

## Обзор угроз безопасности Интернета вещей

*Х.Х. Пахаев<sup>1</sup>, Т.Г. Айгумов<sup>2</sup>, Э.М. Абдулмукуминова<sup>2</sup>*

<sup>1</sup> ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»

<sup>2</sup> ФГБОУ ВО «Дагестанский государственный технический университет»

**Аннотация:** Концепция Интернета вещей (IoT) была представлена Кевином Эштоном в Массачусетском технологическом институте в 1998 году. Видение концепта состоит в том, что объекты, «вещи», связаны друг с другом и, следовательно, создают IoT, в котором каждый объект имеет свою индивидуальную идентичность и может взаимодействовать с другими объектами. Объекты Интернета вещей могут значительно различаться по размеру от малых до самых крупных. Интернет вещей превращает обычные продукты, такие, как автомобили, здания и машины, в интеллектуальные устройства, подключенные объекты, которые могут общаться с людьми, приложениями и друг с другом. В статье мы рассматриваем распространенность Интернета вещей в современном мире и его влияние на различные отрасли. В документе обсуждается угроза безопасности Интернета вещей, в результате чего будут даны рекомендации по безопасности.

**Ключевые слова:** Интернет вещей, NB-IoT, кибербезопасность, угрозы безопасности, компьютерная безопасность.

Устройства, подключенные к Интернету вещей (IoT), стали неотъемлемой частью повседневной жизни. Интернет вещей быстро растет, поскольку все больше и больше устройств подключаются к глобальной сети. Данные и приложения многих устройств IoT конфиденциальны и должны быть доступны только авторизованным лицам. Эти приложения представляют собой компьютерные программы, использующие условия реального или близкого к реальному времени. Это гарантирует стабильность работы. Приложения используют данные потребителей для анализа и прогнозирования будущего с помощью алгоритмов искусственного интеллекта [1].

В 2014 году Объединенный технический комитет Международной организации по стандартизации (ISO) и Международной электротехнической комиссии (IEC) определил IoT как инфраструктуру объектов, людей, систем и информационных ресурсов, связанных между собой интеллектуальными

услугами, которые позволяют им обрабатывать информацию из физического и виртуального мира и реагировать. На уровне приема IoT датчики, размещенные внутри устройств, объектов и оборудования, собирают, измеряют и записывают информацию о физической среде, такую, как температура, влажность, давление газа и движение. Эту информацию можно читать, интегрировать и анализировать на верхних уровнях IoT [2].

NIST использует два акронима: IoT и NoT (так называемая Сеть вещей). IoT считается подмножеством NoT, поскольку IoT имеет свои «вещи», подключенные к Интернету [3]. Напротив, некоторые типы NoT используют только локальные сети (LAN), при этом ни одна из ваших «вещей» не должна быть подключена к Интернету напрямую.

Рост Интернета вещей обусловлен потребностями бизнеса в рамках цифровой трансформации бизнеса. Общее количество подключений к Интернету вещей вырастет с шести миллиардов в 2015 году до 27 миллиардов к 2025 году. Это означает совокупный годовой темп роста (CAGR) в 16%. Что касается роста рынка, то в отчете Berg Insight прогнозируется увеличение мирового рынка сторонних платформ Интернета вещей с 610 миллионов евро в 2015 году до 3,05 миллиарда евро в 2021 году [4].

Решения IoT не только включают несколько технологических областей, таких, как мобильная связь, облако, данные, безопасность, телекоммуникации и сети, но также ведут к межотраслевому использованию данных, например, данные, созданные в умных домашних и промышленных приложениях, используются в автомобильной отрасли, как показано на рис. 1 [5]. Это открывает возможность создания торговых ассоциаций между горизонтальными отраслями, такими, как операторы связи, и вертикальными отраслями, такими, как производители автомобилей, в качестве новых бизнес-моделей. Цифровая трансформация бизнеса, доступная для Интернета

---

вещей, – это гораздо больше, чем просто использование подключенных объектов: она позволяет разрабатывать инновационные бизнес-модели, которые ранее были невозможны [6].



Рис. 1. – Связь Интернета Вещей с отраслями производства [5]

Безопасность Интернета вещей должна включать не только само устройство Интернета вещей. Устройства Интернета вещей обладают минимальной безопасностью и множеством дефектов. Многие считают, что производители Интернета вещей не ставят во главу угла безопасность и конфиденциальность. Но, несмотря на проблемы безопасности, распространение Интернета вещей не прекращается. Поэтому совершенно необходимо, чтобы профессионалы в области безопасности и пользователи научились обеспечивать большую безопасность.

### Угрозы безопасности IoT

#### *А. Угрозы и проблемы безопасности Интернета вещей*

К трем категориям угроз Интернета вещей относятся:

1. Типичные риски в любой интернет-системе.
2. Специфические риски IoT-устройств.
3. Безопасность для предотвращения повреждений, например, из-за неправильного использования приводов [7].

Традиционные методы обеспечения безопасности, такие, как блокирование открытых портов на устройствах, относятся к первой категории (например, холодильник, подключенный к Интернету для отправки информации о товарах и температуре, может использовать незащищенный SMTP-сервер и может быть скомпрометирован ботнетом).

Ко второй категории относятся проблемы, конкретно связанные с оборудованием IoT, например, подключённое устройство может поставить под угрозу вашу защищенную информацию. Некоторые устройства Интернета вещей слишком малы, чтобы поддерживать правильное асимметричное шифрование. Кроме того, любое устройство, которое может подключаться к Интернету, имеет встроенную операционную систему, реализованную в его прошивке, и многие из этих интегрированных операционных систем не разрабатываются с учетом безопасности в качестве основного соображения [8].

IoT – это набор устройств, подключенных к Интернету, которые собирают и обмениваются данными с помощью узлов и контроллеров. Интернет вещей можно определить, как сеть идентифицируемых физических объектов или «вещей», которые могут взаимодействовать между собой, со внешней средой, или и тем, и другим. Благодаря контроллерам и облачной обработке эти устройства могут «думать» и действовать автономно, а также собирать информацию по нескольким причинам. Свойством многих «вещей» является полная интеграция с операционной системой (ОС) или без нее.

IoT, в основном, собирает данные в режиме реального времени, используя все типы сетей (локальная сеть (LAN), глобальная сеть с низким энергопотреблением (LPWAN), сотовая LPWAN (узкополосный IoT и LTE-M) и сотовая связь) с постоянными или прерывистыми подключениями к облаку. Поэтому необходимо хранить данные с отметкой времени, измерять физические параметры, иметь возможность принимать решения на основе данных, собранных этими устройствами. Это необходимо для достижения автоматизированного принятия решений централизованным способом [9].

#### *Б. Угрозы и атаки безопасности Интернета вещей*

Существует четыре возможных способа возникновения угрозы безопасности в Интернете вещей:

- Физические атаки,
- Атаки на окружающую среду,
- Программные атаки,
- Атаки с помощью криптоанализа.

Современные платформы Интернета вещей создаются с использованием технологических решений от самых разных поставщиков. Некоторые из этих платформ представляют собой эклектичное сочетание повторно используемых компонентов из существующих решений для использования на специально разработанных платформах с надеждой на безопасную совместную работу компонентов. Меры безопасности в компонентах IoT, если они существуют, не были разработаны с учетом подсчета зависимостей, возникающих в результате возможностей подключения IoT. Например, промышленные устройства часто не имеют надлежащих механизмов аутентификации, поскольку они разработаны для использования в физически защищенных и изолированных средах. Другой пример – проблема своевременного предоставления обновлений

программного обеспечения или исправлений безопасности для конечных узлов без снижения функциональной безопасности [10].

Требуются полные методы анализа рисков и угроз, а также инструменты администрирования платформ Интернета вещей. Разработка планов смягчения последствий атак Интернета вещей требует понимания типов атак и последовательности действий, которые происходят при их возникновении. Начнем с рассмотрения классификации атак Интернета вещей. Анализ атак на безопасность помогает понять реальное представление о том, как Интернет вещей создает сети, и это позволяет нам определять планы смягчения.

#### *В. Категоризация атак на этапах IoT-процесса*

В целом, процесс IoT можно рассматривать как пятиэтапную последовательность: от сбора данных до доставки данных конечным пользователям. Разнообразие атак подразделяется на пять фаз IoT:

- восприятие данных,
- место хранения,
- интеллектуальная обработка,
- передача информации,
- сквозная доставка.

#### *Г. Требования безопасности IoT*

Безопасность необходимо решать на протяжении всего жизненного цикла IoT, от первоначального проектирования до запуска сервисов. Например, внедрение функций безопасности следует начинать во время изготовления устройства. Подпись кода и обфускация кода – это некоторые шаги, которым производители могут следовать, чтобы гарантировать, что ваше устройство не взломано или злоумышленник не вставит нежелательный код. Основные требования безопасности в сценариях Интернета вещей включают конфиденциальность и доверие к данным.

### *Д. Конфиденциальность Интернета вещей*

Сохранение конфиденциальности в IoT остается серьезной проблемой. Конфиденциальность подразумевает защищённость личной информации, а также возможность контролировать, что происходит с этой информацией. Проблемы конфиденциальности с системами IoT усложняются тем фактом, что система – это больше, чем сумма ее частей. Соображения о конфиденциальности для устройств низкого уровня могут отличаться от проблем, возникающих на уровне анализа данных. В то же время нарушения конфиденциальности на любом уровне системы влияют на всю систему. С интеллектуальных устройств можно собирать множество частной информации. В современных технологиях Интернета вещей контроль над этой информацией осуществляется слабо. Во многих случаях данные собираются пассивно, и из-за этого некоторые нарушения конфиденциальности могут оставаться незамеченными в течение длительного времени.

Главный вопрос о праве собственности на данные IoT – кто какими данными владеет и кто контролирует, куда эти данные направляются – создает важные проблемы с точки зрения регулирования, этических и финансовых моментов. Конечные пользователи считают, что все данные принадлежат им. Исходные группы производителей считают, что они владеют данными, генерируемыми их конечными точками, или, по крайней мере, имеют права доступа к ним. Во многих случаях поставщики услуг считают, что они владеют данными, как и приложение. Проблемы владения данными поставщиков становятся все более сложными по мере того, как Интернет вещей становится более разнородным. Реализованы системы с большим количеством участников из разных организаций. На старых разобранных и неиспользуемых устройствах все еще может храниться много



конфиденциальной информации, и для них необходимо проводить дезинфекцию данных. [11]

Например, холодильник пользователя сообщает о запасах еды, которую вы едите, а ваш фитнес-браслет передает данные о вашей активности, агрегирование этих потоков данных обеспечивает гораздо более подробное и конфиденциальное описание общего состояния здоровья человека. Этот тип сбора данных становится все более распространенным на потребительских устройствах, таких, как телевизоры с искусственным интеллектом и девайсы с функцией персонального помощника. Эти устройства имеют функции распознавания голоса или «зрение», которые позволяют им постоянно слушать разговоры или наблюдать за деятельностью в комнате и выборочно передавать данные в облачную службу для обработки, в которой иногда участвует третье лицо.

#### *Е. Возможности*

Цель Интернета вещей – улучшить качество жизни и предоставить преимущества потребителям и предприятиям. Интернет вещей помогает достичь следующего:

- Снижение потребления энергии
- Улучшения безопасности и защиты
- Улучшения в автоматизации повседневных задач
- Повышение качества жизни

В этом контексте внедрение Интернета вещей можно разделить на пять типов:

1. Промышленный Интернет вещей: способствует улучшению обслуживания клиентов за счет лучшей адаптации продуктов и услуг для клиентов в более короткие сроки. Улучшение связи и коммуникации между сборочной линией и производством, ставшее возможным благодаря IoT, позволяет производителям быть ближе к рыночному спросу и настраивать то,

---



что они строят, в соответствии с потребностями своих клиентов (например, умный завод) [12].

2. Коммерческий Интернет вещей: включает интеллектуальные коммерческие здания.

3. Интернет вещей в здравоохранении: улучшение ухода за пациентами. Например, устройства IoT соединяют пациентов с системами здравоохранения для непрерывного мониторинга медицинских данных. Пациенты могут делиться своими данными с врачами, медсестрами и членами семьи, а также с машинами и алгоритмами, которые обеспечивают автоматическую обратную связь по обработанным данным.

4. Транспортный Интернет вещей: отслеживает состояние грузового транспорта и при необходимости принимает превентивные меры во время перевозки. Например, устройства IoT могут отслеживать пакеты от начала до конца, чтобы определять температуру, местоположение и т.п.

5. Потребительский Интернет вещей: подключенные устройства потребителя, в том числе смарт-телевизоры, интеллектуальные колонки, игрушки, портативные устройства и другие интеллектуальные устройства.

### **Выводы**

В этой статье представлен обзор угроз безопасности Интернета вещей с точки зрения последних разработок, решений для их устранения и новых технологий в развитии. Он показывает первостепенное значение безопасности при разработке жизнеспособных решений Интернета вещей. Надеемся, данная статья поможет вам выбрать безопасные технологии Интернета вещей для вашей организации.

Применение технологии IoT создает возможности и риски для безопасности, поэтому проблемы с устройствами IoT в отношении безопасности огромны. Тщательная оценка рисков безопасности должна предшествовать любому внедрению Интернета вещей, чтобы гарантировать

---

обнаружение всех соответствующих основных проблем. Без достаточной безопасности и защиты данных, IoT не будет успешным в долгосрочной перспективе. Поэтому перед каждым производителем Интернета вещей стоит задача дополнить все этапы процессов разработки, вплоть до эксплуатации оборудования, соответствующими мерами безопасности. В будущей работе важно разработать структуру для выполнения и оценки рисков безопасности в IoT, чтобы гарантировать конфиденциальность, целостность и доступность.

### **Литература**

1. Tanweer A. A Reliable Communication Framework and Its Use in Internet of Things (IoT). 2018. №3. pp. 1-8.
2. Ryan P.J., Watson R.B. Research Challenges for the Internet of Things: What Role Can OR Play? Systems. 2017. 5(1). pp. 1-24.
3. Куприяновский В.П., Шнепс-Шнеппе М.А., Намиот Д.Е., Селезнев С.П., Синягов С.А., Куприяновская Ю.В. Веб Вещей и Интернет Вещей в цифровой экономике // International Journal of Open Information Technologies. 2017. №5. URL: [cyberleninka.ru/article/n/veb-veschey-i-internet-veschey-v-tsifrovoy-ekonomike](http://cyberleninka.ru/article/n/veb-veschey-i-internet-veschey-v-tsifrovoy-ekonomike)
4. Wegner P. Global IoT market size grew 22% in 2021. IoT Analytics. 2022. URL: [iot-analytics.com/iot-market-size](https://www.iot-analytics.com/iot-market-size)
5. Gloukhovtsev M., IoT Security: Challenges, Solutions & Future Prospects. 2018. С. 1–44.
6. Kumar S., Tiwari P., Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data. 2019. 6(111).
7. Tawalbeh L., Muheidat F., Tawalbeh M., Quwaider M. IoT Privacy and Security: Challenges and Solutions, Applied Sciences, 2020, pp. 1-17.
8. Polat G. Security Issues in IoT: Challenges and Countermeasures. Isaca journal. 2019. pp. 1-7.

9. Менциев А.У., Пахаев Х.Х., Айгунов Т.Г. Угрозы безопасности узкополосного Интернета Вещей и меры противодействия // Инженерный вестник Дона, 2021, №10. URL: [ivdon.ru/ru/magazine/archive/n10y2021/7249](http://ivdon.ru/ru/magazine/archive/n10y2021/7249)

10. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети Интернет и контрмеры (обзор) // Инженерный вестник Дона, 2019, №3. URL: [ivdon.ru/ru/magazine/archive/N3y2019/5859](http://ivdon.ru/ru/magazine/archive/N3y2019/5859)

11. Халиев С.У., Пахаев Х.Х. Информационная безопасность в робототехнике // Инженерный вестник Дона, 2019, №4. URL: [ivdon.ru/ru/magazine/archive/n4y2019/5833](http://ivdon.ru/ru/magazine/archive/n4y2019/5833)

12. Тихонова К.В., Гаранова М.В., Бурдова Д.В., Тихонов Д.А. Оптимизация системы управления объектами недвижимости на основе внедрения технологии блокчейн в учетно-регистрационную процедуру // Инженерный вестник Дона, 2019, №3. URL: [ivdon.ru/ru/magazine/archive/N7y2019/6078](http://ivdon.ru/ru/magazine/archive/N7y2019/6078)

## References

1. Tanweer A. A Reliable Communication Framework and Its Use in Internet of Things (IoT). 2018. №3. pp. 1-8.

2. Ryan P.J., Watson R.B. Research Challenges for the Internet of Things: What Role Can OR Play? Systems. 2017. 5(1). pp. 1-24.

3. Kupriyanovsky V.P., Schneps-Shneppe M.A., Namiot D.E., Seleznev S.P., Sinyagov S.A. International Journal of Open Information Technologies. 2017. No. 5. URL: [cyberleninka.ru/article/n/veb-veschey-i-internet-veschey-v-tsifrovoy-ekonomike](http://cyberleninka.ru/article/n/veb-veschey-i-internet-veschey-v-tsifrovoy-ekonomike).

4. Wegner P. Global IoT market size grew 22% in 2021. IoT Analytics. 2022. URL: [iot-analytics.com/iot-market-size](https://www.iot-analytics.com/iot-market-size)

5. Gloukhovtsev M., «IoT Security: Challenges, Solutions & Future Prospects». 2018. С. 1–44.



6. Kumar S., Tiwari P., Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data. 2019. 6(111).
7. Tawalbeh L., Muheidat F., Tawalbeh M., Quwaider M. IoT Privacy and Security: Challenges and Solutions, Applied Sciences, 2020, C. 1-17
8. Polat G. Security Issues in IoT: Challenges and Countermeasures. Isaca journal. 2019. pp. 1-7.
9. Mentsiev A.U., Pakhaev Kh.Kh., Aygumov T.G. Inzhenernyj vestnik Dona, 2021, №10. URL: [ivdon.ru/ru/magazine/archive/n10y2021/7249](http://ivdon.ru/ru/magazine/archive/n10y2021/7249)
10. Mentsiev A.U., Chebieva Kh.S. Inzhenernyj vestnik Dona, 2019, №3. URL: [ivdon.ru/ru/magazine/archive/N3y2019/5859](http://ivdon.ru/ru/magazine/archive/N3y2019/5859)
11. Khaliev M., Pakhaev Kh. Inzhenernyj vestnik Dona, 2019, №4. URL: [ivdon.ru/ru/magazine/archive/n4y2019/5833](http://ivdon.ru/ru/magazine/archive/n4y2019/5833)
12. Tikhonova K.V., Garanova M.V., Burdova D.V., Tikhonov D.A. Inzhenernyj vestnik Dona, 2019, №3. URL: [ivdon.ru/ru/magazine/archive/N7y2019/6078](http://ivdon.ru/ru/magazine/archive/N7y2019/6078)