МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт математики и информационных систем

Факультет автоматики и вычислительной техники

Кафедра систем автоматизации управления

**ПРОГРАММИРОВАНИЕ НА ЯЗЫКЕ PYTHON. РЕАЛИЗАЦИЯ**

**AES-ШИФРОВАНИЯ**Пояснительная записка

Отчёт по дисциплине

«Учебная практика»

ТПЖА 090302.009 ПЗ

Разработал студент гр. ИТб–1301–01–00 \_\_\_\_\_\_\_\_\_\_\_\_/ Зуев А.И./

(подпись)

Руководитель работы \_\_\_\_\_\_\_\_\_\_\_\_/ Родионов К.В./

(подпись)

Работа защищена с оценкой «\_\_\_\_\_\_\_\_\_\_\_\_\_\_» «\_\_»\_\_\_\_\_\_\_\_\_\_2021 г.

Киров 2021

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Утверждаю | | | | | | | | |
| Зав. каф. | | | | | САУ | | | |
|  | | | |  | наименование | | | |
|  | | | |  | Ланских Ю. В. | | | |
| подпись | | | | | Ф.И.О. | | | |
| « |  | » |  | | | 20 | 21 | г. |

ЗАДАНИЕ

на практику

|  |  |
| --- | --- |
| по дисциплине | Учебная практика |
|  | полное название дисциплины |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Студенту | Зуеву А. И. | , обучающемуся по образовательной программе | | |
| 09.03.02 – Информационные системы и технологии | | | | |
| полное название направления подготовки (специальности) | | | | |
| первый | | |  | очная |
| курс обучения | | |  | форма обучения |

|  |  |
| --- | --- |
| Индивидуальные задания, выполняемые в период практики: | 1. Выполнить обучающие задания, приведённые в методических указаниях, для ознакомления с методами работы с языком Python. |
| 2. Реализовать криптографический алгоритм (AES-шифрование (модуль)) при помощи языка Python, не используя библиотечные функции, связанные непосредственно с шифрованием. Разработанная программа должна осуществлять шифрование и дешифрование текста в соответствии с вариантом. В приложении должна быть реализована возможность ввода текста (вручную или загрузка из файла – на усмотрение разработчика), ключа (если этого требует алгоритм) и зашифрованного текста. | |

|  |  |
| --- | --- |
| 1. Исходные данные: | задание в соответствии с вариантом |
| 2. Основные разделы: |  |
| 1. Обучающие задания. Введение в язык Python | |
|  | |
|  | |
| 3. График выполнения: | 28.06 прохождение инструктажей |
| 28.06 – 01.07 выполнение обучающих заданий | |
| 01.07 – 04.07 реализация шифрования и дешифрования | |
| 04.07 – 05.07 оформление отчёта по практике | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Руководитель работы |  |  |  | Родионов К.В. |  |  |
|  |  | Подпись руководителя |  | Ф.И.О. руководителя |  | Дата |
| Задание принял |  |  |  |  |  |  |
|  |  | Подпись обучающегося |  | Ф.И.О. обучающегося |  | Дата |

**Реферат**

Зуев А.И. Программирование на языке Python. Реализация AES-шифрования: ТПЖА.090302.009 ПЗ: Учебная практика / ВятГУ, каф. САУ; рук. К.В. Родионов. – Киров, 2021. ПЗ с., рис., источников, прил.

ПЕРЕЧЕНЬ КЛЮЧЕВЫХ СЛОВ: AES-шифрование, k–means, k–nearest, Python, PyCharm.

Объект исследования и разработки – AES-шифрование.

Цель работы – реализовать криптографический алгоритм (AES-шифрование (модуль)) при помощи языка Python, не используя библиотечные функции, связанные непосредственно с шифрованием.

*Обозначение*

*Наименование*

*Количество*

*листов*

*№ экз.*

*Примеч.*

*Формат*

*№ строки*

Изм.

Лист

№ докум.

Подпись

Дата

Лист

1

*ТПЖА 090302.009 ПЗ*

Разраб.

*Зуев А.И.*

Провер.

Родионов К.В.

Т. контр.

Н. контр.

Утверд.

*Программирование на языке Python. Реализация AES-шифрования*

Литер

Листов

1

*Кафедра САУ,*

*группа ИТб–1301*

*Документация общая*

*Вновь заработанная*

*Пояснительная записка*

*ТПЖА.090302.774 ПЗ*

*А4*

*22*

*27*

*28*

*21*

*19*

*10*

*9*

*8*

*25*

*23*

*18*

*17*

*13*

*7*

*4*

*16*

*11*

*6*

*5*

*3*

*2*

*1*

*14*

*15*

*20*

*24*

*26*

*12*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Содержание   |  |  | | --- | --- | | Введение……………………………………………………………………... | 3 | | 1. Обзор среды программирования и введение в Python…………………. | 4 | | 1.1 Обзор среды программирования PyCharm…………………………….. | 4 | | 1.2 Выполнение обучающих заданий……………………………………… | 5 | | 1.2.1 Алгоритм кластеризации k–means…………………………………… | 5 | | 1.2.2 Алгоритм классификации k ближайших соседей…………………… | 6 | | 1.2.3 Математическая статистика………………………………………….. | 8 | | 1.3 Вывод по разделу 1……………………………………………………… | 12 | | 2 AES-шифрование…………………………………………………………………… | 13 | | 2.1 С чем работает программа | 8 | | 2.2 Вывод по разделу 2 | 9 | | 3 Алгоритмы шифрования и дешифрования | 10 | | 3.1 Шифрование | 10 | | 3.1.2 Вывод на экран | 10 | | 3.1.3 Результат работы программы шифрования | 11 | | 3.2 Дешифрование | 11 | | 3.2.2 Вывод на экран | 11 | | 3.2.3 Результаты работы программы дешифрования | 11 | | 3.3 Вывод по разделу 3 | 12 | | 4 Заключение | 13 | | Приложение А (обязательное) Листинг программного кода, реализация алгоритма шифрования | 14–18 | | Приложение Б (обязательное) Листинг программного кода, реализация алгоритма дешифрования | 19–23 | | Приложение В (справочное) Библиографический список | 24 | | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | |
|  |  |  |  |  |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| *Разраб.* | | *Зуев А.И.* |  |  | *Программирование на языке Python. Реализация AES-шифрования* | *Литер* | | | *Лист* | *Листов* | |
| *Пров.* | | *Родионов К.В.* |  |  |  |  |  | *2* | *1* | |
| *Т.контр* | |  |  |  | *Кафедра САУ,*  *группа ИТб–1301* | | | | | |
| *Н.контр* | |  |  |  |
| *Утверд.* | |  |  |  |
| Введение  Целью учебной практики является изучение основ работы с языком программирования Python путём выполнения обучающих заданий и реализации криптографического алгоритма AES-шифрования.  Python – [высокоуровневый язык программирования](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%81%D0%BE%D0%BA%D0%BE%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D0%B5%D0%B2%D1%8B%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F) общего назначения с динамической строгой типизацией, ориентированный на повышение производительности разработчика и читаемости кода. Язык является полностью объектно-ориентированным — всё является объектами. Python активно развивается, новые версии с добавлением/изменением языковых свойств выходят примерно раз в два с половиной года.  Python поддерживает [структурное](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), [обобщенное](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D0%BE%D0%B1%D1%89%D1%91%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), [объектно-ориентированное](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%BD%D0%BE-%D0%BE%D1%80%D0%B8%D0%B5%D0%BD%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), [функциональное](https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и [аспектно-ориентированное программирование](https://ru.wikipedia.org/wiki/%D0%90%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%BD%D0%BE-%D0%BE%D1%80%D0%B8%D0%B5%D0%BD%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5). Основные архитектурные черты – [динамическая типизация](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%BD%D0%B0%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%82%D0%B8%D0%BF%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F), [автоматическое управление памятью](https://ru.wikipedia.org/wiki/%D0%A1%D0%B1%D0%BE%D1%80%D0%BA%D0%B0_%D0%BC%D1%83%D1%81%D0%BE%D1%80%D0%B0_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)), полная [интроспекция](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D1%80%D0%BE%D1%81%D0%BF%D0%B5%D0%BA%D1%86%D0%B8%D1%8F_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)), механизм [обработки исключений](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%BA%D0%B0_%D0%B8%D1%81%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BD%D0%B8%D0%B9), поддержка [многопоточных вычислений](https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B3%D0%BE%D0%BF%D0%BE%D1%82%D0%BE%D1%87%D0%BD%D0%BE%D1%81%D1%82%D1%8C), высоко уровневые [структуры данных](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85). Поддерживается разбиение программ на [модули](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D1%83%D0%BB%D1%8C_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)), которые, в свою очередь, могут объединяться в пакеты.  История криптографии насчитывает около 4 тысяч лет. Криптография – наука о защите информации и данных, об обеспечении конфиденциальности. В современном мире криптография находит множество различных применений: она используется в сотовой связи, платном цифровом телевидении при подключении к Wi-Fi и на транспорте для защиты билетов от подделок. А, что важнее всего, серверы банков и почтовые клиенты сохраняют пароли пользователей именно с помощью методов шифрования. Они обеспечивают безопасную передачу всей информации в интернете вещей для аутентификации людей и устройств, а также при установлении связи между только устройствами. | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *3* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| 1 Обзор среды программирования и введение в Python.  Для комфортного использования языка Python необходимо изучить среду программирования для этого языка. Я пользуюсь IDE PyCharm.  1.1 Обзор среды программирования PyCharm  PyCharm — интегрированная среда разработки для языка программирования Python. Предоставляет средства для анализа кода, графический отладчик, инструмент для запуска юнит-тестов. PyCharm разработана компанией JetBrains на основе IntelliJ IDEA. Совместима с Windows, macOS, Linux.    Рисунок 1 – Окно среды разработки PyCharm.  1.2 Выполнение обучающих заданий  1.2.1 Алгоритм кластеризации k-means  Алгоритм k-средних (англ. k–means) – один из алгоритмов машинного обучения, решающий задачу кластеризации. Этот алгоритм является неиерархическим, итерационным методом кластеризации, он получил большую популярность благодаря своей простоте, наглядности реализации и достаточно высокому качеству работы.  Кластеризация – это задача поиска в данных определенных групп – кластеров. Кластеры характеризуются внутренней однородностью и внешней изолированностью. | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *4* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| Требуется реализовать алгоритм k-means, с помощью которого выделить два кластера: две группы студентов по их оценкам из таблицы 1 за тесты по физике и математике.  Таблица 1 – Оценки абитуриентов за тесты.   |  |  |  | | --- | --- | --- | | № студента | Физика | Математика | | 1 | 4 | 4 | | 2 | 3 | 3 | | 3 | 5 | 3 | | 4 | 2 | 3 | | 5 | 5 | 5 | | 6 | 3 | 2 | | 7 | 2 | 4 | | 8 | 4 | 5 | | 9 | 5 | 4 | | 10 | 2 | 2 |   Результат работы программы представлен на рисунке 2. Листинг программы приведён в приложении А.  Алгоритм работы k-means представлен ниже:   1. Задается количество кластеров k, которые требуется обнаружить. 2. Центры кластеров изначально инициализируются случайным образом. 3. Каждый из объектов приписывается к ближайшему кластеру. 4. На основании объектов, вошедших в каждый кластер, центры кластеров пересчитываются. 5. Шаги 3 и 4 повторяются до тех пор, пока центры кластеров не стабилизируются, то есть на очередной итерации объекты будут принадлежать тем же кластерам, что и до этого. | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *5* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| Рисунок 2 – Результат работы программы k-means  1.2.2 Алгоритм классификации k-ближайших соседей  Метод ближайших соседей – метрический алгоритм для автоматической классификации объектов или регрессии. В случае использования метода для классификации объект присваивается тому классу, который является наиболее распространённым среди соседей данного элемента, классы которых уже известны.  Пусть у нас имеется матрица объектов X (смотри таблицу 2). Тогда каждая строка таблицы описывает отдельный объект. Каждый столбец таблицы описывает определенный признак объекта.  Таблица 2 - Параметры и виды некоторых обезьян   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | № | Рост | Вес | Вид | № | Рост | Вес | Вид | | 1 | 33 | 21 | Лемур | **9** | 185 | 155 | Горилла | | 2 | 41 | 13 | Лемур | **10** | 193 | 129 | Горилла | | 3 | 18 | 22 | Лемур | **11** | 164 | 135 | Горилла | | 4 | 38 | 34 | Лемур | **12** | 205 | 131 | Горилла | | 5 | 62 | 118 | Шимпанзе | **13** | 145 | 55 | Орангутан | | 6 | 59 | 137 | Шимпанзе | **14** | 168 | 35 | Орангутан | | 7 | 95 | 131 | Шимпанзе | **15** | 135 | 47 | Орангутан | | 8 | 83 | 110 | Шимпанзе | **16** | 138 | 66 | Орангутан | | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *6* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| Результат работы программы представлен на рисунке 3. Листинг программы приведён в приложении Б.  Алгоритм работы k-NN представлен ниже:   1. Измеряем расстояние от объекта obj до каждого объекта в матрице X. 2. Сортируем полученные значения в порядке увеличения расстояния (в начале будут объекты наиболее близкие к obj, в конце – наиболее удаленные). 3. Берем первые k объектов из отсортированного списка, определяем, какой класс встречается там чаще всего. Именно этому классу и принадлежит наш объект obj.     Рисунок 3 - Результат работы алгоритма k-NN | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *7* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| 1.2.3 Математическая статистика  В этом разделе нужно было реализовать несколько подпрограмм. Список заданий представлен ниже:   1. Создать в Python переменную, массив, матрицу с заданными, случайными целочисленными, нулевыми, единичными значениями.   Результат выполненной подпрограммы представлен на рисунке 4.   1. Импортировать переменную (матрицу) из текстового структурированного файла (файл создать вручную: разделители столбцов – пробелы).   Результат выполненной подпрограммы представлен на рисунке 5.   1. Загрузить одномерные данные из каталога data/1D из файла с расширением .mat согласно варианту. Оценить параметры одномерной случайной величины, используя команды NumPy: np.max, np.min, np.median, np.mean, np.var, np.std; команды сохранить в скрипт.   Результат выполненной подпрограммы представлен на рисунке 6.   1. Вывести графики одномерных случайных величин и их плотности распределения. Команды сохранить в скрипт. Подобрать вид распределения одномерной случайной величины и его параметры. На одном графике отобразить случайную величину, уровень среднего значения и дисперсию.   Результат выполненной подпрограммы представлен на рисунках 7-8.   1. Построить и вывести на графике автокорреляцию заданной одномерной величины. Команды сохранить в скрипт.   Результат выполненной подпрограммы представлен на рисунке 9.   1. Импортировать из каталога data/NDфайл \*.matс многомерными даннымисогласно варианту. Первые 5 столбцов считать входными значениями (измерения датчиков, наблюдения и т.д.), последний 6 столбец – выходная величина, для которой требуется установить зависимость от входных величин.   Результат выполненной подпрограммы представлен на рисунке 10. | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *8* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| 1. Построить матрицу корреляции для всех входных и выходных величин. Сделать выводы о зависимости/независимости выходной величины от каждой из входных компонент. Отобразить точечный график для случайных величин, коэффициент корреляции для которых по модулю больше 0.8.   Результат выполненной подпрограммы представлен на рисунке 11.  Листинг программы целиком продемонстрирован в приложении В.    Рисунок 4 - Результат выполнения первой подпрограммы    Рисунок 5 - Результат выполнения второй подпрограммы | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *9* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| Рисунок 6 - Результат выполнения третьей подпрограммы    Рисунок 7 - Результат выполнения четвёртой подпрограммы (график)    Рисунок 8 - Результат выполнения четвёртой подпрограммы (гистограмма) | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *10* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| Рисунок 9 - Результат выполнения пятой подпрограммы    Рисунок 10 - Результат выполнения шестой подпрограммы    Рисунок 11 - Результат выполнения седьмой подпрограммы | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *11* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| 1.3 Вывод по разделу 1  Python широко известен своей лаконичностью и простотой в изучении на практике. После выполнения обучающих заданий были получены знания в работе со средой программирования PyCharm, а вместе с этим и начальные знания в языке программирования Python. | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *12* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
| 2 AES-шифрование  2.1 История Алгоритма AES  Несколько лет назад в США был принят новый правительственный стандарт шифрования, который получил название AES (Advanced EncryptionStandard - улучшенный стандарт шифрования). Вместо того чтобы разрабатывать новый шифр или поручать эту работу конкретным людям, Национальный институт стандартов и технологий (National Institute of Standards and Technology - NIST) обратился за помощью к криптографическому сообществу. В качестве кандидатов на лучший шифр были приняты 15 предложений, из которых затем отобрали пять финалистов. Лучшим шифром был признан Rijndael, созданный Йоаном Дайменом и Винсентом Рейменом. Он и получил статус нового стандарта шифрования.  2.2 Описание алгоритма AES | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *13* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *14* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *15* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.009 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *16* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.774 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *17* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.774 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *18* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.774 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *19* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.774 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *20* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.774 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *21* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.774 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *22* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.774 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *23* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |
|  | | | | | | | | | | | |
|  |  |  |  |  | *ТПЖА 090302.774 ПЗ* | | | | | | *Лист* |
|  |  |  |  |  | *24* |
| *Изм* | *Лист* | *№ докум.* | *Подпись* | *Дата* |