МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2024.145.14

АНАЛИЗ МЕТОДОВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ДЛЯ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

Научная статья

Ощепков Н.В.[1, *], Кротова Е.Л.[2]

[1, 2] Пермский Национальный Исследовательский Политехнический Университет, Пермь, Российская Федерация

* Корреспондирующий автор (maserati_2000[at]mail.ru)

Аннотация

Благодаря стремительному развитию промышленного интернета вещей жизнь общества и государства может кардинально измениться в плане автоматизации многих процессов, происходящих вокруг, но, к сожалению, по мере роста данной технологии, возникают и потенциальные проблемы, связанные с кибербезопасностью. Именно благодаря оценке существующих поверхностей атаки и способов защиты от уязвимостей, можно сформировать дальнейший план действий по созданию и внедрению новых средств защиты для промышленного интернета вещей. В данной статье рассматриваются актуальные угрозы и уязвимости, связанные с IoT, а также анализируются потенциальные стратегии и технологии для обеспечения безопасности данных, защиты сетей и устройств.

Ключевые слова: промышленный интернет вещей (ПИВ), информационная безопасность, iot, iiot.

AN ANALYSIS OF METHODS TO COUNTER THREATS TO THE INDUSTRIAL INTERNET OF THINGS

Research article

Oshchepkov N.V.[1, *], Krotova Y.L.[2]

[1, 2] Perm National Research Polytechnic University, Perm, Russian Federation

* Corresponding author (maserati_2000[at]mail.ru)

Abstract

Due to the rapid development of the Industrial Internet of Things, society and government life can change dramatically in terms of automating many of the surrounding processes, but unfortunately, as this technology grows, so do the potential cybersecurity challenges. It is by assessing existing attack surfaces and how to protect against vulnerabilities that a future roadmap for creating and implementing new defences for the Industrial Internet of Things can be formed. This article examines the current threats and vulnerabilities associated with the IoT and analyses potential strategies and technologies for data security, network and device protection.

Keywords: Industrial Internet of Things (IIoT), information security, iot, iiot.

Введение

ПИВ (промышленный интернет вещей) – система устройств для корпоративно-отраслевого использования, взаимодействующих друг с другом, включающая в себя различные датчики и программное обеспечение для управления производственным процессом в автоматизированном режиме.

В настоящее время промышленный интернет вещей внедрён во многие важные сферы жизнедеятельности человека: здравоохранение, промышленность, логистика, сельское хозяйство, финансы и т.д. Благодаря широкому распространению возникает ряд рисков, связанных с обеспечением безопасности в данных сферах, поскольку любая программная или аппаратная уязвимость может стать серьезной проблемой для отдельно взятой организации или общества.

Руководствуясь статистикой, уже в 2022 году в мире было подключено порядка 14 млрд. устройств ПИВ [1]. При отсутствии должного уровня обеспечения информационной безопасности в данной сфере, последствия могут стать катастрофичными.

В области промышленности в сфере Интернета вещей можно выделить два основных направления развития. Первое – переход от простой производственной модели к экономике услуг, где акцент делается на конечный результат. Второе – улучшение эффективности производственных систем. Технологии ПИВ позволяют оптимизировать производственные процессы, обеспечивать точность операций, сокращать ошибки и время, затраченное на вмешательство человека. Все это способствует увеличению объемов производства различных продуктов.

Недостаток исследований и стандартов в области информационной безопасности и доступности устройств ПИВ представляет собой значительную проблему сегодня, что приводит к растущей тревоге относительно безопасности устройств. Изучение методов и средств защиты информации в контексте ПИВ позволяет разрабатывать и внедрять более эффективные стратегии по обеспечению безопасности промышленных сетей, устройств и данных. Это включает в себя анализ потенциальных угроз, разработку механизмов шифрования, аутентификации и контроля доступа, а также обучение персонала правилам безопасности. Кроме того, изучение методов и средств позволяет более эффективно реагировать на новые угрозы и атаки, а также обеспечивать соблюдение международных стандартов и регулятивных требований в области кибербезопасности.

Исходя из этого, в данной статье будет проведён обзор существующих методов обеспечения информационной безопасности в промышленном интернете вещей, а также сформирован перечень преимуществ и недостатков каждого из подходов.

Методы и принципы исследования

Для полноты картины необходимо перечислить все существующие технологии, используемые в промышленном интернете вещей. Перечислим некоторые из них [2]:

1. Конечные устройства IoT. Включают в себя функционал по обработке, хранению, передаче данных.
2. Межмашинная связь. Вид коммуникации, позволяющий устройствам обмениваться информацией без прямого участия человека.
3. Анализ Big Data. Процесс непрерывного анализа информации, получаемого с устройств ПИВ.
4. Искусственный интеллект. Благодаря развитию данной технологии открываются большие возможности в автоматизации задач, ранее требовавших участие человека.

Поскольку интернет вещей и промышленный интернет вещей тесно связаны, то между ними существуют и схожие проблемы в области безопасности. Ниже будет приведён перечень проблем безопасности для ПИВ [2]:

Уязвимость устройств и систем. Поскольку базовый функционал устройства закладывается на этапе проектирования, большинство устройств ПИВ были разработаны без встроенных средств обеспечения информационной безопасности, которые не могут быть внедрены после начала эксплуатации.

Сложность управления процессами. Данная проблема заключается в сложности обеспечения должного уровня управления процессами ввиду стремления поставщиков устройств ПИВ обеспечить функциональность и эффективность своих устройств минуя вопросы безопасности.

Конвергенция информационных и операционных технологий (ИТ/ОТ). Благодаря внедрению компонентов промышленные системы управления стали более связанными. К сожалению, это привело к появлению новых угроз в области безопасности, поскольку увеличилось использование небезопасных внутренних и внешних сетевых соединений.

Сложность цепочки поставок. Как правило, не многие компании имеют все необходимое для производства устройств ПИВ, поэтому возникает потребность в закупке компонентов у сторонних организаций. Такой подход усложняет процесс управления цепочкой поставок при участии большого количества людей и организаций, а также не может гарантировать отсутствие недекларированных возможностей в поставляемых компонентах.

Устаревшие промышленные системы управления. Существуют компании, вводящие новые системы взамен устаревших, что потенциально может привести к возникновению новых уязвимостей.

Небезопасные протоколы. Устройства ПИВ обмениваются информацией при помощи различных протоколов, безопасность которых обеспечена не в полной мере.

Человеческий фактор. При внедрении новых компонентов или систем, необходимо проводить обучение персонала работе с новыми технологиями, иначе неосведомленность может стать критическим фактором.

Неиспользуемые функции. Как правило, устройства ПИВ обладают широким спектром функциональных возможностей, многие из которых могут оказаться излишними на некоторых предприятиях. Это открывает большие возможности злоумышленникам при проведении кибератаки.

Обеспечение безопасности продукта после его реализации. Необходимо обеспечивать безопасность устройства на протяжении всего периода его существования, даже после окончания его срока службы.

В таблице 1 приведен перечень возможных атак на устройства ПИВ [2]:

Таблица 1 - Перечень возможных атак на устройства ПИВ

DOI: https://doi.org/10.60797/IRJ.2024.145.14.1

Вид атаки
Атака на сетевое соединение между контроллером и исполнительным механизмом
Атака на датчики, изменение считываемых ими значений или их пороговых значений и настроек
Атака на исполнительные механизмы, изменение или саботаж их обычных настроек
Атака на системы администрирования IoT
Использование уязвимостей протокола
Атака на устройства путем ввода команд в системную консоль
Ступенчатые атаки
Манипуляции с источником питания и использование уязвимостей при чтении данных
Вымогательство с использованием вредоносных программ
DDoS-атака с использованием ботнета IoT

Ниже приведено подробное описание некоторых атак :

Атака на сетевое соединение между контроллером и исполнительным механизмом. Данный вид атаки несёт в себе возможность получения злоумышленником несанкционированного доступа к защищаемой информации с целью сбора и возможной подмены передаваемых по сети данных.

Атака на датчики, изменение считываемых ими значений или их пороговых значений и настроек. Суть данной атаки заключается в воздействии злоумышленника с помощью программных средств на предустановленные граничные значения сенсоров с целью изменения технологического процесса или потенциальная возможность

приведения системы, на которой установлено устройство ПИВ, в нерабочее состояние. Это может стать критическим фактором для организации.

Атака на системы администрирования IoT. На наш взгляд, данный тип атаки наиболее опасен, поскольку именно системы администрирования являются «центром» принятия решений: при удачной атаке злоумышленник получает полный контроль над устройствами ПИВ, что открывает для него неограниченные возможности в части управления устройствами, взаимодействия с информацией и может привести к критическим последствиям.

На основе вышеизложенного можно сделать заключение, что устройства ПИВ внедрились в жизнь людей достаточно быстро, при этом данный сегмент требует большой работы в области обеспечения информационной безопасности для качественного функционирования многих сфер жизнедеятельности человека. Именно поэтому, имея сведения о возможных атаках, можно спроектировать модель нарушителя и, в следствие, подготовиться к потенциальным атакам, проанализировав все риски, связанные с ПИВ.

В 2019 году технический комитет Европейского института телекоммуникационных стандартов по кибербезопасности представил стандарт кибербезопасности в Интернете вещей EN 303 645 ETSI. Данный стандарт предназначен для установки основных мер безопасности в сфере интернета вещей, взаимодействующих по сети Интернет. Для соответствия его требованиям, необходимо придерживаться следующих правил :

· Отказ от использования стандартных паролей, установленных производителем устройств ПИВ [3].

· Создание политики раскрытия уязвимостей [3], заключающейся в незамедлительном сообщении экспертами в области информационной безопасности о найденных уязвимостях.

· Вовремя производить обновление программного обеспечения

· Следить за корректностью хранения данных, используемых для обеспечения безопасности устройства и конфиденциальности информации

· Производить обмен информацией только по защищённым каналам связи

· Снизить поверхность атаки

· Использовать только проверенное программное обеспечение и в случае внедрения стороннего ПО, незамедлительно сообщать об этом пользователю устройства

· Обеспечить отказоустойчивость

· Изучить внутренние механизмы сбора и хранения информации на наличие аномалий безопасности

· Обеспечить функционал удаления информации по желанию пользователя

· Обеспечить простоту использования, установки и технического обслуживания устройств пользователей

· Производить проверку входных данных [3].

Существует и универсальная модель мер обеспечения безопасности технологий ПИВ, состоящая из трёх частей [2]:

· политика безопасности,

· организационные меры

· технические меры

Политика безопасности в целом описывает подход к обеспечению информационной безопасности и устанавливает определённые требования к системе. Организация должна придерживаться установленной политики, тогда доверие к поставляемому продукту увеличится, а следовательно возрастут и продажи.

К организационным мерам относятся правила работы с устройствами ПИВ для персонала, действия при инциденте, а также чёткий перечень функций, которые должны выполняться как поставщиками, так и организациями, которые приобрели продукт.

Пункт, связанный с техническими мерами, будет рассмотрен более детально, так как является зоной ответственности поставщика устройств ПИВ. На данный момент используются 3 типа беспроводных сетей [4]:

· энергоэффективные сети малого радиуса действия(Low Power Short Range Networks)

· энергоэффективные сети большого радиуса действия(Low Power Wide Area Networks)

· технологии, основанные на использовании стандартов сотовых сетей в лицензируемом диапазоне (Cellular Network)

Приоритетным вариантом являются LPWAN, к преимуществам которых относится низкая стоимость обслуживания, а также достаточно энерго-эффективная технология при передаче данных по воздуху. Существуют два наиболее распространённых сегмента сетей, являющихся подгруппой стандартов LPWAN. К ним относятся NB-IoT, который работает в определённом лицензируемом спектре частот и LoRaWAN, не требующий лицензии [5], [6], [7], [8]. Оба сегмента используют шифрование: 3GPP(128-256 бит) и AES 128 бит соответственно. Такой подход гарантирует безопасность данных при передаче их по сети, а также устанавливает требования к политике хранения ключей шифрования.

Кроме этого, существует и отечественный комплекс средств криптографической защиты информации(СКЗИ) ViPNet SIES [6], соответствующим требованиям Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Он представляет из себя запрограммированный крипточип, использующий российский стандарт CRISP. Данный криптостандарт обеспечивает целостность и аутентичность информации, при передаче её по сети.

Э. Франка и Г.О. Олаойе в своей статье "Trust Deficit in IIoT: Understanding the factors contributing to the trust deficit in IIoT systems and the impact on industrial operations" рассмотрели слабые места устройств промышленного интернета вещей с точки зрения недостатка доверия. По их мнению, существует множество факторов, вызывающих недоверие у конечного пользователя и организаций к устройствам ПИВ и это не безосновательно. К ним относятся: слабые и неэффективные средства аутентификации и контроля доступом, уязвимые криптографические протоколы, недостаток своевременного обновления аппаратной и программной части устройства и т.д. В качестве решения они отметили

существующие протоколы и средства по обеспечению безопасности при обмене информацией: стандартизованные протоколы защищённого обмена информацией, например MQTT (Message Queuing Telemetry Transport),существующий на данный момент фреймворк Industrial Internet Security Framework (IISF), задающий концепции по разработке безопасного программного обеспечения для устройств ПИВ и т.д.

И. А. Кхан, М.Кешк и др. в своей работе "Enhancing IIoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems" представили надежную модель безопасности, направленную на усиление защиты сетей промышленного Интернета вещей (IIoT) путем развертывания системы обнаружения вторжений на основе глубокого обучения для обнаружения кибератак в режиме реального времени. Их модель, использующая конструкцию автокодировщика с длинной краткосрочной памятью (LSTM), направлена на эффективное выявление инвазивных действий в сетях IICS.

Г. Караджайылмаз и Х.Артунер в своем исследовании "A novel approach detection for IIoT attacks via artificial intelligence" предложили вариант обнаружения вторжений с помощью заранее обученной нейронной сети. Они провели тесты на различных видах атак, например: отказ в обслуживании, человек посередине и старт-стоп атака.

В современном мире промышленные объекты становятся все более уязвимыми для кибератак из-за широкого использования технологий интернета вещей. Угрозы включают в себя взлом устройств, перехват данных, а также нарушение работы системы управления производством. Благодаря рассмотрению существующих угроз и средств защиты, отмеченных в статье Э. Франка и Г.О. Олаойе, формируется понимание, что ключевые факторы необходимо постоянно контролировать и стремиться к их улучшению. В случае игнорирования данных аспектов возрастает вероятность риска для производственного процесса, организации и общества. Исходя из вышеизложенного, следует сказать, что работы по разработке и внедрению передовых средств защиты информации в контексте ПИВ являются актуальной проблемой в современном мире. При разработке новых средств защиты следует обращать внимание на появляющиеся векторы атаки, для повышения защищенности устройств, а также внедрять новые технологии для обнаружения атак.

Заключение

С развитием информационных технологий и оптимизацией производственных процессов, ПИВ стал неотъемлемой составляющей в современных промышленных средах, но при этом существует ряд уязвимостей, использование которых может привести к разрушительным последствиям. В конечном итоге, можно сделать вывод, что сфера ПИВ будет развиваться и масштабироваться, а следовательно, необходимо уделить должное внимание вопросам информационной безопасности, что позволит сохранить надежность и непрерывность работы производств, а также предоставит уверенность в сохранности конфиденциальной информации и повысит эффективность бизнес-процессов.

Конфликт интересов

Не указан.

Рецензия

Артамонов В.А., Международная академия информационных технологий (МНОО "МАИТ), Минск, Беларусь
DOI: https://doi.org/10.60797/IRJ.2024.145.14.2

Conflict of Interest

None declared.

Review

Артамонов V.A., International Academy of information technologies, Minsk, Belarus
DOI: https://doi.org/10.60797/IRJ.2024.145.14.2

Список литературы / References

1. State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally // IoT Analytics. — URL: https://iot-analytics.com/number-connected-iot-devices/ (accessed: 25.02.2024)

2. Верещагина Е.А. Проблемы безопасности Интернета вещей. Учебное пособие / Е.А. Верещагина, И.О. Капецкий, А.С. Ярмонов. — М.: Мир науки, 2021. — URL: https://izd-mn.com/PDF/20MNNPU21.pdf (дата обращения: 25.02.2024)

3. ETSI EN 303 645. ETSI. — URL: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (accessed: 26.02.2024)

4. Наралиев Н.А. Обзор и анализ стандартов и протоколов в области Интернет вещей. Современные методы тестирования и проблемы информационной безопасности IoT / Н.А. Наралиев, Д.И. Самаль // International Journal of Open Information Technologies. — Т. 7, №8. — 2019.

5. Талаев А.Д. Стандарты LPWAN для группового взаимодействия мобильных узлов / А.Д. Талаев, В.В. Бородин // Труды МАИ. — Выпуск № 99.

6. Защита IIoT-систем. Решение для защиты систем промышленного интернета вещей. Infotecs. — URL: https://infotecs.ru/solutions/zashchita-iiot-sistem/?ysclid=lrdfxm42tn759364281 (дата обращения: 03.03.2024)

7. Грамматчиков А. Через три года на каждого россиянина будет приходиться шесть подключенных к сети устройств / А. Грамматчиков // CNews.ru. — URL: https://www.cnews.ru/articles/2020-04-21_cherez_tri_goda_na_kazhdogo_rossiyanina (дата обращения: 30.03.2024)

8. Национальная технологическая инициатива (НТИ). — URL: https://fea.ru/compound/national-technology-initiative (дата обращения: 30.03.2024)

9. Letichevsky A. Basic protocols, message sequence charts, and the verification of requirements specifications / A. Letichevsky // Computer Networks. — 2005. — Vol. 49, issue 5. — P. 661–675. — DOI: 10.1016/j.comnet.2005.05.005.

10. Industrial Internet of Things – IioT: Промышленный интернет вещей // TADVISER. — URL: https://www.tadviser.ru/a/342500 (дата обращения: 30.03.2024).

Список литературы на английском языке / References in English

1. State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally // IoT Analytics. — URL: https://iot-analytics.com/number-connected-iot-devices/ (accessed: 25.02.2024)

2. Vereshchagina E.A. Problemy bezopasnosti Interneta veshchej. Uchebnoe posobie [Internet of Things security issues. Study guide] / E.A. Vereshchagina, I.O. Kapeckij, A.S. YArmonov. — M.: Mir nauki, 2021. — URL: https://izd-mn.com/PDF/20MNNPU21.pdf (accessed: 25.02.2024) [in Russian]

3. ETSI EN 303 645. ETSI. — URL: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (accessed: 26.02.2024)

4. Naraliev N.A. Obzor i analiz standartov i protokolov v oblasti Internet veshchej. Sovremennye metody testirovaniya i problemy informacionnoj bezopasnosti IoT [Review and analysis of standards and protocols in the field of the Internet of Things. Modern testing methods and problems of information security and protection] / N.A. Naraliev, D.I. Samal' // International Journal of Open Information Technologies. — vol. 7, no.8. — 2019 [in Russian].

5. Talaev A.D. Standarty LPWAN dlya gruppovogo vzaimodejstviya mobil'nyh uzlov [LEBANON standards for group interaction of mobile nodes] / A.D. Talaev, V.V. Borodin // Trudy MAI [Works of MAI]. — № 99 [in Russian].

6. Zashchita IIoT-sistem. Reshenie dlya zashchity sistem promyshlennogo interneta veshchej. Infotecs [Protection of Internet systems. A solution for protecting industrial Internet of Things systems. Infotecs]. — URL: https://infotecs.ru/solutions/zashchita-iiot-sistem/?ysclid=lrdfxm42tn759364281 (accessed: 03.03.2024) [in Russian]

7. Grammatchikov A. CHerez tri goda na kazhdogo rossiyanina budet prihodit'sya shest' podklyuchennyh k seti ustrojstv [In three years, there will be six 'network-connected devices' for every Russian] / A. Grammatchikov // CNews.ru. — URL: https://www.cnews.ru/articles/2020-04-21_cherez_tri_goda_na_kazhdogo_rossiyanina (accessed: 30.03.2024) [in Russian]

8. Nacional'naya tekhnologicheskaya iniciativa (NTI) [National Technology Initiative (NTI)]. — URL: https://fea.ru/compound/national-technology-initiative (accessed: 30.03.2024) [in Russian]

9. Letichevsky A. Basic protocols, message sequence charts, and the verification of requirements specifications / A. Letichevsky // Computer Networks. — 2005. — Vol. 49, issue 5. — P. 661–675. — DOI: 10.1016/j.comnet.2005.05.005.

10. Promyshlennyj internet veshchej [Industrial Internet of Things – IioT] // TADVISER. — URL: https://www.tadviser.ru/a/342500 (accessed: 30.03.2024). [in Russian]