Учреждение образования

Белорусский государственный технологический университет

Кафедра полиграфического оборудования и

системы обработки информации

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 10**

«Стандарты безопасности»

по дисциплине «Стандартизация и сертификация

информационных систем и технологий»

Выполнил студент

4 группы 4 курса

Коржова В. С.

Проверил

ст. преп. Сулим П.Е.

Отчет по лабораторной работе

защищен с отметкой баллов

Минск 2024

**Цель:** найти отечественные и зарубежные стандарты в области безопасности информационных систем. Провести их сравнительный анализ.

«Информационная безопасность» — это процесс обеспечения доступности, целостности и конфиденциальности информации.

Под «доступностью» понимается соответственно обеспечение доступа к информации. «Целостность» — это обеспечение достоверности и полноты информации. «Конфиденциальность» подразумевает под собой обеспечение доступа к информации только авторизованным пользователям.

**Стандарт в области безопасности информационных систем РБ:**

<https://rlst.by/informational-resources/virtualnye-vystavki/arhiv-tematicheskih-vystavok-normativno-tehnicheskih-dokumentov/standarty-v-oblasti-informatsionnyh-tehnologij/>

1. СТБ 34.101.31-2020 Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности. — Взамен СТБ 34.101.31-2011; введ. 01.09.21. — Минск, 2020. — ІІІ, 32 с. : табл. — Попр. (ИУ ТНПА № 1-2021). Стандарт устанавливает криптографические алгоритмы шифрования и контроля целостности, а также служебные алгоритмы управления ключами. Стандарт применяется при разработке средств криптографической защиты информации.

2. СТБ 34.101.47-2017, BY. Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел. — Взамен СТБ 34.101.47-2012; введ. 01.09.17. — Минск, 2017. — ІІ, 18 с. Стандарт устанавливает криптографические алгоритмы генерации псевдослучайных чисел. Алгоритмы стандарта могут применяться для построения ключей, синхропосылок, одноразовых паролей, других непредсказуемых или уникальных параметров криптографических алгоритмов и протоколов. Стандарт применяется при разработке, испытаниях и эксплуатации средств криптографической защиты информации.

3. ГОСТ Р 51583-2014, RU. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. — Введ. РБ 01.02.21. — Минск, 2020. — ІІІ, 14 с. : схемы. — Введен впервые. — Попр. (ИУ ТНПА № 1-2021). Стандарт распространяется на создаваемые (модернизируемые) информационные автоматизированные системы, в отношении которых законодательством или заказчиком установлены требования по их защите, и устанавливает содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении, содержание и порядок выполнения работ по защите информации о создаваемой (модернизируемой) автоматизированной системе в защищенном исполнении.

4. ISO/IEC 27001:2013 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (Information technology – Security techniques – Information security management systems – Requirements).

5. ISO/IEC 27002:2013 «Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой информации» (Information technology – Security techniques – Code of practice for information security controls).

**Международные стандарты в области безопасности информационных систем:**

<https://safe-surf.ru/specialists/article/5259/644530/>

1. [BS 7799-1:2005](https://ru.wikipedia.org/wiki/BS_7799-1) — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения *системы управления информационной безопасностью* ([СУИБ](https://ru.wikipedia.org/wiki/%D0%A1%D0%9C%D0%98%D0%91)) организации, определённых на основе лучших примеров мирового опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ
2. [BS 7799-2:2005](https://ru.wikipedia.org/w/index.php?title=BS_7799-2&action=edit&redlink=1) — Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.
3. [BS 7799-3:2006](https://ru.wikipedia.org/w/index.php?title=BS_7799-3&action=edit&redlink=1) — Британский стандарт BS 7799 третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности
4. [ISO/IEC 17799:2005](https://ru.wikipedia.org/wiki/ISO/IEC_17799) — «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности». Международный стандарт, базирующийся на BS 7799-1:2005.
5. [ISO/IEC 27000](https://ru.wikipedia.org/wiki/ISO_27000) — Словарь и определения.

<https://ru.wikipedia.org/wiki/BelT>

**BelT** — государственный стандарт симметричного шифрования и контроля целостности Республики Беларусь. Полное название стандарта — СТБ 34.101.31-2007 «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности». Принят в качестве предварительного стандарта в 2007 году. Введён в действие в качестве окончательного стандарта в 2011 году.

BelT — блочный шифр с 256-битным ключом и 8 циклами криптопреобразований, оперирующий с 128-битными словами. Криптографические алгоритмы стандарта построены на основе базовых режимов шифрования блоков данных. Все алгоритмы стандарта делятся на 8 групп:

* алгоритмы шифрования в режиме простой замены;
* алгоритмы шифрования в режиме сцепления блоков;
* алгоритмы шифрования в режиме гаммирования с обратной связью;
* алгоритмы шифрования в режиме счётчика;
* алгоритм выработки имитовставки ;
* алгоритмы одновременного шифрования и имитозащиты данных;
* алгоритмы одновременного шифрования и имитозащиты ключей;
* алгоритм хеширования;

Первые четыре группы предназначены для обеспечения безопасного обмена сообщениями. Каждая группа включает алгоритм шифрования и алгоритм расшифрования на секретном ключе. Стороны, располагающие общим ключом, могут организовать обмен сообщениями путём их шифрования перед отправкой и расшифрования после получения. В режимах простой замены и сцепления блоков шифруются сообщения, которые содержат хотя бы один блок, а в режимах гаммирования с обратной связью и счётчика — сообщения произвольной длины.

Пятый алгоритм предназначен для контроля целостности сообщений с помощью имитовставок — контрольных слов, которые определяются с использованием секретного ключа. Стороны, располагающие общим ключом, могут организовать контроль целостности при обмене сообщениями путём добавления к ним имитовставок при отправке и проверки имитовставок при получении. Проверка имитовставок дополнительно позволяет стороне получателю убедиться в знании стороной-отправителем секретного ключа, то есть проверить подлинность сообщений.

В шестой группе исходное сообщение задаётся двумя частями: открытой и критической. Алгоритмы защиты предназначены для контроля целостности обеих частей и обеспечения конфиденциальности критической части. При установке защиты вычисляется имитовставка всего сообщения и зашифровывается его критическая часть. При снятии защиты имитовставка проверяется и, если проверка прошла успешно, критическая часть расшифровывается.

В алгоритмах седьмой группы длина защищаемого сообщения должна быть сразу известна, эти алгоритмы рекомендуется применять для защиты ключей. Защищаемый ключ сопровождается открытым заголовком, который содержит открытые атрибуты ключа и одновременно является контрольным значением при проверке целостности. Могут использоваться фиксированные постоянные заголовки, которые служат только для контроля целостности. При установке защиты ключ зашифровывается вместе со своим заголовком. При снятии защиты выполняется обратное преобразование и расшифрованный заголовок сравнивается с контрольным.

Восьмой алгоритм предназначен для вычисления хеш-значений — контрольных слов, которые определяются без использования ключа. Стороны могут организовать контроль целостности сообщений путём сравнения их хеш-значений с достоверными контрольными хеш-значениями. Изменение сообщения с высокой вероятностью приводит к изменению соответствующего хеш-значения и поэтому хеш-значения могут использоваться вместо самих сообщений, например в системах электронной цифровой подписи.

<https://electromicro.ru/resources/wiki/aes/aes1/>

**AES: Стандарт шифрования AES**

AES (Advanced Encryption Standard) — это т. н. «симметричный» алгоритм шифрования, принятый в качестве стандарта и широко используемый в различных областях IT и вообще практически во всех сферах нашей, немыслимой без современных технологий, жизни.

Такую популярность AES завоевал благодаря (относительной) простоте, эффективности выполнения своей основной задачи по шифрованию информации, открытости, надёжности и проверенности временем и конечно благодаря стандартизации и признанию на официальном уровне.

В данный момент AES используется для шифрования информации в интернете, для передачи данных в различных сетях проводным и беспроводным способом, в различных устройствах и гаджетах и т. д., то есть везде, где нужно качественно шифровать информацию, затрачивая при этом минимум вычислительной мощности.

Симметричный алгоритм

AES относится к так называемым «симметричным» алгоритмам, которые для шифрования и расшифровывания информации используют один и тот же криптографический ключ. Вообще, подобный тип шифрования является одним из самых распространённых и давно используемых.

При работе по принципу симметричного шифрования, секретный ключ имеется у обеих сторон взаимодействия (отправителя и получателя информации) и должен храниться и передаваться соответствующим безопасным образом.

Длина ключей в AES может выбираться из нескольких стандартных значений 128,192, 256 бит, в зависимости от решаемой задачи и необходимого уровня защиты данных.

Существуют также и другие алгоритмы шифрования, например, т. н. «несимметричное шифрование» в котором для шифрования и расшифровки используются разные ключи. Каждый тип алгоритма имеет свои достоинства и недостатки и свои области применения, в которых показывают себя наилучшим образом.

Блочное шифрование

AES является также алгоритмом блочного шифрования. Это простая и легко реализуемая на различных платформах концепция шифрования, которая сводится к подстановкам и перестановкам цифр в блоках обрабатываемых данных.

Цитата из википедии: шифр подстановки — это метод шифрования, в котором элементы исходного открытого текста заменяются зашифрованным текстом в соответствии с некоторым правилом. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее.

Шифр перестановки — это метод шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы, пары букв, тройки букв, комбинирование этих случаев и так далее.

Мы здесь не будем приводить полное математическое описание и разбор работы алгоритма AES — для большинства наших читателей и формата популярной статьи это явно избыточно — квалифицированно разобраться в работе алгоритма такой сложности смогут только профессионально подготовленные люди (математики и криптографы), здесь мы только попытаемся популярно объяснить суть производимых алгоритмом AES манипуляций с данными.

Алгоритм шифрования AES основан на принципе подстановок и перестановок и имеет архитектуру для которой характерно:

представление шифруемого блока в виде двумерного байтового массива

шифрование за один раунд всего блока данных

выполнение криптографических преобразований, как над отдельными байтами массива, так и над его строками и столбцами. Это обеспечивает «диффузию» данных одновременно в двух направлениях — по строкам и по столбцам.

|  |  |  |
| --- | --- | --- |
| **Характеристика** | **BelT** | **AES** |
| **Полное название** | СТБ 34.101.31-2007 "Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля целостности" | FIPS PUB 197 "Advanced Encryption Standard (AES)" |
| **Происхождение** | Республика Беларусь | США (разработан NIST) |
| **Год принятия** | Предварительно в 2007, окончательно в 2011 | 2001 |
| **Тип шифра** | Блочный шифр | Блочный шифр |
| **Длина ключа** | 256 бит | 128, 192, 256 бит |
| **Длина блока** | 128 бит | 128 бит |
| **Количество циклов (раундов)** | 8 | 10, 12, 14 (зависит от длины ключа) |
| **Основные режимы шифрования** | Простая замена, сцепление блоков, гаммирование с обратной связью, счётчик | Подстановки и перестановки |
| **Применение** | Главным образом в Республике Беларусь | Широко используется во всем мире в различных областях |
| **Методы контроля целостности** | Алгоритм выработки имитовставки, хеширование | Хеширование, поддержка режимов шифрования для обеспечения целостности |
| **Гибкость конфигурации** | Фиксированная длина ключа и блока | Гибкая конфигурация длины ключа и фиксированная длина блока |
| **Способ применения** | Шифрование данных, контроль целостности, одновременное шифрование и имитозащита | Шифрование данных, обеспечение конфиденциальности и целостности данных в разнообразных приложениях |
| **Устойчивость к атакам** | Специфическая реализация требует детального анализа, но предполагается высокий уровень безопасности | Высокий уровень безопасности, доказанный многочисленными исследованиями и практическим применением |
| **Лицензирование и доступность** | Стандарт государственный, доступен для использования в Республике Беларусь | Открытый стандарт, широко доступен и используется во множестве продуктов и технологий |
| **Процедура выбора стандарта** | Разработан и принят на национальном уровне | Выбран через международный открытый конкурс, проведенный NIST |

**Выводы:** В ходе лабораторной работы были представлены и подробно рассмотрены основные стандарты безопасности информационных систем, как отечественные, так и зарубежные. Особое внимание уделено стандарту BelT, который представляет собой стандарт шифрования в РБ, и стандарту АЕS, аналог вышеупомянутого в США.