

Коновалов Юрий Васильевич,

ФГБОУ ВО «Ангарский государственный технический университет»,
к.т.н., доцент кафедры «Электроснабжение промышленных предприятий»,
e-mail: yrvaskon@mail.ru

Малинин Николай Константинович,

ФГБОУ ВО «Ангарский государственный технический университет», студент гр. ЭЭ-22-1,
Братейко Александр Сергеевич, Корпан Вадим Ярославович,
Ткач Денис Сергеевич, Зайцев Станислав Александрович,
ФГБОУ ВО «Ангарский государственный технический университет», студенты гр. ЭЭ-24-1

КОМПЛЕКСНАЯ СТРАТЕГИЯ БЕЗОПАСНОСТИ

ПРИ ПРИМЕНЕНИИ IoT-ТЕХНОЛОГИИ В ЭНЕРГЕТИКЕ

Konovalov Yu.V., Malinin N.K., Brateiko A.S., Korpan V.Ya., Tkach D.S., Zaitsev S.A.

COMPREHENSIVE SECURITY STRATEGY FOR THE APPLICATION OF IoT TECHNOLOGY IN ENERGY

Аннотация. Рассмотрены варианты решения задачи защиты устройств технологии интернета вещей как наиболее приоритетной в рамках развития комплексной стратегии безопасности в энергетике. Выполнен анализ проблемных аспектов вопроса кибербезопасности и предложены пути их решения.

Ключевые слова: защита, устройства интернета вещей, стратегия, безопасность, энергетика, кибербезопасность.

Abstract. The options for solving the problem of protecting devices of the Internet of Things technology as the most priority in the development of a comprehensive security strategy in the energy sector are considered. An analysis of the problematic aspects of the cybersecurity issue is carried out and ways to solve them are proposed.

Keywords: protection, Internet of Things devices, strategy, security, energy, cybersecurity.

Тренд цифровизации значительного количества отраслей промышленности связан с необходимостью применения технических устройств, которые могут собирать информацию, обрабатывать ее и обмениваться данными между собой, с человеком и серверами в дата-центре или облаке [1-4]. Данная технология получила название промышленного интернета или IoT (Internet of Things – интернет вещей) [5,6].

В 2023 году мировой рынок интернета вещей активно рос, количество подключенных устройств достигло 16,7 млрд. Прогнозы экспертов указывают на то, что к 2027 году число используемых устройств, скорее всего, увеличится до более, чем 29 миллиардов устройств.

К 2030 году глобальный спрос на IoT-решения превысит 620 миллиардов долларов, увеличившись в 3,5 раза за десять лет.

В России компании все чаще применяют IoT-технологии, и, по оценкам института статистических исследований и экономики знаний НИУ ВШЭ, сейчас их

используют уже 16,7% (41,5 тысяч) российских организаций. Наблюдается широкое и постепенное масштабирование IoT-технологий. При этом около 80% от опрошенных специалистов рассматривают задачу защиты устройств интернета вещей как наиболее приоритетную в рамках развития комплексной стратегии безопасности.

Немалую степень озабоченности проявляют заинтересованные лица в вопросе безопасности использования IoT-технологий, а также стабильности связи между устройствами [7].

Проблема безопасности значительно подрывает доверие к интернету вещей, поскольку у представителей бизнеса существуют обоснованные опасения, что хакеры могут красть данные из IoT-систем или устраивать диверсии на производствах, либо атаковать непосредственно потребительские устройства. Объекты энергетики, относящиеся к интеллектуальным устройствам, оснащенные цифровыми датчиками и системами управления, при реализации кибератак могут способствовать развитию системных аварий, массовым отключениям электропитания и получению значительного ущерба на производстве [8-11].

Периодически в средствах массовой информации распространяются сведения о скандалах, связанных со взломом IoT-устройств. В частности, компания LG признала, что ее «умные» телевизоры передают данные третьим лицам, а в США хакер взломал видео-няню и по ночам разговаривал с трехлетним ребенком.

Указанные примеры иллюстрируют проблемы на бытовом уровне, однако производственная сфера подвергается точно таким же опасностям, выражающимся в возможности промышленного шпионажа, создания проблем на производстве, либо возникновения иных актов недобросовестной конкуренции.

Недостаточно эффективное решение вопроса безопасности в итоге может отразиться как на организациях-пользователях, так и на физических лицах, в интересах которых функционируют устройства, обеспечивающие стабильность работы систем энергообеспечения. В связи с этим пользователям IoT-систем еще только предстоит научиться полноценно защищать свои системы.

Кибербезопасностью интернета вещей уже занимается «Лаборатория Касперского» и другие компании. Так, Агентство Европейского союза по сетям и информационной политике при поддержке «Лаборатории Касперского» разработало международные рекомендации по защите промышленного интернета вещей.

Согласно результатам исследования, инциденты с IoT-устройствами входят в тройку угроз с наибольшим финансовым ущербом для компаний, а одной из основных проблем в сфере кибербезопасности промышленных IoT-устройств до сих пор остается отсутствие единых стандартов.

Специалисты отмечают, что на данный момент существует несколько нерешенных аспектов вопроса кибербезопасности, в частности:

- 1) возможность использования уязвимости одного IoT-устройства с целью получения доступа ко всей сети устройств;
- 2) использование незащищенных мобильных технологий;
- 3) использование незащищенной облачной инфраструктуры [12];
- 4) использование небезопасного программного обеспечения;
- 5) стандартные учетные записи от производителя, слабая аутентификация, позволяющие получить доступ любому заинтересованному лицу;
- 6) отсутствие поддержки со стороны производителя для устранения уязвимости;
- 7) значительные затруднения или невозможность обновить программное обеспечение и операционные системы устройств;
- 8) использование текстовых протоколов и ненужных открытых портов передачи данных.

Описанные выше проблемы актуальны для любого сектора экономики, в том числе и для энергетической сферы. Низкий уровень безопасности устройств может повлечь экономические потери всех участников отношений, где используется интернет вещей.

Получив доступ к устройствам, управляющими и контролирующими производство, либо безопасность помещений, коммуникаций злоумышленники могут как спровоцировать остановку технологических процессов, так и аварийные ситуации в жилых домах, производственных помещениях.

Представляется, что решение проблемы безопасности кроется в трех аспектах:

- 1) в установке требований к информационной безопасности IoT-устройств на законодательном уровне;
- 2) разработке новых решений в сфере безопасности производителями IoT-устройств, а также упрощении обслуживания таких устройств;
- 3) соблюдении правил кибербезопасности конечными пользователями IoT-технологий.

Все три задачи должны быть решены в совокупности, в ином случае сделать вывод о полноценном обеспечении надлежащего уровня безопасности IoT невозможно.

Постепенно все три упомянутые категории заинтересованных субъектов подходят к решению обозначенных проблем безопасности. Так, с 1 января 2018 года вступил в силу Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», который был принят с целью

создания отдельных категорий организаций и органов власти, к которым предъявляются повышенные требования в сфере информационной безопасности, в том числе к использованию IoT-технологий.

Кроме того, Федеральной службой по техническому и экспертному контролю разработан проект Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, положения которых призваны описать конкретные стандарты кибербезопасности автоматизированных систем.

С распространением IoT-устройств возрастает и потребность в должном уровне защищенности систем, что отражается в том числе на изготовителях и разработчиках, которые вынуждены подстраиваться под новые требования рынка.

Устаревшие и не отвечающие современным тенденциям информационной безопасности устройства не могут использоваться в технологических процессах в сфере энергетики.

Внедряя эффективные меры, направленные на защиту данных IoT-инфраструктуры на этапе производства, изготовители устройств и программного обеспечения решают множество проблем потребителей.

По наблюдениям специалистов, на данный момент можно говорить о недостаточном уровне обеспечения безопасности, но ожидается позитивная тенденция в решении данного вопроса.

Для конечных потребителей ситуация становится несколько сложнее. Во-первых, их поведение во многом зависит от законодательных предписаний и судебной практики, поскольку вопрос ответственности в разрезе использования IoT-технологий еще только предстоит решить.

Во-вторых, пользователь, будь он обычным горожанином либо специалистом на производстве, сможет, скорее всего, использовать лишь уже готовые решения в сфере информационной безопасности, вложенные изготовителем в IoT-продукты.

До тех пор, пока не станет обычной практикой обеспечение кибербезопасности устройства еще до его использования, не может идти речи о возможности соблюдать требования безопасности самими потребителями.

Конечно же, немаловажным фактором является общий уровень грамотности использования IoT-устройств, который, несомненно, будет расти при общем росте уровня распространенности IoT-систем.

Подводя итог вышесказанному, можно сделать вывод о том, что интернет вещей находится в стадии активного развития, однако эволюционный пик еще далеко впереди, поскольку существует множество проблем, которые будут решаться не одним поколением специалистов отрасли.

Конкретные IoT-устройства применяются в энергетике уже сейчас, однако полноценная реализация всего потенциала технологий интернета вещей будет возможна только при наличии единых стандартов отрасли, установленных на национальном или международном уровне либо же разработанных самими участниками рынка.

До тех пор, пока не поставлена точка в обсуждении действия принципа сетевого нейтралитета, нельзя быть уверенным в том, что данные, передающиеся в рамках IoT-систем, будут достигать конечной цели. Кроме того, уровень информационной безопасности, предоставляемой изготовителями устройств, не слишком высок, что останавливает развитие рынка и технологий интернета вещей.

Однако нельзя не отметить, что общество в целом заинтересовано в прогрессе IoT и предпринимает зависящие от него меры: законодательная база постепенно реформируется, представители сегмента крупного бизнеса вкладывают значительные денежные средства в новые технологии, а специалистами разрабатываются новые принципы взаимодействия и унифицированные протоколы.

Несмотря на активные попытки применения IoT-систем в сфере энергетики, на текущий момент нельзя говорить о том, что эти технологии уже стали традиционной производственной практикой.

Представляется, что в будущем именно благодаря применению систем интернета вещей значительно снизится уровень потребления природных ресурсов, минимизируется риск аварийных ситуаций, а сегодняшние примеры использования IoT станут обычным делом, иллюстрирующим лишь несколько из многих возможностей применения таких технологий.

Главная задача рассматриваемой и активно развивающейся технологии интернета вещей – это сделать сложные рабочие процессы эффективнее: исключить воровство, свести простой к минимуму, повысить безопасность или просто сэкономить электричество.

ЛИТЕРАТУРА

1. **Коновалов, Ю.В.** Тенденции развития мировой энергетики в современных условиях / Ю.В. Коновалов, Н.В. Буякова, Н.К. Малинин, А.А. Терехова, А.С. Хухрянская, Д.А. Марченко // Сборник научных трудов Ангарского государственного технического университета. 2024. № 21. – С. 302-308.

2. **Устинов, Д.А.** Вероятностные характеристики энергопотребления нефтегазодобывающих предприятий / Д.А. Устинов, Ю.В. Коновалов, И.Г. Плотников, А.В. Турышева // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. 2011. № 4 (135). – С. 90-94.

3. **Коновалов, Ю.В.** Применение цифровых регуляторов для оптимального использования компенсирующей способности синхронных двигателей совместно с конденсаторными батареями / Ю.В. Коновалов // Вестник Иркутского государственного технического университета. 2010. № 7(47). – С. 175-182.

4. **Коновалов, Ю.В.** Автоматизация и цифровизация объектов электроэнергетики / Ю.В. Коновалов, А.Е. Вайгачев, А.А. Уваров // Вестник Ангарского государственного технического университета. 2021. № 15. – С. 51-55.

5. Интернет вещей — что это такое и как применять IoT в реальном бизнесе // <https://rb.ru/longread/iot-cards/>.

6. Интернет вещей важнее искусственного интеллекта и робототехники // <http://www.forbes.ru/tehnologii/356213-internet-veshchey-vazhnee-iskusstvennogo-intellekta-i-robotot>.

7. **Kononov, Y.V.** The role of human factor in ensuring the safety of electric power objects after their intellectualization / Y.V. Kononov, N.V. Kuznetsova // Proceedings of IFOST-2016. 11-th International Forum on Strategic Technology. 2016. – С. 378-381.

8. **Коновалов, Ю.В.** Искусственный интеллект в электроэнергетике / Ю.В. Коновалов, А.Е. Вайгачев // Современные технологии и научно-технический прогресс. 2021. № 8. – С. 225-226.

9. **Коновалов, Ю.В.** Электрооборудование и автоматизация архитектуры интернета энергий и ее преимущества в России / Ю.В. Коновалов, Н.С. Жуков // Повышение эффективности производства и использования энергии в условиях Сибири. Материалы Всероссийской научно-практической конференции с международным участием. Иркутск. 2024. – С. 64-69.

10. **Коновалов, Ю.В.** Интеллектуальная электрическая сеть / Ю.В. Коновалов, М.С. Леб, И.Н. Потапов // Современные технологии и научно-технический прогресс. 2023. № 10. – С. 213-214.

11. **Крюков, А.В.** Применение интеллектуальных технологий для электротехнических комплексов на нефтегазодобывающих предприятиях / А.В. Крюков, Ю.В. Коновалов // Сборник научных трудов Ангарского государственного технического университета. 2018. Т.1. № 15. – С. 162-169.

12. **Kononov, Yu.V.** Cloud technologies in energy / Yu.V. Kononov, O.A. Zasukhina // Journal of Physics: Conference Series. 13. Сер. "Computer-Aided Technologies in Applied Mathematics". 2020. – С. 012024.