Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский университет
«Высшая школа экономики»

На правах рукописи

Семенов Александр Михайлович

Методы защищенной передачи данных для низкоресурсных вычислительных устройств

РЕЗЮМЕ ДИССЕРТАЦИИ

на соискание ученой степени кандидата технических наук

Научный руководитель:
кандидат физико-математических наук
Нестеренко Алексей Юрьевич

Москва – 2022

Постановка проблемы и актуальность темы исследования

Эволюция информационно-телекоммуникационных технологий привела к появлению отдельных областей применения вычислительных устройств, характеризуемых специфическими требованиями, областью и условиями эксплуатации. Например, область применения, которую принято называть «Интернет вещей» (Internet of Things, IoT), предоставляет собой концепцию объединения «вещей» физического мира с «вещами» цифрового, позволяющую взаимодействовать «вещам» как между собой, так и с человеком. В рамках «Интернета вещей» также отдельно выделяется область «Промышленный Интернет вещей»(Industrial Internet of Things, IIoT), которая представляет собой некоторую подкатегорию «Интернета вещей», включающую в себя компьютерные сети с подключенными к ним промышленными, производственными объектами и объектами критической информационной инфраструктуры (КИИ). Данные устройства, как правило, оснащены встроенными датчиками, с возможностью удаленного контроля и управления в автоматизированном режиме с минимальным вмешательством человека.

Современные технологии, в основе которых лежат концепции IoT и IIoT, совместно с классическими информационно-телекоммуникационными технологиями, предоставляют беспрецедентные возможности по сбору, автоматизации, анализу и обработке больших объемов данных для потребителей и поставщиков различных услуг в самых разных сферах жизнедеятельности. В настоящее время в Российской Федерации ведется активная работа по стандартизации, унификации и внедрению различных IoT технологий в рамках реализации проектов национальной программы «Цифровая экономика Российской Федерации» путем разработки отечественных решений в данной области.

Актуальность вопросов обеспечения безопасности при использовании различных «умных» решений, построенных на базе использования IoT (IIoT) технологий в настоящее время обусловлена:

- постоянно расширяемой областью применения данных технологий и активной работой по стандартизации, адаптации и унификации решений в области «Интернета вещей», как в Российской Федерации, так и за рубежом;
- национальной программой «Цифровая экономика Российской Федерации»;
- необходимостью обеспечения конкурентоспособности и возможности импотрозамещения при использования данных технологий, как на программном,

так и на аппаратном уровне;

- запретом на использование иностранного программного обеспечения на значимых объектах критической информационной инфраструктуры с 1 января 2025 г. (Указ Президента Российской Федерации от 30.03.2022 №166).

Степень разработанности научной проблемы

Вопросы безопасности IoT-технологий рассматриваются начиная с 2000-ых годов с момента появления первых разработок в данной области. Регулирование области «Интернета вещей» как с точки зрения прикладных вопросов обработки и передачи данных, так и с точки зрения безопасности ведется рядом зарубежных организаций по стандартизации и отраслевых комитетов, среди которых можно выделить: 3GPP, ITU-T, IETF, IRTF, NIST, Wi-Fi Alliance, Zigbee Alliance. Данными организациями были разработаны документы [1, 2, 3, 4, 5], целью которых является регулирование вопросов обеспечения безопасности при использовании IoT-технологий.

В Российской Федерации деятельность по стандартизации в области «Интернета вещей» осуществляется в рамках технических комитетов №194, №26 и №362. В рамках деятельности данных организаций разрабатываются, адаптируются и исследуются различные российские технологии обеспечения безопасности. Среди стандартизированных к настоящему моменту технологий можно выделить следующие спецификации [6, 7, 8, 9, 10, 11, 12, 13, 14].

При отечественной стандартизации технологий «Интернета вещей» обязательным этапом является обоснование безопасности и оценка показателей эффективности мер защиты, обеспечиваемой рекомендуемым к применению решением. Принятые в Российской Федерации подходы к проведению подобного обоснования рассматриваются в работах [15, 16, 17, 18], а также в статье [19]. В зарубежных публикациях принято использовать подходы, основанные на модели Белларе – Рогавея [20] и её модификациях [21, 22, 23, 24], а также модели Конетти – Кравчука [25] и её модификациях [26, 27, 28]; также следует выделить работы [29, 30, 32, 31].

Цель и задачи диссертационной работы Целью диссертационного исследования является разработка механизмов обеспечения защиты передачи данных для низкоресурсных вычислительных устройств.

Для достижения поставленной цели в диссертационной работе решены следу-

ющие **задачи**:

- Выявлены основные уязвимости стека протоколов различных технологий «Интернета вещей» (IoT).
- Разработано семейство криптографических протоколов защищенного взаимодействия для контрольно-измерительных устройств.
- Разработан метод оценки показателей эффективности защиты.
- Получены точные значения параметров эффективности защиты для разработанного семейства протоколов.
- Проведена апробация разработанного семейства протоколов для передачи данных по UDP и TCP.

Теоретическая значимость исследования состоит в развитии методов оценки защитных качеств протоколов защищенного взаимодействия.

Практическая значимость результатов диссертационной работы заключается в разработке нового семейства протоколов защищенного взаимодействия и метода оценки показателей эффективности мер защиты данного семейства протоколов.

Разработанное семейство протоколов защищенного взаимодействия:

- утверждено в качестве рекомендации по стандартизации Р 1323565.1.028-2019, с датой введения в действие 1 сентября 2020 года, для СКЗИ классов от КС1 до КА (приказ Федерального агентства по техническому регулированию и метрологии №1503-ст от 30 декабря 2019);
- включено в перечень стандартизированных протоколов, которые могут быть использованы для организации информационного обмена между компонентами интеллектуальной системы учета электроэнергии (приказ №788 Минцифры России от 30 декабря 2020 года).

Разработанный метод оценки показателей эффективности мер защиты криптографических протоколов применен при проведении работ в рамках Технического комитета по стандартизации №26 «Криптографическая защита информации» при анализе криптографических протоколов ESP и IKEv2 [33].

Результаты, выносимые на защиту:

- классификация уязвимостей технологии «Интернета вещей»;
- семейство протоколов защищенного взаимодействия;
- метод построения формальной модели криптографических протоколов и формализации свойств безопасности;
- метод оценки показателей эффективности защиты в рамках построенной модели;
- теорема о значениях показателей эффективности мер защиты для семейства протоколов защищенного взаимодействия.

Методы исследования

Для решения поставленных задач использовались методы дискретной математики, алгебры, теории чисел, теории алгоритмов и математической логики и теории автоматов (теории графов).

Объектом исследования является разработанное в рамках диссертационного исследования семейство протоколов защищенного взаимодействия, включающее в себя:

- Протокол выработки общего ключа по схеме Диффи-Хеллмана в группе точек эллиптической кривой.
- Протокол аутентификации на основе использования предварительно распределенного ключа и инфраструктуры PKI или алгоритма электронной подписи ГОСТ Р 34.10-2012.
- Протокол передачи прикладных данных, не зависящий от типа используемого транспортного канала и уровня взаимодействия в рамках модели ISO.

Предметом исследования являются показатели эффективности защиты, разработанного в рамках диссертационного исследования семейства протоколов защищенного взаимодействия при помощи предложенного в исследовании метода оценки показателей эффективности защиты.

Личный вклад автора

Проведенное автором аналитическое исследование IoT-технологий позволило сформулировать перечень типовых классов уязвимостей, характерных для IoT-технологий. Автор принимал активное участие в процессе разработки и стандартизации нового семейства криптографических протоколов защищенного взаимодействия контрольных и измерительных устройств. Предложенный автором подход позволил построить модель семейства криптографических протоколов и провести оценку эффективности их защитных мер, а также обосновать выполнение требуемых свойств безопасности. Все результаты, выносимые на защиту, получены лично автором.

Общие выводы исследования

1. Проведен аналитический обзор ряда руководящих документов по созданию защищенных IoT-устройств, IoT-инфраструктур и сервисов, разработанных международными, отраслевыми комитетами и национальными организациями по стандартизации. Изучены спецификации стека протоколов ряда IoT-технологий и научные публикации, посвященные вопросам безопасности данных технологий. Проведена классификация уязвимостей различных стеков протоколов, используемых в технологиях «Интернета вещей». В результате анализа сформулирован перечень основных источников и уязвимостей, характерных для взаимодействия IoT-устройств.

2. Разработано новое семейство протоколов SP-FIOT, включающее в себя протокол выработки общего ключа и транспортный протокол передачи прикладных данных.

3. Предложен метод построения формальной модели криптографических протоколов и формализации в его рамках свойств безопасности.

4. Предложен способ оценки показателей эффективности защиты в рамках построенной модели, позволяющий получать численные оценки трудоемкости и вероятности нарушения исследуемых свойств безопасности криптографических протоколов.

5. Доказана теорема о значениях показателей эффективности для разработанного семейства протоколов защищенного взаимодействия SP-FIOT.

Апробация работы

Результаты, полученные в рамках диссертационной работы, были представлены и обсуждались на следующих научных конференциях:

1. V симпозиум «Современные тенденции в криптографии» CTCrypt'2016 (Ярославль, 2016). Доклад: Analysis of the Russian key-agreement protocols using automated verification tools.

2. The Sixth China-Russia Conference on Numerical Algebra with Applications (CRCNAA 2017) (Москва, 2017). Доклад: Grafting the Herbs family of key exchange protocols onto the TLS tree.

3. 17 Всероссийская конференция «сибирская научная школа-семинар с международным участием «компьютерная безопасность и криптография» – SIBECRYPT'18 (Абакан, 2018). Доклад: Интеграция отечественных протоколов выработки общего ключа в протокол TLS 1.3.

4. Ежегодная межвузовская научно-техническая конференция студентов, аспирантов и молодых специалистов имени Е.В.Арменского (Москва, 2020). Доклад: протокол защищенного взаимодействия средств криптографической защиты информации.

5. Ежегодная межвузовская научно-техническая конференция студентов, аспирантов и молодых специалистов имени Е.В.Арменского (Москва, 2021). Доклад: Методика оценки свойств безопасности криптографических протоколов.

Тезисы представленных докладов опубликованы в [34], [35], [36], [37].

Публикации

По теме диссертационного исследования автором опубликовано шесть печатных работ, две из них в международных изданиях, индексируемых в базе данных Scopus.

Работы, опубликованные автором в рецензируемых научных изданиях, входящих в систему цитирования Scopus

1. Нестеренко А. Ю. Методика оценки безопасности криптографических протоколов / А. Ю. Нестеренко, А. М. Семенов // ПДМ. - 2022. - №56. - С. 33-82.

2. Nesterenko A. Yu. On the practical implementation of Russian protocols for low-resource cryptographic modules / A. Yu. Nesterenko, A. M. Semenov // Journal of Computer Virology and Hacking Techniques. - 2020. - Vol. 16. - №4. - P. 305-312.

Работа, опубликованная автором в рецензируемых научных изданиях, входящих в список рекомендованных журналов НИУ ВШЭ

3. Semenov A. M. Analysis of Russian key-agreement protocols using automated verification tools // Математические вопросы криптографии. 2017. Vol. 8. № 2. P. 131-142.

Работы, опубликованные в других изданиях

4. Нестеренко А. Ю., Семенов А. М. Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств // Безопасность информационных технологий. 2020. Т. 27. № 4. С. 7-16.

5. Нестеренко А. Ю., Лебедев П. А., Семенов А. М., Краткий анализ криптографических механизмов защищенного взаимодействия контрольных и измерительных устройств. Технический комитет по стандартизации «Криптографическая защита информации». «Криптографические исследования». 2019. Сер. б/н. URL: https://tc26.ru/standarts/kriptograficheskie-issledovaniya (дата обращения: 17.07.2022).

6. Ноздрунов В., Семенов А.М., Подходы к криптографической защите коммуникаций в IoT и M2M. Информационная безопасность, № 5, 2019. с. 38–40. URL: https://infotecs.ru/about/press-centr/publikatsii/podkhody-k-kriptograficheskoy-zashchite-kommunikatsiy-v-iot-i-m2m.html (дата обращения: 17.07.2022).

Список литературы

[1] RFC7452 - Architectural Considerations in Smart Object Networking. Internet Architecture Board (IAB). - 2015. - 24 p.

[2] Ross, R., McEvilley, M., and J. Oren, «Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems», NIST Special Publication 800-160, DOI 10.6028/NIST.SP.800-160. November 2016. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/ NIST.SP.800-160.pdf. (дата обращения 01.10.2021).

[3] Internet of Things Security Foundation Establishing Principles for Internet of Things Security. URL: https://iotsecurityfoundation.org/establishing-principles-for-internet-of-things-security. (дата обращения 01.10.2021)

[4] Moore K. Best Current Practices for Securing Internet of Things (IoT) Devices / K. Moore, R. Barnes, H. Tschofenig // IETF-draft, draft-moore-iot-security-bcp-01, January 2018. URL: https://tools.ietf.org/id/draft-moore-iot-security-bcp-01.html (дата обращения 05.05.2022)

[5] European Union Agency for Network and Information Security, Communication network dependencies for ICS/ SCADA Systems, 2017, URL: https://www.enisa.europa.eu/publications/ ics-scada-dependencies. (дата обращения 01.10.2019)

[6] Р 1323565.1.028-2019 Информационная технология. Криптографическая защита информации. Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств, - М.: Стандартинформ, 2019. - 66 с.

[7] Р 1323565.1.032-2020 Информационная технология. Криптографическая защита информации. Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS. - М.: Стандартинформ, 2020. - 40 с.

[8] Р 1323565.1.029-2019 Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем. - М.: Стандартинформ, 2019. - 15 с.

[9] Р 1323565.1.018-2018 Информационная технология. Криптографическая защита информации. Криптографические механизмы аутентификации в кон-

трольных устройствах для автотранспорта. - М.: Стандартинформ, 2018. - 19 с.

[10] ГОСТ Р 70036-2022 «Информационные технологии. Интернет вещей. Протокол беспроводной передачи данных на основе узкополосной модуляции радиосигнала (NB-Fi). - М.: Российский институт стандартизации, 2022. - 56 с.5

[11] ПНСТ Информационные технологии. Интернет вещей. Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопотреблением. URL: https://docs.cntd.ru/document/554596382 (дата обращения 05.05.2022)

[12] ПНСТ Информационные технологии. Архитектура открытой сети радиодоступа. URL: https://www.normacs.info/projects/9439 (дата обращения 05.05.2022)

[13] ПНСТ Информационные технологии. Интерфейсы открытой сети радиодоступа. URL: https://www.normacs.info/projects/10453 (дата обращения 05.05.2022)

[14] ПНСТ Информационные технологии. Интернет вещей. Общие положения. URL: https://allgosts.ru/35/110/pnst_419-2020.pdf (дата обращения 05.05.2022)

[15] Алферов А. П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. - М.: Гелиос АРВ, 2002. - 480 с.

[16] Бабаш А. В. Криптография / А.В. Бабаш, Г.П. Шанкин - М.: Солон-Пресс, 2007. - 512 с.

[17] Качалин И. Ф. Об основных концепциях криптографической стойкости / И.Ф. Качалин, А.С. Кузьмин, Е.А. Суслов // Тезисы XII Всерос. школы-коллоквиума по стохастическим методам и VI Всерос. симпозиума по прикладной и промышленной математике. Сочи-Дагомыс, 1–7 октября 2005 г. С. 982–983

[18] Лось А.Б. Криптографические методы защиты информации. / А.Б. Лось, А.Ю. Нестеренко, М.И. Рожков // - М.: Изд-во Юрайт, 2016. - 473 с.

[19] Нестеренко А. Ю. Методика оценки безопасности криптографических протоколов / А. Ю. Нестеренко, А. М. Семенов // ПДМ. - 2022. - №56. - С. 33-82.

[20] Bellare M. Entity authentication and key distribution / M. Bellare, P. Rogaway // LNCS. - 1993. - Vol. 773. - pp. 232-249

[21] Bellare M. Authenticated key exchange secure against dictionary attacks / M. Bellare, D. Pointcheval, P. Rogaway // LNCS. - 2000. - Vol. 1807. - pp. 139-155

[22] Bellare M.Provably secure session key distribution — the three party case / M. Bellare, P. Rogaway // 27th ACM Symp. Theory Computing. - 1995. - pp. 57–66

[23] Blake-Wilson S. Key agreement protocols and their security analysis / S. Blake-Wilson, D. Johnson, A. Menezes // LNCS. - 1997. - Vol. 1355. - pp. 30–45

[24] Blake-Wilson S. Entity authentication and authenticated key transport protocols employing asymmetric techniques / S. Blake-Wilson, A/ Menezes // LNCS. - 1998. - Vol. 1361. - pp. 137–158

[25] Canetti R. Analysis of key-exchange protocols and their use for building secure channels/ R. Canetti, H. Krawczyk // LNCS. - 2001. - Vol. 2045. - pp. 453-474

[26] LaMacchia B.. Stronger security of authenticated key exchange / B. LaMacchia, K. Lauter, A. Mityagin // LNCS. - 2007. - Vol. 4784. - pp. 1–16

[27] Krawczyk H. HMQV: A high-performance secure Diffie — Hellman protocol / H. Krawczyk // LNCS. - 2005. - Vol. 3621. - pp. 546–566

[28] Menezes A. On the importance of public-key validation in the MQV and HMQV key agreement protocols/ A. Menezes, B. Ustaoglu // LNCS. - 2006. - Vol. 4329. - pp. 133-147

[29] Rabin M. Digitized Signatures and Public Key Functions as Intractable as Factorization / M. Rabin // Technical Report: MIT/LCS/TR-212. MIT Laboratory for Computer Science. - Cambrige. - 1979. - pp. 20.

[30] Goldwasser S. Probabilistic encryption / S. Goldwasser, S. Micali // J. Computer System Sci. - 1984. - Vol. 28. - pp. 270–299

[31] Mao W. Modern Cryptography: Theory and Practice. New Jersey: Prentice Hall, 2003. - 707 p.

[32] Boyd C. Protocols for Authentication and Key Establishment / Boyd C., Mathuria A., and Stebila D. // Second Ed. Berlin; Heidelberg: Springer Verlag. - 2020. - 521 p

[33] Р 1323565.1.035–2021 Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе защиты информации ESP. - М.: Стандартинформ, 2021. - 52 с.

[34] Semenov A., Analysis of Russian key-agreement protocols using automated verification tools, Pre-proceedings of 5th Workshop on Current Trends in Cryptology, CTCrypt 2016 (June 6-8, 2016, Yaroslavl, Russia), с. 23-37

[35] Гребнев С. В., Лазарева Е. В., Лебедев П. А., Нестеренко А. Ю., Семенов А. М. Интеграция отечественных протоколов выработки общего ключа в протокол TLS 1. 3 // ПДМ. Приложение. 2018. №11, с. 62-65. URL: https://cyberleninka.ru/article/n/integratsiya-otechestvennyh-protokolov-vyrabotki-obschego-klyucha-v-protokol-tls-1-3 (дата обращения: 17.07.2022)

[36] Нестеренко А.Ю., Семенов А.М. Протокол защищенного взаимодействия средств криптографической защиты информации // Межвузовская научно-техническая конференция студентов, аспирантов и молодых специалистов имени Е.В. Арменского. Материалы конференции. Москва: 2020, с. 172-174

[37] Нестеренко А.Ю., Семенов А.М. Методика оценки свойств безопасности криптографических протоколов // Межвузовская научно-техническая конференция студентов, аспирантов и молодых специалистов имени Е.В. Арменского. Материалы конференции. Москва: 2021, с. 249-251