УДК 004.03 DOI: 10.34708/GSTOU.2022.57.12.002

КЛЮЧЕВЫЕ ТЕХНОЛОГИИ ШЛЮЗА БЕЗОПАСНОСТИ КОНВЕРГЕНЦИИ IOT

© Л.К. Хаджиева, А.Б. Чадаева
ГГНТУ им. акад. М.Д. Миллионщикова, Грозный, Россия

Данная статья посвящена исследованию наиболее значимых технологий шлюза безопасности конвергенции Интернета вещей. Шлюз является важной технической составляющей Интернета вещей, занимая ключевую позицию связующего звена между сенсорной сетью и традиционной коммуникационной сетью. В рамках этого направления исследований рассмотрены основные сетевые технологии, такие как технология многорежимной связи, технология передачи данных через шлюз, технология надежных вычислений, технология обработки данных, технология шлюза с низким энергопотреблением. В статье также дано подробное рассмотрение протокола Modbus промышленного контроллера и внедрение агрегированного шлюза безопасности Интернета вещей на основе протокола Modbus, сделан обзор связанных исследований и технологий безопасности передачи данных через шлюз. При этом сделан также акцент на энергосберегающий алгоритм маршрутизации оверлейной сети шлюза и механизм пробуждения шлюза из сна для обеспечения работы сети.

Ключевые слова: Интернет вещей, передача данных, шлюз безопасности, протокол Modbus, одноранговая сеть, оверлейная сеть.

Сущность сети в основном отражается в трех аспектах: во-первых, характеристики Интернета вещей (IoT), то есть объекты, которые необходимо подключить к Интернету, должны быть в состоянии обеспечить взаимосвязь. Во-вторых, идентификационные и коммуникативные характеристики, то есть «вещи», включенные в Интернет вещей, должны иметь функцию автоматической идентификации и связи между ними, то есть сетевая система должна обладать характеристиками автоматизации, обратной связи и интеллектуального управления. Отраслевую цепочку IoT можно разделить на восприятие, обработку и передачу информации. Существует три звена: ключевыми технологиями каждого звена являются сенсорная технология, технология интеллектуальной обработки информации и технология сетевой передачи.

С широкомасштабным применением беспроводных датчиков сетевые технологии беспроводных датчиков привлекают все больше и больше внимания, в связи с чем Интернет-технологии играют очень важную роль в период стремительного развития Интернета вещей и станут связующим звеном между сетью восприятия и традиционной коммуникационной сетью, так как шлюзы IoT могут осуществлять преобразование протоколов между сетями восприятия и сетями связи, а также различными типами сетей восприятия. Кроме того, шлюз IoT также имеет функцию управления устройством, и операторы могут использовать устройство шлюза IoT для управления каждым узлом на нижнем уровне, воспринимать соответствующую информацию о каждом узле и осуществлять дистанционное управление. Узел беспроводного датчика собирает соответствующую информацию о данных и отправляет данные на шлюз посредством беспроводной многоступенчатой самоорганизации. Система считывает информацию и отправляет на шлюз. Шлюз, в свою очередь, отправляет данные на сервер, где информация обрабатывается, хранится, а также предоставляет данные на информационную платформу [1].

Обзор связанных исследований. Являясь ядром всей сети, шлюз IoT может реализовывать взаимодействие сети датчиков и сети связи, а также протоколы между различными типами сетей датчиков.

С широкомасштабным применением беспроводных датчиков сетевые технологии беспроводных датчиков привлекают все больше и больше внимания, в связи с чем было предложено множество протоколов маршрутизации, но при этом нет четкого метода классификации протоколов маршрутизации. Многие приложения, очень восприимчивые к характеристикам сетей, в связи с этим используются следующие виды протоколов маршрутизации: ориентированные на данные, протоколы маршрутизации на основе кластера, на основе местоположения, на основе моделей потоков данных и QoS, а также надежные протоколы маршрутизации. Общий метод заключается в рассмотрении топологической структуры сенсорной сети и разделении протоколов маршрутизации на две категории: протоколы плоской маршрутизации и кластерные протоколы маршрутизации.

В последние годы появилось много новых протоколов маршрутизации и методов проектирования сенсорных сетей. Например, используя метод оптимизации трафика в теории графов для выбора маршрутизации, объединение архитектуры протокола уровня MAC и уровня маршрутизации с использованием технологии межуровневой оптимизации, в первую очередь для экономии энергии [2].

В Интернете вещей большое количество датчиков собирает данные на шлюз, в результате чего некоторым узлам шлюза необходимо передавать большие объемы данных в Интернет за короткий период времени, что приводит к перегрузке сети. Технология одноранговой сети шлюза в сочетании с технологией наложенной сети, то есть построение логической сетевой структуры на уровне IP для того, чтобы решить эту проблему. Программный модуль на шлюзе обычно используется для построения сети прикладного уровня и реализации технологии маршрутизации и распределенной передачи прикладного уровня. Сетевая модель наложенной сети сетевого шлюза показана на рисунке 1.

Для построения такой сети можно использовать маршрутизаторы Cisco. Особенности данного решения: простота включения в сеть оператора благодаря наличию моделей с портами Ethernet, SHDSL и ADSL, интегрированные Ethernet-порты, простота установки, использования и возможность дистанционного управления с помощью доступных через сеть инструментов, готовность к внедрению дополнительных сервисов – таких как IP-телефония и видеонаблюдение.

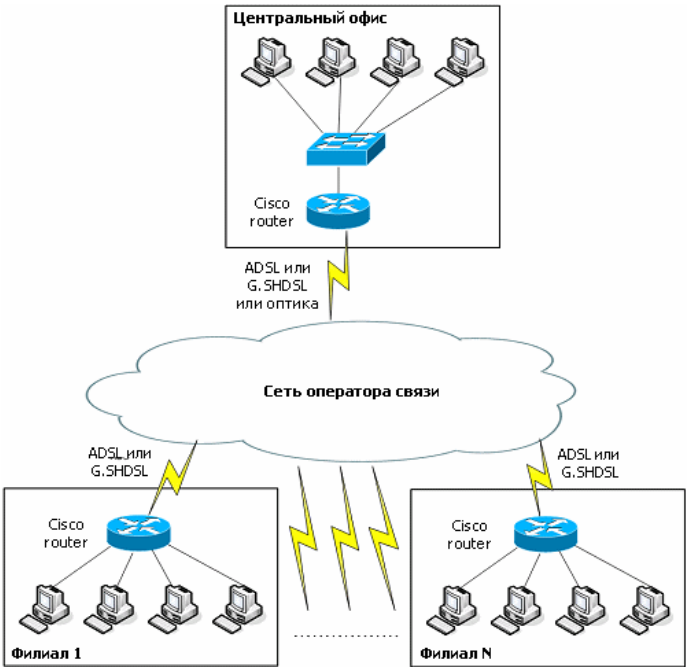

Рис. 1. Диаграмма сетевой модели наложенной сети [3]

Сеть, построенная по данной схеме, обеспечивает надежную и защищенную работу корпоративных приложений и сервисов, таких как электронная почта, платежные терминалы и т. д. Рассмотренное решение обеспечивает базовые сервисы, а при необходимости подключения дополнительных функционалов поверх базовой сети предоставляет возможности развернуть новые сервисы в целях повышения эффективности и управляемости бизнес-процессов [3].

В среде Интернета вещей сосуществуют несколько режимов связи,

таких как WiFi, ZigBee и 3G, LTE, в связи с чем возникает необходимость адаптации к требованиям различных типов продуктов.

Программное радио является основой для реализации многорежимной связи и адаптации. Программное радио делает упор на открытое и простое оборудование в качестве общей платформы, реализацию функций радио с различным прикладным программным обеспечением, можно максимально модернизировать и переконфигурировать.

Основная задача заключается в построении гибкой сети, которая представляет собой открытую, стандартизированную и модульно общую аппаратную платформу. Для ее создания необходимо установить рабочую полосу частот, формат данных, режим шифрования. Различные функции в такой сети, такие как протоколы связи, выполняются программным обеспечением. Если рассмотреть программное обеспечение для определения возможностей беспроводной сети, мы убедимся, что система программного обеспечения включает в себя различные правила беспроводной сигнализации и обработки: программное обеспечение для управления, для преобразования потока сигналов, для исходного кодирования, для кодирования с исправлением ошибок канала, для алгоритмов модуляции и демодуляции.

Технология безопасности, внедряемая в данной разработке, обеспечивает безопасность передаваемого контента и безопасность связи, применяя криптографическую технологию и собственные протоколы криптографической безопасности. Передаваемые файлы и данные проходят поэтапно процедуры: цифровую подпись, цифровую проверку, проверку подписи данных и другие средства безопасности для обеспечения целостности файла и передачи данных. Данная технология включает в себя безопасность на уровне канала и безопасность контента [4].

Технология аппаратного шифрования VPN используется на уровне канала, а протокол связи разработан поверх TCP/IP, при этом частный протокол обмена данными формируется с использованием TLV. Контентная безопасность включает в себя мониторинг порядкового номера потока задач, типа задачи, содержимого и параметров времени. Данная технология выбирает соответствующий метод передачи (блок или короткое сообщение) и метод кодирования в соответствии с содержимым интерактивных данных.

Решение проблемы взаимного доверия основывается на выделении сущностного сегмента, содержащего информацию об идентификации пользователя, информацию об открытом ключе пользователя и цифровую подпись агентства по проверке личности. Согласно требованиям, обмен данными между центром безопасности и отделом мониторинга строится на принципе обеспечения целостности [5].

Целью надежных вычислений является защита критически важных данных в информационных системах, решение все более серьезных проблем компьютерной безопасности и повышение эффективности вычислительных ресурсов. TCPA (Альянс надежных вычислительных платформ) впервые предложил концепцию надежной вычислительной платформы, и ее основная теория основана на аппаратном обеспечении и стандартизации программного обеспечения для защиты от программных атак и обеспечения безопасности данных.

Конкретная реализация надежной вычислительной платформы осуществляется через текущую вычислительную платформу путем добавления нового оборудования и программного обеспечения. TCG разработала ряд технических спецификаций для определения стандартного поведения и функций этих компонентов, в том числе включая основную спецификацию TCG. Trusted Platform Module предназначен для хранения ключей, паролей, и это микроконтроллер для цифровых сертификатов, который может обеспечивать надежные криптографические функции и обычно интегрируется в материнскую плату.

Соединение Trusted Network Connect (TNC), предложенное TCG, в основном направлено на решение проблем безопасности существующей сети. Это открытая архитектура решения сетевой безопасности. Данная архитектура помогает сетевым администраторам внедрять определенную политику безопасности для обеспечения подключения к сети. На шлюзе информация, собранная сенсорными

узлами, объединяется и обрабатывается для получения более эффективных и удобных для пользователя данных, что может снизить потребность в сети. Таким образом, объем передаваемых данных в сети может быть уменьшен. Чтобы уменьшить потребление связи и продлить жизненный цикл сети, данная технология использует архитектуру обработки модуля объединения данных. Для предварительной обработки массивных данных Интернета вещей модуль завершает набор данных [6].

Масштабы Интернета вещей и количество узлов огромны, а проблема энергопотребления сети становится все более серьезной. Для снижения энергопотребления можно использовать:

1. Протокол маршрутизации наложенной сети шлюза с низким энергопотреблением, который выбирает оптимизированный путь передачи для пакета. Совокупный трафик нагрузки на часть ссылки или в устройствах неиспользуемые каналы или устройства отключены, или бездействуют для экономии энергопотребления сети, но сеть необходимо учитывать при объединении.

2. Внедрить многоуровневый механизм сна-пробуждения. Механизм пробуждения и глубина сна в разных состояниях сна различны. По мере увеличения глубины сна соответственно снижается его энергопотребление, а шлюзы и другие системные устройства в разных регионах будут иметь разное время.

3. Проектирование и внедрение шлюза безопасности IoT промышленного управления на базе Modbus – элементами защиты IoT в этом случае также являются доступность, конфиденциальность, идентифицируемость и управляемость, что может сформировать систему безопасности IoT [7].

Рассмотрим протокол связи для контроллера и управления связи, по данному протоколу контроллеры могут связываться с контроллерами и другими устройствами по сети. Открытость, расширяемость и стандартизация протокола связи делают его общепромышленным стандартом. Протокол Modbus можно легко и надежно подключить к промышленной сети для централизованного мониторинга системы, в том числе может применяться и между программируемым логическим контроллером (ПЛК), поддерживающим протокол Modbus, между персональными компьютерами, между удаленными ПЛК [8].

Modbus широко используется и является одним из самых популярных протоколов промышленного управления, поскольку имеет широкую базу приложений. Одним из преимуществ Modbus является отсутствие необходимости в специальных интерфейсных контроллерах, простота программной реализации и элегантность принципов функционирования. Все это снижает затраты на освоение стандарта как системными интеграторами, так и разработчиками контроллерного оборудования.

В России Modbus по распространенности конкурирует только с Profibus. Популярность протокола в настоящее время объясняется, прежде всего, совместимостью с большим количеством оборудования, которое имеет протокол Modbus. Кроме того, Modbus имеет высокую достоверность передачи данных, связанную с применением надежного метода контроля ошибок. Modbus позволяет унифицировать команды обмена благодаря стандартизации номеров (адресов) регистров и функций их чтения-записи. Протокол имеет два режима передачи: RTU и ASCII. По сравнению с протоколом RTU протокол MODBUS ASCII имеет начальный и конечный маркеры, а MODBUS RTU – нет, поэтому обработка пакетов данных в программе протокола ASCII может быть удобнее. MODBUS ASCII передает все видимые символы ASCII, поэтому оно более интуитивно понятно на этапе отладки, а его программу проверки LRC также легче написать, это преимущества MODBUS ASCII. Основным недостатком MODBUS ASCII является низкая эффективность передачи, поскольку он передает все видимые символы ASCII. Для каждого байта данных, передаваемых RTU, если используется ASCII, байт должен быть разделен на два бита. Поскольку в протоколе ASCII есть начальная метка и конечная метка, интервал передачи данных может быть больше 1 секунды, а в режиме MODBUS RTU, поскольку начальная и конечная метки не указываются, протокол предусматривает, что каждый интервал времени между передачей или приемом двух байтов

не может превышать 3,5-кратное время передачи символа. Если временной интервал между двумя символами превышает время передачи символа в 3,5 раза, считается, что кадр данных принят, и начинается новый кадр передачи данных, поэтому существует требование времени для интервала передачи между двумя байтами в Режим РТУ. Это различие между протоколами ASCII и RTU MODBUS может привести к тому, что в некоторых приложениях может использоваться только один из протоколов [9].

Система Untangle поддерживает различные функции, такие как фильтрация спама, блокировка URL-адресов, антивирусный червь, обнаружение вторжений. UTM-устройства реализуют в данном случае технологии межсетевого экрана фильтрации, шлюза прикладного уровня, шлюза уровня схемы и проверки состояния сетевых пакетов, а также шлюза уровня схемы.

Система для достижения изоляции внутренних и внешних сетей. Система Untangle представляет собой прокси-модель, основанную на потоковой обработке. Система Untangle объединяет компоненты с открытым исходным кодом, а также использует функцию IPtables системы Linux, а модуль IPtables имеет функцию фильтрации сетевых пакетов и межсетевого экрана, Untangle также является брандмауэром для проверки состояния сетевых пакетов с собственными функциями защиты от атак. Система Untangle в основном состоит из следующих частей: система Debian-Linux, комбинация Linux-UVM, UVM и полнофункциональные компоненты, веб-интерфейс и система баз данных [10].

Модуль защиты протокола Modbus предоставляет протокол Modbus, определяющий простой блок данных (PDU), который не зависит от низлежащего уровня связи на определенной шине или сети. Отображение протокола Modbus позволяет ввести некоторые дополнительные поля в блок данных приложения (ADU). Служба обмена сообщениями Modbus обеспечивает связь клиент/сервер между устройствами, подключенными через Ethernet в сети TCP/IP [11, 12].

Модуль защиты протокола Untangle-Modbus использует хороший объектно-ориентированный дизайн, и все компоненты приложения безопасности на платформе Untangle называются узлами.

Новые приложения безопасности можно легко разрабатывать на платформе Untangle и быстро развертывать. Untangle основан на TcpSession, который позволяет реализовывать необходимые расширения протокола на прикладном уровне.

Выводы. Из-за все более широкого применения Интернета вещей и взрывного роста масштабов данных датчикам необходимо агрегировать большой объем информационных данных на шлюз, в результате узлу шлюза необходимо за короткое время передать через сеть массив данных в центр сбора данных, что может привести к перегрузке сети. Для этого необходимо улучшить возможности обработки данных шлюза и решить проблему перегрузки сетевой передачи между шлюзом и центральным сервером [13].

В статье рассмотрен Интернет вещей на основе соответствующей технологии одноранговой сети, на прикладном уровне которой строится логическая сеть на основе шлюза – оверлейная сеть шлюза, и предлагаются маршрутизация и передача в оверлейной сети шлюза. В статье показан механизм балансировки нагрузки, который может эффективно решить проблемы надежной передачи больших объемов данных и контроля перегрузки шлюза. Платформа, основанная на надежных вычислительных технологиях и криптографическом приложении, является основным сетевым модулем, несущим ответственность за подтверждение подлинности сенсорных узлов и шлюзов, за предотвращение присоединения вредоносных узлов шлюза для обеспечения безопасного сбора и контроля данных [14].

Механизм стимулирования доверия для передачи данных в предложенной сетевой модели IoT сочетается с сетевой технологией шлюза для обеспечения доверия шлюза управления. Для обеспечения безопасности всей виртуальной сети шлюза предложена схема оптимального установления сети каналов передачи в соответствии с различными уровнями безопасности данных. Рекомендована сетевая передача данных в сочетании с оверлейной

сетью шлюза, а также энергосберегающий алгоритм маршрутизации оверлейной сети шлюза и механизм пробуждения шлюза из сна для обеспечения эффективности работы сети.

ЛИТЕРАТУРА

1. *Хаджиева Л.К., Хаджиев М.Р., Исрахимова А.Т.* Концепция систем IOT для сельскохозяйственных услуг с высокой степенью автономии // Вестник ГГНТУ. Технические науки. Том XVII. №3 (25). Грозный, 2021.
2. *Хаджиева Л.К., Хаджиев М.Р., Хашумов И.У.* Перспективы внедрения технологии 5G и взаимодействие с системой «УМНЫЙ ДОМ» // Вестник ГГНТУ. Технические науки. Том XVII. №4 (26). Грозный, 2021.
3. https://www.osp.ru/lan/2010/11/13005564
4. *Хашумов И.У., Хаджиев М.Р., Мальцагов Х.Х.* Информационная безопасность и уязвимости IOT // Вестник ГГНТУ. Технические науки. Том XVI. №2 (20). Грозный, 2020.
5. Моисеенко Н.А., Джабраилов И.С. Проектирование информационной системы управления организацией: необходимость современности // Вестник ГГНТУ. Технические науки. Том XV. №2 (16). Грозный, 2019.
6. *Хаджиева Л.К., Мальцагов Х.Х.* Анализ технологии «Интернет вещей» (IOT) и ее роль в «Умном доме» // Вестник ГГНТУ. Технические науки. Том XV. №4 (18). Грозный, 2019.
7. *Хаджиева Л.К., Элиханов М.Ш.* Анализ перспективы внедрения технологии 5G и реализации ее возможностей для проектирования системы «УМНЫЙ ДОМ» // Материалы IV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «МИЛЛИОНЩИКОВ-2021» с международным участием ФГБОУ ВО «ГГНТУ им. акад. М.Д. Миллионщикова», Россия, Чеченская Республика, г. Грозный, 18-20 мая 2021 г.
8. *Хасамбиев И.В., Тасуева Х.Х.* Инфокоммуникационные технологии как системы управления объектом // Вестник ГГНТУ. Технические науки. Том XV. №4 (18). Грозный, 2019.
9. *Хаджиев М.Р., Хаджиева Л.К., Пайзулаева Р.Т., Мажитова З.Д.* Защита беспроводной сети передачи данных // Материалы IV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «МИЛЛИОНЩИКОВ-2021» с международным участием ФГБОУ ВО «ГГНТУ им. акад. М.Д. Миллионщикова», Россия, Чеченская Республика, г. Грозный, 18-20 мая 2021 г.
10. *Минцаев М.Ш., Хакимов З.Л., Лабазанов М.А.* Программирование логических контроллеров фирмы SIEMENS // Лабораторный практикум. Грозный, 2021.
11. *Алисултанова Э.Д., Хаджиева Л.К., Исаева М.З.* Профориентационная школьная лаборатория по основам кибербезопасности в сфере интернет вещей (IOT) // Вестник ГГНТУ. Гуманитарные и социально-экономические науки. 2019. Т. 15. №4 (18). С. 51-58.
12. *Murtazaev S.A., Mintsaev M., Salamanova M., Alaskhanov A., Aymenov Z.* Mineral powders dispersion degree effect on the properties of the cementing alkaline system. Materials Science Forum. 2021. Т. 1017. С. 31-40.
13. *Минцаев М.Ш., Эльсункаева Э.В.* Разработка ГИС-модуля для комплексного мониторинга геологической среды Ханкальского месторождения Чеченской Республики.
14. *Минцаев М.Ш., Лабазанов М.А., Исаева М.Р., Муртазова Х.Т.* Обоснование выбора технологической схемы бинарной установки // Геоэнергетика-2019. Материалы IV Всероссийской научно-технической конференции / Под ред. М.Ш. Минцаева. 2019. С. 349-357.

KEY TECHNOLOGIES OF THE IOT CONVERGENCE SECURITY GATEWAY

© L.K. Khadzhieva, A.B. Chadaeva
GSTOU named after M.D. Millionshchikov, Grozny, Russia

The Internet of Things is currently receiving more and more attention. This article is devoted to the study of the key technologies of the Internet of Things Convergence Security Gateway. Gateway is a proven technology of the Internet of Things, and plays an important role in the era of rapid development of IOT. In addition, it will become the link between the sensor network and the traditional communication network. The article discusses network technologies, such as multi-mode communication technology, data transmission technology through the gateway, reliable computing technology, data processing technology, low power gateway technology. The article also discusses in detail the Modbus protocol of an industrial controller and the implementation of an aggregated IoT security gateway based on the Modbus protocol, an overview of related research and security technologies for data transmission through the gateway is made. Finally, the article discusses the energy-saving routing algorithm of the gateway overlay network and the mechanism for waking the gateway from sleep to ensure network operation.

Keywords: Internet of things, data transfer, security gateway, Modbus protocol, peer-to-peer network, overlay network.

REFERENCES

1. Khadzhieva, L. K., Khadzhiev, M.R. and Israkhimova, A.T. (2021) 'Kontseptsiya sistem IOT dlya sel'skokhozyaistvennykh uslug s vysokoi stepen'yu avtonomii'. *Zhurnal «Vestnik GGNTU. Tekhnicheskie nauki».* [The concept of IOT systems for agricultural services with a high degree of autonomy. Journal "Herald of GSTOU. Technical sciences"]. V. XVII. №3 (25). Grozny.
2. Khadzhieva, L.K., Khadzhiev, M.R., Khashumov, I.U. (2021) 'Perspektivy vnedreniya tekhnologii 5G i vzaimodeistvie s sistemoi «UMNYI DOM»'. *«Vestnik GGNTU. Tekhnicheskie nauki»*. [Prospects for the introduction of 5G technology and interaction with the SMART HOUSE system. "Herald of GSTOU. Technical sciences"]. V. XVII. №4 (26). Grozny.
3. Available at: https://www.osp.ru/lan/2010/11/13005564
4. Khashumov, I.U., Khadzhiev, M.R. and Maltsagov, H.Kh. (2020) Information security and IOT vulnerabilities. Volume XVI. №2 (20). Grozny.
5. Moiseenko, N.A. and Dzhabrailov, I.S. (2019) *«Vestnik GGNTU. Tekhnicheskie nauki»*. [Designing an information system for managing an organization: the need for modernity. "Herald of GSTOU. Technical sciences"]. Volume XV. №2(16). Grozny.
6. Khadzhieva, L.K. and Maltsagov, Kh.Kh. (2019) 'Analiz tekhnologii «Internet veshchei» (IOT) i ee rol' v «Umnom dome»'. *Vestnik GGNTU. Tekhnicheskie nauki».* Analysis of the technology "Internet of Things" (IOT) and its role in the "Smart Home" "Herald of GSTOU. Technical sciences"]. Volume XV. №4 (18). Grozny.
7. Khadzhieva, L.K. and Elikhanov, M.Sh. (2021) 'Analiz perspektivy vnedreniya tekhnologii 5G i realizatsii ee vozmozhnostei dlya proektirovaniya sistemy «UMNYI DOM»'. *Materialy IV Vserossiiskoi nauchno-prakticheskoi konferentsii studentov, aspirantov i molodykh uchenykh «MILLIONShchIKOV-2021» s mezhdunarodnym uchastiem FGBOU VO «GGNTU im. akad. M.D. Millionshchikova»*. [Analysis of the prospects for the introduction of 5G technology and the implementation of its capabilities for the design of the "SMART HOUSE" system'. Proceedings of the IV All-Russian scientific and practical conference of students, graduate students and young scientists "MILLIONSCHIKOV-2021" with international participation - GSTOU named after acad. M.D. Millionshchikov, Russia, Chechen Republic, Grozny, May 18-20, 2021.

8. Khasambiev, I.V. and Tasueva, Kh.Kh. (2019) 'Infokommunikatsionnye tekhnologii kak sistemy upravleniya ob"ektom'. *Vestnik GGNTU. Tekhnicheskie nauki».* [Infocommunication technologies as object management systems. "Herald of GSTOU. Technical sciences"]. Volume XV. №4 (18). Grozny, 2019.
9. Khadzhiev, M.R., Khadzhieva, L.K., Paizulaeva, R.T., Mazhitova, Z.D. (2021) 'Zashchita besprovodnoi seti peredachi dannykh' *Materialy IV Vserossiiskoi nauchno-prakticheskoi konferentsii studentov, aspirantov i molodykh uchenykh «MILLIONShchIKOV-2021» s mezhdunarodnym uchastiem FGBOU VO «GGNTU im. akad. M.D. Millionshchikova.* [Protection of the wireless data transmission network. Proceedings of the IV All-Russian scientific and practical conference of students, graduate students and young scientists "MILLIONSCHIKOV-2021" with international participation – GSTOU named after akad.M.D. Millionshchikov", Russia, Chechen Republic, Grozny, May 18-20, 2021.
10. Mintsaev, M.Sh., Khakimov, Z.L. and Labazanov, M.A. (2021) Programmirovanie logicheskikh kontrollerov firmy SIEMENS. Laboratornyi praktikum. [Programming logic controllers from SIEMENS. Laboratory workshop], Grozny.
11. Alisultanova, E.D., Khadzhieva, L.K. and Isaeva, M.Z. (2019) 'Proforientatsionnaya shkol'naya laboratoriya po osnovam kiberbezopasnosti v sfere internet veshchei (IOT)'. *Vestnik GGNTU. Gumanitarnye i sotsial'no-ekonomicheskie nauki.* [Vocational guidance school laboratory on the basics of cybersecurity in the field of the Internet of things (IOT).Herald of GSTOU. Humanitarian, social and economic sciences]. V. 15. №4 (18). Pp. 51-58.
12. Murtazaev, S.A., Mintsaev, M., Salamanova, M., Alaskhanov, A. and Aymenov, Z. (2021) 'Mineral powders dispersion degree effect on the properties of the cementing alkaline system'. *Materials Science Forum.* V. 1017. S. 31-40.
13. Mintsaev, M.Sh. and Elsunkaeva, E.V. Razrabotka GIS-modulya dlya kompleksnogo monitoringa geologicheskoi sredy khankal'skogo mestorozhdeniya chechenskoi respubliki. [Development of a GIS-module for complex monitoring of the geological environment of the Khankala field of the Chechen Republic].
14. Mintsaev, M.Sh., Labazanov, M.A., Isaeva, M.R. and Murtazova, Kh.T. (2019) 'Obosnovanie vybora tekhnologicheskoi skhemy binarnoi ustanovki'. *V sbornike: Geoenergetika - 2019. Materialy IV Vserossiiskoi nauchno-tekhnicheskoi konferentsii.* Pod redaktsiei M.Sh. Mintsaeva. [Justification for the choice of the technological scheme of a binary installation. Proceedings: Geoenergy - 2019. Materials of the IV All-Russian Scientific and Technical Conference. In M.Sh. Mintsaev (Ed.). Pp. 349-357.