundation. OWASP Internet of Things Project: OWASP IoT Top 10. – URL: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10 (accessed: 10.06.2025).

6. Understanding the Mirai Botnet / M. Antonakakis [et al.] // Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada. – USENIX,

2017. – P. 1093–1110. – URL: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis (accessed: 10.06.2025).

7. *Gandhi V.* 2023 ThreatLabz Report Indicates 400% Growth in IoT Malware Attacks // Zscaler Blog. – 2023, October 24. – URL: https://www.zscaler.com/blogs/security-research/2023-threatlabz-report-indicates-400-growth-iot-malware-attacks (accessed: 10.06.2025).

8. Static analysis for discovering IoT vulnerabilities / P. Ferrara, A.K. Mandal, A. Cortesi, F. Spoto // International Journal on Software Tools for Technology Transfer. – 2020. – Vol. 23 (1). – P. 71–88. – DOI: 10.1007/s10009-020-00592-x.

9. Kaspersky Securelist. Обзор угроз для IoT-устройств в 2023 году. – 2023, 21 сентября. – URL: https://securelist.ru/iot-threat-report-2023/108088/ (дата обращения: 10.06.2025).

10. How AI/ML complements SCADA systems in manufacturing // RapidCanvas. – 2023, July 13. – URL: https://www.rapidcanvas.ai/blogs/how-ai-ml-complements-scada-systems-in-manufacturing (accessed: 10.06.2025).

11. *Miller J.F.* Supply chain attack framework: MITRE technical report. – 2013, December. – URL: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf (accessed: 10.06.2025).

12. Industrial Internet Consortium (IIC). Industrial Internet Reference Architecture (IIRA). – 2022. – URL: https://www.iiconsortium.org/iira/ (accessed: 12.02.2025).

13. National Institute of Standards and Technology (NIST). CVE-2021-45522 Detail // National Vulnerability Database (NVD). – 2021. – URL: https://nvd.nist.gov/vuln/detail/CVE-2021-45522 (accessed: 10.06.2025).

14. Cloudflare Radar. DDoS Threat Report 2025 Q1 / Cloudflare, Inc. – 2025. – URL: https://radar.cloudflare.com/reports/ddos-2025-q1 (accessed: 10.06.2025).

15. *Hejase H.J., Kazan H., Moukadem I.* Advanced Persistent Threats (APT): An awareness // Journal of Economics and Economic Education Research. – 2020. – Vol. 21, iss. 6. – DOI: 10.13140/RG.2.2.31300.65927.

16. Ars Technica. New wave of data-destroying ransomware attacks hits QNAP NAS devices. – 2022. – URL: https://arstechnica.com/information-technology/2022/09/new-wave-of-data-destroying-ransomware-attacks-hits-qnap-nas-devices/ (accessed: 11.06.2025).

17. Protect Against “FrostyGoop” ICS Malware Targeting Operational Technology / Dragos, Inc. – 2024. – URL: https://www.dragos.com/blog/protect-against-frostygoop-ics-malware-targeting-operational-technology/ (accessed: 11.06.2025).

18. Eclipse Foundation. IoT and Embedded Developer Survey Report 2024. – URL: https://5413615.fs1.hubspotusercontent-na1.net/hubfs/5413615/Eclipse%

20IoT%20White%20Papers%20and%20Case%20Studies/IoT%20and%20Embedded%20Survey%20Report%202024.pdf (accessed: 11.06.2025).

19. MQTT vulnerabilities, attack vectors and solutions in the internet of things (IoT) / A.J. Hintaw, S. Manickam, M.F. Aboalmaaly, S. Karuppayah // IETE Journal of Research. – 2021. – Vol. 69 (6). – P. 3368–3397. – DOI: 10.1080/03772063.2021.1912651.

20. Positive Technologies. Киберугрозы для промышленности: Industrial IoT. – 2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-dlya-promyshlennosti-industrial-iot/ (дата обращения: 11.06.2025).

21. National Institute of Standards and Technology (NIST). CVE-2025-27840 Detail // National Vulnerability Database (NVD). – 2025 – URL: https://nvd.nist.gov/vuln/detail/CVE-2025-27840 (accessed: 11.06.2025).

22. MITRE Corporation. Common Vulnerabilities and Exposures (CVE). 2025. – URL: https://cve.mitre.org/ (accessed: 21.03.2025).

23. RTL Nieuws. Verkeerslichten hacken tienduizenden Nederland lek nog jaren te misbruiken. – 2024. – URL: https://www.rtl.nl/nieuws/artikel/5473143/verkeerslichten-hacken-tienduizenden-nederland-lek (accessed: 11.06.2025).

24. Microsoft Security Blog. Storm-0501 ransomware attacks expanding to hybrid cloud environments. – 2024. – URL: https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/ (accessed: 11.06.2025).

25. ФСТЭК России. Банк данных угроз безопасности информации: Уязвимость 2017-01429. – URL: https://bdu.fstec.ru/vul/2017-01429 (дата обращения: 11.06.2025).

26. *Blanton S.* IoT security risks, stats, and trends to know in 2025 // JumpCloud Blog. – 2025. – URL: https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025 (accessed: 11.06.2025).

27. MITRE Corporation. MITRE ATT&CK®: A Knowledge Base of Adversary Tactics and Techniques. – URL: https://attack.mitre.org (accessed: 11.06.2025).

28. OWASP Foundation. OWASP Risk Rating Calculator. – URL: https://www.owasp-risk-rating.com/ (accessed: 11.06.2025).

Кравченко Алексей Алексеевич, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – безопасность киберфизических систем. E-mail: kravchenko.2020@stud.nstu.ru

Пермяков Руслан Анатольевич, ведущий инженер лаборатории искусственного интеллекта и информационных технологий Федерального государственного бюджетного учреждения науки «Институт вычислительной математики и математической геофизики» Сибирского отделения Российской академии наук. Основное направление научных исследований – безопасность киберфизических систем. E-mail: pra@yandex.ru

DOI: 10.17212/2782-2230-2025-2-52-75

Internet of things (IoT): Security threats in automated systems*

A.A. Kravchenko[1], R.A. Permyakov[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Protection. E-mail: kravchenko.2020@stud.nstu.ru*
[2] *ICM&MG SB RAS, 6, Ac. Lavrentieva Prospekt, Novosibirsk, 630090, Russian Federation, Lead Engineer at the Laboratory of Artificial Intelligence and Information Technologies. E-mail: pra@yandex.ru*

The advancement and widespread adoption of Internet of Things (IoT) technology have led to an increasing number of diverse devices being integrated into unified systems, connected to the Internet, and transmitting various data without human intervention. However, consumer-grade devices often fail to ensure the security and confidentiality of transmitted data. The IoT has begun to play a huge role not only in the lives of ordinary people and organizations, but has also provided new opportunities for hackers. The inclusion of millions of devices in DDoS attacks, access to confidential user data, new attack vectors on infrastructure and the ability to bypass standard security measures has turned the IoT from a convenient tool into a source of threats. This article presents an analysis of the threat landscape associated with the use of IoT devices in automated control systems, including key attack scenarios and methods targeting automated systems.

Keywords: IoT, Industrial IoT (IIoT), smart home, cybersecurity, communication protocol, threat landscape, threat model, MITRE ATT&CK

REFERENCES

1. ITU-T Recommendation Y.4000/Y.2060: Overview of the Internet of Things. June 2012. Available at: https://www.itu.int/rec/T-REC-Y.2060 (accessed 10.06.2025).

* *Received 14 May 2025.*

2. Hozdić E. Smart factory for industry 4.0: a review. *International Journal of Modern Manufacturing Technologies*, 2015, vol. 7 (1), pp. 28–35. Available at: https://www.researchgate.net/publication/282791888_Smart_factory_for_industry_40_A_review (accessed 10.06.2025).

3. Vaishnavi S. Gunge, Pratibha S. Yalagi. Smart home automation: a literature review. *International Journal of Computer Applications. National Seminar on Recent Trends in Data Mining (RTDM 2016)*, pp. 6–10. Available at: https://scispace.com/papers/smart-home-automation-a-literature-review-2bd4e0mlpp (accessed 10.06.2025).

4. IoT Analytics. *Number of connected IoT devices in 2024: 17 billion globally*. 2024, September 3. Available at: https://iot-analytics.com/number-connected-iot-devices/ (accessed 10.06.2025).

5. OWASP Foundation. *OWASP Internet of Things Project: OWASP IoT Top 10*. Available at: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10 (accessed 10.06.2025).

6. Antonakakis M., et al. Understanding the Mirai Botnet. *Proceedings of the 26th USENIX Security Symposium*, Vancouver, BC, Canada, 2017, pp. 1093–1110. Available at: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis (accessed 10.06.2025).

7. Gandhi V. 2023 ThreatLabz Report Indicates 400% Growth in IoT Malware Attacks. *Zscaler Blog*, 2023, October 24. Available at: https://www.zscaler.com/blogs/security-research/2023-threatlabz-report-indicates-400-growth-iot-malware-attacks (accessed 10.06.2025).

8. Ferrara P., Mandal A.K., Cortesi A., Spoto F. Static analysis for discovering IoT vulnerabilities. *International Journal on Software Tools for Technology Transfer*, 2020, vol. 23 (1), pp. 71–88. DOI: 10.1007/s10009-020-00592-x.

9. Kaspersky Securelist. *IoT Threat Report 2023*. 2023, 21 September. Available at: https://securelist.ru/iot-threat-report-2023/108088/ (accessed 10.06.2025).

10. How AI/ML complements SCADA systems in manufacturing. *RapidCanvas*, 2023, July 13. Available at: https://www.rapidcanvas.ai/blogs/how-ai-ml-complements-scada-systems-in-manufacturing (accessed 10.06.2025).

11. Miller J.F. *Supply chain attack framework*. MITRE technical report. 2013, December. Available at: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf (accessed 10.06.2025).

12. Industrial Internet Consortium (IIC). Industrial Internet Reference Architecture (IIRA). 2022. Available at: https://www.iiconsortium.org/iira/ (accessed 12.02.2025).

13. National Institute of Standards and Technology (NIST). CVE-2021-45522 Detail. *National Vulnerability Database (NVD)*. 2021. Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-45522 (accessed 10.06.2025).

14. Cloudflare, Inc. *Cloudflare Radar. DDoS Threat Report 2025 Q1*. 2025. Available at: https://radar.cloudflare.com/reports/ddos-2025-q1 (accessed 10.06.2025).

15. Hejase H.J., Kazan H., Moukadem I. Advanced Persistent Threats (APT): An awareness. *Journal of Economics and Economic Education Research*, 2020, vol. 21, iss. 6. DOI: 10.13140/RG.2.2.31300.65927.

16. Ars Technica. *New wave of data-destroying ransomware attacks hits QNAP NAS devices*. 2022. Available at: https://arstechnica.com/information-technology/2022/09/new-wave-of-data-destroying-ransomware-attacks-hits-qnap-nas-devices/ (accessed 11.06.2025).

17. Dragos, Inc. *Protect Against "FrostyGoop" ICS Malware Targeting Operational Technology*. 2024. Available at: https://www.dragos.com/blog/protect-against-frostygoop-ics-malware-targeting-operational-technology/ (accessed 11.06.2025).

18. Eclipse Foundation. *IoT and Embedded Developer Survey Report 2024*. Available at: https://5413615.fs1.hubspotusercontent-na1.net/hubfs/5413615/Eclipse%20IoT%20White%20Papers%20and%20Case%20Studies/IoT%20and%20Embedded%20Survey%20Report%202024.pdf (accessed 11.06.2025).

19. Hintaw A.J., Manickam S., Aboalmaaly M.F., Karuppayah S. MQTT vulnerabilities, attack vectors and solutions in the internet of things (IoT). *IETE Journal of Research*, 2021, vol. 69 (6), pp. 3368–3397. DOI: 10.1080/03772063.2021.1912651.

20. Positive Technologies. Cyber threats to industry: industrial IoT. 2024. (In Russian). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-dlya-promyshlennosti-industrial-iot/ (accessed 11.06.2025).

21. National Institute of Standards and Technology (NIST). CVE-2025-27840 Detail. *National Vulnerability Database (NVD)*. 2025. Available at: https://nvd.nist.gov/vuln/detail/CVE-2025-27840 (accessed 11.06.2025).

22. MITRE Corporation. *Common Vulnerabilities and Exposures (CVE)*. 2025. Available at: https://cve.mitre.org/ (accessed 21.03.2025).

23. RTL Nieuws. *Tienduizenden verkeerslichten in Nederland te hacken, lek nog jaren te misbruiken* [Traffic Light Hack Exposes Data of Thousands of Dutch Citizens]. 2024. Available at: https://www.rtl.nl/nieuws/artikel/5473143/verkeerslichten-hacken-tienduizenden-nederland-lek (accessed 11.06.2025).

24. Microsoft Security Blog. *Storm-0501 ransomware attacks expanding to hybrid cloud environments*. 2024. Available at: https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/ (accessed 11.06.2025).

25. FSTEC of Russia. Vulnerability Database: Vulnerability 2017-01429. (In Russian). Available at: https://bdu.fstec.ru/vul/2017-01429 (accessed 11.06.2025).

26. Blanton S. IoT security risks, stats, and trends to know in 2025. *JumpCloud Blog*, 2025. Available at: https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025 (accessed 11.06.2025).

27. MITRE Corporation. MITRE ATT&CK®: A Knowledge Base of Adversary Tactics and Techniques. Available at: https://attack.mitre.org (accessed 11.06.2025).

28. OWASP Foundation. *OWASP Risk Rating Calculator*. Available at: https://www.owasp-risk-rating.com/ (accessed 11.06.2025).

Для цитирования:

Кравченко А.А., *Пермяков Р.А.* Интернет вещей (IoT): угрозы безопасности в автоматизированных системах // Безопасность цифровых технологий. – 2025. – № 2 (117). – С. 52–75. – DOI: 10.17212/2782-2230-2025-2-52-75.

For citation:

Kravchenko A.A, Permyakov R.A. Internet veshchei (IoT): ugrozy bezopasnosti v avtomatizirovannykh sistemakh [Internet of things (IoT): Security threats in automated systems]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2025, no. 2 (117), pp. 52–75. DOI: 10.17212/2782-2230-2025-2-52-75.