УДК 004 **DOI:10.34670/AR.2024.62.12.052**

Анализ моделей интернет-безопасности: различные стратегии безопасности на разных уровнях IOT

Матыгов Мовсар Мусаевич

Ассистент,
Чеченский государственный университет им. А.А. Кадырова,
364093, Российская Федерация, Грозный, ул. Асланбека Шерипова, 32;
e-mail: Matygov.Movsar@gmail.com

Абдулмукминова Фатима Мурадовна

Студент,
Дагестанский государственный технический университет,
367015, Российская Федерация, Махачкала, пр. Имама Шамиля, 70;
e-mail: fabdulmukminova@inbox.ru

Абдулмукминова Элиза Мурадовна

Студент,
Дагестанский государственный технический университет,
367015, Российская Федерация, Махачкала, пр. Имама Шамиля, 70;
e-mail: eguri@inbox.ru

Аннотация

Интернет вещей – это киберконвергентная система, которая включает в себя вещи, коммуникации, целевые приложения и инструменты анализа данных, поддерживающие уникальную идентификацию каждого объекта. Технологии IoT играют важнейшую роль в создании киберконвергентных систем благодаря широкому применению в различных сферах жизни, таких как промышленность, социальная сфера, здравоохранение, создание комфортной среды. Целью модели безопасности IoT является обеспечение конфиденциальности, целостности и доступности данных, передаваемых между устройствами, а также обеспечение конфиденциальности и безопасности конечных пользователей. Создание и использование IoT-систем оказывает непосредственное влияние на безопасность и конфиденциальность всех задействованных и связанных с ними компонентов. Представленное исследование представляет собой анализ архитектурных моделей IoT со сквозной поддержкой безопасности. Проведенный обзор литературы раскрывает проблемы различных аспектов безопасности, с которыми сталкивается IoT-среда. По мере того, как количество IoT-устройств растет и используется в различных доменах и приложениях, количество угроз и огромных рисков безопасности и конфиденциальности увеличивается, создавая Интернет уязвимостей. Использование знания-ориентированного подхода позволяет ускорить процесс проектирования средств безопасности для IoT с учетом специфики сферы их применения, на основе обобщенной

онтологии. Проведенный анализ показывает необходимость обеспечения безопасности в контексте IoT и отличие от других систем в связи с неоднородностью IoT.

Для цитирования в научных исследованиях

Матыгов М.М., Абдулмукминова Ф.М., Абдулмукминова Э.М. Анализ моделей интернет-безопасности: различные стратегии безопасности на разных уровнях IOT // Экономика: вчера, сегодня, завтра. 2024. Том 14. № 2А. С. 565-572. DOI:10.34670/AR.2024.62.12.052

Ключевые слова

Интернет вещей, киберконвергентная система, модель безопасности, конфиденциальность, IoT.

Введение

Интернет вещей (IoT) является необходимой частью современных компьютеризированных систем в различных сферах человеческой деятельности. IoT – это концепция компьютерной сети физических объектов (вещей), оснащенных встроенными технологиями взаимодействия друг с другом или с внешней средой, которая рассматривает организацию таких сетей как явление, способное изменять экономические и социальные процессы, что исключает необходимость участия человека в плане действий и операций. В целом, технологии IoT собирают, обмениваются и обрабатывают данные, чтобы динамически адаптироваться к конкретному контексту, трансформируя деловой мир и то, как мы живем в целом [Робертс, 1986].

IoT – это киберконвергентная система [Максимов, 2001], которая включает в себя вещи, средства связи, целевые приложения и инструменты анализа данных, поддерживающие уникальную идентификацию каждого объекта. Киберконвергентная система представляет собой комбинацию кибернатических систем и киберобъектов различного назначения для обеспечения функционирования целевых объектов в киберсвязанных мирах. Кибернатика – это целостная область исследований для систематического изучения кибератаров в киберпространстве, их свойств и функций, а также их связей и отношений с объектами в физическом, социальном и ментальном пространстве. Для кибернатики характерно не только воспроизводство человеческого интеллекта (например, рациональное чувство, принятие решений и управление и т.д.), но и заимствование природных свойств, например, динамики, самоадаптации, энергосбережения [Тихонин, 2007].

Растущий масштаб и сложность IoT-систем, с одной стороны, и угрозы безопасности, с другой, требуют разработки моделей и инструментов управления безопасностью, адаптированных к специфике сценария использования. Цель исследования – проанализировать модели безопасности интернета вещей для формулирования общих подходов в практическом применении в различных сферах деятельности.

Основная часть

С распространением приложений IoT растут и риски кибератак, нацеленных на различные уровни и компоненты Интернета вещей. IoT – это точка входа в организацию, на которую нацелены киберпреступники с целью совершения вредоносных действий: подслушивания, кражи информации, нарушения операционной деятельности, вывода из строя оборудования и

т.д. Современные решения безопасности, доступные для защиты систем с использованием IoT, ставят производителей и операторов в сложное положение. Как правило, такие решения нацелены на периферийные области IoT и сдерживают кибератаки и угрозы только после их идентификации [Кубарев, 2018].

Выявление различных проблем безопасности для систем IoT, в том числе:

– отсутствие стандартизации;

– слабая аутентификация или ее отсутствие;

– недостаточная защищенность программного обеспечения;

– недостаточная безопасность сети;

– ограниченная физическая охрана;

– недостаточная защита данных;

– невозможность обновления или ремонта устройств;

– ограниченный надзор со стороны регулирующих органов;

– сложность баланса между безопасностью и производительностью.

Быстрый рост числа подключенных конечных точек Интернета вещей в различных сегментах отрасли и типах устройств способствовал повсеместному подключению, периферийным вычислениям и доступности надежной облачной платформы для выполнения рабочих нагрузок приложений, управляемых данными. Количество атак на IoT-системы увеличивается пропорционально росту их размера и сложности. Риски безопасности систем IoT часто связаны с:

– нарушениями безопасности транспортных средств, связанными с рисками взлома, которые происходят без ведома водителя.

– вмешательство в работу IoT-устройств. Одним из наиболее распространенных применений устройств IoT является вмешательство в их прошивку, что может привести к потере или повреждению данных;

– кража данных. Еще одной распространенной угрозой безопасности IoT является кража данных, которая часто делается для получения доступа к финансовой или личной информации;

– небезопасное подключение к Интернету: отсутствие стандартов безопасности может сделать устройства IoT уязвимыми для атак, и это также может включать хакерские атаки.

– уязвимости в прошивках IoT с открытым исходным кодом. Многие устройства Интернета вещей построены с прошивкой с открытым исходным кодом, которая может быть уязвима для атак [Максимов, www].

Не существует единого решения, которое могло бы защитить все устройства Интернета вещей от всех типов угроз, но есть несколько общих стратегий, которые могут помочь снизить риски, связанные с этими устройствами. Первая стратегия основана на правильной настройке и защите всех IoT-устройств. В рамках этой стратегии вы можете настроить учетные записи пользователей и пароли, брандмауэры и антивирусное программное обеспечение, а также регулярно устанавливать обновления безопасности.

Вторая стратегия заключается в использовании защищенных беспроводных сетей для подключения IoT-устройств к корпоративным или глобальным сетям. Это помогает защитить против атак и гарантируют, что конфиденциальные данные не передаются по незащищенным сетям.

Третья стратегия основана на постоянной ситуационной осведомленности об угрозах безопасности IoT-устройств и внедрении соответствующих защитных решений для их защиты от атак. Это гарантирует, что устройства правильно настроены и защищены от атак, а личная

информация не будет скомпрометирована.

Существуют различные эталонные модели IoT, предложенные различными разработчиками, включая ENISA [ГОСТ…, 2002], ISO/IEC [Коврига, Максимов, 2001], ITU-T [Натров, 2007], Cisco, Intel, IBM [Щеглов, 2015] и т.д. Вопросы безопасности являются частью этих эталонных моделей. Такие модели обеспечивают формальную основу для реализации безопасности и оценки зрелости этих реализаций. Модель безопасности IoT относится к набору мер безопасности и протоколов, которые защищают устройства, сети и системы от кибератак и утечек данных. Целью модели безопасности IoT является обеспечение конфиденциальности, целостности и доступности данных, передаваемых между устройствами, а также обеспечение конфиденциальности и безопасности конечных пользователей.

При построении моделей безопасности IoT используются два подхода:

– реализация уровня безопасности в многоуровневой архитектуре, охватывающей весь стек от коммуникационного уровня в IoT edge домене до уровня аналитических приложений;
– сквозное внедрение защитных решений во всех точках, от периферийных устройств через сети и интеграционные платформы до аналитических приложений.

Модель безопасности Интернета вещей сталкивается с рядом проблем, которые могут повлиять на ее эффективность в защите устройств Интернета вещей и данных, которые они собирают и передают.

Сложность: устройства Интернета вещей становятся все более сложными, с растущим числом компонентов и систем, которые необходимо защитить. Эта сложность затрудняет реализацию комплексного решения безопасности, которое может эффективно защитить все аспекты системы Интернета вещей.

Неадекватные меры безопасности: многие IoT-устройства требуют более адекватных мер безопасности, таких как шифрование, брандмауэры и системы обнаружения вторжений. Это делает такие устройства уязвимыми для атак и эксплуатации злоумышленниками. Устаревшее программное обеспечение: многие устройства Интернета вещей работают с устаревшим программным обеспечением, которое производитель больше не поддерживает. Это затрудняет применение обновлений безопасности или исправлений к таким устройствам, делая их уязвимыми для атак.

Ограниченная вычислительная мощность: многие устройства Интернета вещей имеют ограниченную вычислительную мощность, память и емкость хранилища, что затрудняет запуск на них традиционного программного обеспечения безопасности. Это делает такие устройства уязвимыми для атак, поскольку злоумышленники могут использовать известные уязвимости в этих устройствах, чтобы получить доступ к конфиденциальным данным или получить контроль над устройством.

Плохо спроектированные протоколы: протоколы, используемые для связи между устройствами Интернета вещей и Интернетом, могут быть плохо спроектированы, что делает их уязвимыми для использования. Например, некоторые протоколы могут использовать незашифрованную связь, что упрощает злоумышленникам перехват и манипулирование передаваемыми данными.

Недостаточная прозрачность: мониторинг и управление безопасностью устройств Интернета вещей может быть сложной задачей, поскольку они часто развертываются в удаленных или труднодоступных местах. Это затрудняет быстрое выявление угроз безопасности и реагирование на них.

Поведение пользователей: безопасность IoT-устройств также зависит от поведения

пользователей. Например, пользователи могут использовать слабые пароли, пренебрегать обновлениями программного обеспечения или небрежно обращаться с данными, которыми они делятся в Интернете, подвергая риску свои устройства и данные.

Функциональная совместимость: по мере того, как количество устройств IoT продолжает расти, возникает потребность в функциональной совместимости между ними, что может затруднить реализацию согласованного подхода к безопасности во всей экосистеме IoT.

Отсутствие стандартов безопасности: Экосистема IoT состоит из огромного количества устройств от разных производителей, каждое из которых имеет свои стандарты безопасности. Это затрудняет единый подход к обеспечению безопасности всей системы.

Плохое тестирование: Большинство разработчиков IoT не уделяют первоочередного внимания безопасности и не проводят эффективное тестирование уязвимостей для выявления слабых мест в системах IoT. Для каждой среды Интернета вещей необходимо провести оценку рисков, чтобы проанализировать угрозы, которые могут повлиять на различные активы, определить вероятные сценарии атак и поместить их в контекст определенной службы Интернета вещей, определив, какие опасности являются критическими, а какие нет, а какие можно смягчить.

Пакет документов Industry IoT Consortium (IIC) IoT Security Maturity Model (SMM), состоящий из Практического руководства, профильных документов и руководства по картографированию, предоставляет подробную модель и подход для достижения соответствующего уровня управления безопасностью, технологий и операционной зрелости для удовлетворения потребностей бизнеса. Пакет документов ISA/IEC 62443, разработанный Международным обществом автоматизации (ISA) и его комитетом ISA99, представляет собой валидированный, понятный и принятый набор руководящих принципов, который используется в различных отраслях, включая производство, коммунальные услуги, такие как электроснабжение, водоснабжение, газ, транспортные системы, а также строительные системы. Эти рекомендации полезны для заинтересованных сторон, включая владельцев активов, поставщиков продуктов и услуг. Не существует простого универсального решения, которое могло бы удовлетворить потребности в безопасности для каждой системы.

У организаций разные потребности, и разные системы требуют разной силы механизмов защиты. Одна и та же технология может применяться по-разному и в разной степени, в зависимости от потребностей. SMM помогает организациям расставлять приоритеты для повышения безопасности. Зрелость системы безопасности отражает правильное соответствие выбора потребностям компании. Модель зрелости безопасности способствует эффективному и продуктивному сотрудничеству между заинтересованными сторонами в бизнесе и техническими специалистами. Лица, принимающие бизнес-решения, менеджеры по бизнес-рискам и владельцы систем Интернета вещей, реализующие стратегию внедрения методов обеспечения безопасности с соответствующей зрелостью, могут сотрудничать с аналитиками, архитекторами, разработчиками, системными интеграторами и другими заинтересованными сторонами, ответственными за техническую реализацию. Они также могут принимать во внимание мнения регулирующих органов и других сторон, таких как страховые компании.

Системные архитекторы, проектировщики, тестировщики и установщики должны убедиться в том, что требования к приложению выбраны правильно и что реализация правильно реализует эти требования. SMM определяет зрелость безопасности как степень уверенности в том, что текущее состояние безопасности соответствует всем потребностям организации в безопасности и всем требованиям, связанным с безопасностью организации [Борисов, 2012].

Зрелость безопасности – это мера понимания общего текущего подхода к безопасности, включая людей, процессы и технологии, включая их необходимость, преимущества и стоимость поддержки. К факторам, способствующим этому, относятся конкретные угрозы для отраслевой вертикали организации, требования безопасности, нормативные, этические и нормативные требования, профиль угроз организации и уникальные риски, присутствующие в среде.

Существует два ортогональных измерения оценки зрелости безопасности: комплексность и охват. Комплексность определяет степень глубины, согласованности и надежности методов обеспечения безопасности. Использование полноты в этой модели снижает сложность за счет совместного рассмотрения различных аспектов, таких как осведомленность организации о безопасности, степень принятия практик и применение практик. Например, более высокий уровень сложности моделирования угроз требует более автоматизированного, систематического и продвинутого подхода. Покрытие отражает степень соответствия потребностям отрасли или системы. Он фиксирует степень настройки мер безопасности, поддерживающих домены, поддомены или методики зрелости безопасности. Такие настройки обычно требуются для решения отраслевых или системных ограничений систем Интернета вещей.

Заключение

Подводя итог, разнообразие, неоднородность, сложность и пространственное распределение IoT-систем обуславливают соответствующие трудности при построении их систем безопасности. Сложность обеспечения безопасности Интернета вещей связана с ограничениями устройств и отсутствием стандартов, в том числе специфичных для Интернета вещей. Интернет вещей экспоненциально становится частью нашей повседневной жизни, повышая эффективность, предоставляя неограниченные услуги, улучшая качество жизни и обеспечивая удобство за счет подключения различных технологий, устройств и приложений.

По мере того, как количество IoT-устройств растет и используется в различных доменах и приложениях, количество угроз и огромных рисков безопасности и конфиденциальности увеличивается, создавая Интернет уязвимостей. Использование знания-ориентированного подхода позволяет ускорить процесс проектирования средств безопасности для IoT с учетом специфики сферы их применения, на основе обобщенной онтологии. Проведенный анализ показывает необходимость обеспечения безопасности в контексте IoT и отличие от других систем в связи с неоднородностью IoT.

Библиография

1. Борисов В.В. Нечеткие модели и сети. М.: Горячая линия – Телеком, 2012. 284 с.
2. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. М., 2002. URL: https://docs.cntd.ru/document/1200029952
3. Коврига С.В., Максимов В.И. Когнитивная технология оперативного управления развитием сложных социально-экономических объектов во внешней среде // Когнитивный анализ и управление развитием ситуаций (CASC'2001). Т. 1. М., 2001. С. 104-160.
4. Кубарев А. Иранские хакеры перепродавали исследования престижных вузов Англии. 2018. URL: https://polit.info/420847-iranskie-khakery-pereprodavali-issledovaniya-prestizhnykh-vuzov-anglii
5. Максимов В.И. Когнитивные технологии – от незнания к пониманию // Когнитивный анализ и управление развитием событий (CASC'2001). Т. 1. М., 2001. С. 4-41.
6. Максимов В.И. Когнитивные технологии для поддержки принятия управленческих решений // Технологии информационного общества 98 – Россия. URL: http://www.iis.ru/events/19981130/maximov.ru.html

7. Натров В.В. Определение целей и функций системы когнитивного мониторинга объекта защиты // Известия ВолгГТУ. Серия: Концептуальное проектирование в области образования, техники, технологий. 2007. Вып. 2. № 2. С. 46-48.
8. Робертс Ф.С. Дискретные математические модели с приложениями для решения биологических и экономических задач. М.: Наука, 1986. 496 с.
9. Тихонин А.В., Заболотский М.А., Полякова И.А. Применение когнитивного моделирования в управлении специалистами по подготовке кадров // Управление большими системами. 2007. Вып. 16. С. 91-98.
10. Щеглов А.Ю. Математические модели и методы формального проектирования системы защиты информационных систем. СПб., 2015. 93 с.

Analysis of internet security models: different security strategies at different IOT levels

Movsar M. Matygov

Assistant,
Chechen State University,
364049, 32, Sheripova str., Grozny, Russian Federation;
e-mail: Matygov.Movsar@gmail.com

Fatima M. Abdulmukminova

Student,
Dagestan State Technical University,
367015, 70, Imama Shamilya ave., Makhachkala, Russian Federation;
e-mail: fabdulmukminova@inbox.ru

Eliza M. Abdulmukminova

Student,
Dagestan State Technical University,
367015, 70, Imama Shamilya ave., Makhachkala, Russian Federation;
e-mail: eguri@inbox.ru

Abstract

The Internet of Things is a cyber-convergent system that includes things, communications, target applications and data analysis tools that support the unique identification of each object. IoT technologies play a crucial role in the creation of cyber-convergent systems due to their wide application in various spheres of life, such as industry, the social sphere, healthcare, and the creation of a comfortable environment. The purpose of the IoT security model is to ensure the confidentiality, integrity and availability of data transmitted between devices, as well as to ensure the privacy and security of end users. The creation and use of IoT systems have a direct impact on the security and confidentiality of all involved and related components. The presented research is an analysis of IoT architectural models with end-to-end security support. The literature review reveals the problems of various aspects of security faced by the IoT environment. As the number of IoT devices grows and is used in various domains and applications, the number of threats and huge security and privacy risks increases, creating an Internet of vulnerabilities. Using a knowledge-oriented approach allows

you to speed up the process of designing security tools for IoT, considering the specifics of their scope of application, based on a generalized ontology. The analysis shows the need for security in the context of IoT and the difference from other systems due to the heterogeneity of IoT.

For citation

Matygov M.M., Abdulmukminova F.M., Abdulmukminova E.M. (2024) Analiz modelei internet-bezopasnosti: razlichnye strategii bezopasnosti na raznykh urovnyakh IOT [Analysis of internet security models: different security strategies at different IOT levels]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 14 (2A), pp. 565-572. DOI:10.34670/AR.2024.62.12.052

Keywords

Internet of Things, cyber-convergent system, security model, privacy, IoT.

References

1. Borisov V.V. (2012) *Nechetkie modeli i seti* [Fuzzy models and networks]. Moscow: Goryachaya liniya – Telekom Publ.
2. (2002) *GOST R ISO/MEK 15408-2002. Informatsionnaya tekhnologiya. Metody i sredstva bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologii* [GOST R ISO/IEC 15408-2002. Information technology. Security methods and means. Criteria for assessing the security of information technologies]. Moscow. Available at: https://docs.cntd.ru/document/1200029952 [Accessed 03/03/2024]
3. Kovriga S.V., Maksimov V.I. (2001) Kognitivnaya tekhnologiya operativnogo upravleniya razvitiem slozhnykh sotsial'no-ekonomicheskikh ob"ektov vo vneshnei srede [Cognitive technology for operational management of the development of complex socio-economic objects in the external environment]. In: *Kognitivnyi analiz i upravlenie razvitiem situatsii (CASC'2001). T. 1* [Cognitive analysis and management of the development of situations (CASC'2001). Vol. 1]. Moscow.
4. Kubarev A. (2018) *Iranskie khakery pereprodavali issledovaniya prestizhnykh vuzov Anglii* [Iranian hackers resold research from prestigious universities in England]. Available at: https://polit.info/420847-iranskie-khakery-pereprodavali-issledovaniya-prestizhnykh-vuzov-anglii [Accessed 03/03/2024]
5. Maksimov V.I. (2001) Kognitivnye tekhnologii – ot neznaniya k ponimaniyu [Cognitive technologies – from ignorance to understanding]. In: *Kognitivnyi analiz i upravlenie razvitiem situatsii (CASC'2001). T. 1* [Cognitive analysis and management of the development of situations (CASC'2001). Vol. 1]. Moscow.
6. Maksimov V.I. Kognitivnye tekhnologii dlya podderzhki prinyatiya upravlencheskikh reshenii [Cognitive technologies to support management decision making]. In: *Tekhnologii informatsionnogo obshchestva 98 – Rossiya* [Technologies of the Information Society 98 – Russia]. Available at: http://www.iis.ru/events/19981130/maximov.ru.html [Accessed 03/03/2024]
7. Natrov V.V. (2007) Opredelenie tselei i funktsii sistemy kognitivnogo monitoringa ob"ekta zashchity [Determination of the goals and functions of the system of cognitive monitoring of the object of protection]. *Izvestiya VolgGTU. Seriya: Kontseptual'noe proektirovanie v oblasti obrazovaniya, tekhniki, tekhnologii* [News of VolgSTU. Series: Conceptual design in the field of education, engineering, technology], 2, 2, pp. 46-48.
8. Roberts F.S. (1986) *Diskretnye matematicheskie modeli s prilozheniyami dlya resheniya biologicheskikh i ekonomicheskikh zadach* [Discrete mathematical models with applications for solving biological and economic problems]. Moscow: Nauka Publ.
9. Shcheglov A.Yu. (2015) *Matematicheskie modeli i metody formal'nogo proektirovaniya sistemy zashchity informatsionnykh sistem* [Mathematical models and methods for formal design of information systems security systems]. St. Petersburg.
10. Tikhonin A.V., Zabolotskii M.A., Polyakova I.A. (2007) Primenenie kognitivnogo modelirovaniya v upravlenii spetsialistami po podgotovke kadrov [Application of cognitive modeling in the management of training specialists]. *Upravlenie bol'shimi sistemami* [Management of large systems], 16, pp. 91-98.