

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ В СФЕРЕ ПРОИЗВОДСТВА

А.В. Виноградский, Мустафа Абдулкадим Аль-Амиди Дхаир, Аль-Судани Зайд
Али Хуссейн

Кафедра «Защита информации», РТУ «МИРЭА», г. Москва

Аннотация. В данной статье рассмотрены основные проблемы безопасности при применении технологии интернета вещей в сфере производства, а также возможные негативные последствия, которые могут быть вызваны данными проблемами.

Ключевые слова: умное производство, технологии в промышленности, интернет вещей, IoT.

SECURITY PROBLEMS OF THE INTERNET OF THINGS IN THE FIELD OF PRODUCTION

A.V. Vinogradskiy, Mustafa Abdulkadhim Al-Ameedee Dhahir., Al-Soudany Zaid
Ali Hussein

Department of Information security, RTU MIREA, Moscow

Abstract. This article discusses the main security problems in the application of Internet of Things technology in the field of production, as well as possible negative consequences that may be caused by these problems.

Keywords: smart manufacturing, industrial technologies, Internet of things, IoT.

Интернет вещей (IoT), как технология стремительно проникает в различные отрасли и сферы. Идея создания “умного производства”, а также использования “умных” устройств в сфере промышленного производства уже давно не является чем-то новым. Умные сенсоры, устройства мониторинга и автоматизированные системы управления могут значительно повысить эффективность в промышленности. Технология Интернета вещей способна значительно упростить многие процессы в сфере производства различных продуктов, но также данная технология создаёт большой простор для проблем с информационной безопасностью. В данной статье будут рассмотрены основные проблемы, связанные с безопасностью IoT в сфере производства.

Уязвимости устройств – одна из основных проблем, свойственных технологии интернета вещей. Здесь серьёзную роль играет экономия производителей на безопасности. Заинтересованность производителей в первой очереди в разработке устройств за наименьшую себестоимость в кратчайшие

сроки. Так как такой продукт направлен на массового потребителя, не погруженного в вопросы безопасности, большинство производителей просто пренебрегают внедрением достаточных ресурсов и систем безопасности, в силу их дороговизны. По тем же причинам многие устройства интернета вещей имеют ограниченные ресурсы, что затрудняет последующее внедрение сложных механизмов защиты. Часто они используют устаревшие операционные системы или программное обеспечение с известными уязвимостями. Это делает их легкой мишенью для злоумышленников, которые могут получить доступ к системам управления и манипулировать ими. Данная проблема особенно актуальна на крупных промышленных предприятиях, где нарушение работы даже одного устройства может сильно повлиять на важные процессы.

Сбор и передача данных – это одни из ключевых аспектов работы IoT в производстве. Безопасность этих данных закономерно часто оказывается под угрозой. Исходя из слабой защищенности и значительных объёмов информации в IoT-системах, технология представляет большую область для возможных утечек информации. Такая информация, как характеристики продукта, условия обработки или данные контроля качества могут быть перехвачены, что может привести к утечке ценной информации. Всё это может привести к промышленному шпионажу со стороны конкурентов и даже к последующим финансовым потерям для производителя.

Существуют также серьёзные инфраструктурные риски. Интернет вещей в производстве зависит от сложной инфраструктуры, включающей в себя облачные сервисы и локальные сети. Атаки на эти инфраструктуры могут привести к серьёзным сбоям в работе, как отдельных устройств, так и целой экосистемы. Самым простым примером послужит ситуация, если злоумышленники получают доступ к центральной системе управления экосистемой, тогда они могут отключить важные датчики или коммуникации, что может испортить целые партии продукта.

Очевидным решением для обеспечения безопасности является создание нормативов, которым должны соответствовать IoT-системы. В сфере IoT существует проблема отсутствия законодательных актов, норм, стандартов и правил. На данный момент практически отсутствуют стандарты и законодательные акты, которые могли бы урегулировать процесс создания безопасных устройств и их внедрения. Что крайне затрудняет оценку рисков и выработку общих рекомендаций по защите. То же самое применимо и к процессу построения IoT-инфраструктур в производственной сфере, из-за чего крайне сложно обеспечить должный уровень безопасности даже на крупном предприятии. Без четких регуляторных норм и стандартов, производители рискуют сталкиваться с различными угрозами, которые могут привести к потере данных или даже саботажу операций.

Одной из актуальных проблем также является проблема совместимости устройств. Существует большое разнообразие устройств и протоколов связи, используемых в IoT. Из-за такого разнообразия, а также отсутствия нормативов и стандартов по построению IoT-систем образуются серьёзные проблемы для

совместимости устройств, а также интеграции новых. Все эти факторы также затрудняют интеграцию систем безопасности и могут создавать «белые пятна», которые злоумышленники могут использовать для своих атак. Без стандартов безопасности и сертификации устройства могут оказаться уязвимыми.

Как и любая экосистема, IoT требует постоянного обслуживания и обновления. Данная концепция относительно нова и специалистов в области данной технологии недостаточно, при этом существующим специалистам часто не хватает знаний в области информационной безопасности, из-за чего даже настроенная правильно система может иметь множество проблем с безопасностью. Проблема обслуживания вызвана не только недостатком квалифицированных специалистов, но и сложностями с обеспечением безопасности ПО и при дальнейшем обновлении IoT-устройства. На данный момент только растёт количество выпускаемых решений для IoT. Отсюда следует и следующая проблема - обеспечить безопасность при установке обновлений к IoT достаточно сложно, как правило специфика пользовательских интерфейсов, доступных пользователям, не позволяет использовать традиционные механизмы обновления.

Необходимо также учитывать и социальные аспекты внедрения IoT в производство. Большинство работников не имеют должных знаний и компетенций при работе с технологиями интернета вещей. Этот фактор также часто усугубляется отсутствием необходимых мероприятий и правил в условиях производственного сектора. Отсутствие правил и политики безопасности при работе с IoT-устройствами вызывают значительные проблемы и увеличивают вероятность человеческого фактора при работе с IoT-устройствами.

Выводы

Технологии IoT предоставляют большой спектр возможностей для реализации полезных функций в сфере производства какого-либо продукта. Но несмотря на все преимущества, которые предоставляет интернет вещей в промышленной сфере, проблемы безопасности остаются актуальными и требуют значительного внимания. Концепция на данный момент, крайне слабо защищена, и проблемы, которые могут возникнуть в процессе её эксплуатации могут быть крайне серьёзны при применении её в сфере производства. Для решения этих проблем необходимо разрабатывать и внедрять комплексные меры по защите устройств и данных, обеспечивать обучение сотрудников и проведение соответствующих мероприятий в области кибербезопасности и сотрудничать с производителями оборудования для улучшения безопасности их продуктов. Только так можно будет минимизировать риски и обеспечить устойчивое развитие IoT-технологий в сфере производства.

Список литературы

1. Федотов Н. Н. Форензика – компьютерная криминалистика. Москва : Юридический Мир, 2007. 432 с.

2. Росляков А.В., Ванышин С.В., Гребешков А.Ю. Интернет вещей : учебное пособие по направлению подготовки «Инфокоммуникационные технологии и системы связи» 11.03.02 – бакалавриат и 11.04.02 – магистратура. Самара: ПГУТИ, 2015. 136 с.

3. Nieto A., Rios R., Lopez J. IoT-Forensics Meets Privacy: Towards Cooperative Digital Investigations // Sensors. 2018. Vol. 18, issue 2. 492. doi:10.3390/s18020492.

References

1. Fedotov N. N. Forensics – computer forensics. Moscow : Yuridicheskiy Mir, 2007. 432 p.

2. Roslyakov A.V., Vanyashin S.V., Grebeshkov A.Yu. Internet of Things : textbook in the field of training "Infocommunication technologies and communication systems" 03/11/02 – bachelor's degree and 04/11/02 – master's degree. Samara: PGUTI, 2015. 136 p.

3. Nieto A., Rios R., Lopez J. IoT-Forensics Meets Privacy: Towards Cooperative Digital Investigations // Sensors. 2018. Vol. 18, issue 2. 492. doi:10.3390/s18020492.