УДК 004.05

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Башлыкова А.А., Рожок А.А.

МИРЭА - Российский технологический университет, 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: bashlykova_a_a_mirea@mail.ru, ed4mky@yandex.ru

Статья посвящена обзору проблем в функциональной безопасности интернета вещей. Основной целью статьи является анализ существующих проблем в функциональной безопасности интернета вещей, выявление причин данных проблем. В статье рассмотрены подходы к архитектуре интернета вещей, проанализированы существующие проблемы в безопасности протоколов интернета вещей, предложены пути повышения функциональной безопасности интернета вещей.

Ключевые слова: интернет вещей, функциональная безопасность, архитектура интернета вещей, протоколы передачи данных, информационная безопасность, индустрия 4.0

ACTUAL PROBLEMS OF FUNCTIONAL SAFETY IN THE INTERNET OF THINGS

Bashlykova A.A., Rozhok A.A.

MIREA - Russian Technological University, 119454, Moscow, 78 Vernadskogo Avenue, Russia e-mail: bashlykova_a_a_mirea@mail.ru, ed4mky@yandex.ru

The article contains an overview of the problems in the functional safety of the Internet of Things. The main purpose of the article is to analyze the existing problems in the functional security of the Internet of Things, to identify the causes of these problems. The article discusses approaches to the architecture of the Internet of Things, analyzes the existing problems in the security of IoT protocols, suggests ways to improve the functional security of the Internet of Things.

Key words: internet of things, functional safety, architecture of the internet of things, data transfer protocol, information security, industry 4.0

Введение

Интернет вещей – обширное понятие, которое подразумевает собой совокупность различных устройств, взаимодействующих с окружающей средой и обменивающихся друг с другом информацией по специальным технологиям передачи данных [6]. Появление интернета вещей на рынке IT-систем существенно повлияло на повседневную жизнь людей. Например, приложения для «умного дома», взаимодействующие с различными устройствами, такие как термостаты, замки, переключатели, системы наблюдения, автоматизируют большинство рутинных операций. Несмотря на широкое распространение, интернет вещей до сих пор вызывает у специалистов сомнения по поводу безопасности. Огромное количество уязвимостей в IoT системах ставит под вопрос дальнейшую интеграцию этих систем в различные сферы, поэтому необходимо провести анализ существующих проблем функциональной безопасности в IoT системах, а также предложить различные пути повышения функциональной безопасности.

Концепция IoT систем

Для рассмотрения IoT систем с точки зрения функциональной безопасности, важно понять архитектуру таких систем. Концепция IoT системы заключается в том, что к единому центру обработки данных через специальные шлюзы подключается определенное количество устройств, способных реагировать на окружающую среду. На рисунке 1. представлена многоуровневая эталонная схема интернета-вещей.

Модель состоит из четырех уровней, а также возможностей управления и безопасности системы:

- уровень периферийного оборудования;

– сетевой уровень;
– уровень услуг;
– уровень приложений.

Каждый уровень имеет свои собственные компоненты, стандарты связи и протоколы.

Рисунок 1. Многоуровневая эталонная схема интернета-вещей

Первый уровень – всевозможное периферийное оборудование, такое как RFID, этикетки со штрих-кодом, исполнительные механизмы и интеллектуальные устройства. Предполагается, что в будущем все устройства будут поддерживать IPv6.

Второй уровень – сеть и передача данных. Данные могут передаваться как по проводной, так и беспроводной связи. Чаще всего используются беспроводные протоколы CAN bus, OPC UA, BLE, WiFi, Bluetooth, LPWAN, Sigfox, ZigBee, Zwave. Важным элементом является шлюз - сетевое оборудование, которое выполняет множество функций, таких, как объединение десятков датчиков или интеллектуальных устройств. Конфигурация шлюза может настраиваться индивидуально под каждый проект. Одно из основных преимуществ использования IoT-шлюзов – это возможность агрегации данных, поступающих от других устройств.

Уровень услуг обеспечивает связь между датчиками и уровнем приложений. Прикладной уровень содержит приложения IoT и использует различные протоколы, такие как протокол ограниченного приложения (CoAP), протокол передачи телеметрии очереди сообщений (MQTT), протокол расширенной очереди сообщений (AMQP) и протокол расширяемого обмена сообщениями и присутствия (XMPP).

Уровень приложений предоставляет пользователю все необходимые данные о состоянии системы, а также различные интерфейсы для совершения каких - либо действий. В большинстве IoT систем представляет собой мобильное приложение, подключающееся в облако, где происходит обработка данных. В промышленных системах представляет собой специальный пост, на котором через интерфейс происходит взаимодействие пользователя с системой.

Концепция Индустрии 4.0

Индустрия 4.0 - название текущей тенденции автоматизации и обмена данными в производственных технологиях, включая киберфизические системы, интернет вещей, облачные вычисления, искусственный интеллект [4]. Данная концепция подразумевает интеграцию в автоматизированные системы управления технологическим процессом современные информационные технологии. На рисунке 2 изображена общая концепция Индустрии 4.0.

Концепция Индустрии 4.0, по большей части схожа с стандартной концепцией интернета вещей, но все же имеет свои особенности. Во-первых, к системе на уровне периферии предъявляются жесткие требования, особенно к функциональной безопасности в соответствии с международным стандартом IEC 61508. Во-вторых, в индустрии 4.0 активно используются киберфизические системы, таких как шлемы с дополненной реальностью, промышленные экзоскелеты и т.п. В-третьих, производство интегрируется с достаточно сложной ERP системой предприятия. Интеграция с ERP системами в настоящее время затруднена, так как модули большинства таких систем и их архитектура недостаточно гибкие и масштабируемы для Индустрии 4.0.

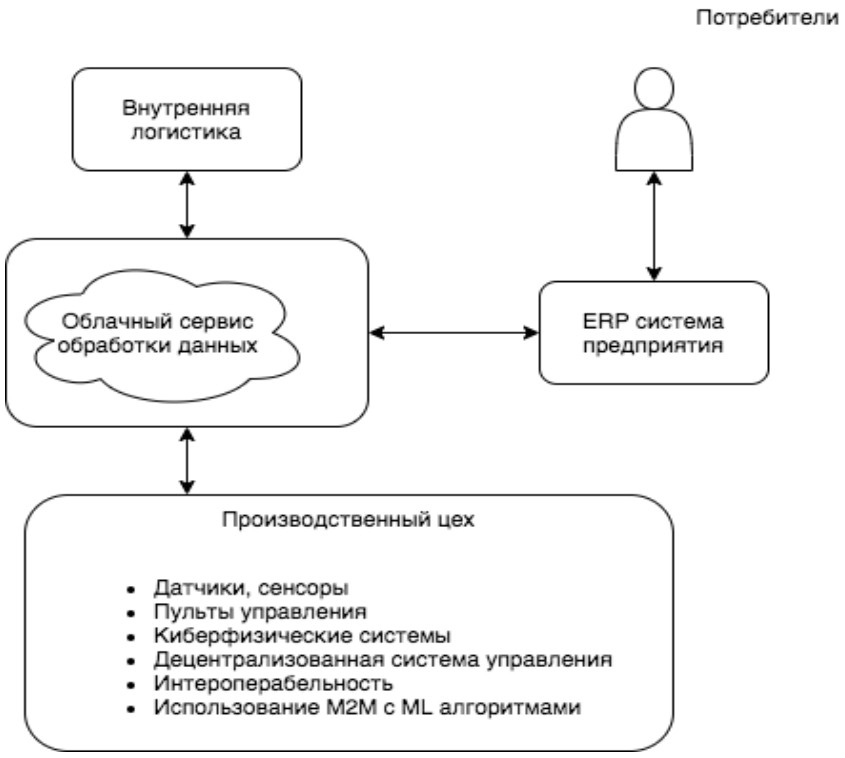

Рисунок 2. Концепция IoT систем в индустрии 4.0

Архитектура IoT систем

IoT системы в настоящее время применяются в разных сферах. Наиболее частыми решения по IoT системам предлагаются в следующих сферах:

- умный дом;
- умный город;
- предсказание погоды/катаклизмов;
- отслеживание транспорта;
- офисные корпоративные системы;
- индустрия 4.0;
- автомобильная промышленность;

Для каждой из этих областей нет единой, стандартизированной архитектуры IoT систем, так как каждая отрасль по - своему уникальна. Для каждой области предоставляется свой набор требований и правил к функционированию и безопасности системы. Это является одной из главных проблем в области IoT систем – отсутствие общепринятой эталонной архитектуры[4].

Несмотря на то, что все IoT системы имеют общие компоненты, каждый производитель предлагает свои решения в отдельных элементах архитектуры IoT систем. В таблице 1 приведены предложения по эталонной архитектуре IoT систем.

Наличие большого количества подходов к стандартизации означает то, что данная проблема не будет решена в ближайшее время. Соответственно, под вопросом стоит безопасность таких систем как со стороны информационной, так и функциональной безопасности.

Функциональная безопасность в IoT

Функциональная безопасность является неотъемлемой частью безопасности IoT систем, так как она напрямую взаимодействует с окружающим миром через периферйиные устройства. Под функциональной безопасностью в соответствии со стандартом IEC-62021 подразумевается - часть общей безопасности процесса и основная система управления процессом, которая зависит от правильного функционирования приборной системы безопасности и других слоев защиты[3].

Таблица 1. Сравнительный анализ предложений по эталонной архитектуре IoT систем

Название	**Разработчик**	**Применение**	**Описание**
Azure IoT	Microsoft	Умный дом, умный город	Опирается на стандартную концепцию интернета – вещей, но с активным использованием ML решений для обработки данных. Разделяет потоки данных на два пути: горячий и холодный. Горячий путь анализирует данные в режиме реального времени, холодный – с более большими интервалами. Обработка данных ведется с помощью облачного решения PaaS[8]
Intel IoT	Intel	Умный дом, умный город, Корпоративные системы	Архитектура подразумевает взаимодействие с GCP (Google Cloud Platform). Активное использование ML алгоритмов нацелено не только на обработку данных, но и на безопасность системы. Максимально ориентирована на продукты от Intel
Предварительный национальный стандарт российской федерации	ПАО Ростелеком, АО «ВНИИС», АО «РВК»,	Унифицированный стандарт для разных IoT систем	Разработанный стандарт, нацеленный на создание единого принципа построения IoT систем, который может позволить упростить интеграцию различных систем, масштабируемость элементов, интеграцию систем в уже существующие решения[3]
IEE P2143 - 2019	IEEE	Международный стандарт для всех IoT систем	Стандарт, важным аспектом которого,я является безопаность интернета-вещей.
ISO/IEC 30141	ISO/IEC JTC1	Международный стандарт	Стандарт, который включает в себе дополнения из различных стандартов: ISO/IEC 14543 – домашние электронные системы, ISO/IEC 23005 – архитектура управления медиа, Sensor Network Reference Architecture - ISO/IEC 29182[7]

Стандарт IEC – 62061 по большей части относится для любых отраслей промышленности, где имеется необходимость в использовании программируемых систем безопасности. В самом общем виде стандарт определяет следующие аспекты безопасности системы:

– определяет Модель развития системы безопасности;

– определяет два подхода к системам безопасности: системы, обеспечивающие защиту и непрерывность контроля по средней частоте опасных отказов, и системы, обеспечивающие защиту и контроль по средней вероятности опасного отказа в течение предопределенного интервала времени;

– определяет концепцию безопасного допуска.

– устанавливает 4 уровня безопасного допуска.

В данном стандарте определяется 4 уровня интегральной безопасности в зависимости от конкретной вероятности отказа выполнения требуемой функции:

– защита оборудования и продукции;

– защита оборудования и продукции, защита от травматизма;

– защита обслуживающего персонала и населения;

– защита от общей катастрофы;

Тенденция развития IoT систем постепенно распространяет этот стандарт не только на промышленность, но и на другие сферы жизни.

Проблемы функциональной безопасности в IoT системах

Несмотря на то, что электроника относительно стандартизирована и может работать длительное время без перебоев, одним из потенциальных рисков является перехват управления на уровне физических устройств. При

несанкционированном доступе, есть возможность заставить систему управления выполнять опасные функции. В этом случае информационная и функциональная безопасность являются двумя сторонами одного и того же явления.

В настоящее время решения по внедрению IoT не подразумевают полной гарантии по безопасности. Например, по данным Лаборатории Касперского с 2018 по 2019гг. количество атак на IOT системы выросло с 12млн. до 105млн. В таблице 2 приведены наиболее частые причины взлома IoT систем.

Таблица 2. Причины взлома IoT систем

Причина	**Описание**
Централизованная архитектура IOT систем	Многие IOT системы представляют собой «базовую станцию», обрабатывающее большой объем информации с устройств, подключенных к ней. Взлом центрального кластера означает полный доступ ко всей IOT системе
Уязвимости в протоколах передачи данных	Большое количество уязвимостей на разных уровнях, с высокой динамикой изменения.
Устаревшие прошивки девайсов, обновление методов шифрования	Некоторые производители не могут своевременно обновлять прошивку устройств, обновлять свои системы под постоянно меняющиеся условия кибербезопасноти.
Стандартные заводские настройки	Зачастую заводские настройки не подразумевают особенности функционирования различных систем, поэтому настройки безопасности одинаковы для всех условий

На физическом уровне попытки взлома практически невозможны. Единственные угрозы – низкое качество периферийного устройства, внешнее воздействие.

Самой уязвимой частью является передача данных между устройствами. Различные протоколы IoT систем разработаны и оптимизированы для различных сценариев и вариантов использования. В таблице 3 приведены протоколы передачи данных с наибольшей вероятностью для несанкционированного доступа.

Таблица 3. Протоколы передачи данных с высокой степенью несанкционированного доступа

Название протокола	**Уровень передачи**	**Особенности**	**Безопасность**
Bluetooth	Физический	Малый радиус действия,	Несмотря на наличие уязвимостей, протокол защищен на достаточном уровне. Уровень защиты также зависит от настроек.
Zigbee	Физический	Популярный протокол передачи данных в IoT системах	При перезагрузке или в режиме подключения новых устройств хаб ZigBee передает в локальную сеть ключи, может и без шифрования. Легкий перехват
Wi-Fi/802.11	Физический	Стандартный, наиболее массовый протокол передачи данных, с высокой зоной покрытия.	Огромное количество возможностей анализа трафика. WPA2 ненадежен в открытых сетях, многие устройства все еще используют предыдущие версии сертификации устройств. Самый ненадежный протокол.
LPWAN	Канальный уровень данных	Беспроводная технология для передачи данных на большие расстояния	Неустойчив к подмене кода, глушению канала связи, глушению избранного конечного устройства. Открытые ID устройств в эфире.

TCP	Транспортировка	Основной протокол передачи данных интернета	Актуальные уязвимости - Name:Wreck, Ripple20, URGENT/11, Amnesia:33. Уязвимости в операционных системах FreeBSD и Nucleus NET связаны с тем, как эти стеки реализуют систему доменных имён (DNS). Все они позволят злоумышленнику либо вывести устройство из строя и отключить его, либо получить контроль над ним.

На основе вышеизложенного можно сделать вывод, что передача данных в IoT системах подвержена большому риску перехвата, в системе невысокая устойчивость к определению подмены устройства. Важно понимать, как поведет система в случае изменения параметров, передаваемых с периферийных устройств.

Обычно это заложено в программный код, где посредством обработки исключений и набором правил, выполняется определенный сценарий. В большинстве случаев, если контур системы выполняет некритичную функцию, то система может продолжить работу с незначительными изменениями. В случае, если отключается важный контур системы, или с него поступают неправильные данные, то система в большинстве случаев останавливает свою работу и дальнейшее функционирование становится невозможным до полного исправления ситуации.

Методы повышения функциональной безопасности

Для того, чтобы повысить уровень безопасности в IoT системах, можно использовать определенные методы. Использование лучших практик и стандартов написания кода позволит ускорить разработку, легко анализировать и быстро принимать соответствующие меры по изменению определенных участков кода. МЭК 61508 требует внедрять безопасное использование языков программирования. Например, для микроконтроллеров систем безопасности предпочтение отдается языку C, а не C++. При этом рекомендуется использовать ограниченное множество конструкций языка. Для разработки важно использовать сертифицированные инструменты, библиотеки, компиляторы.

Важно уделять большое внимание на тестирование IoT систем. Тщательная проработка всевозможных ситуаций, разработка большого количества тест-кейсов, нагрузочное тестирование, функциональное тестирование, могут улучшить безопасность IoT системы. Важно проработать все сценарии, где пользователь может совершать ошибки. Некоторые производители уделяют данным процессам меньше времени, стараясь как можно быстрее выпустить продукт на рынок.

Резервирование элементов достаточно сложное, но эффективное решение. Такой подход значительно снижает вероятность отказов участков систем, но это существенно увеличивает себестоимость проекта. Резервирование важно обеспечивать как на физическом уровне, так и на уровне передачи информации. Передачу информации можно осуществлять по нескольким каналам, разделяя их по важности и периодичностью передаваемых данных. Также возможно использовать особое резервирование, где одна и та же функция выполняется разными путями, например, с применением разного оборудования или разного программного обеспечения. Самодиагностика устройств также может существенно повысить функциональную безопасность IoT системы.

Заключение

Безопасность IoT систем недостаточно высокая. Существующие протоколы передачи данных имеют большое количество уязвимостей, позволяющие при несанкционированном доступе, управлять различными участками системы. Не все IoT системы имеют высокую отказоустойчивость ввиду того, что требования к функциональной безопасности стали более серьезными только с распространением индустрии 4.0. Количество подключаемых устройств растет, но лишь немногие производители, разработчики предлагают решения, которые наиболее проработаны в безопасности функционирования. Разные подходы к архитектуре IoT системы затрудняют стандартизацию в данной области. В статье были предложены методы, которые могут повысить функциональную безопасность IoT систем. Один из наиболее доступных методов – тщательное тестирование системы, предполагающее проработку всевозможных вариантов событий, происходящих в работе системы.

Список литературы

1. Грингард С. Интернет вещей. Будущее уже здесь / С. Грингард. - М.: Альпина Паблишер, 2016 - 188 с.

2. B. Sniderman, M. Mahto, and M. Cotteleer, “Industry 4.0 and manufacturing ecosystems: Exploring the world of connected enterprises,” Deloitte University Press, February 2016, pp. 2-14.

3. ГОСТ Р МЭК 62061-2015// [Электронный ресурс] – Режим доступа. – Url: https://docs.cntd.ru/document/1200120811 (дата обращения: 28.03.2021).

4. N. G. Nayak, F. Dürr and K. Rothermel, “Software-defined environment for reconfigurable manufacturing systems, “ Internet of Things (IOT), 2015 5th International Conference on the, Seoul, 2015, pp. 122-129.

5. Функциональная безопасность – старшая сестра информационной безопасности, Часть 1 из 7// [Электронный ресурс] – Режим доступа. – Url: https://habr.com/ru/post/308634/ (дата обращения: 12.04.2021)

6. Попов Е. В. Умные города : монография / Е. В. Попов, К. А. Семячков. — Москва : Издательство Юрайт, 2020 - 346 с.

7. ISO/IEC 30141:2018 Internet of Things (IoT) — Reference Architecture// [Электронный ресурс] – Режим доступа. – Url: https://www.iso.org/standard/65695.html (дата обращения: 04.04.2021)

8. Эталонная архитектура Интернета вещей Azure// [Электронный ресурс] – Режим доступа. – Url: https://docs.microsoft.com/ru-ru/azure/architecture/reference-architectures/iot (дата обращения: 12.04.2021)

References

1. Gringard S. Internet of Things. The future is already here / S. Gringard. - M .: Alpina Publisher, 2016 - 188 p.

2. B. Sniderman, M. Mahto, and M. Cotteleer, “Industry 4.0 and manufacturing ecosystems: Exploring the world of connected enterprises,” Deloitte University Press, February 2016, pp. 2-14.

3. GOST R IEC 62061-2015 // [Electronic resource] - Access mode. - Url: https://docs.cntd.ru/document/1200120811 (date of access: 28.03.2021).

4. N. G. Nayak, F. Dürr and K. Rothermel, “Software-defined environment for reconfigurable manufacturing systems,“ Internet of Things (IOT), 2015 5th International Conference on the, Seoul, 2015, pp. 122-129.

5. Functional security is the elder sister of information security, Part 1 of 7 // [Electronic resource] - Access mode. - Url: https://habr.com/ru/post/308634/ (date accessed: 04/12/2021)

6. Popov EV Smart cities: monograph / EV Popov, KA Semyachkov. - Moscow: Yurayt Publishing House, 2020 - 346 p.

7. ISO / IEC 30141: 2018 Internet of Things (IoT) - Reference Architecture // [Electronic resource] - Access mode. - Url: https://www.iso.org/standard/65695.html (date accessed: 04/04/2021)

8. Reference architecture of the Internet of things Azure // [Electronic resource] - Access mode. - Url: https://docs.microsoft.com/ru-ru/azure/architecture/reference-architectures/iot (date accessed: 12.04.2021)