# Введение

В последние десятилетия сетевые технологии прочно вошли в жизнь человека. Изначально они были представлены локальными сетями, затем была создана сеть Интернет. В настоящее время одним из бурно развивающихся направлений сетевых технологий является интернет вещей (Internet of Things, IoT). Так, за период 2015-2018 гг. доля IoT-устройств среди всех устройств увеличилась с 27% до 39%, и, согласно прогнозу, достигнет 63% к 2025 году[[1]](#footnote-1).

Интернет вещей – это вычислительная сеть физических предметов (устройств, «вещей»), оснащенных встроенной технологией для взаимодействия друг с другом или с внешней средой[[2]](#footnote-2).

**Актуальность исследования.** Одной из важных задач при проектировании IoT является обеспечение должного уровня безопасности передаваемых данных. Особенно это важно для медицинских устройств[[3]](#footnote-3). Уже сейчас правительства развитых стран начинают принимать законы, регламентирующие защиту IoT-устройств[[4]](#footnote-4)[[5]](#footnote-5)[[6]](#footnote-6). В то же время фактическая безопасность устройств интернета вещей оставляет желать лучшего. Так, согласно исследованию корпорации HP 2014-го года, 70% устройств IoT передавали данные, в том числе конфиденциального характера, вообще без шифрования[[7]](#footnote-7)! По этой причине изучение и развитие средств защиты IoT-устройств является актуальной задачей.

Безопасность устройств с ограниченными энергетическими ресурсами (а именно такими являются устройства интернета вещей) изучает раздел криптографии, называемый легковесной криптографией (lightweight cryptography, LWC). Также возможны термины «облегченная криптография», «малоресурсная криптография», «низкоэнергетическая криптография». Она рассматривает криптографические алгоритмы в контексте их требовательности к ресурсам устройства и количеству логических элементов, требуемых для реализации алгоритмов. Рассматриваемые ею алгоритмы называются алгоритмами легковесной криптографии (легковесными алгоритмами, LW-алгоритмами). LW-алгоритмы могут иметь программную или аппаратную реализацию.

**Объектом исследования** являются алгоритмы легковесной криптографии, ориентированные на использование в устройствах интернета вещей.

**Предметом исследования** являются следующие характеристики легковесных алгоритмов: тип алгоритма, требования к устройству, производительность. Алгоритмы рассматриваются с точки зрения программной реализации.

**Целью исследования** является сравнение легковесных алгоритмов и определение степени их пригодности к использованию в устройствах IoT.

Для достижения выбранной цели поставлены следующие **задачи**:

1. Провести теоретический обзор источников по темам легковесной криптографии и интернета вещей.
2. Обзор существующих стандартов и технических решений.
3. Анализ алгоритмов.
4. Реализовать избранные алгоритмы и проверить гипотезы из п. 3.
5. Ранжировать алгоритмы по степени пригодности к использованию в устройствах IoT. Сформулировать рекомендации по их использованию.

**Гипотеза исследования.** Предполагается, что значительное число классических шифров с определенным ослаблением могут использоваться в качестве легковесных алгоритмов. С другой стороны, многие алгоритмы и классы алгоритмов по тем или иным соображениям однозначно не могут быть использованы в качестве LW-алгоритмов. Ряд алгоритмов может быть использован наилучшим образом при определенных условиях. Может быть создана методика, позволяющая приблизительно оценить производительность реализации легковесного алгоритма с использованием только персонального компьютера, без необходимости взаимодействия с низкоресурсными устройствами.

В данной работе используются такие **методы исследования**, как:

* анализ технической литературы
* изучение существующих спецификаций алгоритмов, стандартов, технологических систем
* декомпозиция алгоритмов
* сравнение алгоритмов, подходов к шифрованию, структурных частей алгоритмов
* реализация алгоритмов (на языке С)
* определение методологии их тестирования
* реализация конкретной методики тестирования
* анализ результатов тестирования
* синтез выводов по результатам тестирования
* обобщение результатов работы

Данное исследование имеет высокую **практическую значимость.** Результаты исследования могут быть использованы при выборе алгоритма шифрования и режима его работы при проектировании системы защиты вычислительной сети IoT. Кроме того, работа в данном направлении может быть продолжена: следующим шагом возможна оптимизация существующих легковесных алгоритмов или создание новых LW-алгоритмов. Предложенная методология тестирования времени работы алгоритмов и их энергопотребления может быть использована при тестировании других алгоритмов. Можно также исследовать «побочные» вопросы, появившиеся в процессе выполнения работы.

Введение раскрывает актуальность, определяет степень научной разработки темы, объект, предмет, цель, задачи и методы исследования, раскрывает теоретическую и практическую значимость работы.

В первой главе содержатся краткое теоретическое введение в тему криптографии и интернета вещей, описываются основные угрозы безопасности систем IoT.

Во второй главе вводится понятие легковесных криптографических алгоритмов. Описываются требования к ним и их применение для нейтрализации угроз безопасности системам IoT, оно сравнивается с нейтрализацией угроз в системах общего назначения). Проводится анализ различных видов алгоритмов на пригодность их для такого применения, рассматриваются наиболее популярные их представители.

В третьей главе описывается методология тестирования производительности и энергопотребления легковесных криптоалгоритмов на ПК.

В четвертой главе содержится информация о реализации алгоритмов в программном коде, способе и порядке тестирования производительности алгоритмов, а также дальнейшей обработки результатов тестирования. Проводится анализ полученных результатов.

В заключении подводятся итоги работы, приводятся краткие перспективы использования результатов работы.

1. <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> [↑](#footnote-ref-1)
2. <https://www.gartner.com/en/information-technology/glossary/internet-of-things> [↑](#footnote-ref-2)
3. <https://cyberleninka.ru/article/n/o-nekotoryh-voprosah-informatsionnoy-bezopasnosti-meditsinskih-ustroystv> [↑](#footnote-ref-3)
4. <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation> [↑](#footnote-ref-4)
5. <https://www.kommersant.ru/doc/3924324> [↑](#footnote-ref-5)
6. <https://rg.ru/2016/10/13/evrokomissiia-predlozhila-zashchitit-internet-veshchej-ot-kiberatak.html> [↑](#footnote-ref-6)
7. <https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676> [↑](#footnote-ref-7)