МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Анализ методов обнаружения стеганографических объектов в интернете вещей

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Гендляра Сергея Максимовича

Научный руководитель
доцент к. ф.-м. н., доцент _____ А. В. Жаркова
19.01.2026 г.

Заведующий кафедрой
д. ф.-м. н., профессор _____ М. Б. Абросимов
19.01.2026 г.

Саратов 2026

ВВЕДЕНИЕ

Интернет вещей (IoT) представляет собой парадигму, в рамках которой физические устройства, оснащенные сенсорами, средствами обработки данных и сетевыми интерфейсами, образуют распределенные системы. Основной функцией этих систем является автоматизированный сбор, обмен и первичная обработка информации. Широкое внедрение IoT в критические области, включая промышленную автоматизацию, энергетику, транспорт и телемедицину, формирует устойчивый запрос на методы обеспечения конфиденциальности и целостности передаваемых данных.

Существующие разработки в области стеганографии для IoT в значительной степени ориентированы на мультимедийные форматы данных. Это объясняется высокой избыточностью изображений, аудио- и видеопотоков, что предоставляет широкие возможности для внедрения скрытых сообщений. Однако значительная часть служебного и управляющего трафика в IoT-экосистемах имеет иной формат: текстовые конфигурации, журналы событий, сигнальные данные сетевых протоколов и двоичные файлы прошивок. Методы эффективного и незаметного сокрытия информации в таких типах носителей исследованы в недостаточной степени.

Данная работа направлена на заполнение указанного пробела. Исследование концентрируется на трех взаимодополняющих направлениях стеганографии, адаптированных к ресурсным ограничениям и характеру трафика IoT-среды. Во-первых, рассматривается модификация алгоритма LSB для работы с текстовыми файлами. Во-вторых, исследуется методика использования полей заголовков сетевых пакетов для создания скрытого канала связи. В-третьих, анализируются фундаментальные принципы бинарной стеганографии применительно к исполняемым файлам и прошивкам. Практическая реализация и проверка работоспособности данных методов выполняется в среде сетевого моделирования Cisco Packet Tracer, что позволяет воспроизводить реалистичные сценарии взаимодействия IoT-устройств.

Целью работы является исследование и разработка комплекса методов стеганографии, ориентированных на защиту данных в IoT-средах посредством их скрытия в нетрадиционных для данной области типах носителей.

Для достижения указанной цели требуется решить следующие задачи:

1) провести анализ актуальных методов стеганографии с точки зрения их применимости в условиях ограниченных ресурсов и специфики трафика IoT-систем;

2) разработать и формально описать модифицированный алгоритм LSB, обеспечивающий встраивание данных в текстовые файлы, характерные для конфигурации и логирования IoT-устройств;

3) предложить методику организации скрытого канала связи путем контролируемой модификации служебных полей заголовков сетевых пакетов, характерных для стека протоколов TCP/IP;

4) систематизировать принципы бинарной стеганографии для обеспечения целостности и аутентичности двоичных данных, таких как прошивки устройств;

5) реализовать и апробировать разработанные методы в среде Cisco Packet Tracer с целью демонстрации их функциональности и оценки основных характеристик в условиях, имитирующих реальное IoT-окружение.

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и 5 приложений. Общий объем работы – 66 страниц, из них 43 страницы – основное содержание, включая 11 рисунков и 1 таблицу, список использованных источников из 21 наименования.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел дипломной работы «Основные определения» содержит систематизацию и детальное толкование ключевых терминов, используемых в области стеганографии и интернета вещей. Четкое разграничение понятий необходимо для обеспечения терминологической однозначности при анализе методов скрытой передачи данных и их обнаружения в специфичной среде интернета вещей (Internet of Things, IoT). Определения охватывают два взаимосвязанных блока: аппарат стеганографии и основы архитектуры интернета вещей.

Понятийный аппарат стеганографии включает фундаментальные концепции, описывающие процесс скрытия информации. Стеганография определяется как совокупность методов, скрывающих сам факт передачи или хранения данных, в отличие от криптографии, защищающей их содержание. Стегоконтейнер рассматривается как любой цифровой объект (файл или сетевой пакет), подвергаемый модификации для размещения вложения. Процессы внедрения и извлечения сообщения, а также роль стеганографических ключей (открытых и закрытых) формализуют модель защищенного скрытого канала связи. Отдельно вводится понятие стегоанализа как набора методов противодействия, направленных на обнаружение факта использования стеганографии.

Базовые концепции интернета вещей и сетевого взаимодействия задают контекст для прикладного исследования. Интернет вещей определяется как сетевая инфраструктура физических объектов, оснащенных средствами сбора, обработки и обмена данными. PDU (Protocol Data Unit) описывается как структурированный блок данных сетевого протокола, выступающий в работе в качестве потенциального стегоконтейнера[1]. SBC (Session Border Controller)

[1] Driss, M. Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions [Электронный ресурс] / L. Beriche, M. Driss, S. B. Atitallah, S. Rekik // IEEE Access [Электронный ресурс]. – 2025. – 32 с. – URL: ieeexplore.ieee.org/document/10975763/ (дата обращения: 15.12.2025). – Загл. с экрана. – Яз. англ.

определяется как сетевое устройство контроля сессий, функциональность которого в практической части работы реализуется в модуле защитника для анализа трафика.

Таким образом, сформированный в первом разделе терминологический базис создает основу для последующего анализа. Он позволяет четко дифференцировать компоненты стеганографической системы (контейнер, сообщение, ключ) и элементы архитектуры интернета вещей.

Второй раздел дипломной работы «Архитектурная модель IoT» посвящен анализу структуры, ключевых характеристик и ограничениям систем интернета вещей. Понимание этих аспектов является критически важным для обоснования выбора и адаптации стеганографических методов, которые должны эффективно функционировать в стесненных и неоднородных условиях IoT-среды.

Многоуровневая эталонная архитектура представлена в виде четырех последовательных слоев. Физический (сенсорный) уровень выполняет функцию интерфейса между аналоговыми и цифровыми системами, осуществляя сбор первичных данных через датчики, камеры и актуаторы. Сетевой уровень обеспечивает конвергенцию и передачу данных от множества периферийных устройств с использованием гетерогенного набора проводных и беспроводных протоколов связи (от Zigbee и LoRaWAN до сотовых сетей 4G/5G). Уровень обработки данных и сервисов представляет собой вычислительное ядро, где происходит трансформация сырых данных в ценную информацию с применением технологий больших данных и машинного обучения, часто в парадигме граничных вычислений. Прикладной уровень предоставляет конечным пользователям или другим системам предметно-ориентированные сервисы через интуитивные интерфейсы и инструменты мониторинга[1].

Фундаментальные ограничения и вызовы безопасности IoT формируют специфичный контекст для проектирования защитных механизмов. К ним относятся: жесткая ограниченность ресурсов (маломощные процессоры, ограниченная память, автономное питание) периферийных устройств, высокая

степень гетерогенности аппаратного и программного обеспечения, усложняющая унификацию решений, уязвимость к широкому спектру кибератак (DDoS, атаки типа «человек посередине», компрометация устройств для включения в ботнеты)[2], конфликт между требованиями безопасности и производительности, исключающий использование традиционных ресурсоемких криптографических примитивов, необходимость обеспечения безопасности в реальном времени для критически важных приложений, таких как телемедицина или автономный транспорт.

Таким образом, проведенный в разделе анализ архитектуры IoT выявляет уникальный набор технологических ограничений и угроз информационной безопасности. Эти факторы напрямую обусловливают потребность в легковесных, адаптивных и незаметных методах защиты данных, к которым могут быть отнесены исследуемые стеганографические подходы.

Третий раздел дипломной работы «Стеганография и интернет вещей» содержит сравнительный анализ классических и специализированных стеганографических методов с точки зрения их соответствия особенностям и ограничениям среды интернета вещей. Целью раздела является обоснование выбора наиболее релевантных подходов для дальнейшей практической реализации.

Общий принцип и классификация стеганографии основаны на скрытии факта передачи путем модификации избыточности цифрового контейнера с использованием стеганографического ключа. В работе проводится детальная классификация методов по типу медиаконтейнера. Стеганография в изображениях, основанная на модификации наименее значащих бит в пространственной или частотной области, характеризуется высокой вместимостью, но может быть ресурсозатратна для обработки.

[2] Atitallah, S. B. A Novel Detection and Multi-classification Approach for IoT-malware Using Random Forest Voting of Fine-tuning Convolutional Neural Networks [Электронный ресурс] / S. B. Atitallah, M. Driss, I. Almomani // National Library of Medicine [Электронный ресурс]. – 2022. – Vol. 22, № 11. – 22 с. – URL: https://pubmed.ncbi.nlm.nih.gov/35684922/ (дата обращения: 15.12.2025). – Загл. с экрана. – Яз. англ.

Аудиостеганография использует психоакустические модели для внедрения данных в невоспринимаемые слухом компоненты сигнала, что актуально для устройств с микрофонами.

Видеостеганография использует пространственно-временную избыточность видеопотока, представляя интерес для систем наблюдения.

Текстовая и сетевая стеганография выделяются как наиболее адекватные в контексте интернета вещей. Текстовая стеганография включает лингвистические (манипуляции с синонимами, синтаксисом), структурные и гибридные методы. Ее преимущество – работа с данными низкой избыточности, характерными для служебных сообщений, конфигураций и логов IoT-устройств.

Сетевая стеганография использует в качестве контейнера не содержимое пакетов, а служебные поля их заголовков (IP, TCP) или временные параметры трафика. Методы делятся на внутрипротокольные, межпротокольные и гибридные, обеспечивая высокую скрытность, так как маскируются под легитимный сетевой шум.

Таким образом, проведенный анализ позволяет заключить, что несмотря на распространенность мультимедийных методов, именно текстовая и сетевая стеганография в наибольшей степени соответствуют особенностям устройств интернета вещей. Они оперируют типами данных, преобладающими в IoT-трафике (текстовые конфигурации, служебные пакеты), и предъявляют минимальные требования к вычислительным ресурсам и пропускной способности каналов связи, что делает их предпочтительным объектом исследования для разработки практических методов скрытой передачи, ориентированных на устройства с ограниченными возможностями.

Четвертый раздел дипломной работы «Реализация методов стеганографии в сети с различными устройствами интернета вещей» представляет собой детальное описание трех адаптированных алгоритмов скрытой передачи и архитектуры виртуальной тестовой среды для их верификации.

Формальное описание адаптированных стеганографических алгоритмов включает их математические модели и пошаговые процедуры.

Модифицированный алгоритм LSB для текстовых файлов. Классический метод наименее значащего бита адаптирован для работы с символами текста (ASCII-кодами). Процесс включает преобразование сообщения в бинарную последовательность, проверку емкости текстового контейнера и циклическую замену младшего бита в коде каждого символа. Формально описаны функции внедрения и извлечения, а также критерии успеха: сохранение читаемости текста и корректность восстановления сообщения.

Алгоритм Header для сетевых пакетов. Метод основан на контролируемой модификации служебных полей заголовков IP-пакетов. Внедрение бита информации осуществляется через управление четностью числового поля или прямой заменой его младшего бита. Алгоритм предполагает итеративную обработку выбранных полей в последовательности передаваемых пакетов. Ключевые требования – минимальность изменений и сохранение валидности пакетов для сетевого стека.

Базовый бинарный алгоритм. Представляет собой метод прямой вставки данных в структурированные поля пакета, служащий упрощенным эталоном для последующего сравнения эффективности и скрытности. Данные разбиваются на блоки и добавляются в пакет как отдельный структурный элемент.

Проектирование виртуальной тестовой IoT-среды выполнено в симуляторе Cisco Packet Tracer. Архитектура среды моделирует полный цикл обработки данных: от периферийных устройств интернета вещей данные через роутер поступают на устройство передачи, который внедряет сообщение одним из алгоритмов. В соответствии с рисунком 1 можно наблюдать, что настройка системы прошла успешно.

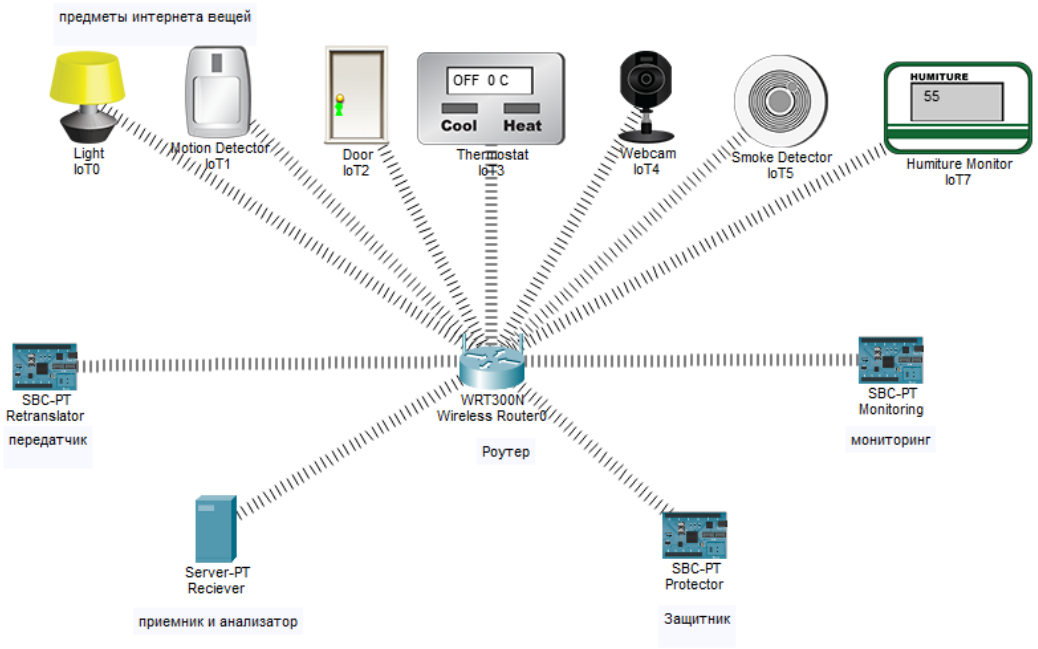

Рисунок 1 – Конфигруация виртуальной сети Cisco Packet Tracer

Далее пакет принимается приемником и автоматически перенаправляется защитнику, выполняющему функцию по стегоанализу. Безопасные пакеты пересылаются в систему мониторинга, а опасные – блокируются. Передатчик поддерживает три режима работы: ручной ввод сообщения, демонстрационный и режим чистого мониторинга без стеганографии.

Таким образом, в данном разделе осуществлен переход от теоретической к практической части работы. Формально описанные алгоритмы предлагают конкретные реализации стеганографии, учитывающие ресурсные ограничения IoT. Спроектированная виртуальная среда адекватно моделирует типичную IoT-экосистему и вводит в нее критически важный компонент безопасности – активный стегоанализатор. Это позволяет не только продемонстрировать работоспособность методов скрытой передачи, но и исследовать эффективность механизмов их обнаружения в условиях, приближенных к реальным.

Пятый раздел дипломной работы «Демонстрация работы созданного программного обеспечения» содержит результаты тестирования реализованной системы, включая визуализацию рабочего цикла и сравнительный

количественный анализ трех стеганографических алгоритмов по ключевым метрикам производительности и скрытности.

Демонстрация рабочего цикла системы визуализирована через интерфейс Cisco Packet Tracer и поэтапно иллюстрирует взаимодействие всех компонентов. Передатчик в одном из трех режимов формирует пакет данных, содержащий телеметрию IoT-устройств и при необходимости стеганографическую вставку. Приемник перенаправляет полученный пакет на анализ. Защитник инспектирует пакет: при обнаружении метаданных стеганографии пакет блокируется, а в консоль выводится предупреждение и извлеченное сообщение. В противном случае пакет признается безопасным и пересылается далее. Система мониторинга финально принимает и отображает только данные из верифицированных безопасных пакетов, обеспечивая оператору очищенный от скрытых угроз обзор состояния системы.

Сравнительный анализ алгоритмов проведен на фиксированном сообщении длиной 1000 символов. Для оценки использовались четыре критерия: среднее время вложения одного пакета, среднее время его анализа защитником, общее количество сгенерированных пакетов и общее время выполнения операции передачи. В соответствии с таблицей 1 можно наблюдать, что бинарный алгоритм является самым быстрым по внедрению, но генерирует относительно много пакетов и имеет низкое время анализа из-за простоты обнаружения. Модифицированный LSB-алгоритм продемонстрировал наилучший баланс: умеренное время вложения и анализа при эффективном использовании пропускной способности. Алгоритм Header показал самое малое время вложения, но оказался недостаточно эффективным по другим параметрам: для передачи сообщения потребовалось почти в три раза больше пакетов, чем у алгоритма LSB, а время анализа оказалось на несколько порядков выше, что делает его непрактичным для передачи значительных объемов данных. Цель сравнительного анализа – объективная оценка компромиссов, присущих каждому из методов

Таблица 1– Сравнение стеганографических алгоритмов

Критерии сравнения	LSB	Header	Бинарный
Среднее время вложения (мс)	1	21	1
Среднее время анализа (мс)	138	440	201
Количество сообщений	3249	8961	2942
Общее время выполнения (с)	3441	9511	3144

Таким образом, практическая демонстрация подтвердила корректность функционирования всей разработанной системы – от скрытой передачи до активного обнаружения. Модифицированный алгоритм LSB для текста подтвердил свой статус оптимального решения для IoT, предложив наилучшее соотношение скрытности, эффективности использования канала и вычислительных затрат. Исходя из полученных результатов, можно наблюдать, что тексто-ориентированные методы стеганографии хорошо подходят для ресурсно-ограниченных сред, подобных интернету вещей.

ЗАКЛЮЧЕНИЕ

В ходе проведенного исследования была выполнена систематизация методов компьютерной стеганографии применительно к задачам защиты данных в системах интернета вещей. Работа позволила получить следующие основные результаты и выводы:

1) проанализированы особенности архитектуры IoT, выявлены ключевые ограничения (ресурсные, сетевые) и специфические угрозы информационной безопасности, актуализирующие потребность в легковесных методах скрытой передачи данных;

2) проведен сравнительный анализ классических методов стеганографии (в изображениях, аудио, видео) и менее изученных применительно к IoT подходов – текстовой и сетевой стеганографии. Установлено, что последние в большей степени соответствуют ограничениям IoT-среды;

3) разработаны и формально описаны три алгоритма: модифицированный алгоритм LSB для текстовых файлов, алгоритм скрытия данных в служебных полях заголовков IP-пакетов и базовый алгоритм бинарной стеганографии. Для каждого алгоритма представлена полная спецификация, включая процедуры внедрения и извлечения;

4) осуществлена программная реализация данных алгоритмов и их апробация в смоделированной IoT-среде с использованием Cisco Packet Tracer. Создана виртуальная сеть, демонстрирующая работоспособность методов на различных типах IoT-устройств в условиях, имитирующих реальный трафик;

5) было осуществлено сравнение быстродействия работы реализованных алгоритмов.

Таким образом, поставленные задачи решены, цель работы достигнута.