ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

***«*САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»**

**ИНСТИТУТ КОМПЬЮТЕРНЫХ НАУК И ТЕХНОЛОГИЙ**

**ВЫСШАЯ ШКОЛА ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ И СУПЕРКОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ**

**Отчет о прохождении   
стационарной производственной практики (научно-исследовательской работы на тему:**

«Сравнительный анализ легковесных криптографических алгоритмов для устройств интернета вещей»**)**

Момота Даниэля Михайловича, гр. 3530903/60301

**Направление подготовки:** 09.03.03 Прикладная информатика

|  |
| --- |
| **Место прохождения практики:** СПбПУ, ИКНТ, ВШИСиСТ |

*(указывается наименование профильной организации или наименование структурного подразделения*

|  |
| --- |
|  |

*ФГАОУ ВО «СПбПУ», фактический адрес)*

**Сроки практики:** с 03.02.2020 по 14.04.2020.

**Руководитель практики от ФГАОУ ВО «СПбПУ»:**

|  |
| --- |
| Сергеев Анатолий Васильевич, к.т.н., доцент |

*(Ф.И.О., уч. степень, должность)*

|  |
| --- |
| **Консультант от ФГАОУ ВО «СПбПУ»:**  Кудрявцев Дмитрий Вячеславович, к.т.н., доцент |

*(Ф.И.О., должность)*

|  |
| --- |
|  |

**Оценка:**

Руководитель практики

от ФГАОУ ВО «СПбПУ» Сергеев А.В.

Консультант

от ФГАОУ ВО «СПбПУ» Кудрявцев Д.В.

Обучающийся Момот Д.М.

Дата:

Оглавление

[Термины и определения, используемые в отчете 3](#_Toc38060128)

[Перечень сокращений и обозначений, используемых в отчете 5](#_Toc38060129)

[Введение 6](#_Toc38060130)

[Глава 1. Критерии легковесности алгоритма 8](#_Toc38060131)

[Глава 2. Сравнительный обзор легковесных качеств криптографических алгоритмов 10](#_Toc38060132)

[2.1. Блочные алгоритмы 10](#_Toc38060133)

[2.1.1. Алгоритм AES 10](#_Toc38060134)

[2.1.2. Алгоритм ГОСТ 28147-89 10](#_Toc38060135)

[2.1.3. Алгоритмы PRESENT и CLEFIA 10](#_Toc38060136)

[2.2. Потоковые алгоритмы 11](#_Toc38060137)

[2.2.1. Алгоритмы Enocoro и Trivium 11](#_Toc38060138)

[2.3. Хэш-функции 11](#_Toc38060139)

[Глава 3. Планируемая методология практического определения легковесности шифра 12](#_Toc38060140)

[Заключение 13](#_Toc38060141)

[Список литературы 14](#_Toc38060142)

# Термины и определения, используемые в отчете

Информация – сведения, передаваемые одними людьми другим людям устным, письменным или каким-либо другим способом, а также сам процесс передачи или получения этих сведений [БСЭ].

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [ГОСТ Р 50922-2006]. Утечка – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками [ГОСТ Р 53114-2008].

Криптография — инженерно-техническая дисциплина, изучающая математические методы защиты информации (шифры). Криптография включает в себя криптосинтез и криптоанализ. Криптосинтез изучает подходы к разработке шифров. Криптоанализ изучает подходы к вскрытию шифров [Ященко, стр 16-17].

Интернет вещей (Internet of things) – это вычислительная сеть физических предметов (устройств, «вещей»), оснащенных встроенной технологией для взаимодействия друг с другом или с внешней средой[[1]](#footnote-1). Такими предметами могут быть, например, бытовые приборы, транспортные средства, датчики и метки радиочастотной идентификации (RFID).

Легковесная криптография (lightweight cryptography) – раздел криптографии, рассматривающий алгоритмы, ориентированные на использование в устройствах с ограниченными энергетическими ресурсами (а именно такими являются устройства интернета вещей). Также возможны термины «облегченная криптография», «малоресурсная криптография», «низкоэнергетическая криптография».

Алгоритмы, рассматриваемые легковесной криптографией, называются алгоритмами легковесной криптографии (легковесными алгоритмами). Они могут иметь программную или аппаратную реализацию (т. е. фокусироваться на оптимизацию программной или аппаратной части).

GE-мера (эквивалентный логический элемент) – отражает количество логических элементов, присутствующих на плате и доступных для использования при вычислении алгоритмов, в данном случае криптографических. Аналог размера микросхемы.

Бизнес-требования к системе — определяют назначение системы, описываются в документе о видении (vision) и границах проекта (scope).

Симметричные шифры – способ шифрования, в котором для [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и [расшифровывания](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BA%D0%B0) применяется один и тот же криптографический [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)).

Блочный шифр – разновидность [симметричного](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%8B%D0%B5_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B) [шифра](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80), оперирующего группами бит фиксированной длины – блоками, характерный размер которых меняется в пределах 64‒256 бит.

Раунд шифрования – один из последовательных шагов обработки данных в алгоритме блочного шифрования.

Потоковый шифр – это [симметричный шифр](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80), в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста.

# Перечень сокращений и обозначений, используемых в отчете

IoT – интернет вещей

LWC – легковесная криптография

LW-алгоритм – легковесный алгоритм

GE – gate equivalent, эквивалентный логический элемент

RFID – radio frequency identification, радиочастотная идентификация

ЦП – центральный процессор

# 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. 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[[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.

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

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

1. Формулировка соображений, по которым определяется степень «легковесности» криптографического алгоритма или группы алгоритмов.
2. Сравнительный обзор различных типов криптографических алгоритмов. Выявление тех из них, которые точно не могут быть легковесными.
3. Теоретический анализ избранных представителей остальных типов алгоритмов. Оценка их «легковесности».
4. Планируемая методология практического тестирования «легковесности» избранных алгоритмов.

# Глава 1. Критерии легковесности алгоритма

Легковесный алгоритм должен быть ориентирован на применение в устройствах с ограниченными энергетическими ресурсами (например, не более 15 микроватт для RFID-меток[[8]](#footnote-8)), а также с ограниченным объемом памяти и размер микросхемы (GE-мера). Время работы часто должно быть низким: например, для систем автоматического осуществления дорожных сборов время работы должно быть менее 10 миллисекунд [Жуков, стр 29].

Итак, ограничения аппаратной части:

* размер микросхемы;
* потребляемая энергия.

Ограничения программной части:

* объем программного кода;
* размер потребляемой оперативной памяти;
* время работы.

В некоторых случаях также присутствуют дополнительные ограничения, такие как:

* ширина полосы рабочих частот канала связи;
* пропускная способность канала связи.

С другой стороны, перед проектировщиком алгоритма стоят бизнес-требования. В данном случае они следующие:

* обеспечение требуемого уровня безопасности;
* низкие требования к аппаратной части (а значит, и стоимости устройства);
* высокая производительность.

Обычно легко оптимизировать два из трех требований, а вот обеспечить выполнение всех трех – весьма трудная задача.

Также следует отметить существование различных подходов к оценке качества легковесных криптографических алгоритмов.

Для сравнения программных реализаций используют требования к памяти и приблизительное количество тактов процессора (точное количество тактов зависит от архитектуры конкретного ЦП, конвейеризации, иногда длины команд в опкодах).

Для аппаратных реализаций в качестве критерия сравнения используется размер микросхемы (GE) и время работы в тактах ЦП, иногда также энергопотребление.

Требуемый размер микросхемы для легковесного алгоритма не должен превышать 1000 GE. Он зависит от архитектуры реализации, которая, в свою очередь, зависит от приоритета: оптимизация площади, оптимизация скорости и т. д. Оптимизация площади достигается за счет последовательной архитектуры (обрабатывающей информацию побайтно), оптимизация скорости – за счет распараллеливания и конвейеризации, что влечет увеличение размера.

Основные требования к малоресурсным алгоритмам определены в стандарте ISO 29192[[9]](#footnote-9).

# Глава 2. Сравнительный обзор легковесных качеств криптографических алгоритмов

Стандартными подходами при создании легковесной криптографической системы являются:

* Использование классических криптографических алгоритмов, если это возможно.
* Модификация (путем ослабления) криптографического алгоритма: уменьшение числа раундов (в блочном алгоритме), упрощение одного раунда, уменьшение длины блока и другие.
* Разработка новых решений на программном или аппаратном уровне.

Второй и третий пути являются весьма трудными, так как требуется доказать, что криптостойкость ослабленного шифра (а тем более нового шифра) соответствует требованиям.

## 2.1. Блочные алгоритмы

Эти алгоритмы не требуют начальной инициализации (могут работать почти без задержки), что позволяет эффективно использовать их для шифрования небольших объемов данных. Тем не менее, пропускная способность у них ниже, чем у потоковых шифров.

### 2.1.1. Алгоритм AES

Данный алгоритм известен своей высокой надежностью, сочетающейся со значительной пропускной способностью (до 70 Гб/сек). Однако он не подходит для легковесной криптографии, так как аппаратная реализация требует более 250000 GE. В то же время наиболее компактная реализация AES требует 2500 GE [Moradi], что уже часто приемлемо.

### 2.1.2. Алгоритм ГОСТ 28147-89

Является DES-подобным алгоритмом. Для него существует одна из наиболее компактных реализаций: всего 615 GE [Poschmann].

### 2.1.3. Алгоритмы PRESENT и CLEFIA

В стандарт ISO 29192-2 (Block ciphers) включены два алгоритма: PRESENT (размер блока 64 бит, ключа – 80 или 128 бит) и CLEFIA (размер блока 128 бит, ключа – 128, 192 или 256 бит). Реализация CLEFIA с 128-битным ключом занимает 2488 GE [Akishita], PRESENT c 80-битовым ключом – 1000 GE [Rolfes].

## 2.2. Потоковые алгоритмы

Потоковые алгоритмы нуждаются в начальной инициализации, т. е. имеют задержку (latency), однако часто имеют большую пропускную способность (throughput), чем блочные шифры.

Согласно ряду исследований [см Жуков], в условиях применения на низкоэнергетических устройствах, потоковые шифры не дают значительного преимущества в скорости. Из-за большого времени инициализации они неудобны для обработки небольших массивов информации. Кроме того, большинство потоковых шифров требуют много памяти для хранения внутреннего состояния. Поэтому для встраиваемых систем (например, RFID-метка, периодически отправляющая небольшой пакет данных) потоковые шифры не очень подходят.

### 2.2.1. Алгоритмы Enocoro и Trivium

Эти два шифра включены в состав ISO/IEC 29192-3 (Stream ciphers). В конфигурации для Enocoro: размер знака выходной гаммы (текста) 8 бит, ключа – 80 или 128 бит, для Trivium 1 и 80 бит соответственно.

## 2.3. Хэш-функции

Хэш-функция часто имеет достаточно сложную структуру. В своем составе она обычно имеет другой алгоритм, шифрующий данные по блокам. Это влечет значительную зависимость легковесности хэш-функции от используемого блочного шифра. В целом, на данный момент это направление не слишком развито, главным образом потому, что сейчас главным образом развиваются хэш-функции общего вида [Жуков].

# Глава 3. Планируемая методология практического определения легковесности шифра

Для оценки берется программная реализация алгоритма. Планируется реализация криптографического алгоритма на языке С++, как наиболее приближенном к ассемблерным инструкциям и в то же время достаточно легком для чтения и отладки. Планируется вначале написать «наивную» реализацию, затем попробовать улучшить ее с помощью использования таких техник, как оптимизация циклов, удаление излишних операций с памятью, раскрутка циклов, удаление зависимостей данных, реассоциация и др.

Кроме того, потребуется написать модули для точного определения времени работы функции. Обработка результатов тестирования потребует применения методов математической статистики и обработки экспериментальных данных.

# Заключение

В рамках научно-исследовательской работы проведено исследование в русле легковесной криптографии. Сформулированы критерии качества и пригодности к использованию для легковесного алгоритма. Проведен анализ различных видов алгоритмов на их пригодность для использования в качестве легковесных криптографических алгоритмов. Продумана методология тестирования легковесных качеств шифра.

По результатам работы написан отчет.

# Список литературы

1. Введение в криптографию / под ред. В. В. Ященко. – 4-е изд., доп. – Москва: Издательство МЦНМО, 2012. – 342 с.
2. Жуков, А. Е. Легковесная криптография / А.Е. Жуков // Вопросы кибербезопасности. – 2015. – № 1.
3. Moradi A., Poschmann A., Ling S., Paar C., Wang H. Pushing the Limits: A Very Compact and a Threshold Implementation of AES”, EUROCRYPT 2011, LNCS 6632, pp. 69-88, Springer-Verlag, 2011.
4. Poschmann A., Ling S., Wang H. 256 Bit Standardized Crypto for 650 GE GOST Revisited, In CHES 2010, Lecture Notes in Computer Science v. 6225, pp. 219-233, 2010.
5. Rolfes C., Poschmann A., Leander G., Paar C. Ultra-Lightweight implementations for smart devices - security for 1000 gate equivalents. In Proceedings of the 8th Smart Card Research and Advanced Application IFIP Conference CARDIS 2008, Lecture Notes in Computer Science v. 5189, pp. 89-103, 2008.
6. Akishita T., Hiwatari H. Very Compact Hardware Implementations of the Blockcipher CLEFIA. Selected Areas in Cryptography 2011– SAC 2011, LNCS 7118, pp. 278–292, 2012.

1. <https://www.gartner.com/en/information-technology/glossary/internet-of-things> [↑](#footnote-ref-1)
2. <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> [↑](#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)
8. ISO/IEC 18000-3:2004 Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13.56 MHz [↑](#footnote-ref-8)
9. ISO/ IEC FDIS 29192 – Information technology – Security techniques – Lightweight cryptography. [↑](#footnote-ref-9)