С. Е. Белевец, А. А. Оленников
Тюменский государственный университет, г. Тюмень
УДК 004.056

АНАЛИЗ СУЩЕСТВУЮЩЕЙ НОРМАТИВНО-ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ ДЛЯ IIoT РАБОТАЮЩИХ НА РЫНКЕ РФ

Аннотация. Все больше компаний стремятся повысить свою конкурентоспособность и производительность с помощью технологий интернета вещей, однако уровень безопасности, как говорят эксперты, не повышается и обеспечен слабо. Нормативная составляющая и сертификация IoT (промышленных и пользовательских) до сих пор остается открытым вопросом, что может привести к неблагоприятным последствиям для компании и пользователей.

Ключевые слова: интернет вещей, нормативно-технические документы, автоматизированная система управления технологическим процессом (АСУ ТП), информационная безопасность, сертификация, IoT, промышленный интернет вещей (IIoT), кибератака.

Введение. Сегодня сфера интернета вещей развивает быстрыми темпами, появляется все больше подключенных к интернету устройств. Люди стараются оптимизировать как можно больше технических процессов для получения выгоды [1]. Вместе с пользовательскими IoT развиваются и промышленные и тогда речь заходит о глобальной безопасности [2]. Оборудования оснащают контроллерами и интерфейсами, чтобы следить за состоянием предприятия, ведь в некоторых производствах даже малейшие изменения в функционировании оборудования могут привести к серьезным потерям со стороны финансов или людей [3,4]. Происходит подобное как по вине не налаженного администрирования, так и вследствие хакерской атаки [5]. Все это возможно предотвратить внедрением нормативно-технической документации на законодательном уровне [3].

Проблема исследования. В России действует система, в основе которой следование указам правительства, когда речь заходит о промышленной инфраструктуре. И несмотря на то, что уже несколько лет в разные сферы деятельности внедряется IIoT, не существует единой сертификации и четкой системы функционирования для

промышленного интернета вещей. Целью данного исследования является анализ отечественных и зарубежных решений в области безопасности, касающихся промышленного интернета вещей, для сбора сведений о том, как разные страны приближаются к стандартам безопасности IIoT.

Материалы и методы. Основной целью данный работы является анализ существующих нормативно-технических документов зарубежных вендоров, как действующих, так на рекомендательной основе, а также оценить их подходы к составлению и внедрению таких документов, чтобы выявить общие нормы для безопасности IIoT в России и оценить готовность рынка к обеспечению надлежащей безопасности. Для составления анализа прежде всего необходимо изучить состояние рынка с участием IIoT в РФ и зафиксировать существующие пробелы в безопасности, выявленные на умном производстве, а также провести сравнение с существующими стандартами и развитием безопасности IIoT за пределами России.

Сегодня IoT стал незаменимым атрибутом на производстве, будь то система умного дома или какие-то решения в сфере промышленности, в сельских и других отраслях. При внедрении таких технологий первое, о чем должен думать пользователь и производитель, достаточно ли безопасно разработанное устройство. Если рассматривать пользовательские IoT, иными словами интернет вещей, применимый в быту, то приоритет безопасности отдается конфиденциальности и на основании данного приоритета разрабатываются соответствующие требования к устройствам и их функционалу (те же стандарты политики конфиденциальности). Однако приоритеты промышленного интернета вещей представляют собой доступность, целостность, аутентичность и затем конфиденциальность. Говоря простым языком, IIoT первостепенно обязаны выполнять соответствующие организационно-технические мероприятия и трансформации на производстве, включая введение четкой сертификации и стандартизации продуктов на правовом уровне.

С какими проблемами безопасности сталкивается Российский рынок во время использования IIoT.

Как было сказано выше, подход в работе с промышленным интернетом вещей отличается от пользовательских. Используется

уникальное сетевое оборудование и протоколы [4]. Важнейшим аспектом является их устойчивая работа, а именно, как и какой контроллер может отработать ту или иную атаку, учитывая уже имеющуюся нагрузку с базового устройства, а также устойчиво или со сбоями будет работать контроллер.

В производстве могут использоваться устаревшие устройства, однако выполняющие свой функции. Проблема состоит в отсутствии поддержки и обновлений со стороны производителя. Причиной могут быть санкции или отказ от старых технологий. Обновление должно быть регулярным и поставляться из надежных источников во избежание появления новых дыр в безопасности.

Механизмы отката к старой версии и другие уязвимости прошивки приводят к искусственному раскрытию доступа к контроллерам для внешних сетей, неустойчивой работе, а следовательно, и ошибкам саботажного характера (сбои, временные задержки, коррекции параметров). Особенно остро этот вопрос стоит в отношении зарубежных прошивок, протоколы шифрования которых не поддерживаются в России.

В следствии отсутствия норм обеспечения безопасности промышленных IoT в России на законодательном уровне, компании продолжают нести потери активов и другие последствия. Среди угроз, характерных для IIoT также отмечают [5]:

- Выход из строя элементов системы или отказ в обслуживании;
- Непреднамеренные повреждения вследствие ошибки администрирования, конфигурации или использования;
- Отключение электропитания или сервисов;
- Природные, техногенные и другие катастрофы;
- Ошибки в работе как со стороны провайдера, так и программного обеспечения;
- Взлом системы, сбор информации;
- Вывод из строя путем физических атак;
- Угрозы на законодательном уровне, такие как несоблюдение договорных требований производителя или несоблюдения местных законов, нормативных актов.

Обеспечение безопасности предоставляемых устройств должен брать на себя производитель. Однако этот факт мотивирует их не так

сильно, как повышение своей производительности и быстрый выход на рынок. По данным аналитиков J'son & Partners Consulting количество подключенных устройств интернета вещей в России составило почти 30 млн, это рост на 16% в 2021 г., в сравнении с 2020. Количество желающих автоматизировать свое производство растет крайне быстро и прослеживается тенденция выстраивания приоритета, в котором сокращение сроков окупаемости умного производства превыше безопасности. Данная проблема существует в силу того, что отсутствует стандарт тестирования умных устройств как до начала эксплуатации, так и в процессе использования.

Человеческий факто продолжает быть частью угроз безопасности информационных систем. Внедрение новых технологий интернета вещей приводит к тому, что производственные работники и инженеры вынуждены работать с новыми типами данных, интерфейсами, системами и сетями новыми способами. Регулирование этого вопроса и поддерживание актуальных знаний сотрудников крайне важно, так как некоторые работники не знают о рисках, связанных со сбором, анализом и обработкой таких данных и систем.

Это не означает, что компании, использующие умное производство, не осуществляют тестирование своих технических продуктов или решений и не проводят организационно-технические мероприятия для сотрудников. Однако привлекаемые специалисты в области безопасности умного производства опираются скорее на свои знания и обобщенные стандарты, нежели на регламентированные документы, отвечающие всем требованиям в работе с производственными IoT.

Какие нормативные документы и сертификации действуют в России

Первым этапом в создании стандарта обеспечения безопасности как промышленных, так и пользовательских IoT является введение терминологии и определений. В России на данный момент нет четкой терминологии для интернета вещей. В национальных стандартах РФ просматривается только аббревиатура технологии IoT как технология интернета вещей. Промышленный IoT не выделен как значимый объект КИИ, то есть ему не присвоена категория значимости, и он не включен в реестр значимых объектов критической

информационной инфраструктуры. В федеральных законах IIoT также не определен, однако если интернет вещь применяется на предприятии, отнесенном к КИИ, то выполняются соответствующие федеральные законы. Это 187-ФЗ «О КИИ», 152-ФЗ «О персональных данных» и 149-ФЗ «Об информации, информационных технологиях и о защите информации». Также можно отнести к приказам ФСТЭК номер 235 и 239, обеспечивающие требования к созданию систем и обеспечению безопасности значимых объектов КИИ в Российской Федерации.

Действующий стандарт ISO/IEC 27001, призванный поддерживать и улучшать подходы к рискам в процессе создания, внедрения, функционирования, мониторинга, анализа и поддержки информационной безопасности. Данный стандарт также содержит требования к производителям и высшему руководству обязывая предоставлять гарантии, что система менеджмента ИБ выполняется надлежащим образом.

Не так давно в России пытались внедрить стандарт LaRaWan как протокол для высокоемких сетей, чтобы в одной сети находились миллионы устройств. Однако несмотря на преимущества, вроде низкого энергопотребления и большого радиуса действия, большинство крупных операторов связи не стали переходить на LaRaWan, посчитав его небезопасным (работал на нелицензированных частотах). Вместе с этим протокол высокоемкой сети начал приводить к убыткам, так как от сети не требовалось поддержания миллионов устройств. В будущем к сети будет подключаться все больше устройств, но пока что важно предоставлять применимые и уместные решения для разработчиков и производителей.

Развитие безопасности промышленного интернета вещей в России происходит не так быстро, как хотелось бы, однако продолжает спонсироваться и модернизироваться. До 2030 года в промышленный IoT планируется вложить 90 млрд рублей, а также увеличить долю рынка отечественных индустриальных решений на 30% [6]. Продвижение в защите IIoT будет также со стороны федеральных органов власти: ФСТЭК будет выделено 400 млн рублей на создание банка угроз и уязвимостей безопасности как для АСУ ТП, так и для промышленных интернет вещей.

Техническим комитетом «Кибер-физические системы» в рамках проекта «Программы национальной стандартизации на 2020 год» было разработано общее положение «Информационные технологии. Интернет вещей промышленный. Общее положение», призванное описать общие принципы развития инновационных технологий сетей в области IIoT [6]. Данный стандарт разработан на основе международного (национальный стандарт Великобритании) ISO/IEC TR 30166:2020 «Интернет вещей. Промышленный интернет вещей».

Правовое регулирование стандартов интернета вещей позволило бы слаженно и достаточно безопасно функционировать большому количеству устройств, сократив при этом время реагирования на инциденты и время восстановления. А также упразднить недобросовестное отношение производителей и высшего руководства к безопасности устройств на этапе проектирования, не уступая качественным характеристикам.

Развитие безопасности интернета вещей в других странах

У каждой страны свое представление о том, кто и как должен формировать безопасность интернет вещей. Подход Великобритании схож с Российским, где весь процесс разработки стандартизации и сертификации отдают в руки государства и следуют соответствующему регламенту.

Другие страны Евросоюза применяют обратную стратегию и предлагают напрямую производителям разрабатывать стандарты и нормы для пользовательского и промышленного IoT. Исходя уже из анализа, проведенного ими, формируются регламенты. ЕС стремится обеспечить безопасность интернет вещей и ускорить развитие в этой области посредством многочисленных политических действий, включая создание альянсов и экспертных центров, разработку нормативных документов и запуск пилотных проектов. В исследовании ENISA “Надлежащие практики обеспечения безопасности Интернета вещей в контексте умного производства”[3] важный вклад и обратную связь внесло множество крупных и авторитетных компаний: CISCO, Microsoft Corporation, Kaspersky Lab, Internet Society, NATO Energy Security Center of Excellence, IBM, Huawei Technologies Co., Ltd., European Organization for Nuclear Research

(CERN), Applied Risk, 443 Consulting, Federal agency for information security (BSI) и многие другие. Однако большинство документаций, предлагаемые ENISA все же посвящены безопасности пользовательских IoT.

США и Индия не стремятся к формированию отдельных отраслей права для регулирования интернета вещей, но принимают участие в решении вопросов кибербезопасности. Ярким примером инициатив Министерства внутренней безопасности США, а также NIST и других организаций выступают различные публикации: «Стратегические принципы обеспечения безопасности интернета вещей», «Производственный профиль системы кибербезопасности», «Руководство по кибербезопасности устройств IoT для федерального правительства» и многие другие документы. Не рассмотренные страны продвинулись в сертификации пользовательских IoT [7].

Результаты. В ходе исследования были изучены слабые стороны безопасности промышленного интернета вещей и как нормативно-технические документации поспособствуют их минимизации. Отмечено, как быстрый рост урегулирования документации отстает от внедрения различных IIoT и как это влияет на работу специалистов по безопасности, производственные процессы, оборудование и общую готовность производственного рынка. Результатом работы стал анализ того, как разные страны относятся к процессу создания и внедрения сертификации и технических документов

Заключение. Сегодня, в силу роста применения умных вещей, критически необходим баланс между техническими характеристиками и безопасностью. Такой баланс обеспечит официальная нормативно-техническая документация, что приведет к надежному и целостному функционированию промышленного производства.

СПИСОК ЛИТЕРАТУРЫ

1. Пастух С.Ю. Рыночный потенциал интернета вещей / С.Ю. Пастух, Е.Е. Володина [и др.]. Текст : электронный //Электросвязь. — 2016. — № 9. — С. 28-32. — URL: http://nirit.org/wp-content/uploads/2016/03/123.pdf (дата обращения 10.05.2023).
2. Panchal A.C. Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures / A.C. Panchal, V.M. Khadse, P.N. Mahalle.

IEEE Global Conference on Wireless Computing and Networking. — Text : electronic // IEEE. — 2018. — P. 124-130.
3. Сексембаева М. А. Особенности обеспечения безопасности в промышленном Интернете вещей / М. А. Сексембаева. — Текст : электронный // E-Scio. — 2019. — № 5 (32). — С. 382-394. — URL: https:// cyberleninka.ru/article/n/osobennosti-obespecheniya-bezopasnosti-v-promyshlennom-internete-veschey/viewer (дата обращения: 01.04.2023).
4. Наралиев Н.А., Самаль Д.И. Обзор и анализ стандартов и протоколов в области Интернет вещей. Современные методы тестирования и проблемы информационной безопасности IoT / Н.А. Наралиев, Д.И. Самаль. — Текст : электронный // International Journal of Open Information Technologies. — 2019. — Т. 7, № 8. — С. 94-104. — URL: https:// cyberleninka.ru/article/n/obzor-i-analiz-standartov-i-protokolov-v-oblasti-internet-veschey-sovremennye-metody-testirovaniya-i-problemy-informatsionnoy/viewer (дата обращения: 01.04.2023).
5. Good Practices for Security of Internet of Things in the context of Smart Manufacturing / The European Union Agency for Network and Information Security. — URL: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot (date of the application 20.04.2023). — Text : electronic.
6. CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. / European Telecommunications Standards Institute. — URL: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (date of the application 20.04.2023). — Text : electronic.
7. Panorama of IoT cyber security regulations across the world. / cetome. — URL: https://cetome.com/panorama (date of the application 01.05.2023). — Text : electronic.
8. Консорциум кодекс : Электронный фонд актуальных правовых и нормативно-технических документов: [сайт]. — URL: https://docs.cntd.ru/ (дата обращения 01.05.2023). — Текст: электронный.
9. Начато публичное обсуждение стандарта «Интернет вещей промышленный. Общие положения». — Текст: электронный // Технический комитет 194 : официальный сайт. — 2020. — URL: http://tc194.ru/iot_general (дата обращения 03.04.2023).
10. Tadviser: Государство. Бизнес. Технологии : [сайт]. — URL: https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_Internet_of_Things_(IoT) (дата обращения 02.04.2023). — Текст : электронный.