МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное автономное образовательное учреждение высшего образования

«Санкт-Петербургский политехнический университет Петра Великого»

На правах рукописи

Шкоркина Елена Николаевна

АУТЕНТИФИКАЦИЯ УСТРОЙСТВ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ С ДЕЛЕГИРОВАНИЕМ ВЫЧИСЛЕНИЙ В ГРАНИЧНОЙ АРХИТЕКТУРЕ

2.3.6 – Методы и системы защиты информации, информационная безопасность (технические науки)

Направленность: 10.06.01_01 – Методы и системы защиты информации, информационная безопасность

Академическая степень **Исследователь. Преподаватель-исследователь**

НАУЧНЫЙ ДОКЛАД

Научный руководитель: д.т.н., доцент, профессор ИКиЗИ,

Александрова Елена Борисовна

Санкт-Петербург, 2022

Научный доклад выполнен в Институте кибербезопасности и защиты информации федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого»

Научный руководитель: д.т.н., доцент, профессор ИКиЗИ,
Александрова Елена Борисовна

Рецензент: д.т.н., доцент, профессор ИКиЗИ,
Полтавцева Мария Анатольевна

С научным докладом можно ознакомиться в библиотеке ФГАОУ ВО «Санкт–Петербургский политехнический университет Петра Великого» и на сайте Электронной библиотеки СПбПУ по адресу: http://elib.spbstu.ru.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. Повышение степени интегрированности в повседневную жизнь электронных потребительских устройств Интернета вещей (ИВ) в архитектуре самоорганизующихся сетей (СС) при тесном взаимодействии физических и информационных процессов приводит к возникновению новых задач, касающихся как построения сетей при соблюдении требований к передаче данных и к алгоритмам взаимодействия, так и аспектов безопасности, основополагающим из которых является аутентификация. Их решение осложнено невозможностью зачастую достичь приемлемой скорости реализации защитных механизмов из-за вычислительных ограничений устройств, их высокой мобильности, большого числа взаимодействующих узлов СС и необходимости принятия решений исходя из аккумулированной информации большого объема.

Необходимость разработки отечественных систем, функционирующих в критических сферах и имеющих встроенные механизмы предупреждения киберфизических нарушений безопасности информации, закреплена, в том числе, в законах и нормативно-правовых актах Российской Федерации. Кроме того, создание безопасных систем СС соответствует стратегическим целям Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г.

Присущие СС строгие требования по стоимости узлов влекут за собой ограниченные вычислительные и энергетические возможности устройств. Для эффективной реализации протоколов аутентификации зачастую используются алгоритмы криптографического аутсорсинга, позволяющие передать одному или нескольким внешним вычислителям (серверам) некоторые математические операции из состава трудоемкого защитного преобразования. Существенное удорожание инфраструктуры сети при внедрении аутсорс-сервера перекрывает все преимущества такого способа снижения нагрузки на низкоресурсное устройство.

Использование облачных технологий, очевидное на первый взгляд, в сетях Интернета вещей не работает на должном уровне. Во-первых, большое количество передаваемых данных не позволяет осуществлять обработку в режиме реального

времени, во-вторых, географическая удаленность серверов от устройств привносит в сеть физическое ограничение скорости, неприемлемое для Интернета вещей. Данные недостатки привели к созданию концепции граничных вычислений, архитектура которых предполагает иерархическую организацию взаимодействия низкоресурсных устройств между собой с и облачными серверами через граничный сервер. Однако новая архитектура сети не позволяет использовать уже известные протоколы по причине того, что они предусматривают равное распределение вычислительной нагрузки между участниками. Известные протоколы, созданные для данной парадигмы, не учитывают все модели взаимодействия устройств при аутентификации.

В рамках данной работы предлагается использовать разработанный протокол аутентификации управляющего устройства на исполнительном с распределением ключей защищенного управления, функционирующий на основе гибридной концепции делегирования вычислений с единым сервером, в рамках которой в составе данного протокола с граничными вычислениями используются методы криптографического аутсорсинга.

Степень разработанности темы исследования. Исследованию безопасности архитектуры граничных вычислений посвящены работы группы зарубежных авторов К. Ша, Т. А. Ян, В. Вэй и С. Давари, а также группы российских авторов В. В. Рябоконь, А. А. Кузькина, С. Ю. Тутова и А. С. Махова. Протоколы аутентификации устройств граничной архитектуры описаны в работах А. Шахидинежад, К. Каура, Н. Кумана, А. Яна.

Объектом исследования являются СС электронных потребительских устройств, в отношении которых совершаются деструктивные воздействия.

Предметом исследования являются подходы и методы аутентификации с делегированием вычислений в граничной архитектуре СС.

Целью работы является обеспечение защищенного взаимодействия низкоресурсных узлов СС на основе концепции граничной аутентификации с гибридным делегированием вычислений.

Для достижения поставленной цели в работе решались следующие **задачи**:

1. Анализ специфики построения систем аутентификации в архитектуре граничных вычислений, определение моделей взаимодействия связанных устройств.

2. Разработка протокола аутентификации управляющих устройств с распределением ключей защиты данных в архитектуре граничных вычислений и протокола защищенного управления; определение криптографических наборов различных уровней стойкости системы (классической и постквантовой).

3. Выбор аутсорс-алгоритмов делегирования вычислений для сложных вычислительных задач из состава выбранных криптографических наборов.

4. Разработка метода гибридного делегирования вычислений в модели с одним сервером, определение модели безопасности и оценка эффективности.

5. Разработка рекомендаций по практическому применению предложенного подхода аутентификации и схемы защищенного управления в СС.

Методы исследования включают в себя теорию информационной безопасности, методы математического моделирования, теории чисел, алгебраической геометрии и криптографии.

Научная новизна полученных результатов:

1. Разработана комплексная модель взаимодействия узлов СС в граничной архитектуре.

2. Впервые предложен протокол аутентификации в архитектуре граничных вычислений, позволяющий аутентифицировать управляющее устройство на исполнительном с проверкой подлинности граничного сервера и распределением ключей последующего защищенного управления.

3. Впервые разработана схема защищенного управления исполнительным устройством в граничной архитектуре, использующая ключи, выработанные в рамках протокола аутентификации, и функционирующая с использованием того же множества криптографических алгоритмов.

4. Впервые предложена методика гибридного делегирования вычислений на основе концепции граничных и аутсорс-вычислений в модели с одним доверенным сервером.

Теоретическая значимость работы определяется эффективностью предложенного подхода к построению системы аутентификации в граничной архитектуре на основе принципа гибридного делегирования вычислений с точки зрения потребления ресурсов узлом СС, а также его высокой степенью применимости; разработанным для данного подхода протоколом и выбранными криптографическими наборами.

Практическая значимость результатов работы заключается в возможности применения предложенного метода и протокола для реализации системы аутентификации электронных потребительских устройств СС в граничной архитектуре. Полученные в ходе работы результаты позволяют:

– предупредить угрозы нарушение безопасности информации и сохранить устойчивость функционирования самоорганизующихся сетей благодаря разработанному протоколу аутентификации управляющего устройства на исполнительном с распределением ключей;

– осуществлять защищенное управление устройствами СС без существенных задержек в режиме реального времени благодаря методике гибридного делегирования вычислений;

– обеспечивать стойкость системы аутентификации и управления по отношению к атакам с использованием квантового компьютера при реализации криптографического набора с протоколами инкапсуляции ключей и цифровой подписи на решетках (CRYSTALS-Kyber и CRYSTALS-Dilithium).

Положения, выносимые на защиту:

1. Протокол аутентификации управляющих устройств с распределением ключей защищенного управления в архитектуре граничных вычислений, учитывающий специфику самоорганизующихся сетей.

2. Схема защищенного управления исполнительным устройством, расширяющая протокол аутентификации в части использования выработанных ключей.

3. Метод гибридного делегирования вычислений на основе концепции граничных и аутсорс-вычислений в модели с одним доверенным сервером.

Внедрение результатов работы. Полученные основные научные результаты диссертационного исследования использованы при реализации гранта Российского Фонда Фундаментальных Исследований 20-37-90110 «Криптографические преобразования для самоорганизующихся сетей в условиях ограниченных ресурсов».

Достоверность и обоснованность результатов, представленных в диссертации, подтверждается всесторонним анализом предшествующих научных работ в данной области, полученными экспериментальными данными и апробацией результатов в научных публикациях и докладах на конференциях.

Соответствие специальности научных работников. Полученные научные результаты соответствуют следующим пунктам «Области исследования» паспорта специальности научных работников 2.3.6 «Методы и системы защиты информации, информационная безопасность»:

– Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет (п. 5);

– Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа (п. 12).

– Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов (п. 19).

Апробация работы. Основные результаты исследований и научных разработок докладывались и обсуждались на следующих конференциях: международная конференция «Региональная информатика (РИ-2016)» (Санкт-Петербург, 2016 г.), научно-практическая конференция с международным

участием «Неделя науки СПбГПУ» (Санкт-Петербург, 2017 г.), научно-техническая конференция «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2017–2022 гг.), межрегиональная конференция «Информационная безопасность регионов России» (Санкт-Петербург, 2017 и 2021 гг.), международная конференция «Fourth World Conference on Smart Trends in Systems, Security and Sustainability WorldS4» (Лондон (Великобритания), 2022 г.).

Основные результаты научно-квалификационной работы победили в конкурсе грантов Правительства Санкт-Петербурга для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга, в 2017, 2019, 2020 и 2022 годах.

Публикации. Результаты научно-квалификационной работы отражены в 21 публикации, в том числе в 4 публикациях в рецензируемых журналах из перечня ВАК РФ, а также 6 публикациях в изданиях из перечня Scopus и Web of Science.

Объем и структура научно-квалификационной работы. Работа состоит из введения, четырех глав, заключения и списка литературы из 27 наименований. Общий объем работы составляет 57 страниц, в том числе 15 рисунков и 8 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы научно-квалификационной работы, поставлена цель работы, определены задачи. Выделены положения, выносимые на защиту, научная новизна и практическая значимость работы.

В первой главе приведены результаты исследования принципов функционирования СС, областей их практического применения и угроз безопасности информации.

Анализ типов СС показал, что вне зависимости от выполняемых на разнородных низкоресурсных устройствах задач крайне высокими являются риски нарушения киберфизических свойств безопасности. Модель защиты СС при этом функционирует без возможности использования организационных методов

(отсутствие нелегитимного доступа к устройствам, невозможность считывания побочных электромагнитных излучений и наводок и т. д.). Реализация аутентификации – основополагающего механизма безопасности СС – осложнена необходимостью обработки информации в режиме реального времени с учетом постоянного изменения топологии сети и высокого энергопотребления в случае летающих и автомобильных СС. Анализ атак на СС показа их преимущественную связь с использованием беспроводной сети и строгими требованиями по стоимости, влекущими за собой малые вычислительные и энергетические возможности устройств и отсутствие защиты от вскрытия. В основном действия злоумышленника направлено на чтение конфиденциальной информации, целенаправленный вывод узла из строя, а также перехват управления устройством.

Выполнена классификация СС по характеру выполняемых на устройствах приложений: Самоорганизующиеся сети можно классифицировать по характеру выполняемых на устройствах приложений (см. рисунок 1):

1) WSN (Wireless Sensors Networks) – беспроводные сети сенсорных устройств, используемые для сбора показаний (температура, влажность, освещенность и др.) с различных умных датчиков по расписанию. Для них характерно малое время нахождения в сети и малые объемы передачи данных.

2) WMN (Wireless Mesh Networks) – беспроводные сети на основе ячеистой топологии, функционирующие поверх существующей сети, в которых каждое устройство представляет собой как клиента, так и маршрутизатора.

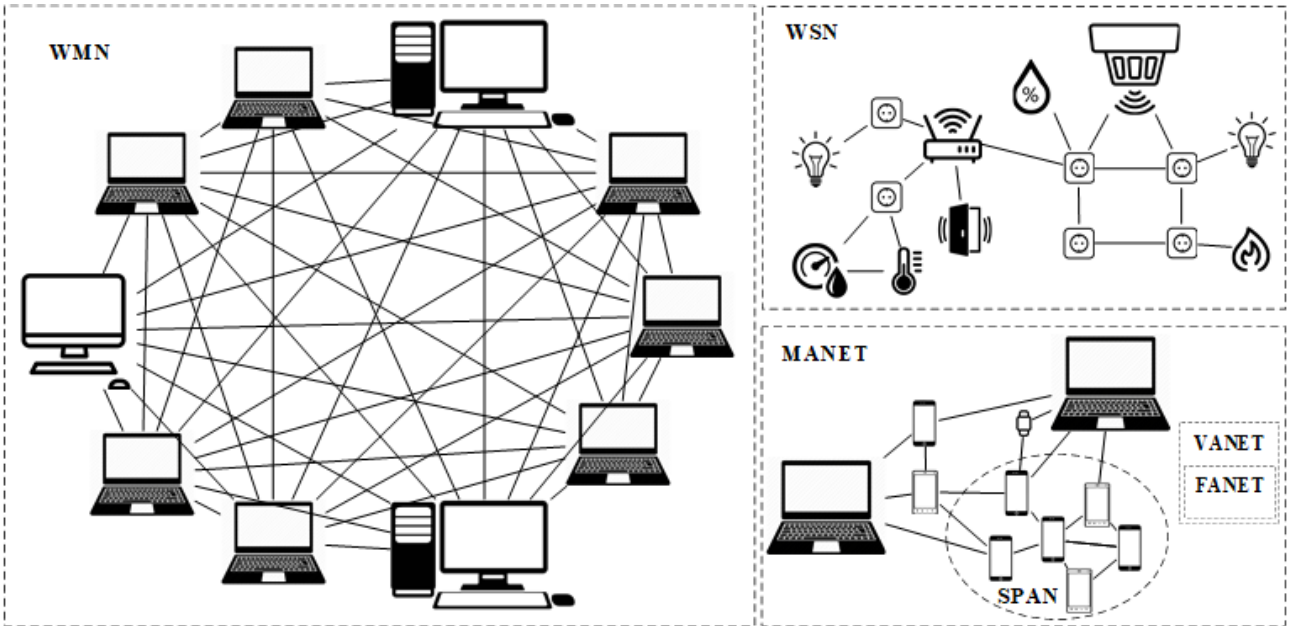

Рисунок 1 – Классификация самоорганизующихся сетей

3) MANET (Mobile Ad Hoc Networks) – мобильные самоорганизующиеся сети – любые сети, предназначенные для объединения мобильных устройств (сотовых и умных телефонов, ноутбуков, автомобилей, любых летательных аппаратов, в том числе и беспилотных) без привязки к единой локации. По типу используемых устройств в рамках MANET можно выделить:SPAN (Smart phone Ad Hoc Network) – одноранговая сеть смартфонов, взаимодействующих в пределах досягаемости друг друга без использования сетей сотовых операторов, точек беспроводного доступа и т. д.

– VANET (Vehicular Ad Hoc Networks) – подмножество MANET, включающее в себя мобильные самоорганизующиеся сети автомобилей, летательных аппаратов, мобильных судов и других транспортных средств. Их важной особенностью является высокая скорость перемещения устройств, повышенные требования конфиденциальности, целостности и доступности сообщений в таких сетях. Кроме того, архитектуры таких сетей содержат неподвижные объекты инфраструктуры (базовые станции).

– FANET (Flying Ad Hoc Networks) – подмножество VANET, включающее в себя летательные аппараты (преимущественно, беспилотные (БПЛА)) и, как следствие, отличающееся высокой мобильностью узлов, в том числе и по

вертикали, значительными расстояниями между устройствами (низкой плотностью сети), частыми изменениями топологии сети и ограниченными вычислительными и энергетическими возможностями. Из-за таких характеристик к устройствам FANET-сети предъявляются требования по удельному весу и ограничения для мощности беспроводных передатчиков, выполнение которых позволяет сохранить время работы БПЛА. Архитектура такой сети может быть как распределенной, таки иерархической.

Анализ различий в характеристиках их функционирования показал, что в мобильных сетях, особенно летающих, функционируют самые мобильные и энергоемкие узлы.

Выявлены факторы, влияющие на реализацию защитных преобразований в СС: преимущественное использование низкоресурсных устройств, связанное со строгими требованиями по стоимости; физическое ограничение скорости передачи данных даже при использовании сетей мобильной связи четвертого поколения (4G); возможность активного перемещения устройств и децентрализованность сети; необходимость обработки данных в режиме реального времени; разнородность используемых криптографических протоколов.

Анализ способов передачи данных в СС показал необходимость перехода к сетям связи пятого поколения (5G), позволяющим не только повысить скорость передачи данных, но и снизить энергозатраты устройств.

Рассмотрены интеллектуальные транспортные системы в качестве примера инфраструктуры, в рамках которой используются такие типы СС как беспроводные сети сенсорных устройств, одноранговые сети смартфонов, автомобильные и летающие СС.

Во второй главе приведен разработанный протокол аутентификации управляющего устройства на исполнительном с распределением ключей защищенного управления.

Выделены особенности, делающие граничные вычисления перспективным решением для использования в сетях Интернета вещей, особенно самоорганизующихся: обработка данных в режиме реального времени с

возможностью принятия решения об аутентификации, дополнительная защита подсетей связанных устройств за счет внедрения в граничные сервера функционала средств обнаружения и предотвращения вторжений, возможность совмещения с базовой станцией связи стандарта 5G, делегирование вычислительной нагрузки с низкоресурсных устройств ИВ на граничный сервер.

Рассмотрены модели взаимодействия устройств в рамках иерархической архитектуры граничных вычислений. Сделан вывод об отсутствии решения для аутентификации одного устройства ИВ (управляющего) на другом (исполнительном) через граничный сервер в соответствии со схемой, приведённой на рисунке 2.

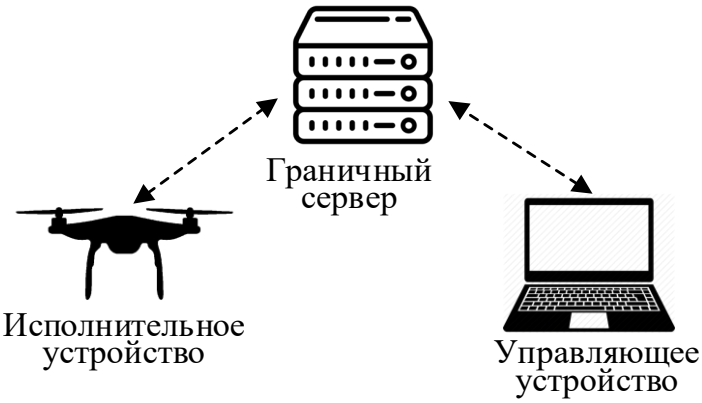

Рисунок 2 – Модель взаимодействия двух устройств ИВ в рамках протокола аутентификации в граничной вычислительной архитектуре

Разработанный протокол аутентификации состоит из двух фаз: инициализации и аутентификации с распределением ключей управления.

На этапе инициализации выполняется распределение симметричного ключа аутентификации K_{auth}, получение граничным сервером от доверенной стороны значения подписи $Sign_{ES}$ для своих уникальных идентификационных данных ID_{ES}, а также загрузка открытого ключа центра регистрации в управляющее и исполнительное устройства для проверки подписи $Sign_{ES}$.

Аутентификация с распределением ключей управления состоит из шагов, приведенных на рисунке 3. Используются различные типы криптографических алгоритмов (асимметричное E/D и симметричное шифрование E^{sym}/D^{sym}, аутентифицированное шифрование $E^{sym}_{auth}/D^{sym}_{auth}$, проверка подписи $Verify()$),

асимметричные ключи подписи ($Pk_{Dev_1}^{ENC}, Sk_{Dev_1}^{ENC}$) и шифрования ($Pk_{Dev_1}^{ENC}, Sk_{Dev_1}^{ENC}$) граничного сервера, а также случайные значения r, q.

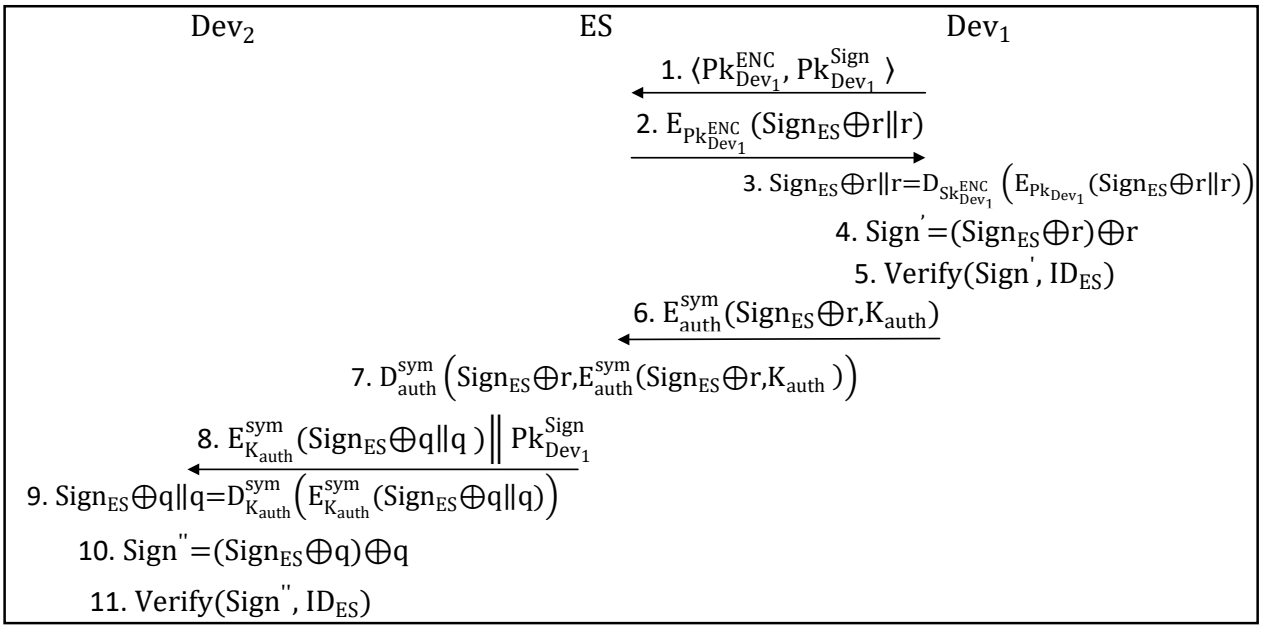

Рисунок 3 – Схема протокола аутентификации с установлением ключей управления

Обоснована безопасность разработанного протокола от атаки подмены сервера, криптоанализа по известному открытому тексту и атак, направленных на истощение энергоресурсов исполнительного устройства (Energy-draining DDoS).

Разработана схема защищённого управления исполнительным устройством через граничный сервер с использованием распределенных ключей $K_1 = Sign_{ES} \oplus r$ и $K_2 = Sign_{ES} \oplus q$, состоящая из шагов, приведенных на рисунке 4.

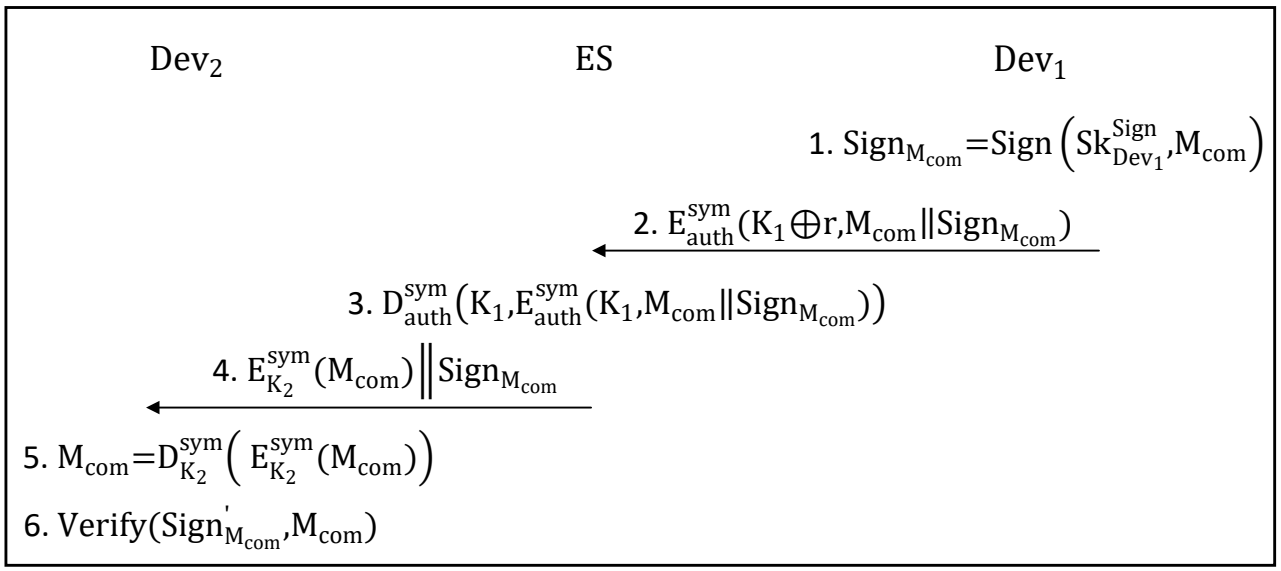

Рисунок 4 – Схема защищенного управления исполнительным устройством

Протокол аутентификации и схема защищенного управления обладают гибкостью в части выбора используемых криптографических алгоритмов и протоколов, поскольку определены только их типы. При этом множество, с использованием которого будет осуществляться функционирование, должно быть подобрано на основе модели угроз системы. Если возможность выполнения нарушителем эффективного квантового криптоанализа не учитывается, целесообразно использовать набор протоколов классического уровня стойкости, в противном случае – постквантового. С учетом того, что исполнительное устройство гарантированно является низкоресурсным, алгоритмы должны быть выполнимы за разумное время без потери актуальности передаваемой информации.

Выбраны криптографические наборы протокола аутентификации и схемы управления двух уровней стойкости: классической и постквантовой. Для первого определены схема шифрования Эль-Гамаля на эллиптических кривых, блочный шифр в режиме счетчика (PRESENT, «Магма» или AES-128), режим аутентифицированного шифрования (MGM с использованием шифра «Магма» или режим GCM шифра AES-128), а также протокол подписи (ECDSA или ГОСТ Р 34.10–2018). Второй включает в себя алгоритмы инкапсуляции ключей и подписи на решетках (CRYSTALS-Kyber, CRYSTALS-Dilithium), а также аналогичные режимы для более стойких блочных шифров («Кузнечик» или AES-256).

На рисунке 5 показана схема внедрения алгоритма инкапсуляции CRYSTALS-Kyber в разработанный протокол аутентификации, предполагающая на шаге 1 передачу вместо открытого ключа шифрования соответствующего ключа инкапсуляции $Pk_{Dev_1}^{Exp}$, а также выработку на шаге 2 по алгоритму $Encaps()$ общего ключа K, имеющего шифртекст c. Далее формируется шифрограмма $E_K^{sym}(Sign_{ES} \oplus r \| r)$ и передается вместе с шифртекстом (шаги 3–4). Для получения управляющим устройством общего ключа выполняется алгоритм $Decaps()$. Схема взаимодействия граничного сервера и исполняющего устройства остается без изменений.

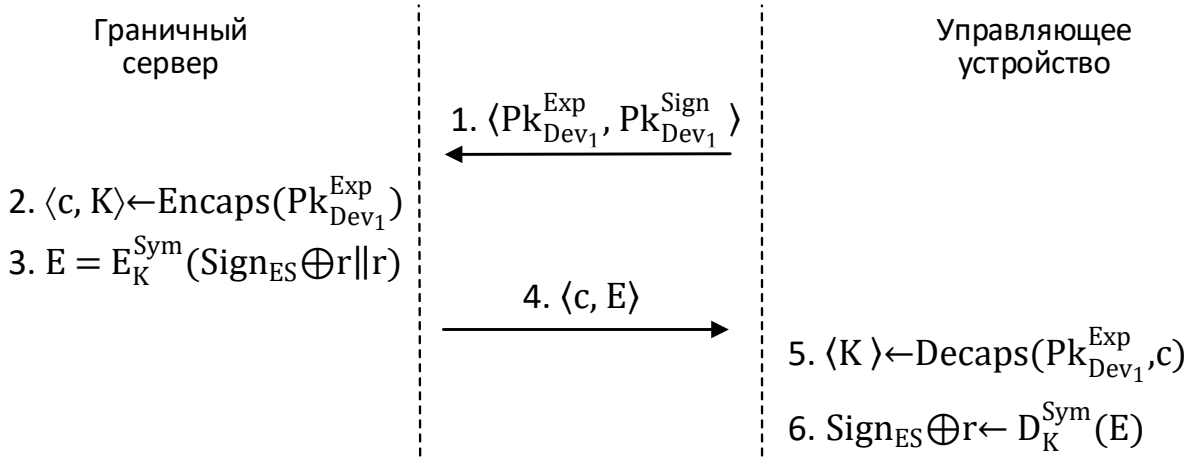

Рисунок 5 – Внедрение постквантового алгоритма инкапсуляции ключа CRYSTALS-Kyber в разработанный протокол аутентификации

В третьей главе рассмотрены принципы и отличительные особенности методов криптографического аутсорсинга и граничных вычислений в контексте делегирования трудоемких задач. Выявлено, что алгоритмы первой концепции могут функционировать с использованием как одного, так и двух аутсорс-серверов, а в модели безопасности внешние вычислители учитываются исключительно как недоверенные с возможностью сговора или без нее. Вторая концепция отличается неравномерным (несимметричным) распределением вычислительных операций за счет расположения между узлом Интернета вещей и управляющим модулем граничного сервера, отправляющего запрос аутентификации только после успешного выполнения части взаимодействия с устройством, инициирующим обмен.

Предлагается использовать разработанный протокол аутентификации управляющего устройства на исполнительном с распределением ключей защищенного управления, функционирующий на основе гибридной концепции делегирования вычислений, в рамках которой в составе данного протокола с граничными вычислениями используются методы криптографического аутсорсинга. Функционал внешнего аутсорс-вычислителя, граничного сервера и базовой станции связи стандарта 5G предлагается объединить в едином устройстве.

Для разработанного протокола аутентификации и схемы управления предлагается использовать гибридную концепцию делегирования вычислений с единым сервером, предполагающей использование методов криптографического аутсорсинга в протоколе с граничными вычислениями. Целесообразность его применения возникает тогда, когда характеристики устройства (как правило, исполнительного) не позволяют выполнить криптографическую функцию эффективно: при аутентификации на крайне низкоресурсном устройстве ИВ и / или обеспечении постквантовой стойкости системы.

Для такой концепции, при условии выполнения аутентификации граничного сервера, предложено не предъявлять требования по безопасности, связанные с обеспечением нераскрываемости промежуточных или итоговых данных внешним вычислителем. Сделан вывод об избыточности использования аутсорс-алгоритмов с повышенной безопасностью, а также дополнительных механизмов, позволяющих отличить намеренные действия вредоносного сервера от случайных ошибок, таких как протокол неоспоримой подписи.

Модель безопасности гибридного делегирования вычислений для разработанного протокола аутентификации и схемы управления с учетом всех особенностей граничной вычислительной архитектуры определена как модель с одним доверенным сервером.

Основной трудоемкой математической операцией криптографического набора классической стойкости определено умножение точки эллиптической кривой (ЭК) на число, для постквантовой стойкости – умножение матрицы на скаляр. Для первой операции выбран аутсорс-алгоритм $ScalarMult$ с одним

сервером, позволяющий снизить трудоемкость операции до одного умножения, одного сложения и трех приведений по модулю в простом поле. Форма маскирования искомого скаляра позволяет сформировать для каждого из запросов на аутсорс-вычисление множество предвычисленных значений.

Оценка эффективности применения выбранного аутсорс-алгоритма $ScalarMult$ выполнена на основе полученных для микроконтроллера ESP8266 замеров времени выполнения криптографических операций в группе точек ЭК с использованием библиотеки micro-ecc, приведенных в таблице 1.

Таблица 1 – Результаты измерений времени выполнения операций в группе точек ЭК на микроконтроллере ESP8266

Операция в группе точек ЭК	Время, мкс
Вычисление обратного	1629
Умножение в простом поле	1511
Сложение различных точек ЭК	6 397
Умножение точки ЭК на число	71 267

С учетом множества операций, выполнение которых требуется, посчитано общее время выполнения алгоритма, составившее 155573 мкс без применения алгоритма $ScalarMult$ и 26 864 мкс с аутсорсингом (см. таблицу 2).

Таблица 2 – Состав и количество операций алгоритмов проверки подписей операций ECDSA и ГОСТ Р 34.11–2018

Алгоритм / Операция/время	ECDSA / ГОСТ Р 34.10–2018	ECDSA / ГОСТ Р 34.10–2018 с применением $ScalarMult$
Вычисление обратного	1	1
Умножение в простом поле	2	2 + 2
Сложение различных точек ЭК	1	1 + 2
Умножение точки ЭК на число	2	0
Время, мкс	155 573	26 864

Практически показана эффективность применения протокола $ScalarMult$, соответствующая уменьшению времени выполнения алгоритма проверки подписи в 5,7 раз.

Анализ аутсорс-алгоритмов умножения матрицы на скаляр показал, что известные решения являются исключительно подходами с повышенной

безопасностью на основе гомоморфного шифрования и разделения секрета. С учетом ранее сделанного вывода о нецелесообразности использования таких методов, предлагается использовать граничный сервер в качестве компьютера-компаньона и передавать исполнительному устройству вместе с запросом на аутентификацию значение $MSB(Az-ct)$, вычисление которого необходимо при проверке подписи CRYSTALS-Dilithium. Сложность выполнения функции проверки подписи в таком случае снизится до одного вычисления значения хэш-функции.

В четвертой главе предложены конкретные способы применения разработанной системы аутентификации и защищенного управления.

Показана схема удаленного обновления прошивки сенсора, типовая для любого исполнительного узла СС. Аутентификация центра управления с использованием K_{auth}^{light} приведена на рисунке 6, а защищенное обновление программного обеспечения P_{light} «по воздуху» с использованием распределенных граничным сервером ключей $K_1^{cnt} = Sign_{ES} \oplus r_1$ и $K_2^{light} = Sign_{ES} \oplus q_1$ – на рисунке 7.

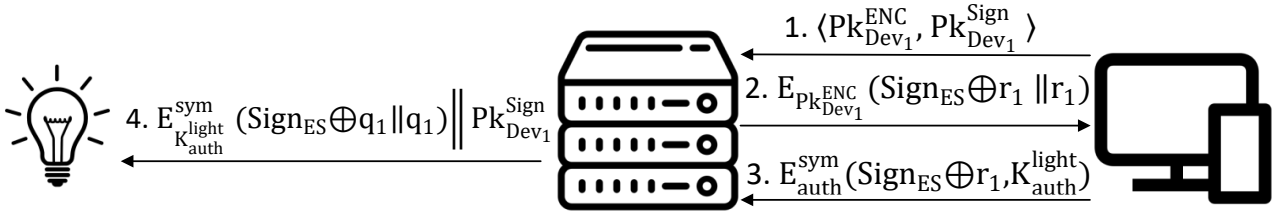

Рисунок 6 – Выполнение протокола аутентификации с использованием ключа K_{auth}^{light}

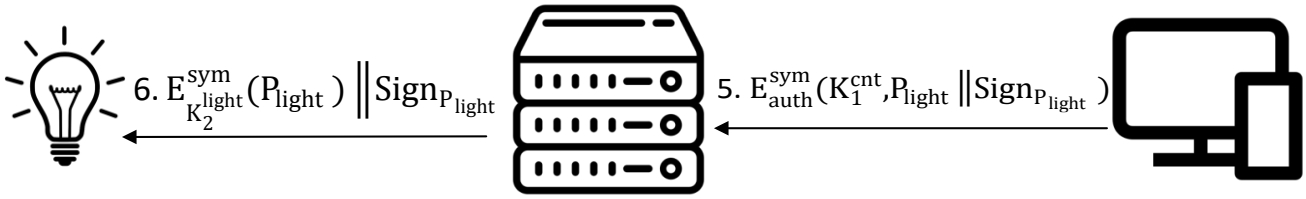

Рисунок 7 – Удаленное обновление прошивки сенсора «по воздуху» с использованием ключей K_1^{light} и K_2^{light}

Показана схема принудительного снижения скорости автомобиля, функционирующего в рамках СС типа VANET. Если УУ инициирует

аутентификацию через граничный сервер впервые, либо срок её действия истек, протокол выполняется полностью аналогично схеме, приведенной на рисунке 6, с использованием ключа аутентификации K_{auth}^{car} и уникальных r_2 и q_2. В противном случае считается, что фаза взаимодействия УУ и граничного сервера пройдена, для их защищенного взаимодействия распределен ключ K_1^{cnt} и остается выполнить упрощенную аутентификацию, представленную на рисунке 8.

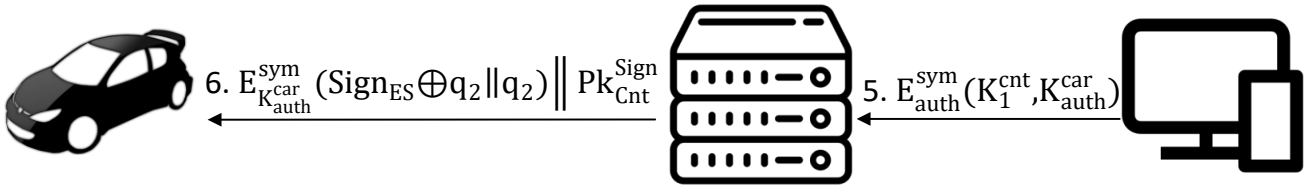

Рисунок 8 – Упрощенная аутентификация УУ на ТС

В результате распределяется $K_2^{car} = Sign_{ES} \oplus q_2$ и Pk_{Cnt}^{Sign}, схема использования которых вместе с K_1^{cnt} для отправки команды $M_{spd} = ID_{car} \| speed$ принудительного снижения скорости автомобиля с идентификатором ID_{car} до значения $speed$ приведена на рисунке 9.

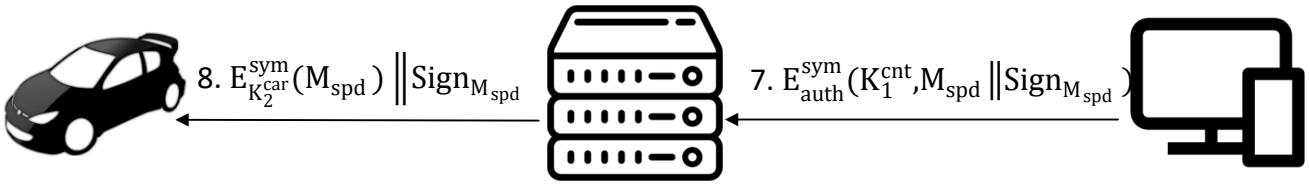

Рисунок 9 – Аутентифицированное принудительное снижение скорости транспортного средства

Приведен пример использования системы аутентификации для характерной мобильным СС широковещательной рассылки таблиц маршрутизации, данных переконфигурации сети, а также общих для группы узлов команд управления.

Пусть в системе предварительно распределен для всех устройств группы БПЛА ключ K_{auth}^{drn}, а от граничного сервера УУ уже распределен K_1^{cnt}. Тогда широковещательную аутентификацию группой БПЛА предлагается выполнять в соответствии со схемой, приведенной на рисунке 10.

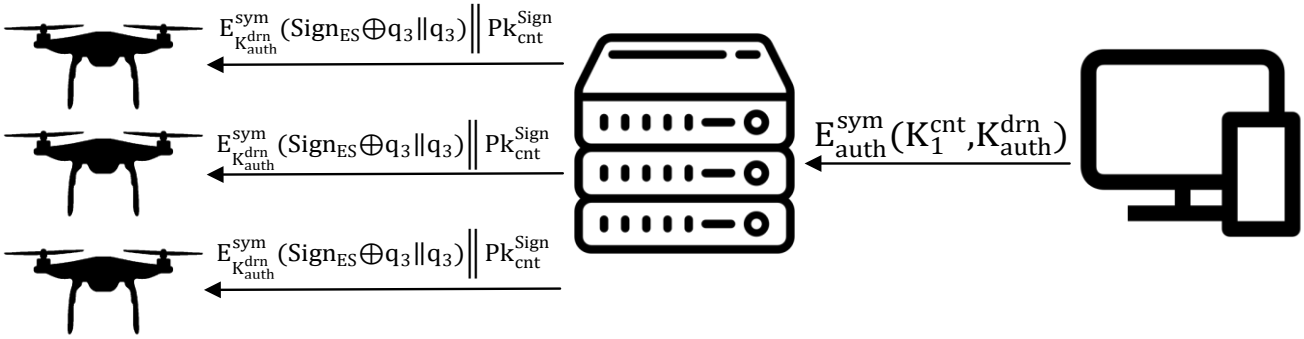

Рисунок 10 – Широковещательная аутентификация группой БПЛА

Соответствующая схема широковещательного управления группой БПЛА с с использованием ключа K_2^{drn} приведена на рисунке 11.

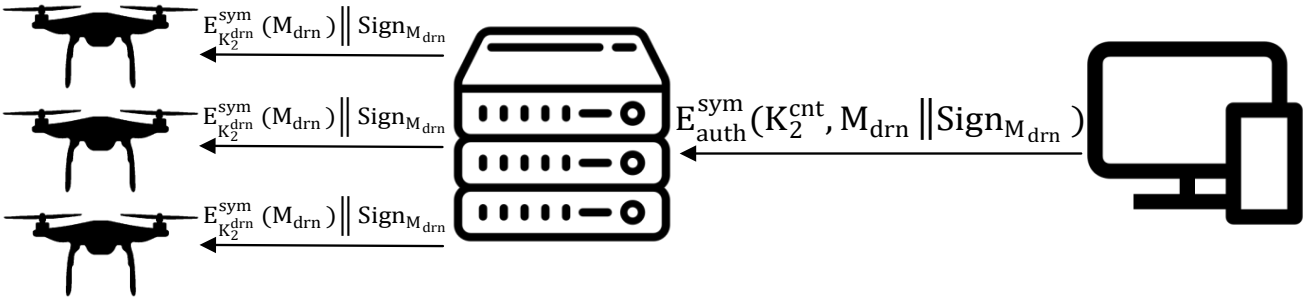

Рисунок 11 – Широковещательное управление группой БПЛА

В заключении приведены основные результаты, полученные в ходе выполнения научно-квалификационной работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Исследованы особенности и принципы функционирования СС с точки зрения обеспечения безопасности, классифицированы типы СС по характеру выполняемых на устройствах приложений, выявлены и систематизированы угрозы нарушения безопасности, приведены сферы применения СС.

2. Разработан протокол аутентификации управляющего устройства на исполнительном с распределением ключей защищенного управления, гибкость которого обеспечивается за счет возможности выбора конкретных криптографических алгоритмов для заданных типов. Приведены доказательства его безопасности, показывающие защиту от подмены сервера, атак по известному

открытому тексту и атак, направленных на истощение энергоресурсов исполнительного устройства (Energy-draining DDoS).

3. Разработана схема защищенного управления исполнительным устройством, расширяющая протокол аутентификации в части использования выработанных ключей. Определены криптографические наборы двух уровней стойкости системы: классической и постквантовой.

4. Предложен метод гибридного делегирования вычислений, позволяющий при аутентификации большого количества устройств или обеспечении постквантовой стойкости не снижать эффективность криптографического протокола за счет использования методов криптографического аутсорсинга в протоколе с граничными вычислениями. Для модели безопасности метода предлагается снижение требования по не раскрываемости промежуточных или итоговых данных внешним вычислителем при выполнении его аутентификации. Для криптографического набора протокола и схемы защищенного управления классического уровня стойкости выполнена оценка эффективности выбранного аутсорс-алгоритма умножения точки ЭК на число.

5. Разработаны рекомендации по практическому применению протоколов аутентификации и защищенного управления в самоорганизующихся сетях для защищенного удаленного обновления прошивок устройств, реализации механизма принудительного снижения скорости транспортного средства VANET-сети, а также широковещательной аутентификации и управления группой БПЛА.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях из перечня ВАК РФ:

1. Шкоркина Е. Н. Трехсторонний протокол установления ключа на билинейных отображениях с использованием аутсорс-технологий / Александрова Е. Б., Шкоркина. Е. Н. //Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 3. – С. 102–108.

2. Шкоркина Е. Н. Применение неоспоримой подписи на эллиптических кривых для верификации сервера при аутсорс-вычислениях /Александрова Е. Б., Шкоркина Е. Н. // Проблемы информационной безопасности. Компьютерные системы. – 2018. – № 1. – С. 97–101.

3. Шкоркина Е. Н. Обеспечение постквантового уровня стойкости систем квантово-защищенной связи / Шкоркина Е. Н., Александрова Е. Б. // Проблемы информационной безопасности. Компьютерные системы. – 2020. – № 2. – С. 35–39.

4. Шкоркина Е. Н. Аутентификация управляющих устройств в сети Интернета вещей с архитектурой граничных вычислений / Александрова Е. Б., Облогина А. Ю., Шкоркина Е. Н. // Проблемы информационной безопасности. Компьютерные системы. – 2021. – № 2. – С. 82–88.

Публикации из перечня SCOPUS и Web of Science:

1. Shkorkina E. N. Tripartite outsourcing key-agreement protocol on bilinear pairings / Aleksandrova E. B., Shkorkina E. N. //Automatic Control and Computer Sciences. – 2016. – V. 50. – №. 8. – P. 796–801.

2. Shkorkina E. N. Using Undeniable Signature on Elliptic Curves to Verify Servers in Outsourced Computations / Aleksandrova E. B., Shkorkina E. N. // Automatic Control and Computer Sciences. – 2018. – V. 52. – №. 8. – P. 1160-1163.

3. Shkorkina E. N. Securing Post-Quantum Resistance for Quantum-Protected Communication Systems / Shkorkina E. N., Aleksandrova E. B. // Automatic Control and Computer Sciences. – 2020. – V. 54. – №. 8. – P. 949-951.

4. Shkorkina E. N. Authentication of Control Devices in the Internet of Things with the Architecture of Edge Computing / Aleksandrova E. B., Oblogina A. Y.,

Shkorkina E. N. // Automatic Control and Computer Sciences. – 2021. – V. 55. – №. 8. – P. 1087–1091.

5. Shkorkina E. Threshold Isogeny-Based Group Authentication Scheme / Aleksandrova, E., Pendrikova, O., Shtyrkina, A., Shkorkina, E., Yarmak, A., & Tick, J.//Algorithms and Solutions Based on Computer Technology. – Springer, Cham, 2022. – С. 117–126.

6. Shkorkina E. Authentication protocol for intelligent electronic devices in an edge IoT environment with key agreement / Shkorkina E. // 2022 Sixth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4 2022). – IEEE, 2022.

Наиболее значимые публикации в других изданиях:

1. Шкоркина Е. Н. Реализация криптосистем на билинейных отображениях с использованием аутсорс-алгоритмов / Александрова Е. Б., Шкоркина Е. Н. // Материалы научно-технической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Издательство Политехнического университета, 2016. – № 25. – С. 66.

2. Шкоркина Е. Н. Применение аутсорс-протоколов в одноранговых самоорганизующихся сетях беспилотных летательных аппаратов / Александрова Е. Б., Шкоркина Е. Н. // Материалы научно-технической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Издательство Политехнического университета, 2017. – № 26. – С. 41–42.

3. Шкоркина Е. Н. Использование неоспоримой подписи для верификации аутсорс-сервера / Шкоркина Е. Н., Александрова Е. Б. //Информатика и кибернетика (ComCon-2017): сборник докладов студенческой научной конференции Института компьютерных наук и технологий 3–8 апреля 2017 года. – СПб.: Издательство Политехнического университета, 2017 – С.245–249.

4. Шкоркина Е. Н. Обеспечение конфиденциальности и целостности данных, передаваемых беспилотными летательными аппаратами в Арктическом регионе / Шкоркина Е. Н., Александрова Е. Б. // Информационная безопасность регионов России (ИБРР-2017): Материалы конференции, Санкт-Петербург, 01–03

ноября 2017 года. – СПб: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. – С. 383–385.

5. Шкоркина Е. Н. Оценка эффективности применения аутсорсинга для построения маломощных криптосистем / Шкоркина Е. Н., Александрова Е. Б. // Неделя науки СПбПУ: Материалы научной конференции с международным участием, Санкт-Петербург, 19–24 ноября 2018 года. – СПб: Издательство Политехнического университета, 2018. – С. 161–163.

6. Шкоркина Е. Н. Применение личностных схем шифрования с подписью совместно с аутсорсингом в VANET/FANET-сетях / Шкоркина Е. Н., Александрова Е. Б. // Материалы научно-технической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Издательство Политехнического университета, 2018. – № 27. – С. 82.

7. Шкоркина Е. Н. Принципы реализации симметричных криптографических алгоритмов на малоресурсных устройствах / Шкоркина Е. Н., Александрова Е. Б. // Материалы научно-технической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Издательство Политехнического университета, 2020. – № 29. – С. 114–115.

8. Шкоркина Е. Н., Облогина А. Ю., Александрова Е. Б. Применение методов делегирования вычислений при решении задачи аутентификации низкоресурсных узлов //Материалы научно-технической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Издательство Политехнического университета, 2021. – № 30. – С. 53–54.

9. Шкоркина Е. Н. Реализация алгоритмов на основе изогений суперсингулярных эллиптических кривых в самоорганизующихся сетях / Крамсаков Е. Ю., Шкоркина Е. Н., Александрова Е. Б. // Материалы научно-технической конференции «Методы и технические средства обеспечения безопасности информации». СПб.: Издательство Политехнического университета, 2021. – № 30. – С. 52–53.

10. Шкоркина Е. Н. Аутентификация в граничной вычислительной архитектуре с выработкой ключей защиты данных / Шкоркина Е. Н. // Материалы научно-технической конференции «Методы и технические средства обеспечения

безопасности информации». СПб.: Издательство Политехнического университета, 2022. – № 31. – С. 178–179.

11. Шкоркина Е. Н. Криптографические наборы протокола аутентификации низкоресурсных устройств в граничной вычислительной архитектуре / Шкоркина Е. Н. // Материалы конференции «Информационные технологии в управлении» (ИТУ-2022), 2022.