www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2021.2.3

УДК 004.49
ББК 32.972.53

КОНЦЕПЦИЯ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ЗАЩИТЫ IIoT-УСТРОЙСТВ

Виктор Викторович Лобызов

Специалист, кафедра информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Вадим Юрьевич Шевцов

Ассистент, кафедра информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Одним из главных вопросов при эксплуатации устройств IIoT является защита от внешних атак и угроз. В связи с ростом количества IIoT-систем, также происходит увеличение рисков связанных с безопасностью устройств промышленного интернета вещей. В работе подробно рассматриваются технологии IIoT-систем угрозы и методы защиты от них. Предложена концепция программно-аппаратного комплекса защиты IIoT-устройств.

Ключевые слова: промышленный интернет вещей, угрозы интернета вещей, средство защиты интернета вещей, виртуальная частная сеть, шлюз промышленного интернета вещей.

Интернет вещей – новый тренд в развитии информационных технологий, активно распространяющийся как связанные между собой функциональные узлы, по умолчанию имеющие средства для обеспечения взаимодействия напрямую между собой или с внешней средой. Разработка таких сетей представляется явлением, которое может в корне изменить мировую экономику, а также общественные процессы. В результате применения данного пласта информационных технологий необходимость непосредственного контроля человека за действиями и операциями будет исключена. Одним из распространенных бытовых примеров является «умный дом» – это вычислительная сеть связанных между собой устройств при помощи различных протоколов передачи данных, с возможностью доступа к данной сети из внешней сети. Так, благодаря IoT, возможно настроить устройства в доме путем удаленного доступа.

IoT развивается не только в сфере продаж частным лицам, но и в промышленности, в том числе государственной. Наблюдаются высокие темпы роста устройств, подключаемых к IoT в промышленности, начиная от торговли и финансов, заканчивая энергетикой и коммунальными службами, использующими умные электростанции и умные счетчики. Таким образом, на сегодняшний день стоит рас-

сматривать дополнительную область на основе интернета вещей: IIoT (Idustrial Internet of Things) – промышленный интернет вещей, ключевое отличие которого заключается в том, что масштабы системы и управляемой ею информации носят глобальный характер, что повышает требования к различным параметрам IIoT-системы. То есть в данном случае в качестве примера можно говорить о системах «умный город», где объектами могут выступать отдельные автоматизированные системы, транспортные средства, светофоры, камеры и прочие объекты города, доступ к которым имеется из одной вычислительной сети.

Рассмотрим, с помощью каких протоколов передачи данных происходит взаимодействие внутри промышленной зоны, а также самой промышленной зоны с глобальной сетью.

Сенсоры и актуаторы находятся в периферии, и для коммуникации могут использовать как обычные, так и специальные протоколы взаимодействия, либо также само соединение может быть как проводным, так и беспроводным. Среди беспроводных сетей распространены LoRa ZigBee, SigFox, 2G, 3G, 4G, WiFi. При проводном подключении к шлюзу – Modbus, USB, Ethernet, PLC, оптические технологии. Все протоколы объединяют устройства в сети, и впоследствии эти сети становятся частью одной сети.

С точки зрения шлюзов, отделяющих вычислительную сеть устройств от интернета, на данный момент времени строго специализированных протоколов не существует. Все разработки пока ведутся без учета стандартизации. Однако прогресс в построении систем IIoT не остается в стороне от угроз информационной безопасности, так как такие системы в своей основе часто используют уже устоявшиеся технологии, особенно при построении сетей передачи данных, основанных на модели OSI [6].

В контексте процессов IIoT-систем сбор и отправка данных идут непрерывно в режиме реального времени. К примеру, данные, информирующие о текущей нагрузке промышленного оборудования, информация для управления дорожным движением. Устройства, отправляющие такие данные, могут содержать уязвимости, следствием которых при определенных условиях могут стать нежелательные утечки информации. В результате это может приводить к обману сенсоров, фальсификации данных, поступающих в программу, на сервер, а также анализируемых оператором. Более того, воздействие непосредственно на актуаторы может привести к серьезным последствиям. Например, получение несанкционированного доступа к конечным устройствам, имеющего целью организацию атаки на инфраструктуру компании или предприятия через IIoT-устройства, в том числе через IIoT-шлюзы (центральный элемент IIoT-системы), может приводить к заражению устройств всей промышленной зоны объекта IIoT. Схожий сценарий событий произошел с интернетом вещей, когда популярная версия вредоносной сети ботов Mirai поразила более 5 миллионов устройств типов IoT и IIoT во многих странах мира. В итоге вследствие атаки была заражена большая часть роутеров одного немецкого провайдера, что повлекло за собой серьезные репутационные потери [9].

Высокий риск получения НСД к правам администратора устройств IIoT и фальсификация данных на пути их передачи существует также, если промышленный интернет вещей используется в робототехнике. Робот может получать/передавать неправильные данные о состоянии и выполнять вредоносные действия [7].

На основании угроз из БДУ ФСТЭК [1] (см. табл. 1) можно сделать вывод, что для защиты передаваемых данных, в том числе по специальным протоколам (например MQTT), необходима организация частой виртуальной сети.

В рамках предложенной концепции был выбран протокол MQTT, так как он наиболее универсален с точки зрения возможных реализаций. Также данный протокол – один из тех, которые стандартизированы специально для IIoT-систем: ГОСТ Р 58603-2019 «Информационные технологии. Интернет вещей. Протокол организации очередей доставки телеметрических сообщений MQTT. Версия 3.1.1» [3], который является частью ПНСТ 419-2020 «Информационные технологии. Интернет вещей. Общие положения».

Для реализации защиты с использованием VPN был выбран протокол Wireguard по следующим причинам:

1) поддержка соверменных надежных алгоритмов шифрования;

2) компактная реализация протокола (4000 строк кода);

3) по умолчанию встроен в открытые системы (ОС на основе ядра Linux);

4) функциональность при построении сетей;

5) высокий уровень защищенности в связи с минимальным числом возможных конфигураций безопасности;

6) достаточная производительность для построения IIoT-систем в сравнении с другими протоколами и технологиями прострoения виртуальных частных сетей.

Отдельно следует отметить требования регуляторов к системам промышленного интернета вещей. IIoT-системы не могут попадать под действие федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ [8], так как обязательным условием для реализации таких систем является использование открытых сетей, что недопустимо для объектов критической информационной инфраструктуры в рамках одной системы.

Однако IIoT-система, согласно нормативным документам, может являться системой АСУ ТП. В данном случае для применения выбранного VPN как средства защиты информации, необходимо определить класс защищенности системы, а после применить СЗИ соответствующего класса защиты с использованием протокола Wireguard и проверить на соответствие требованиям к мерам защиты для класса защищенности АСУ ТП. Однако класс защищенности IIoT может быть любым, в зависимости от многих факторов и в первую очередь масштаба системы, поэтому некорректно будет определять и класс СЗИ. С использованием протокола Wireguard в качестве осноного при построении VPN система будет соответствовать всем мерам из таблиц ГОСТ Р МЭК 62443-3-3-2016 [4] (см. табл. 2), которым сможет соответствовать данный VPN, исходя из своего функционала.

После того, как выбран протокола передачи данных, архитектура IIoT-системы и средства защиты информации, рассмотрим концепцию IIoT-шлюза.

В информационной инфраструктуре промышленного интернета вещей существует множество датчиков и исполнительных механизмов, взаимодействующих с оборудованием и окружающей средой [5]. Каждый объект имеет несколько датчиков, отслеживающих состояние и контролирующих ключевые параметры, связанные с производством. Каждый датчик и исполнительный механизм присоединены к микроконтроллеру, который отвечает за сбор данных или управление переключателем с помощью заранее определенного набора команд. Микроконтроллер вместе с датчиками питанием, способным осуществлять передачу данных, называется сенсорным узлом. Это автономное развертываемое устройство, которое собирает данные, генерируемые датчиками. Сенсорному узлу не хватает вычислительной мощности, памяти и хранилища для работы с данными локально. Он использует сети с низким энергопотреблением для отправки данных в центральное место. Связь между узлами датчиков и центральным концентратором может быть основана на беспроводных технологиях, таких как ZigBee,

Таблица 1

Угрозы систем IIoT из БДУ ФСТЭК и способы перекрытия

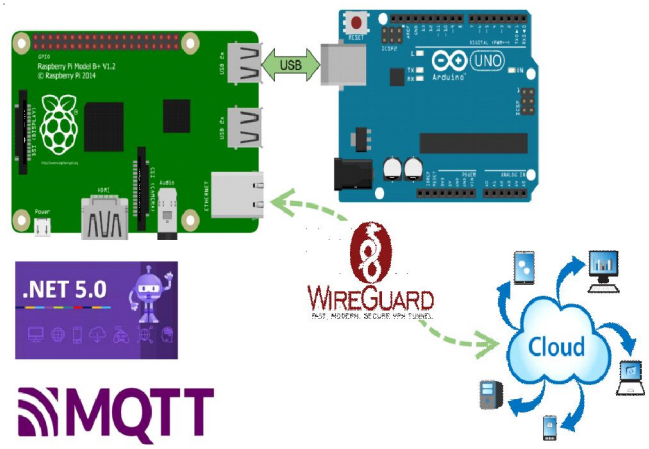
Угрозы	Способ перекрытия
УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети	Шифрование/ VPN/Межсетевые экраны
УБИ.212: Угроза перехвата управления информационной системой	VPN/Межсетевые экраны
УБИ.069: Угроза неправомерных действий в каналах связи	VPN/Межсетевые экраны
УБИ.075: Угроза несанкционированного доступа к виртуальным каналам передачи	VPN/Межсетевые экраны
УБИ.112: Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Шифрование/VPN
УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	VPN

Bluetooth Low Energy, или же может использовать проводные подключения, такие как: PoE, USB. Концентратор, который действует как агрегатор нескольких необработанных наборов данных, генерируемых узлами датчиков, называется шлюзом IIoT. Шлюз интернета вещей выполняет несколько ролей. Одна из первых задач шлюза – преобразовать и нормализовать данные. Наборы данных, генерируемые сенсорными узлами, будут в разных форматах. Некоторые из устаревших узлов используют проприетарные протоколы, в то время как современные могут полагаться на открытые протоколы для большей совместимости. Шлюз получает разнородные наборы данных от множества узлов датчиков и преобразует их в стандартный формат, понятный на следующем этапе конвейера обработки данных. Вторая роль шлюза IIoT – преобразование протокола [2]. Поскольку сенсорные узлы не могут использовать энергоемкие Wi-Fi или Ethernet, они используют маломощные сети связи. Шлюз поддерживает несколько протоколов связи для приема входящих данных, отправляемых узлами датчиков. Он использует различные протоколы для исходящей связи, которые обычно подключают шлюз к процессу, запущенному в облаке. Некоторые из популярных исходящих протоколов, используемых в контексте интернета вещей, – это MQTT, CoAP, AMQP. В некоторых ситуациях шлюз также может обрабатывать данные и выдавать сообщения в режиме реального времени. Но лучше оставить это мощным конвейерам потоковой обработки, работающим в облаке. На схеме ниже (рисунок) представлена концепция развертывания шлюза интернета вещей.

Таблица 2

Соотнесение SR и RE с уровнями SL (из ГОСТ Р МЭК 62443-3-3-2016)

FR 3	Целостность системы (SI)
SR 3.1	Целостность коммуникации
SR 3.1 RE 1	Защита целостности средствами криптографии
SR 3.5	Валидация входных данных
FR 4	Конфиденциальность данных (DC)
SR 4.1	Конфиденциальность информации
SR 4.1 RE 1	Защита конфиденциальности информации в ходе ее хранения или передачи через недоверенные сети
SR 4.3	Использование криптографии
FR 5	Ограничение потока данных (RDF)
SR 5.1	Сегментация сети
SR 5.1 RE 1	Физическая сегментация сети
SR 5.2	Защита границ зоны
SR 5.2RE 1	Отказ по умолчанию, разрешение по исключению
SR 5.2 RE 2	Островной режим



Концепция шлюза IIoT-системы

Предлагаемая концепция предполагает использовать в качестве IIoT-шлюза аппаратный комплекс из Arduino UNO, Raspberry PI совместно с приложением на .NET 5, реализующим публикацию сообщений, посредством выбранного протокола передачи данных и выбранного средства защиты информации. Основная идея программно-аппаратного комплекса состоит в том, чтобы организовать защищенную передачу данных между IIoT-устройствами и сервером. Данный программно-аппаратный комплекс, по сути, является сильно усредненной имитацией устройств компаний, которые проектируют решения для промышленного интернета вещей, однако такое решение использует свободные технологии и отличается модульностью, оттого более гибкое и удобное. Тем не менее, исходя из сравнения с его аналогами, является достаточно близким к рыночным решениям для использования в качестве опытного образца.

СПИСОК ЛИТЕРАТУРЫ

1. Банк данных угроз безопасности информации. – Электрон. дан. – Режим доступа: https://bdu.fstec.ru/threat. – Загл. с экрана.

2. Безопасность в IoT: Стратегия всесторонней защиты. – Электрон. дан. – Режим доступа: https://habr.com/ru/company/microsoft/blog/315578/. – Загл. с экрана.

3. ГОСТ Р 58603-2019. Информационные технологии. Интернет вещей. Протокол организации очередей доставки телеметрических сообщений MQTT. Версия 3.1.1 – Электрон дан. – Режим доступа: https://docs.cntd.ru/document/1200168775. – Загл. с экрана.

4. ГОСТ Р МЭК 62443-3-3-2016. Сети промышленной коммуникации. Безопасность сетей и систем. Требования к системной безопасности и уровни безопасности. – Электрон. дан. – Режим доступа: :https://docs.cntd.ru/document/1200135801. – Загл. экрана.

5. Орешкина, Д. Эталонная архитектура безопасности интернета вещей (IoT). Часть 1 / Д. Орешкина. – Электрон. дан. – Режим доступа: https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1. – Загл. с экрана.

6. Орешкина, Д. Эталонная архитектура безопасности Интернета вещей (IoT). Часть 2 / Д. Орешкина. – Электрон. дан. – Режим доступа:: https://www.anti-malware.ru/practice/solutions/iot-reference-architecture-protection-part-2. – Загл. с экрана.

7. Топ-10 угроз безопасности IoT. – Электрон. дан. – 18.12.2018. – Режим доступа: https://itsecforu.ru/2018/12/18/топ-10-угроз-безопасности-iot/. – Загл. с экрана.

8. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – Электрон. дан. – Режим доступа: https://base.garant.ru/71730198/. – Загл. с экрана.

9. Холмогоров, В. По следам Mirai. Разбираемся, как трояны поражают IoT, на примере самого злого из них / В. Холмогоров. – Электрон. дан. – 22.01.2019. – Режим доступа: https://xakep.ru/2019/01/22/mirai/. – Загл. с экрана.

REFERENCES

1. *Bank dannyh ugroz bezopasnosti informacii* [Data Bank of Information Security Threats]. URL: https://bdu.fstec.ru/threat.

2. *Bezopasnost' v IoT: Strategija vsestoronnej zashhity* [IoT Security: Comprehensive Protection Strategy]. URL: https://habr.com/ru/company/microsoft/blog/315578.

3. *GOST R 58603-2019. Informacionnye tehnologii. Internet veshhej. Protokol organizacii ocheredej dostavki telemetricheskih soobshhenij MQTT. Versija 3.1.1* [GOST R 58603-2019. Information Technology. Internet of Things. Message Queuing Telemetry Transport (MQTT) v3.1.1]. URL: https://docs.cntd.ru/document/1200168775.

4. *GOST R MJeK 62443-3-3-2016. Seti promyshlennoj kommunikacii. Bezopasnost' setej i sistem. Trebovanija k sistemnoj bezopasnosti i urovni bezopasnosti* [GOST R IEC 62443-3-3-2016. Industrial Communication Networks. Network and System Security. Part 3-3. System Security Requirements and Security Levels]. URL: https://docs.cntd.ru/document/1200135801.

5. Oreshkina D. *Jetalonnaja arhitektura bezopasnosti interneta veshhej (IoT). Chast' 1* [Reference Security Architecture of the Internet of Things (IoT). Part One]. URL: https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1.

6. Oreshkina D. *Jetalonnaja arhitektura bezopasnosti interneta veshhej (IoT). Chast' 2* [Reference Security Architecture of the Internet of Things (IoT). Part Two]. URL: https://www.anti-malware.ru/practice/solutions/iot-reference-architecture-protection-part-2.

7. *Top-10 ugroz bezopasnosti IoT* [Top-10 Threats to IoT], December 18, 2018. URL: https://itsecforu.ru/2018/12/18/топ-10-угроз-безопасности-iot.

8. *Federal'nyj zakon ot 26.07.2017 № 187-FZ «O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii»* [Federal Law No. 187-FZ Dated July 26, 2017 "On the Security of the Critical Information Infrastructure of the Russian Federation"]. URL: https://base.garant.ru/71730198.

9. Holmogorov V. *Po sledam Mirai. Razbiraemsja, kak trojany porazhajut IoT, na primere samogo zlogo iz nih* [Following the Steps of Mirai. Exploring the Way Trojans Attack IoT Using the Example of the Strongest of Them], 2019, January 22. URL: https://xakep.ru/2019/01/22/mirai.

THE CONCEPT OF A HARDWARE-SOFTWARE SYSTEM FOR PROTECTING IIoT DEVICES

Viktor V. Lobyzov

Specialist, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Vadim Y. Shevtsov

Assistant, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp.Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The Internet of Things is a new trend in the development of information technologies, actively spreading as interconnected functional nodes that by default have the means to ensure interaction directly with each other, or with the external environment. The development of such networks is a phenomenon that can radically change the world economy, as well as social processes. As a result of the application of this layer of information technologies, the need for direct human control over actions and operations will be eliminated. One of the most common household examples is a "smart home" – a computer network of interconnected devices using various data transfer protocols with the ability to access this network from an external network. So, thanks to IoT, it is possible to configure devices in the house by remote access. The paper deals with the main security methods against attacks and threats of IIoT devices. The information infrastructure was analyzed, an idea of the architecture of IIoT systems was obtained, and the information transmission path was identified. An analysis of the IIoT regulatory framework governing security, architecture and data exchange in IIoT systems has been carried out, documents governing the Industrial Internet of Things have been identified. The best communication protocol has been identified. Subsequently, the threats of the protocol were selected, and possible means and methods of protection were identified. For IIoT gateways, the concept of a hardware-software complex was presented as a prototype, and a comparison was made with existing solutions.

Key words: Industrial Internet of Things, Internet of Things threats, Internet of Things protection tool, virtual private network, Industrial Internet of Things gateway.