

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ПЕТРОЗАВОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт математики и информационных технологий  
Кафедра информатики и математического обеспечения

Никаноров Роман Павлович

Отчет по курсу «Верификация программного обеспечения»  
Отчет о тестировании гибридной криптосистемы

Направление 09.03.04 — Программная инженерия

Преподаватель: к.ф.-м.н., доцент К.А. Кулаков

# Содержание

<b>1</b>	<b>Объект тестирования</b>	<b>3</b>
1.1	Описание программы . . . . .	3
1.2	Архитектура программы . . . . .	3
1.3	Интерфейс программы . . . . .	4
<b>2</b>	<b>Стратегия тестирования</b>	<b>5</b>
2.1	Используемые окружение и инструменты . . . . .	5
2.2	Стратегия блочного тестирования . . . . .	6
2.3	Стратегия интеграционного тестирования . . . . .	12
2.4	Стратегия аттестационного тестирования . . . . .	13
2.5	Критерии прохождения тестов . . . . .	15
2.6	Критерии приостановки тестирования . . . . .	15
2.7	Критерии возобновления тестирования . . . . .	15
<b>3</b>	<b>Детальный план тестов</b>	<b>15</b>
3.1	Блочное тестирование . . . . .	15
3.2	Интеграционное тестирование . . . . .	31
3.3	Аттестационное тестирование . . . . .	40
3.4	Специальное тестирование . . . . .	46
<b>4</b>	<b>Покрытие кода тестами</b>	<b>47</b>
<b>5</b>	<b>Пример реализации тестов</b>	<b>47</b>
<b>6</b>	<b>Журнал тестирования</b>	<b>49</b>
6.1	Блочное тестирование . . . . .	49
6.2	Интеграционное тестирование . . . . .	51
6.3	Аттестационное тестирование . . . . .	52
6.4	Специальное тестирование . . . . .	52
<b>7</b>	<b>Результаты</b>	<b>53</b>

# 1 Объект тестирования

## 1.1 Описание программы

Программа представляет собой десктоп-приложение гибридной криптосистемы, которая включает в себя следующий функционал:

1. Генерация ключевой пары RSA.
2. Шифрование и расшифрование документа или каталога симметричным криптоалгоритмом AES в режиме шифрования EAX с размером поппе 16 байт.
3. Шифрование и расшифрование сеансового ключа симметричного алгоритма при помощи ключей RSA.
4. Формирование и проверка цифровой подписи документа.

Полученные шифротексты, ключи и каталоги сохраняются в виде файлов и каталогов.

## 1.2 Архитектура программы

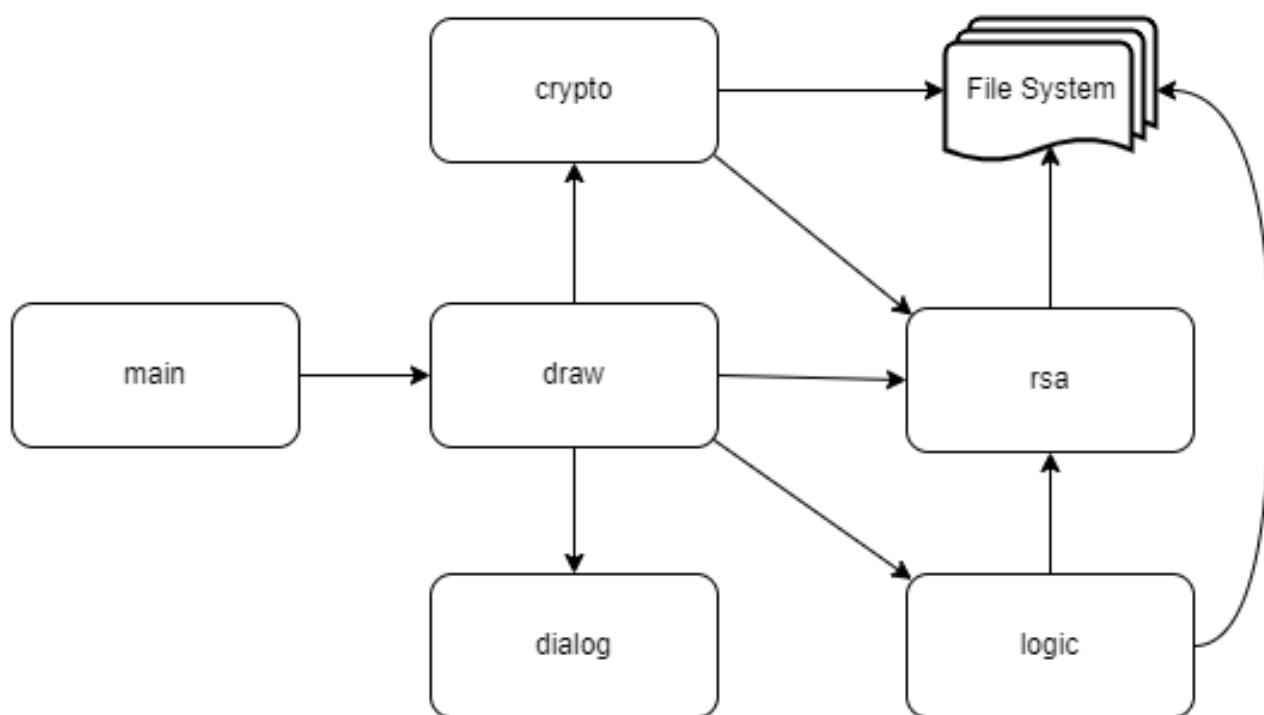


Рис. 1: Архитектура

Программа состоит из следующих модулей:

- main – точка входа в программу;

- draw – основной модуль для отображения интерфейса приложения и взаимодействия с ним;
- dialog – модуль всплывающего диалога;
- crypto – модуль для работы с симметричным алгоритмом AES;
- rsa – модуль для работы с алгоритмом RSA;
- logic – модуль, хранящий в себе логику программы, не попадающую ни в какой другой модуль.

### 1.3 Интерфейс программы

Интерфейс поделён на две области:

- Настройка сессии - содержит списки для выбора сторон шифрования, поле для секретного кода и список сессионных ключей сторон, а так же кнопки для добавления и удаления сторон и ключей.
- Область файла - содержит поле для выбора файла, поле отображения содержимого файла и кнопки взаимодействия с ним: “Зашифровать”, “Расшифровать”, “Подписать” и “Проверить”.

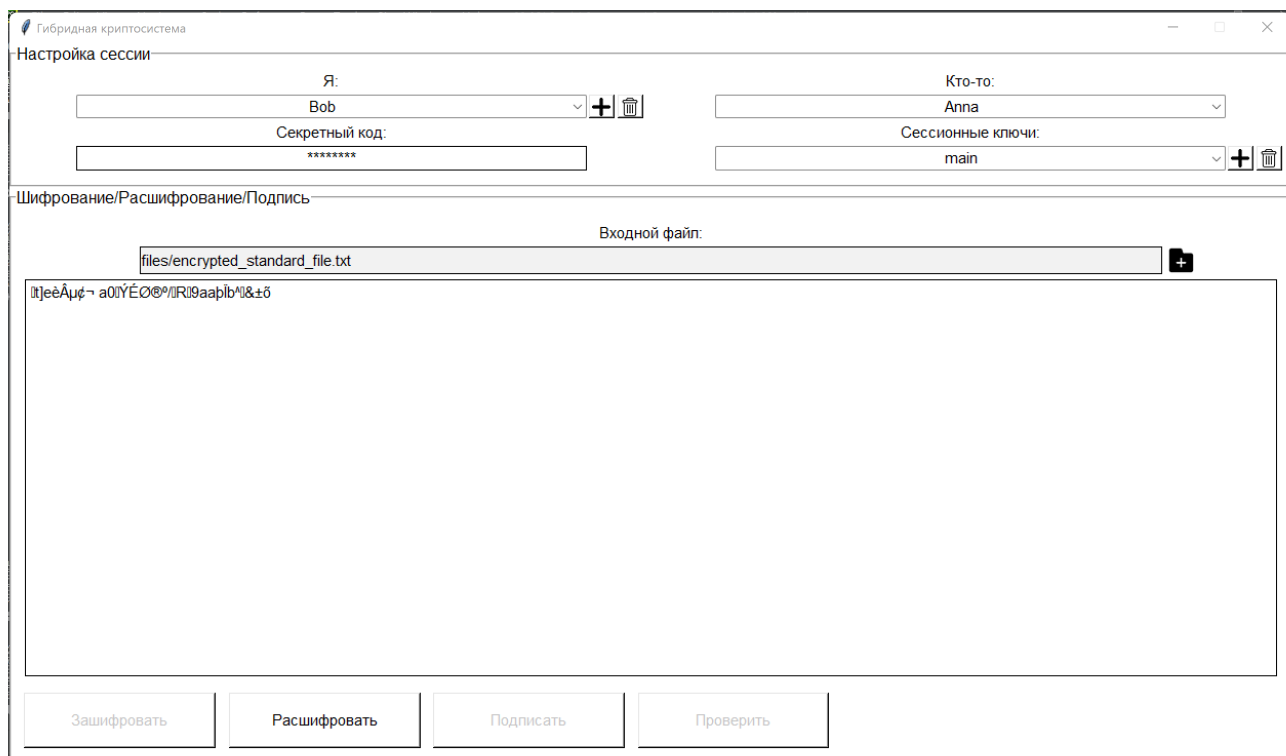


Рис. 2: Интерфейс

## 2 Стратегия тестирования

### 2.1 Используемые окружение и инструменты

Для проведения тестов будут использоваться библиотеки `pytest` и `unittest` для Python. Общий вид тестов выглядит следующим образом:

```
import unittest

class NameTestCase(unittest.TestCase):
    @classmethod
    def setUpClass(cls):
        # Настройки, применяемые до тестов
        pass

    def test_name(self):
        # Получаем данные из модуля
        my_value = 0
        # Сравниваем полученные данные с правильными
        self.assertEqual(0, my_value)

    @classmethod
    def tearDownClass(cls):
        # Настройки, применяемые после тестов
        pass

if __name__ == '__main__':
    unittest.main()
```

Рис. 3: Общий вид тестов

На выходе получаем следующий вывод:

```

===== short test summary info =====
FAILED tests/test_path.py::FirstTestCase::test_incorrect_value - AssertionError: 0 != 1
FAILED tests/test_path.py::SecondTestCase::test_incorrect_name - AssertionError: 'Bob' != 'Anna'
===== 2 failed, 2 passed in 0.10s =====

```

Рис. 4: Вывод тестов

## 2.2 Стратегия блочного тестирования

**Блочное тестирование** – процесс, позволяющий проверить на корректность единицы исходного кода, наборы из одного или более программных модулей вместе с соответствующими управляющими данными, процедурами использования и обработки. Идея состоит в том, чтобы писать тесты для каждой нетривиальной функции или метода. Это позволяет достаточно быстро проверить, не привело ли очередное изменение кода к регрессии, то есть к появлению ошибок в уже оттестированных местах программы, а также облегчает обнаружение и устранение таких ошибок.

Подробное описание модулей, если не сказано обратного, модуль/функция будут тестироваться:

- `main` – служит только для запуска основного цикла интерфейса, тестирование не требуется.
- `draw` – модуль интерфейса, инициализирует, размещает и обрабатывает взаимодействие с элементами интерфейса.
  - `get_options()` – возвращает четыре значения настройки сессии: имя получателя, имя отправителя, название сессионного ключа и секретный код отправителя.
  - `update_state()` – обновляет состояние интерфейса: обновляет список сессионных ключей пары и изменяет состояние кнопок взаимодействия с файлом, частичное тестирование, тестируется интеграционными тестами.
  - `validate_name(name)` – проверяет доступность нового имени пользователя.
    - \* `name: String` – проверяемое имя.
  - `add_name(name, code)` – добавляет новое имя в списки сторон и генерирует для него пару ключей RSA.
    - \* `name: String` – имя пользователя.
    - \* `code: String` – секретный код.

- `delete_name_button_clicked()` – полностью удаляет пользователя, в том числе и связанные с ним файлы, частичное тестирование, тестируется интеграционными тестами.
- `validate_key_name(name)` – проверяет доступность имени сессионного ключа.
  - \* `name: String` – название ключа.
- `generate_new_keys(name, code)` – вызывает генерацию ключей RSA пользователя, частичное тестирование, тестируется интеграционными тестами.
  - \* `name: String` – имя пользователя.
  - \* `code: String` – секретный код.
- `delete_key_button_clicked()` – обрабатывает нажатие кнопки удаления сессионного ключа: удаляет ключ из списка и связанные с ним файлы, частичное тестирование, тестируется интеграционными тестами.
- `generate_session_key(key_name):` – вызывает генерацию сессионного ключа, частичное тестирование, тестируется интеграционными тестами.
  - \* `key_name: String` – название сессионного ключа.
- `clear_buttons_state()` – сбрасывает состояние кнопок взаимодействия с файлом.
- `change_buttons_state(buttons, states)` – меняет состояние кнопок.
  - \* `buttons: list[tkinter.Button]` – виджеты кнопок.
  - \* `states: list[Bool]` – состояния кнопок - активны/неактивны.
- `check_buttons_state()` – проверяет необходимое состояние кнопок по настройке сессии и изменяет при необходимости.
- `add_file_button_click()` – обрабатывает нажатие кнопки добавления файла: открывает диалог выбора файла и отображает его содержимое при выборе, частичное тестирование, тестируется интеграционными тестами.
- `encrypt_file_button_clicked()` – обрабатывает нажатие кнопки шифрования файла, тестируется интеграционными тестами.
- `decrypt_file_button_clicked()` – обрабатывает нажатие кнопки расшифрования файла, тестируется интеграционными тестами.
- `sign_file_button_clicked()` – обрабатывает нажатие кнопки подписи файла, тестируется интеграционными тестами.

- `verify_file_button_clicked()` – обрабатывает нажатие кнопки проверки подписи файла, тестируется интеграционными тестами.
- `draw_all()` – размещает виджеты интерфейса и настраивает их поведение, тестирование не требуется, так как отсутствует логика.
- `dialog` – модуль диалоговых окон добавления новых пользователей и ключей, тестирование не будет проводиться, так как нет сложной логики, только настройка виджетов и их отображение.
- `crypto` – модуль симметричного алгоритма AES.
  - `generate_session_key(size)` – генерирует сессионный ключ заданного размера - набор байт.
  - `encrypt_file(session_key, in_path, out_path)` – шифрует файл.
    - \* `session_key`: bytes – сессионный ключ.
    - \* `in_path`: String – путь к шифруемому файлу.
    - \* `out_path`: String – путь к зашифрованному файлу.
  - `decrypt_file(session_key, in_path, out_path)` – расшифровывает файл.
    - \* `session_key`: bytes – сессионный ключ.
    - \* `in_path`: String – путь к зашифрованному файлу.
    - \* `out_path`: String – путь к расшифрованному файлу.
  - `sign_file_and_encrypt(private_key, public_key, in_path, out_path)` – подписывает файл и сохраняет зашифрованную подпись в файл, частичное тестирование, тестируется интеграционными тестами.
    - \* `private_key`: RsaKey – приватный ключ подписывающего.
    - \* `public_key`: RsaKey – публичный ключ проверяющего.
    - \* `in_path`: String – путь к подписываемому файлу.
    - \* `out_path`: String – путь к зашифрованной подписи.
  - `sign_file(private_key, in_path, out_path)` – подписывает файл и сохраняет подпись в файл.
    - \* `private_key`: RsaKey – приватный ключ подписывающего.
    - \* `in_path`: String – путь к подписываемому файлу.
    - \* `out_path`: String – путь к подписи.



- `verify_sign_and_decrypt(public_key, private_key, file_path, signature_path)` – расшифровывает и проверяет подпись для файла, частичное тестирование, тестируется интеграционными тестами.
  - \* `public_key: RsaKey` – публичный ключ подписывающего.
  - \* `private_key: RsaKey` – приватный ключ проверяющего.
  - \* `file_path: String` – путь к расшифрованному файлу.
  - \* `signature_path: String` – путь к зашифрованной подписи.
- `verify_sign(public_key, file_path, signature_path)` – расшифровывает и проверяет подпись для файла.
  - \* `public_key: RsaKey` – публичный ключ подписывающего.
  - \* `file_path: String` – путь к расшифрованному файлу.
  - \* `signature_path: String` – путь к подписи.
- `rsa` – модуль для работы с алгоритмом RSA.
  - `save_private_key(keys, secret_code, path)` – шифрует приватный ключ, используя секретный код, и сохраняет его в файл.
    - \* `keys: RsaKey` – ключи RSA.
    - \* `secret_code: String` – секретный код.
    - \* `path: String` – путь к файлу.
  - `save_public_key(keys, path)` – сохраняет публичный ключ в файл.
    - \* `keys: RsaKey` – ключи RSA.
    - \* `path: String` – путь к файлу.
  - `generate_keys(secret_code, private_key_path, public_key_path)` – генерирует ключи RSA и сохраняет их в файлы.
    - \* `secret_code: String` – секретный код.
    - \* `private_key_path: String` – путь к приватному ключу.
    - \* `public_key_path: String` – путь к публичному ключу.
  - `check_secret_code(secret_code, path)` – проверяет секретный код на правильность.
    - \* `secret_code: String` – секретный код.
    - \* `path: String` – путь к приватному ключу.

- `get_public_key(path)` – считывает и возвращает публичный ключ из файла.
  - \* `path: String` – путь к публичному ключу.
- `get_private_key(secret_code, path)` – считывает и возвращает приватный ключ из файла.
  - \* `secret_code: String` – секретный код.
  - \* `path: String` – путь к приватному ключу.
- `get_public_key_pair(public_key)` – возвращает пару (e, n) открытого ключа.
  - \* `public_key: RsaKey` – открытый ключ RSA.
- `get_private_key_pair(private_key)` – возвращает пару (d, n) закрытого ключа.
  - \* `private_key: RsaKey` – закрытый ключ RSA.
- `encrypt(message, public_key, out_path)` – шифрует сообщение и сохраняет его в файл.
  - \* `message: String` – сообщение.
  - \* `public_key: RsaKey` – публичный ключ RSA.
  - \* `out_path: String` – путь к файлу для сохранения.
- `decrypt(private_key, in_path, mode)` – считывает зашифрованное сообщение из файла и расшифровывает его.
  - \* `private_key: RsaKey` – приватный ключ RSA.
  - \* `in_path: String` – путь к зашифрованному сообщению.
  - \* `mode: String` – вид расшифрованного сообщения ('bytes', 'str').
- `logic` – модуль, хранящий в себе логику программы, не попадающую ни в какой другой модуль.
  - `get_signature_path(path, from_name)` – получает путь к подписи.
    - \* `path: String` – путь к подписываемому файлу.
    - \* `from_name: String` – имя отправителя.
  - `get_encrypted_file_path(common_path)` – получает путь к зашифрованному файлу.
    - \* `common_path: String` – путь к шифруемому файлу.
  - `get_decrypted_file_path(encrypted_path)` – получает путь к расшифрованному файлу.

- \* `encrypted_path: String` – путь к зашифрованному файлу.
- `get_session_key_path(from_name, to_name, key_name)` – получает путь к сессионному ключу.
  - \* `from_name: String` – имя отправителя.
  - \* `to_name: String` – имя получателя.
  - \* `key_name: String` – название сессионного ключа.
- `get_private_key_path(name)` – получает путь к приватному ключу.
  - \* `name: String` – имя владельца ключа.
- `get_public_key_path(name)` – получает путь к публичному ключу.
  - \* `name: String` – имя владельца ключа.
- `read_session_key(from_name, to_name, key_name, code)` – получает сессионный ключ пары, частичное тестирование, тестируется интеграционными тестами.
  - \* `from_name: String` – имя отправителя.
  - \* `to_name: String` – имя получателя.
  - \* `key_name: String` – название сессионного ключа.
  - \* `code: String` – секретный код получателя.
- `save_session_key(from_name, to_name, key_name, key)` – сохраняет сессионный ключ в файлы (в открытом и зашифрованном виде), частичное тестирование, тестируется интеграционными тестами.
  - \* `from_name: String` – имя отправителя.
  - \* `to_name: String` – имя получателя.
  - \* `key_name: String` – название сессионного ключа.
  - \* `key: bytes` – сессионный ключ.
- `delete_session_keys(from_name, to_name, key_name)` – удаляет все файлы, связанные с сессионным ключом.
  - \* `from_name: String` – имя отправителя.
  - \* `to_name: String` – имя получателя.
  - \* `key_name: String` – название сессионного ключа.
- `replace_object_data(object, data)` – заменяет текст виджетов `Text` или `Entry`.
  - \* `object: tkinter.TextEntry` – виджет.

- \* data: String – текст.
- delete\_files(dir\_path, part) – удаляет все файлы в каталоге, имеющие в названии part.
  - \* dir\_path: String – путь к каталогу.
  - \* part: String – часть имени файла.
- load\_name\_box(box, values, name) – заполняет список пользователей.
  - \* box: tkinter.ttk.Combobox – виджет списка выбора.
  - \* values: [String] – массив значений списка.
  - \* name: String – from - отправитель, to - получатель.
- load\_keys\_box(box, values, from\_name, to\_name) – заполняет список сессионных ключей пары.
  - \* box: tkinter.ttk.Combobox – виджет списка выбора.
  - \* values: [String] – массив значений списка.
  - \* from\_name: String – имя отправителя.
  - \* to\_name: String – имя получателя.
- delete\_from\_combobox(box, values, value) – удаляет из списка элемент.
  - \* box: tkinter.ttk.Combobox – виджет списка выбора.
  - \* values: [String] – массив значений списка.
  - \* value: String – удаляемый элемент
- check\_and\_create\_dirs() – проверяет и создаёт отсутствующие каталоги.

## 2.3 Стратегия интеграционного тестирования

**Интеграционное тестирование** – одна из фаз тестирования программного обеспечения, при которой отдельные программные модули объединяются и тестируются в группе. Интеграционное тестирование в качестве входных данных использует модули, над которыми было проведено модульное тестирование, группирует их в более крупные множества и выполняет тесты, определённые в плане тестирования для этих множеств, и представляет их в качестве выходных данных.

Интеграционное тестирование будет проходить восходящим способом. Сначала каждый модуль пройдёт блочное тестирование, затем взаимодействующие модули протестируются в парах и в конце они протестируются собранные вместе. Схему интеграции можно представить в следующем виде:

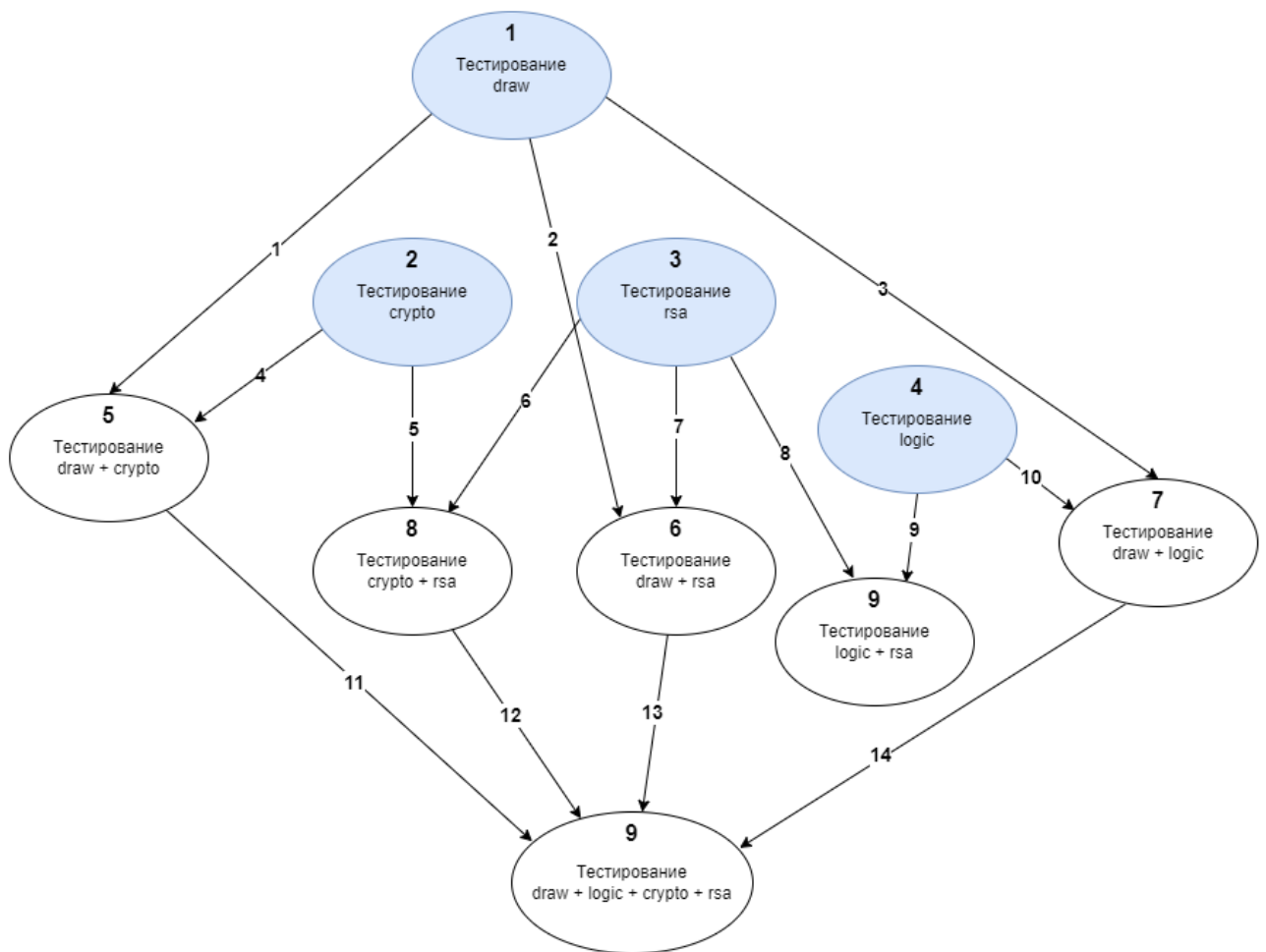


Рис. 5: Интегральная схема

## 2.4 Стратегия аттестационного тестирования

**Аттестационное тестирование** – процесс тестирования пользователем, являющийся по сути первичным обнаружением ошибок. Методы ручного тестирования достаточно эффективны с точки зрения нахождения ошибок, так что один или несколько из них должны использоваться в каждом программном проекте.

В аттестационных тестах планируется проверить следующий функционал:

- правильное заполнение списков выбора сторон;
- добавление пользователя:
  - нового;
  - существующего;
  - с пустым именем;
  - с пустым секретным кодом;
  - с неправильным повтором кода;

- отмена добавления;
  - закрытие диалога.
- удаление пользователя;
- правильное заполнение списка сессионных ключей сторон;
- добавление сессионного ключа:
  - нового;
  - существующего;
  - с пустым именем;
  - отмена добавления;
  - закрытие диалога.
- возможность выбора любого файла;
- правильное отображение содержимого файла:
  - пустого файла;
  - маленького файла;
  - большого файла.
- кликабельность кнопок:
  - для простого файла;
  - для зашифрованного файла;
  - для расшифрованного файла без подписи;
  - для расшифрованного файла с подписью;
- шифрование файла;
- расшифрование файла:
  - неправильный секретный код;
  - неправильный сессионный ключ;
  - правильный секретный код и сессионный ключ.

- подпись файла;
  - неправильный секретный код;
  - правильный секретный код.
- проверка подписи.

## 2.5 Критерии прохождения тестов

Тест считается пройденным если во время его прохождения не выявлено критических ошибок и получен результат, совпадающий с ожидаемым.

## 2.6 Критерии приостановки тестирования

Тестирование должно быть приостановлено, если во время его выполнения выявлена критическая ошибка или полученные результаты не совпадают с ожидаемыми.

## 2.7 Критерии возобновления тестирования

Тестирование возобновляется после локализации и устранения причины приостановки тестирования.

# 3 Детальный план тестов

## 3.1 Блочное тестирование

<b>№ теста</b>	Б-D1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_options()</code> модуля <code>draw</code>
<b>Входные данные</b>	Имена сторон <code>name1</code> и <code>name2</code> , имя ключа <code>main</code> , секретный код <code>code</code>
<b>Ожидаемый результат</b>	Получены четыре значения: <code>name1</code> , <code>name2</code> , <code>main</code> и <code>code</code>

Таблица 1: Тест № Б-D1

<b>№ теста</b>	Б-D2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>update_state()</code> модуля <code>draw</code>
<b>Входные данные</b>	Имена сторон <code>name1</code> и <code>name2</code> , имеется два файла сессионных ключей пары <code>main1</code> и <code>main2</code>
<b>Ожидаемый результат</b>	Список сессионных ключей имеет только два ключа <code>main1</code> и <code>main2</code> , все кнопки неактивны

Таблица 2: Тест № Б-D2

<b>№ теста</b>	Б-D3.1
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции <code>validate_name(name)</code> модуля <code>draw</code> при пустом имени
<b>Входные данные</b>	<code>name</code> является пустой строкой
<b>Ожидаемый результат</b>	-1 - валидация не прошла

Таблица 3: Тест № Б-D3.1

<b>№ теста</b>	Б-D3.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции <code>validate_name(name)</code> модуля <code>draw</code> при существующем имени
<b>Входные данные</b>	<code>name=name1</code> , лист имён пользователя содержит имя <code>name1</code>
<b>Ожидаемый результат</b>	-1 - валидация не прошла

Таблица 4: Тест № Б-D3.2

<b>№ теста</b>	Б-D3.3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>validate_name(name)</code> модуля <code>draw</code> при новом имени
<b>Входные данные</b>	<code>name=name77</code> , лист имён пользователя не содержит имени <code>name77</code>
<b>Ожидаемый результат</b>	0 - валидация прошла

Таблица 5: Тест № Б-D3.3

<b>№ теста</b>	Б-D4
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>add_name(name, code)</code> модуля <code>draw</code>
<b>Входные данные</b>	<code>name=name7</code> , <code>code=code7</code> , листы <code>сторон=[name1, name2, name3]</code> , активными выбраны <code>name1</code> , стоит заглушка на функцию <code>generate_new_keys(name, code)</code>
<b>Ожидаемый результат</b>	В листах <code>сторон</code> появилось имя <code>name7</code> , выбранным в списке отправителя стало имя <code>name7</code> , лист <code>сессийных</code> ключей пустой

Таблица 6: Тест № Б-D4

<b>№ теста</b>	Б-D5.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>delete_name_button_clicked()</code> модуля <code>draw</code> с двумя именами
<b>Входные данные</b>	листы <code>сторон=[name1, name2]</code> , активными выбрано <code>name1</code> , созданы файлы ключей для <code>name1</code>
<b>Ожидаемый результат</b>	листы <code>сторон=[name2]</code> , активным стало <code>name2</code> , файлы ключей для <code>name1</code> не существуют

Таблица 7: Тест № Б-D5.1



<b>№ теста</b>	Б-D5.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции delete_name_button_clicked() модуля draw с одним именем
<b>Входные данные</b>	листы сторон=[name2], активными выбрано name2, созданы файлы ключей для name2
<b>Ожидаемый результат</b>	листы сторон=[], подписи листов стали , файлы ключей для name2 не существуют

Таблица 8: Тест № Б-D5.2

<b>№ теста</b>	Б-D6.1
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции validate_key_name(name) модуля draw с пустым названием
<b>Входные данные</b>	name=""
<b>Ожидаемый результат</b>	-1 - валидация не прошла

Таблица 9: Тест № Б-D6.1

<b>№ теста</b>	Б-D6.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции validate_key_name(name) модуля draw с "encrypted_" в названии
<b>Входные данные</b>	name=encrypted_name
<b>Ожидаемый результат</b>	-1 - валидация не прошла

Таблица 10: Тест № Б-D6.2

<b>№ теста</b>	Б-D6.3
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции validate_key_name(name) модуля draw с существующим названием ключа
<b>Входные данные</b>	name=name1, keys_box_values содержит name1
<b>Ожидаемый результат</b>	-1 - валидация не прошла

Таблица 11: Тест № Б-D6.3

<b>№ теста</b>	Б-D6.4
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции validate_key_name(name) модуля draw с новым названием ключа
<b>Входные данные</b>	name=name2, keys_box_values=[name1, name3]
<b>Ожидаемый результат</b>	0 - валидация прошла

Таблица 12: Тест № Б-D6.4

<b>№ теста</b>	Б-D7
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции generate_session_key(key_name) модуля draw
<b>Входные данные</b>	key_name=name1, заглушки на функции generate_session_key() модуля crypto и save_session_key(from_name, to_name, key_name, key) модуля logic
<b>Ожидаемый результат</b>	В keys_box_values появился новый ключ name1, в списке ключей активным стал name1

Таблица 13: Тест № Б-D7

<b>№ теста</b>	Б-D8
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции clear_buttons_state() модуля draw
<b>Входные данные</b>	Параметр state виджетов кнопок encrypt_button, decrypt_button, sign_button, verify_button равен disable
<b>Ожидаемый результат</b>	В keys_box_values появился новый ключ name1, в списке ключей активным стал name1

Таблица 14: Тест № Б-D8

<b>№ теста</b>	Б-D9
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции change_buttons_state(buttons, states) модуля draw
<b>Входные данные</b>	buttons - массив кнопок с параметром state равным disable, states - массив true значений
<b>Ожидаемый результат</b>	Параметр state всех кнопок в массиве buttons стал равен normal

Таблица 15: Тест № Б-D9

<b>№ теста</b>	Б-D10.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции check_buttons_state() модуля draw, нет имени отправителя
<b>Входные данные</b>	Текст виджета from_box пустой, значение параметра state кнопок name_delete_button, key_add_button, key_delete_button равен normal
<b>Ожидаемый результат</b>	Параметр state этих кнопок стал равен disable

Таблица 16: Тест № Б-D10.1

<b>№ теста</b>	Б-D10.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>check_buttons_state()</code> модуля <code>draw</code> , нет имени получателя
<b>Входные данные</b>	Текст виджета <code>from_box</code> равен <code>name</code> , <code>to_box</code> пустой, значение параметра <code>state</code> кнопки <code>name_delete_button</code> равен <code>disable</code> , а кнопок <code>key_add_button</code> и <code>key_delete_button</code> равен <code>normal</code>
<b>Ожидаемый результат</b>	Параметр <code>state</code> этих кнопок стал равен противоположному

Таблица 17: Тест № Б-D10.2

<b>№ теста</b>	Б-D10.3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>check_buttons_state()</code> модуля <code>draw</code> , есть имена сторон и ключа
<b>Входные данные</b>	Текст виджетов <code>from_box=name1</code> , <code>to_box=name2</code> , <code>keys_box=key</code> , значение параметра <code>state</code> кнопок <code>name_delete_button</code> , <code>key_add_button</code> , <code>key_delete_button</code> равен <code>disable</code>
<b>Ожидаемый результат</b>	Параметр <code>state</code> этих кнопок стал равен <code>normal</code>

Таблица 18: Тест № Б-D10.3

<b>№ теста</b>	Б-D10.4
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>check_buttons_state()</code> модуля <code>draw</code> , путь к файлу пустой
<b>Входные данные</b>	Текст виджета <code>file_entry</code> пустой, значение параметра <code>state</code> кнопок <code>encrypt_button</code> , <code>decrypt_button</code> , <code>sign_button</code> , <code>verify_button</code> равен <code>normal</code>
<b>Ожидаемый результат</b>	Параметр <code>state</code> этих кнопок стал равен <code>disable</code>

Таблица 19: Тест № Б-D10.4

<b>№ теста</b>	Б-D10.5
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>check_buttons_state()</code> модуля <code>draw</code> , файл зашифрован
<b>Входные данные</b>	Путь к файлу содержит <code>encrypted_</code> , <code>state</code> кнопок равен <code>normal</code> , <code>disable</code> , <code>normal</code> , <code>normal</code>
<b>Ожидаемый результат</b>	Параметр <code>state</code> этих кнопок изменился на противоположный

Таблица 20: Тест № Б-D10.5

<b>№ теста</b>	Б-D10.6
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>check_buttons_state()</code> модуля <code>draw</code> , файл расшифрован и есть файл с подписью
<b>Входные данные</b>	Путь к файлу содержит <code>decrypted_</code> , файл с подписью файла существует, <code>state</code> кнопок равен <code>disable</code> , <code>normal</code> , <code>disable</code> , <code>disable</code>
<b>Ожидаемый результат</b>	Параметр <code>state</code> этих кнопок изменился на противоположный

Таблица 21: Тест № Б-D10.6

<b>№ теста</b>	Б-D10.7
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>check_buttons_state()</code> модуля <code>draw</code> , файл расшифрован и нет файла с подписью
<b>Входные данные</b>	Путь к файлу содержит <code>decrypted_</code> , файл с подписью файла не существует, <code>state</code> кнопок равен <code>disable</code> , <code>normal</code> , <code>disable</code> , <code>normal</code>
<b>Ожидаемый результат</b>	Параметр <code>state</code> этих кнопок изменился на противоположный

Таблица 22: Тест № Б-D10.7

<b>№ теста</b>	Б-D10.8
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>check_buttons_state()</code> модуля <code>draw</code> , файл является простым и выбран ключ
<b>Входные данные</b>	Путь к файлу не содержит <code>encrypted_</code> и <code>decrypted_</code> , текст виджета <code>keys_box</code> равен <code>key</code> , <code>state</code> кнопок равен <code>disable</code> , <code>normal</code> , <code>disable</code> , <code>normal</code>
<b>Ожидаемый результат</b>	Параметр <code>state</code> этих кнопок изменился на противоположный

Таблица 23: Тест № Б-D10.8

<b>№ теста</b>	Б-D10.9
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>check_buttons_state()</code> модуля <code>draw</code> , файл является простым и ключ не выбран
<b>Входные данные</b>	Путь к файлу не содержит <code>encrypted_</code> и <code>decrypted_</code> , текст виджета <code>keys_box</code> пустой, <code>state</code> кнопок равен <code>normal</code> , <code>normal</code> , <code>disable</code> , <code>normal</code>
<b>Ожидаемый результат</b>	Параметр <code>state</code> этих кнопок изменился на противоположный

Таблица 24: Тест № Б-D10.9

<b>№ теста</b>	Б-D11
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>add_file_button_click()</code> модуля <code>draw</code> , файл не выбран
<b>Входные данные</b>	Текст виджета <code>file_entry=path</code> , заглушка на функцию <code>askopenfilename</code> модуля <code>fd</code> , возвращающая пустой путь
<b>Ожидаемый результат</b>	Текст виджета <code>file_entry</code> не изменился

Таблица 25: Тест № Б-D11

<b>№ теста</b>	Б-C1.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>generate_session_key(size)</code> модуля <code>crypto</code> , нужный размер сессионного ключа
<b>Входные данные</b>	<code>size=16</code>
<b>Ожидаемый результат</b>	Массив байт размером 16

Таблица 26: Тест № Б-C1.1

<b>№ теста</b>	Б-C1.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>generate_session_key(size)</code> модуля <code>crypto</code> , два ключа различаются
<b>Входные данные</b>	<code>size=16</code>
<b>Ожидаемый результат</b>	Два полученных массива байт различаются

Таблица 27: Тест № Б-C1.2

<b>№ теста</b>	Б-C2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>encrypt_file(session_key, in_path, out_path)</code> модуля <code>crypto</code> , содержимое файла изменяется
<b>Входные данные</b>	<code>session_key=generate_session_key()</code> , <code>in_path="input.txt"</code> , <code>out_path="output.txt"</code> , <code>output</code> файл не существует, <code>input</code> файл содержит фразу "Secret message"
<b>Ожидаемый результат</b>	<code>output</code> файл существует, его содержимое отличается от "Secret message"

Таблица 28: Тест № Б-C2

<b>№ теста</b>	Б-С3.1
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции <code>decrypt_file(session_key, in_path, out_path)</code> модуля <code>crypto</code> , неправильный сессионный ключ
<b>Входные данные</b>	<code>session_key=generate_session_key()</code> , <code>in_path="input.txt"</code> , <code>out_path="output.txt"</code> , <code>output</code> файл не существует, <code>input</code> файл содержит зашифрованное методом <code>encrypt_file()</code> сообщение
<b>Ожидаемый результат</b>	<code>output</code> файл существует, его содержимое отличается от исходного сообщения и является неразборчивым

Таблица 29: Тест № Б-С3.1

<b>№ теста</b>	Б-С3.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>decrypt_file(session_key, in_path, out_path)</code> модуля <code>crypto</code> , правильный сессионный ключ
<b>Входные данные</b>	<code>session_key=ключу</code> , используемому в <code>encrypt_file()</code> , <code>in_path="input.txt"</code> , <code>out_path="output.txt"</code> , <code>output</code> файл не существует, <code>input</code> файл содержит зашифрованное методом <code>encrypt_file()</code> сообщение
<b>Ожидаемый результат</b>	<code>output</code> файл существует, его содержимое совпадает с исходным сообщением

Таблица 30: Тест № Б-С3.2

<b>№ теста</b>	Б-С4
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>sign_file(private_key, in_path, out_path)</code> модуля <code>crypto</code>
<b>Входные данные</b>	<code>private_key</code> любой приватный ключ, <code>in_path="input.txt"</code> , <code>out_path="output.txt"</code> , <code>output</code> файл не существует, <code>input</code> файл имеет любое содержимое
<b>Ожидаемый результат</b>	<code>output</code> файл существует, его содержимое совпадает с исходным с дополнительной подписью

Таблица 31: Тест № Б-С4

<b>№ теста</b>	Б-С5.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>verify_sign_and_decrypt(public_key, private_key, file_path, signature_path)</code> модуля <code>crypto</code> , подпись верна
<b>Входные данные</b>	<code>public_key</code> - пара приватного ключа, используемого для подписи файла, <code>private_key</code> пара публичного ключа, используемого для шифрования подписи, <code>file_path="input.txt"</code> , <code>signature_path="sign.txt"</code> , содержимое файла является частью файла с подписью, за исключением подписи
<b>Ожидаемый результат</b>	True

Таблица 32: Тест № Б-С5.1

<b>№ теста</b>	Б-С5.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции <code>verify_sign_and_decrypt(public_key, private_key, file_path, signature_path)</code> модуля <code>crypto</code> , подпись ложна
<b>Входные данные</b>	<code>public_key</code> - не пара приватного ключа, используемого для подписи файла, <code>private_key</code> пара публичного ключа, используемого для шифрования подписи, <code>file_path="input.txt"</code> , <code>signature_path="sign.txt"</code> , содержимое файла является частью файла с подписью, за исключением подписи
<b>Ожидаемый результат</b>	False

Таблица 33: Тест № Б-С5.2

<b>№ теста</b>	Б-С6.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>verify_sign(public_key, file_path, signature_path)</code> модуля <code>crypto</code> , подпись верна
<b>Входные данные</b>	<code>public_key</code> - пара приватного ключа, используемого для подписи файла, <code>file_path="input.txt"</code> , <code>signature_path="sign.txt"</code> , содержимое файла является частью файла с подписью, за исключением подписи
<b>Ожидаемый результат</b>	True

Таблица 34: Тест № Б-С6.1

<b>№ теста</b>	Б-С6.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции <code>verify_sign(public_key, file_path, signature_path)</code> модуля <code>crypto</code> , подпись ложна
<b>Входные данные</b>	<code>public_key</code> - пара приватного ключа, не используемого для подписи файла, <code>file_path="input.txt"</code> , <code>signature_path="sign.txt"</code> , содержимое файла является частью файла с подписью, за исключением подписи
<b>Ожидаемый результат</b>	False

Таблица 35: Тест № Б-С6.2

<b>№ теста</b>	Б-R1.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>save_private_key(keys, secret_code, private_key_path)</code> модуля <code>rsa</code> , правильные ключи
<b>Входные данные</b>	Правильные ключи, файл по пути <code>private_key_path</code> не существует
<b>Ожидаемый результат</b>	Файл по пути <code>private_key_path</code> существует

Таблица 36: Тест № Б-R1.1

<b>№ теста</b>	Б-R1.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции <code>save_private_key(keys, secret_code, private_key_path)</code> модуля <code>rsa</code> , неправильные ключи
<b>Входные данные</b>	Неправильные ключи
<b>Ожидаемый результат</b>	Ошибка <code>ValueError</code>

Таблица 37: Тест № Б-R1.2

<b>№ теста</b>	Б-R2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>save_public_key(keys, secret_code, public_key_path)</code> модуля <code>rsa</code>
<b>Входные данные</b>	Файл по пути <code>public_key_path</code> не существует
<b>Ожидаемый результат</b>	Файл по пути <code>public_key_path</code> существует

Таблица 38: Тест № Б-R2

<b>№ теста</b>	Б-R3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>generate_keys(secret_code, private_key_path, public_key_path)</code> модуля <code>rsa</code>
<b>Входные данные</b>	Файлы по путям <code>private_key_path</code> и <code>public_key_path</code> не существуют
<b>Ожидаемый результат</b>	<code>True</code> , Файлы по путям <code>private_key_path</code> и <code>public_key_path</code> существуют

Таблица 39: Тест № Б-R3

<b>№ теста</b>	Б-R4.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>check_secret_code(secret_code, private_key_path)</code> модуля <code>rsa</code> , код подходит к ключу
<b>Входные данные</b>	<code>secret_code</code> является кодом ключа, файл по пути <code>private_key_path</code> содержит зашифрованный приватный ключ
<b>Ожидаемый результат</b>	<code>True</code>

Таблица 40: Тест № Б-R4.1

<b>№ теста</b>	Б-R4.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции <code>check_secret_code(secret_code, private_key_path)</code> модуля <code>rsa</code> , код не подходит к ключу
<b>Входные данные</b>	<code>secret_code</code> не является кодом ключа, файл по пути <code>private_key_path</code> содержит зашифрованный приватный ключ
<b>Ожидаемый результат</b>	<code>False</code>

Таблица 41: Тест № Б-R4.2



<b>№ теста</b>	Б-R5.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_public_key(public_key_path)</code> модуля <code>rsa</code> , файл содержит ключ
<b>Входные данные</b>	Файл по пути <code>public_key_path</code> содержит публичный ключ
<b>Ожидаемый результат</b>	Возвращается публичный ключ

Таблица 42: Тест № Б-R5.1

<b>№ теста</b>	Б-R5.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции <code>get_public_key(public_key_path)</code> модуля <code>rsa</code> , файл не содержит ключ
<b>Входные данные</b>	Файл по пути <code>public_key_path</code> не содержит публичный ключ
<b>Ожидаемый результат</b>	Выбрасывается ошибка <code>ValueError</code>

Таблица 43: Тест № Б-R5.2

<b>№ теста</b>	Б-R6.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_private_key(secret_code, private_key_path)</code> модуля <code>rsa</code> , правильный код
<b>Входные данные</b>	<code>secret_code</code> подходит к ключу, файл по пути <code>private_key_path</code> содержит приватный ключ
<b>Ожидаемый результат</b>	Возвращается приватный ключ

Таблица 44: Тест № Б-R6.1

<b>№ теста</b>	Б-R6.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции <code>get_private_key(secret_code, private_key_path)</code> модуля <code>rsa</code> , неправильный код
<b>Входные данные</b>	<code>secret_code</code> не подходит к ключу, файл по пути <code>private_key_path</code> содержит приватный ключ
<b>Ожидаемый результат</b>	Выбрасывается ошибка <code>ValueError</code>

Таблица 45: Тест № Б-R6.2

<b>№ теста</b>	Б-R6.3
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции <code>get_private_key(secret_code, private_key_path)</code> модуля <code>rsa</code> , файл не содержит ключ
<b>Входные данные</b>	Файл по пути <code>private_key_path</code> не содержит ключ
<b>Ожидаемый результат</b>	Выбрасывается ошибка <code>ValueError</code>

Таблица 46: Тест № Б-R6.3

<b>№ теста</b>	Б-R7
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_public_key_pair(public_key)</code> модуля <code>rsa</code>
<b>Входные данные</b>	<code>public_key</code> публичный ключ RSA
<b>Ожидаемый результат</b>	<code>public_key.e</code> , <code>public_key.n</code>

Таблица 47: Тест № Б-R7

<b>№ теста</b>	Б-R8
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_private_key_pair(private_key)</code> модуля <code>rsa</code>
<b>Входные данные</b>	<code>private_key</code> приватный ключ RSA
<b>Ожидаемый результат</b>	<code>private_key.d</code> , <code>private_key.n</code>

Таблица 48: Тест № Б-R8

<b>№ теста</b>	Б-R9
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>encrypt(messages, public_key, out_path)</code> модуля <code>rsa</code>
<b>Входные данные</b>	<code>public_key</code> публичный ключ RSA, <code>messages</code> ="Message", файл по пути <code>out_path</code> не существует
<b>Ожидаемый результат</b>	Файл по пути <code>out_path</code> существует, его содержимое не равно <code>messages</code> и неразборчиво

Таблица 49: Тест № Б-R9

<b>№ теста</b>	Б-R10
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>decrypt(private_key, in_path, mode)</code> модуля <code>rsa</code>
<b>Входные данные</b>	<code>private_key</code> приватный ключ RSA, <code>messages</code> ="Message", файл по пути <code>in_path</code> зашифрован, <code>mode</code> ="str"
<b>Ожидаемый результат</b>	Осмысленное расшифрованное сообщение

Таблица 50: Тест № Б-R10

<b>№ теста</b>	Б-L1.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_signature_path(path, from_name)</code> модуля <code>logic</code> , путь к файлу содержит <code>decrypted</code>
<b>Входные данные</b>	<code>path</code> = <code>decrypted_sign.txt</code> , <code>from_name</code> = <code>name</code>
<b>Ожидаемый результат</b>	"signatures/name/sign.txt"

Таблица 51: Тест № Б-L1.1

<b>№ теста</b>	Б-L1.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_signature_path(path, from_name)</code> модуля <code>logic</code> , путь к файлу не содержит <code>decrypted</code>
<b>Входные данные</b>	<code>path=sign.txt, from_name=name</code>
<b>Ожидаемый результат</b>	“ <code>signatures/name_sign.txt</code> “

Таблица 52: Тест № Б-L1.2

<b>№ теста</b>	Б-L2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_encrypted_file_path(common_path)</code> модуля <code>logic</code>
<b>Входные данные</b>	<code>common_path=file.txt</code>
<b>Ожидаемый результат</b>	“ <code>files/encrypted_file.txt</code> “

Таблица 53: Тест № Б-L2

<b>№ теста</b>	Б-L3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_decrypted_file_path(encrypted_path)</code> модуля <code>logic</code>
<b>Входные данные</b>	<code>encrypted_path=encrypted_file.txt</code>
<b>Ожидаемый результат</b>	“ <code>files/decrypted_file.txt</code> “

Таблица 54: Тест № Б-L3

<b>№ теста</b>	Б-L4.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_session_key_path(from_name, to_name, key_name)</code> модуля <code>logic</code> , зашифрованный ключ
<b>Входные данные</b>	<code>from_name=name1, to_name=name2, key_name=encrypted_key</code>
<b>Ожидаемый результат</b>	“ <code>keys/session_keys/name2_to_name1_encrypted_key.txt</code> “

Таблица 55: Тест № Б-L4.1

<b>№ теста</b>	Б-L4.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_session_key_path(from_name, to_name, key_name)</code> модуля <code>logic</code> , простой ключ
<b>Входные данные</b>	<code>from_name=name1, to_name=name2, key_name=key</code>
<b>Ожидаемый результат</b>	“ <code>keys/session_keys/name1_to_name2_key.txt</code> “

Таблица 56: Тест № Б-L4.2

<b>№ теста</b>	Б-L5
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_private_key_path(name)</code> модуля <code>logic</code>
<b>Входные данные</b>	<code>name=name1</code>
<b>Ожидаемый результат</b>	<code>"keys/private_keys/name1.txt"</code>

Таблица 57: Тест № Б-L5

<b>№ теста</b>	Б-L6
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>get_public_key_path(name)</code> модуля <code>logic</code>
<b>Входные данные</b>	<code>name=name1</code>
<b>Ожидаемый результат</b>	<code>"keys/public_keys/name1.txt"</code>

Таблица 58: Тест № Б-L6

<b>№ теста</b>	Б-L7
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>delete_session_keys(from_name, to_name, key_name)</code> модуля <code>logic</code>
<b>Входные данные</b>	<code>from_name=name1, to_name=name2, key_name=key</code> , существуют файлы сессионных ключей сторон
<b>Ожидаемый результат</b>	Файлы сессионных ключей сторон не существуют

Таблица 59: Тест № Б-L7

<b>№ теста</b>	Б-L8
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>replace_object_data</code> модуля <code>logic(object, data)</code> модуля <code>logic</code>
<b>Входные данные</b>	<code>object=tkinter.Text</code> с текстом= <code>Text</code> , <code>data=New text</code>
<b>Ожидаемый результат</b>	Текст виджета изменился на <code>New text</code>

Таблица 60: Тест № Б-L8

<b>№ теста</b>	Б-L9
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>change_color(object, color, mode)</code> модуля <code>logic</code>
<b>Входные данные</b>	<code>object=tkinter.Entry, color=black, mode=bg</code>
<b>Ожидаемый результат</b>	Значение параметра <code>bg</code> виджета <code>object</code> стал равен <code>black</code>

Таблица 61: Тест № Б-L9

<b>№ теста</b>	Б-L10
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции delete_files(dir_path, part) модуля logic
<b>Входные данные</b>	dir_path=dir/, part=file_part, существует 2 файла в каталоге dir_path с именами first_file_part.txt и file_part_second.txt
<b>Ожидаемый результат</b>	Эти 2 файла не существуют

Таблица 62: Тест № Б-L10

<b>№ теста</b>	Б-L11.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции load_name_box(box, values, name) модуля logic, нет файлов
<b>Входные данные</b>	box=tkinter.Combobox, values=[name1, name2], name=from, файлов с именем пользователя не существует
<b>Ожидаемый результат</b>	Массив values и текст box пустые

Таблица 63: Тест № Б-L11.1

<b>№ теста</b>	Б-L11.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции load_name_box(box, values, name) модуля logic, файлы существуют
<b>Входные данные</b>	box=tkinter.Combobox, values=[name3, name4], name=to, существует 2 файла пользователей с именами name1.txt и name2.txt
<b>Ожидаемый результат</b>	Массив values=[name1, name2] и текст box=name1

Таблица 64: Тест № Б-L11.2

<b>№ теста</b>	Б-L12.1
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка функции load_keys_box(box, values, from_name, to_name) модуля logic, не выбраны стороны
<b>Входные данные</b>	box=tkinter.Combobox, values=[], from_name=from, to_name=""
<b>Ожидаемый результат</b>	Массив values=[] и текст box не изменился

Таблица 65: Тест № Б-L12.1

<b>№ теста</b>	Б-L12.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции load_keys_box(box, values, from_name, to_name) модуля logic, стороны выбраны
<b>Входные данные</b>	box=tkinter.Combobox, values=[name3, name4], from_name=from, to_name=to, существует 2 файла ключей сторон с именами key1.txt и key2.txt
<b>Ожидаемый результат</b>	Массив values=[key1, key2] и текст box=key1

Таблица 66: Тест № Б-L12.2

<b>№ теста</b>	Б-L13.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции delete_from_combobox(box, values, value) модуля logic, значение не было выбрано
<b>Входные данные</b>	box=tkinter.Combobox, values=[name1, name2], выбрано name1, value=name2
<b>Ожидаемый результат</b>	Массив values=[name1] и текст box=name1

Таблица 67: Тест № Б-L13.1

<b>№ теста</b>	Б-L13.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции delete_from_combobox(box, values, value) модуля logic, значение было выбрано, остались другие значения
<b>Входные данные</b>	box=tkinter.Combobox, values=[name1, name2], выбрано name1, value=name1
<b>Ожидаемый результат</b>	Массив values=[name2] и текст box=name2

Таблица 68: Тест № Б-L13.2

<b>№ теста</b>	Б-L13.3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции delete_from_combobox(box, values, value) модуля logic, значение было выбрано, других значений нет
<b>Входные данные</b>	box=tkinter.Combobox, values=[name1], выбрано name1, value=name1
<b>Ожидаемый результат</b>	Массив values=[] и текст box пустой

Таблица 69: Тест № Б-L13.3

<b>№ теста</b>	Б-L14
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>check_and_create_dirs()</code> модуля <code>logic</code>
<b>Входные данные</b>	Каталогов с именами <code>[keys/, keys/private_keys/, keys/public_keys/, keys/session_keys/, files/, signatures/]</code> не существует
<b>Ожидаемый результат</b>	Каталоги из списка существуют

Таблица 70: Тест № Б-L14

### 3.2 Интеграционное тестирование

<b>№ теста</b>	И-DL1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>update_state()</code> модуля <code>draw</code> с вызовом функции <code>load_keys_box()</code> модуля <code>logic</code> для заполнения списка сессионных ключей
<b>Входные данные</b>	<code>keys_box_values=[]</code> , <code>from_box_value=name1</code> , <code>to_box_value=name2</code> , существует 3 файла с сессионными ключами <code>main1</code> , <code>main2</code> и <code>main3</code>
<b>Ожидаемый результат</b>	Виджет <code>keys_box</code> содержит массив <code>keys_box_values=[main1, main2, main3]</code>

Таблица 71: Тест № И-DL1

<b>№ теста</b>	И-DL2.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>delete_name_button_clicked()</code> модуля <code>draw</code> с вызовом функции <code>delete_files()</code> модуля <code>logic</code> для удаления файлов
<b>Входные данные</b>	<code>from_box_value=name1</code> , существуют файлы, связанные с именем пользователя
<b>Ожидаемый результат</b>	Файлы, связанные с именем пользователя не существуют

Таблица 72: Тест № И-DL2.1

<b>№ теста</b>	И-DL2.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>delete_name_button_clicked()</code> модуля <code>draw</code> с вызовом функции <code>delete_from_combobox(box, values, name)</code> модуля <code>logic</code> для удаления элементов списка виджетов
<b>Входные данные</b>	<code>from_box_value=name2</code> , <code>from_box_values=to_box_values=[name2, name3]</code>
<b>Ожидаемый результат</b>	<code>from_box_values=to_box_values=[name1, name3]</code>

Таблица 73: Тест № И-DL2.2

<b>№ теста</b>	И-DL3.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции delete_key_button_clicked() модуля draw с вызовом функции delete_session_keys() модуля logic для удаления файлов сессионных ключей
<b>Входные данные</b>	from_box_value=name1, to_box_value=name2, keys_box_value=main1, существуют файлы сессионных ключей сторон для 2 ключей: main1 и main2
<b>Ожидаемый результат</b>	Существуют файлы сессионных ключей сторон только для 1 ключа - main2

Таблица 74: Тест № И-DL3.1

<b>№ теста</b>	И-DL3.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции delete_key_button_clicked() модуля draw с вызовом функции delete_from_combobox() модуля logic для удаления элементов списка виджетов
<b>Входные данные</b>	keys_box_value=main1, keys_box_values=[main1, encrypted_main1, main2, main3]
<b>Ожидаемый результат</b>	keys_box_values=[main2, main3]

Таблица 75: Тест № И-DL3.2

<b>№ теста</b>	И-DL4.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции add_file_button_click() модуля draw с вызовом функции change_color() модуля logic для изменения цвета виджета
<b>Входные данные</b>	Параметр readonlybackground виджета file_entry равен red
<b>Ожидаемый результат</b>	Параметр readonlybackground виджета file_entry равен gray95

Таблица 76: Тест № И-DL4.1

<b>№ теста</b>	И-DL4.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции add_file_button_click() модуля draw с вызовом функции replace_object_data() модуля logic для изменения текста виджетов
<b>Входные данные</b>	Текст виджетов file_entry и file_text пустой, заглушка на функцию askopenfilename модуля fd, возвращающая path="input.txt", файл по этому пути существует и имеет текст File text
<b>Ожидаемый результат</b>	Текст виджета file_entry равен input.txt, а виджета file_text равен File text

Таблица 77: Тест № И-DL4.2



<b>№ теста</b>	И-DL5
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции encrypt_file_button_clicked() модуля draw с вызовом функции get_encrypted_file_path() модуля logic для получения пути к зашифрованному файлу
<b>Входные данные</b>	Текст виджета file_entry равен file.txt, пустая заглушка на функцию read_session_key() модуля logic, заглушка на функцию encrypt_file() модуля crypto, создающая файл по пути encrypted_path, файл files/encrypted_file.txt не существует
<b>Ожидаемый результат</b>	Файл files/encrypted_file.txt существует

Таблица 78: Тест № И-DL5

<b>№ теста</b>	И-DL6
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции decrypt_file_button_clicked() модуля draw с вызовом функции get_decrypted_file_path() модуля logic для получения пути к расшифрованному файлу
<b>Входные данные</b>	Текст виджета file_entry равен encrypted_file.txt, пустая заглушка на функцию read_session_key() модуля logic, заглушка на функцию decrypt_file() модуля crypto, создающая файл по пути decrypted_path, файл files/decrypted_file.txt не существует
<b>Ожидаемый результат</b>	Файл files/decrypted_file.txt существует

Таблица 79: Тест № И-DL6

<b>№ теста</b>	И-DL7
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции sign_file_button_clicked() модуля draw с вызовом функции get_private_key_path() модуля logic для получения пути к приватному ключу
<b>Входные данные</b>	Текст виджета file_entry не пустой, from_box_value=name1, заглушка на функцию get_private_key() модуля rsa, создающая файл по пути private_key_path, файл keys/private_keys/name1.txt не существует
<b>Ожидаемый результат</b>	Файл keys/private_keys/name1.txt существует

Таблица 80: Тест № И-DL7

<b>№ теста</b>	И-DL8.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>verify_file_button_clicked()</code> модуля <code>draw</code> с вызовом функции <code>get_public_key_path()</code> модуля <code>logic</code> для получения пути к публичному ключу
<b>Входные данные</b>	Текст виджета <code>file_entry</code> не пустой, <code>to_box_value=name1</code> , заглушка на функцию <code>get_public_key()</code> модуля <code>rsa</code> , создающая файл по пути <code>public_key_path</code> , файл <code>keys/public_keys/name1.txt</code> не существует
<b>Ожидаемый результат</b>	Файл <code>keys/public_keys/name1.txt</code> существует

Таблица 81: Тест № И-DL8.1

<b>№ теста</b>	И-DL8.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>verify_file_button_clicked()</code> модуля <code>draw</code> с вызовом функции <code>get_signature_path()</code> модуля <code>logic</code> для получения пути к подписи
<b>Входные данные</b>	Текст виджета <code>file_entry</code> равен <code>file.txt</code> , <code>to_box_value=name1</code> , пустые заглушки на функции <code>get_public_key()</code> модуля <code>rsa</code> и <code>get_public_key_path()</code> модуля <code>logic</code> , заглушка на функцию <code>verify_sign()</code> модуля <code>crypto</code> , создающая файл по пути <code>2 + signature_path</code> , файл <code>2signatures/name1_file.txt</code> не существует
<b>Ожидаемый результат</b>	Файл <code>2signatures/name1_file.txt</code> существует

Таблица 82: Тест № И-DL8.2

<b>№ теста</b>	И-DC1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>generate_session_key()</code> модуля <code>draw</code> с вызовом функции <code>generate_session_key()</code> модуля <code>crypto</code> для генерации сессионного ключа
<b>Входные данные</b>	Заглушка на функцию <code>save_session_key()</code> модуля <code>logic</code> , сохраняющая <code>session_key</code> в файл <code>output.txt</code> , файл <code>output.txt</code> не существует
<b>Ожидаемый результат</b>	Файл <code>output.txt</code> существует и содержит набор из 16 байт

Таблица 83: Тест № И-DC1

<b>№ теста</b>	И-DC2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции encrypt_file_button_clicked() модуля draw с вызовом функции encrypt_file() модуля crypto для шифрования файла
<b>Входные данные</b>	file_entry_value=file.txt, заглушка на функцию get_encrypted_file_path() модуля logic, возвращающая encrypted_file.txt, заглушка на функцию read_session_key() модуля logic, возвращающая сессионный ключ, файл по пути encrypted_file.txt не существует
<b>Ожидаемый результат</b>	Файл encrypted_file.txt существует и содержит неразборчивый текст, отличный от file.txt

Таблица 84: Тест № И-DC2

<b>№ теста</b>	И-DC3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции decrypt_file_button_clicked() модуля draw с вызовом функции decrypt_file() модуля crypto для расшифрования файла
<b>Входные данные</b>	file_entry_value=encrypted_file.txt, заглушка на функцию get_decrypted_file_path() модуля logic, возвращающая decrypted_file.txt, заглушка на функцию read_session_key() модуля logic, возвращающая сессионный ключ, использующийся для шифрования файла encrypted_file.txt, файл по пути decrypted_file.txt не существует
<b>Ожидаемый результат</b>	Файл decrypted_file.txt существует и содержит исходный осмысленный текст зашифрованного файла

Таблица 85: Тест № И-DC3

<b>№ теста</b>	И-DC4
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции sign_file_button_clicked() модуля draw с вызовом функции sign_file() модуля crypto для подписи файла
<b>Входные данные</b>	file_entry_value=file.txt, заглушка на функцию get_private_key() модуля rsa, возвращающая приватный ключ, заглушка на функцию get_signature_path() модуля logic, возвращающая signature.txt, файл по пути signature.txt не существует
<b>Ожидаемый результат</b>	Файл signature.txt существует и содержит текст файла file.txt с подписью

Таблица 86: Тест № И-DC4

<b>№ теста</b>	И-DC5
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>verify_file_button_clicked()</code> модуля <code>draw</code> с вызовом функции <code>verify_sign()</code> модуля <code>crypto</code> для проверки подписи
<b>Входные данные</b>	<code>file_entry_value=decrypted_file.txt</code> , заглушка на функцию <code>get_public_key()</code> модуля <code>rsa</code> , возвращающая публичный ключ, заглушка на функцию <code>get_signature_path()</code> модуля <code>logic</code> , возвращающая <code>signature.txt</code> , файл по пути <code>signature.txt</code> подписан
<b>Ожидаемый результат</b>	Текст виджета <code>signature_label</code> равен “Подпись верна“

Таблица 87: Тест № И-DC5

<b>№ теста</b>	И-DR1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>generate_new_keys(name, code)</code> модуля <code>draw</code> с вызовом функции <code>generate_keys()</code> модуля <code>rsa</code> для генерации пары ключей RSA
<b>Входные данные</b>	<code>name=name1</code> , <code>code=code1</code> , файлы <code>keys/_private_keys/name1.txt</code> и <code>keys/_public_keys/name1.txt</code> не существуют
<b>Ожидаемый результат</b>	Файлы существуют

Таблица 88: Тест № И-DR1

<b>№ теста</b>	И-DR2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>sign_file_button_clicked()</code> модуля <code>draw</code> с вызовом функции <code>get_private_key()</code> модуля <code>rsa</code> для получения приватного ключа
<b>Входные данные</b>	Текст виджета <code>code_entry</code> равен <code>code1</code> , заглушка на функцию <code>get_private_key_path()</code> модуля <code>logic</code> , возвращающая <code>private.txt</code> , заглушка на функцию <code>sign_file()</code> модуля <code>crypto</code> , сохраняющая <code>private_key</code> в файл <code>output.txt</code> , файл <code>output.txt</code> не существует, файл <code>private.txt</code> содержит приватный ключ с кодом <code>code1</code>
<b>Ожидаемый результат</b>	Файл <code>output.txt</code> существует и его содержимое совпадает с файлом <code>private.txt</code>

Таблица 89: Тест № И-DR2

<b>№ теста</b>	И-DR3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>verify_file_button_clicked()</code> модуля <code>draw</code> с вызовом функции <code>get_public_key()</code> модуля <code>rsa</code> для получения публичного ключа
<b>Входные данные</b>	Заглушка на функцию <code>get_public_key_path()</code> модуля <code>logic</code> , возвращающая <code>public.txt</code> , заглушка на функцию <code>verify_sign()</code> модуля <code>crypto</code> , сохраняющая <code>public_key</code> в файл <code>output.txt</code> , файл <code>output.txt</code> не существует, файл <code>public.txt</code> содержит публичный ключ
<b>Ожидаемый результат</b>	Файл <code>output.txt</code> существует и его содержимое совпадает с файлом <code>public.txt</code>

Таблица 90: Тест № И-DR3

<b>№ теста</b>	И-CR1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>sign_file_and_encrypt(private_key, public_key, in_path, out_path)</code> модуля <code>crypto</code> с вызовом функции <code>encrypt()</code> модуля <code>rsa</code> для шифрования подписи
<b>Входные данные</b>	Ключи RSA, <code>in_path=input.txt</code> , <code>out_path=output.txt</code> , файл <code>output.txt</code> не существует
<b>Ожидаемый результат</b>	Файл <code>output.txt</code> существует и его содержимое отличается от <code>input.txt</code> и больше размером

Таблица 91: Тест № И-CR1

<b>№ теста</b>	И-CR2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>verify_sign_and_decrypt(public_key, private_key, file_path, signature_path)</code> модуля <code>crypto</code> с вызовом функции <code>decrypt()</code> модуля <code>rsa</code> для расшифрования подписи
<b>Входные данные</b>	Ключи RSA, <code>file_path=file.txt</code> , <code>signature_path=sign.txt</code> , файл <code>sign.txt</code> содержит подписанное и зашифрованное содержимое файла <code>file.txt</code>
<b>Ожидаемый результат</b>	True

Таблица 92: Тест № И-CR2

<b>№ теста</b>	И-LR1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>read_session_key(from_name, to_name, key_name, code)</code> модуля <code>logic</code> с вызовом функций <code>get_private_key()</code> и <code>decrypt()</code> модуля <code>rsa</code> для получения приватного ключа и расшифровки сессионного ключа
<b>Входные данные</b>	<code>from_name=name1, to_name=name2, key_name=key, code=code1</code> , в файле <code>keys/private_key/name1.txt</code> содержится приватный ключ, в файле <code>keys/session_keys/name1_to_name2_key.txt</code> сессионный ключ
<b>Ожидаемый результат</b>	Возвращается набор из 16 байт - исходный сессионный ключ

Таблица 93: Тест № И-LR1

<b>№ теста</b>	И-LR2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>save_session_key(from_name, to_name, key_name, key)</code> модуля <code>logic</code> с вызовом функций <code>get_public_key()</code> и <code>encrypt()</code> модуля <code>rsa</code> для получения публичного ключа и шифрования сессионного ключа
<b>Входные данные</b>	<code>from_name=name1, to_name=name2, key_name=key, code=code1</code> , в файле <code>keys/public_key/name1.txt</code> содержится приватный ключ, в файле <code>keys/session_keys/name1_to_name2_key.txt</code> сессионный ключ, файл <code>keys/session_keys/name1_to_name2_encrypted_key.txt</code> не существует
<b>Ожидаемый результат</b>	Файл <code>keys/session_keys/name1_to_name2_encrypted_key.txt</code> существует и его содержимое отличается от файла <code>keys/session_keys/name1_to_name2_key.txt</code>

Таблица 94: Тест № И-LR2

<b>№ теста</b>	И-A1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>generate_session_key(key_name)</code> модуля <code>draw</code> с вызовом функций <code>generate_session_key()</code> модуля <code>crypto</code> для генерации сессионного ключа, функции <code>save_session_key()</code> модуля <code>logic</code> для сохранения ключа и функций <code>get_public_key()</code> и <code>encrypt()</code> модуля <code>rsa</code> для шифрования ключа
<b>Входные данные</b>	<code>from_box_value=name1, to_box_value=name2, key_name=key</code> , файл <code>keys/public_keys/name2.txt</code> содержит публичный ключ, файл <code>keys/session_keys/name1_to_name2_encrypted_key.txt</code> не существует
<b>Ожидаемый результат</b>	Файл <code>keys/session_keys/name1_to_name2_encrypted_key.txt</code> существует и его размер 16 байт

Таблица 95: Тест № И-A1

<b>№ теста</b>	И-А2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции encrypt_file_button_clicked() модуля draw с вызовом функций get_encrypted_file_path(), read_session_key(), replace_object_data() модуля logic, функции encrypt_file() модуля crypto и функций get_private_key() и decrypt() модуля rsa
<b>Входные данные</b>	file_entry_value=file.txt, from_box_value=name1, to_box_value=name2, keys_box_value=key, code_entry_value=code1, существуют файлы публичных, приватных и сессионных ключей сторон, файл encrypted_file.txt не существует
<b>Ожидаемый результат</b>	Файл encrypted_file.txt существует и его содержимое отличается от file.txt

Таблица 96: Тест № И-А2

<b>№ теста</b>	И-А3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции decrypt_file_button_clicked() модуля draw с вызовом функций get_decrypted_file_path(), read_session_key(), replace_object_data() модуля logic, функции decrypt_file() модуля crypto и функций get_private_key() и decrypt() модуля rsa
<b>Входные данные</b>	file_entry_value=encrypted_file.txt, from_box_value=name1, to_box_value=name2, keys_box_value=key, code_entry_value=code1, существуют файлы публичных, приватных и сессионных ключей сторон, файл decrypted_file.txt не существует
<b>Ожидаемый результат</b>	Файл decrypted_file.txt существует и содержит исходное содержимое файла encrypted_file.txt до шифрования

Таблица 97: Тест № И-А3

<b>№ теста</b>	И-А4
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции sign_file_button_clicked() модуля draw с вызовом функций get_private_key_path(), get_signature_path(), change_color() модуля logic, функции sign_file() модуля crypto и функций get_private_key() модуля rsa
<b>Входные данные</b>	file_entry_value=file.txt, from_box_value=name1, to_box_value=name2, code_entry_value=code1, существуют файлы публичных и приватных ключей сторон, файл signature/name1_file.txt не существует
<b>Ожидаемый результат</b>	Файл signature/name1_file.txt и содержит текст из файла file.txt и подпись name1

Таблица 98: Тест № И-А4

<b>№ теста</b>	И-А5
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка функции <code>verify_file_button_clicked()</code> модуля <code>draw</code> с вызовом функций <code>get_public_key_path()</code> , <code>get_signature_path()</code> , <code>change_color()</code> модуля <code>logic</code> , функции <code>verify_file()</code> модуля <code>crypto</code> и функции <code>get_public_key()</code> модуля <code>rsa</code>
<b>Входные данные</b>	<code>file_entry_value=decrypted_file.txt</code> , <code>from_box_value=name1</code> , <code>to_box_value=name2</code> , <code>code_entry_value=code1</code> , существуют файлы публичных и частных ключей сторон и файл с подписью файла
<b>Ожидаемый результат</b>	Значение параметра <code>fg</code> виджета <code>signature_label</code> равно <code>lightgreen</code>

Таблица 99: Тест № И-А5

### 3.3 Аттестационное тестирование

<b>№ теста</b>	А-1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка правильности заполнения списка пользователей
<b>Входные данные</b>	В приложении есть или отсутствуют пользователи
<b>Ожидаемый результат</b>	В списках присутствуют все существующие пользователи

Таблица 100: Тест № А-1

<b>№ теста</b>	А-2.1
<b>Тип теста</b>	Позитивный
<b>Описание И</b>	Проверка добавления нового пользователя
<b>Входные данные</b>	Нажатие кнопки добавления пользователя, заполнение данных нового пользователя, нажатие кнопки создать
<b>Ожидаемый результат</b>	Новый пользователь появился в списках сторон

Таблица 101: Тест № А-2.1

<b>№ теста</b>	А-2.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка добавления существующего пользователя
<b>Входные данные</b>	Нажатие кнопки добавления пользователя, заполнение данных с именем существующего пользователя, нажатие кнопки создать
<b>Ожидаемый результат</b>	Поле имени пользователя подсветилось красным

Таблица 102: Тест № А-2.2



<b>№ теста</b>	А-2.3
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка добавления пользователя с пустым именем
<b>Входные данные</b>	Нажатие кнопки добавления пользователя, заполнение данных с пустым именем пользователя, нажатие кнопки создать
<b>Ожидаемый результат</b>	Поле имени пользователя подсветилось красным

Таблица 103: Тест № А-2.3

<b>№ теста</b>	А-2.4
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка добавления пользователя с пустым секретным кодом
<b>Входные данные</b>	Нажатие кнопки добавления пользователя, заполнение данных с пустым секретным кодом, нажатие кнопки создать
<b>Ожидаемый результат</b>	Поле секретного кода подсветилось красным

Таблица 104: Тест № А-2.4

<b>№ теста</b>	А-2.5
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка добавления пользователя с неправильным повтором секретного кода
<b>Входные данные</b>	Нажатие кнопки добавления пользователя, заполнение данных с неправильным повтором секретного кода, нажатие кнопки создать
<b>Ожидаемый результат</b>	Поле повтора секретного кода подсветилось красным

Таблица 105: Тест № А-2.5

<b>№ теста</b>	А-2.6
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка добавления пользователя с отменой добавления
<b>Входные данные</b>	Нажатие кнопки добавления пользователя, заполнение данных пользователя, нажатие кнопки отмена
<b>Ожидаемый результат</b>	В списке сторон не появился новый пользователь

Таблица 106: Тест № А-2.6

<b>№ теста</b>	А-2.7
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка добавления пользователя с закрытием диалогового окна
<b>Входные данные</b>	Нажатие кнопки добавления пользователя, заполнение данных пользователя, закрытие диалогового окна
<b>Ожидаемый результат</b>	В списке сторон не появился новый пользователь

Таблица 107: Тест № А-2.7

<b>№ теста</b>	А-3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка удаления пользователя
<b>Входные данные</b>	Выбор пользователя в списке, нажатие кнопки удаления
<b>Ожидаемый результат</b>	Пользователь пропал из списков сторон, активным стал первый пользователь в списке

Таблица 108: Тест № А-3

<b>№ теста</b>	А-4
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка правильности заполнения списка сессионных ключей
<b>Входные данные</b>	В приложении есть или отсутствуют сессионные ключи двух сторон
<b>Ожидаемый результат</b>	В списке сессионных ключей присутствуют только все существующие ключи сторон

Таблица 109: Тест № А-4

<b>№ теста</b>	А-5.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка добавления нового сессионного ключа сторон
<b>Входные данные</b>	Нажатие кнопки добавления сессионного ключа, ввод названия нового ключа, нажатие кнопки сгенерировать
<b>Ожидаемый результат</b>	В списке сессионных ключей появился новый ключ с введенным названием

Таблица 110: Тест № А-5.1

<b>№ теста</b>	А-5.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка добавления существующего сессионного ключа сторон
<b>Входные данные</b>	Нажатие кнопки добавления сессионного ключа, ввод названия существующего ключа, нажатие кнопки сгенерировать
<b>Ожидаемый результат</b>	Поле названия ключа подсветилось красным

Таблица 111: Тест № А-5.2

<b>№ теста</b>	А-5.3
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка добавления сессионного ключа сторон с пустым именем
<b>Входные данные</b>	Нажатие кнопки добавления сессионного ключа, нажатие кнопки сгенерировать
<b>Ожидаемый результат</b>	Поле названия ключа подсветилось красным

Таблица 112: Тест № А-5.3

<b>№ теста</b>	А-5.4
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка добавления сессионного ключа сторон с отменой добавления
<b>Входные данные</b>	Нажатие кнопки добавления сессионного ключа, ввод названия ключа, нажатие кнопки отмены
<b>Ожидаемый результат</b>	Новый ключ не появился в списке ключей

Таблица 113: Тест № А-5.4

<b>№ теста</b>	А-5.5
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка добавления сессионного ключа сторон с закрытием диалогового окна
<b>Входные данные</b>	Нажатие кнопки добавления сессионного ключа, ввод названия ключа, закрытие диалогового окна
<b>Ожидаемый результат</b>	Новый ключ не появился в списке ключей

Таблица 114: Тест № А-5.5

<b>№ теста</b>	А-6
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка возможности выбора любого файла в окне выбора файла
<b>Входные данные</b>	Нажатие кнопки выбора файла
<b>Ожидаемый результат</b>	Есть возможность выбрать файл любого расширения

Таблица 115: Тест № А-6

<b>№ теста</b>	А-7.1
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка правильного отображения содержимого пустого файла
<b>Входные данные</b>	Нажатие кнопки выбора файла, выбор пустого файла
<b>Ожидаемый результат</b>	Поле содержимого файла пустое

Таблица 116: Тест № А-7.1

<b>№ теста</b>	А-7.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка правильного отображения содержимого маленького файла
<b>Входные данные</b>	Нажатие кнопки выбора файла, выбор маленького файла
<b>Ожидаемый результат</b>	В поле содержимого файла находятся данные из файла

Таблица 117: Тест № А-7.2

<b>№ теста</b>	А-7.3
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка правильного отображения содержимого большого файла
<b>Входные данные</b>	Нажатие кнопки выбора файла, выбор большого файла
<b>Ожидаемый результат</b>	В поле содержимого файла находятся данные из файла, есть полоса прокрутки

Таблица 118: Тест № А-7.3

<b>№ теста</b>	А-8.1
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка кликабельности кнопок при выборе простого файла
<b>Входные данные</b>	Выбор сторон сессии и сессионного ключа, выбор файла, не содержащего в названии “encrypted” и “decrypted”
<b>Ожидаемый результат</b>	Кликабельны только кнопки “Зашифровать” и “Подписать”

Таблица 119: Тест № А-8.1

<b>№ теста</b>	А-8.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка кликабельности кнопок при выборе зашифрованного файла
<b>Входные данные</b>	Выбор сторон сессии и сессионного ключа, выбор файла, содержащего в названии “encrypted”
<b>Ожидаемый результат</b>	Кликабельна только кнопка “Расшифровать”

Таблица 120: Тест № А-8.2

<b>№ теста</b>	А-8.3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка кликабельности кнопок при выборе расшифрованного файла без подписи
<b>Входные данные</b>	Выбор сторон сессии и сессионного ключа, выбор файла, содержащего в названии “decrypted” и не имеющего файла подписи
<b>Ожидаемый результат</b>	Кликабельны только кнопки “Зашифровать” и “Подписать”

Таблица 121: Тест № А-8.3

<b>№ теста</b>	А-8.4
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка кликабельности кнопок при выборе расшифрованного файла с подписью
<b>Входные данные</b>	Выбор сторон сессии и сессионного ключа, выбор файла, содержащего в названии “decrypted” и имеющего файл подписи
<b>Ожидаемый результат</b>	Кликабельны только кнопки “Зашифровать”, “Подписать” и “Проверить”

Таблица 122: Тест № А-8.4

<b>№ теста</b>	А-9
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка шифрования файла
<b>Входные данные</b>	Выбор сторон сессии и сессионного ключа, выбор файла, не содержащего в названии “encrypted“, нажатие кнопки “Зашифровать“
<b>Ожидаемый результат</b>	Путь к файлу в поле файла изменился на путь к зашифрованному файлу, содержимое файла приняло неразборчивый вид

Таблица 123: Тест № А-9

<b>№ теста</b>	А-10.1
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка расшифрования файла с неправильным секретным кодом
<b>Входные данные</b>	Выбор сторон сессии и сессионного ключа, ввод неправильного секретного кода, выбор зашифрованного файла, нажатие кнопки “Расшифровать“
<b>Ожидаемый результат</b>	Поле секретного кода подсветилось красным

Таблица 124: Тест № А-10.1

<b>№ теста</b>	А-10.2
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка расшифрования файла с неправильным сессионным ключом
<b>Входные данные</b>	Выбор сторон сессии и неправильного сессионного ключа, ввод секретного кода, выбор зашифрованного файла, нажатие кнопки “Расшифровать“
<b>Ожидаемый результат</b>	Путь к файлу в поле файла изменился на путь к расшифрованному файлу, содержимое файла изменилось но осталось в неразборчивом виде

Таблица 125: Тест № А-10.2

<b>№ теста</b>	А-10.3
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка расшифрования файла с правильными ключом и кодом
<b>Входные данные</b>	Выбор сторон сессии и сессионного ключа, ввод секретного кода, выбор зашифрованного файла, нажатие кнопки “Расшифровать“
<b>Ожидаемый результат</b>	Путь к файлу в поле файла изменился на путь к расшифрованному файлу, содержимое файла изменилось и приняло разборчивый исходный вид

Таблица 126: Тест № А-10.3

<b>№ теста</b>	A-11.1
<b>Тип теста</b>	Негативный
<b>Описание</b>	Проверка подписи файла с неправильным секретным кодом
<b>Входные данные</b>	Выбор сторон сессии и сессионного ключа, ввод неправильного секретного кода, выбор простого файла, нажатие кнопки “Подписать”
<b>Ожидаемый результат</b>	Поле секретного кода подсвечивается красным

Таблица 127: Тест № A-11.1

<b>№ теста</b>	A-11.2
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка подписи файла с правильным секретным кодом
<b>Входные данные</b>	Выбор сторон сессии и сессионного ключа, ввод секретного кода, выбор простого файла, нажатие кнопки “Подписать”
<b>Ожидаемый результат</b>	Появилось сообщение об успешной подписи файла

Таблица 128: Тест № A-11.2

<b>№ теста</b>	A-12
<b>Тип теста</b>	Позитивный
<b>Описание</b>	Проверка правильной проверки подписи
<b>Входные данные</b>	Выбор сторон сессии и сессионного ключа, выбор подписанного файла, нажатие кнопки “Проверить”
<b>Ожидаемый результат</b>	Появилось сообщение об успешной проверке подписи

Таблица 129: Тест № A-12

### 3.4 Специальное тестирование

<b>№ теста</b>	S-1
<b>Описание</b>	Проверка уникальности генерируемых сессионных ключей среди 5000 ключей
<b>Ожидаемый результат</b>	Все ключи являются уникальными

Таблица 130: Тест № S-1

<b>№ теста</b>	S-2
<b>Описание</b>	Проверка уникальности генерируемых пар ключей RSA среди 1000 пар
<b>Ожидаемый результат</b>	Все пары ключей являются уникальными

Таблица 131: Тест № S-2

<b>№ теста</b>	S-3
<b>Описание</b>	Проверка схожести файла и его зашифрованного варианта
<b>Ожидаемый результат</b>	У файлов различные количества согласных, гласных и цифр

Таблица 132: Тест № S-3

<b>№ теста</b>	S-4
<b>Описание</b>	Проверка наличия исходных слов в зашифрованном файле
<b>Ожидаемый результат</b>	Все слова исходного файла не встречаются в зашифрованном файле

Таблица 133: Тест № S-4

<b>№ теста</b>	S-5
<b>Описание</b>	Проверка времени шифрования большого файла размером 2 Гб
<b>Ожидаемый результат</b>	Время шифрования файла не превышает 5 секунд

Таблица 134: Тест № S-5

<b>№ теста</b>	S-6
<b>Описание</b>	Проверка времени шифрования большого файла размером 5 Гб
<b>Ожидаемый результат</b>	Время шифрования файла не превышает 10 секунд

Таблица 135: Тест № S-6

## 4 Покрытие кода тестами

Расчет тестового покрытия относительно исполняемого кода программного обеспечения проводится по формуле:

$$T_{cov} = \frac{L_{tc}}{L_{code}} * 100\%$$

где:

$T_{cov}$  – тестовое покрытие,

$L_{tc}$  – количество строк кода, покрытых тестами,

$L_{code}$  – общее количество строк кода.

Таким образом общее покрытие тестами равно:

$$T_{cov} = \frac{669}{836} * 100\% = 80\%$$

## 5 Пример реализации тестов

В качестве примера приведу реализацию блочных тестов B-D6.1-4 функции `validate_key_name(name)` модуля `draw`:

```

class DrawValidateKeyNameTestCase(unittest.TestCase):
    old_keys = None

    @classmethod
    def setUpClass(cls):
        cls.old_keys = draw.keys_box_values
        draw.keys_box_values = ["name1", "name3"]

    def test_empty_name(self):
        key_name = ""
        result = draw.validate_key_name(key_name)
        self.assertEqual(-1, result)

    def test_encrypted_name(self):
        key_name = "encrypted_name"
        result = draw.validate_key_name(key_name)
        self.assertEqual(-1, result)

    def test_exist_name(self):
        key_name = "name1"
        result = draw.validate_key_name(key_name)
        self.assertEqual(-1, result)

    def test_new_name(self):
        key_name = "name2"
        result = draw.validate_key_name(key_name)
        self.assertEqual(0, result)

    @classmethod
    def tearDownClass(cls):
        draw.keys_box_values = cls.old_keys

```

Рис. 6: Пример блочных тестов Б-D6.1-4



## 6 Журнал тестирования

### 6.1 Блочное тестирование

№ теста	Дата	Тестирующий	Попытка	Результат
Б-D1	12.12.22	Никаноров Р.П.	1	Пройден
Б-D2	12.12.22	Никаноров Р.П.	1	Пройден
Б-D3.1	12.12.22	Никаноров Р.П.	1	Пройден
Б-D3.2	12.12.22	Никаноров Р.П.	1	Пройден
Б-D3.3	12.12.22	Никаноров Р.П.	1	Пройден
Б-D4	12.12.22	Никаноров Р.П.	1	Пройден
Б-D5.1	12.12.22	Никаноров Р.П.	1	Пройден
Б-D5.2	12.12.22	Никаноров Р.П.	1	Пройден
Б-D6.1	12.12.22	Никаноров Р.П.	1	Пройден
Б-D6.2	12.12.22	Никаноров Р.П.	1	Пройден
Б-D6.3	12.12.22	Никаноров Р.П.	1	Пройден
Б-D6.4	12.12.22	Никаноров Р.П.	1	Пройден
Б-D7	12.12.22	Никаноров Р.П.	1	Пройден
Б-D8	13.12.22	Никаноров Р.П.	1	Пройден
Б-D9	13.12.22	Никаноров Р.П.	1	Пройден
Б-D10.1	13.12.22	Никаноров Р.П.	1	Пройден
Б-D10.2	13.12.22	Никаноров Р.П.	1	Пройден
Б-D10.3	13.12.22	Никаноров Р.П.	1	Пройден
Б-D10.4	13.12.22	Никаноров Р.П.	1	Пройден
Б-D10.5	13.12.22	Никаноров Р.П.	1	Пройден
Б-D10.6	13.12.22	Никаноров Р.П.	1	Пройден
Б-D10.7	13.12.22	Никаноров Р.П.	1	Пройден
Б-D10.8	13.12.22	Никаноров Р.П.	1	Пройден
Б-D10.9	13.12.22	Никаноров Р.П.	1	Пройден
Б-D11	13.12.22	Никаноров Р.П.	1	Пройден
Б-С1.1	12.12.22	Никаноров Р.П.	1	Пройден
Б-С1.2	12.12.22	Никаноров Р.П.	1	Пройден
Б-С2	12.12.22	Никаноров Р.П.	1	Пройден
Б-С3.1	12.12.22	Никаноров Р.П.	1	Пройден
Б-С3.2	12.12.22	Никаноров Р.П.	1	Пройден
Б-С4	13.12.22	Никаноров Р.П.	1	Пройден
Б-С5.1	13.12.22	Никаноров Р.П.	1	Пройден
Б-С5.2	13.12.22	Никаноров Р.П.	1	Пройден
Б-С6.1	13.12.22	Никаноров Р.П.	1	Пройден
Б-С6.2	13.12.22	Никаноров Р.П.	1	Пройден
Б-R1.1	13.12.22	Никаноров Р.П.	1	Пройден
Б-R1.2	13.12.22	Никаноров Р.П.	1	Пройден
Б-R2	13.12.22	Никаноров Р.П.	1	Пройден
Б-R3	13.12.22	Никаноров Р.П.	1	Пройден
Б-R4.1	13.12.22	Никаноров Р.П.	1	Пройден
Б-R4.2	13.12.22	Никаноров Р.П.	1	Пройден
Б-R5.1	13.12.22	Никаноров Р.П.	1	Пройден
Б-R5.2	13.12.22	Никаноров Р.П.	1	Пройден

Б-R6.1	13.12.22	Никаноров Р.П.	1	Пройден
Б-R6.2	13.12.22	Никаноров Р.П.	1	Пройден
Б-R6.3	13.12.22	Никаноров Р.П.	1	Пройден
Б-R7	13.12.22	Никаноров Р.П.	1	Пройден
Б-R8	13.12.22	Никаноров Р.П.	1	Пройден
Б-R9	13.12.22	Никаноров Р.П.	1	Пройден
Б-R10	13.12.22	Никаноров Р.П.	1	Пройден
Б-L1.1	14.12.22	Никаноров Р.П.	1	Пройден
Б-L1.2	14.12.22	Никаноров Р.П.	1	Пройден
Б-L2	14.12.22	Никаноров Р.П.	1	Пройден
Б-L3	14.12.22	Никаноров Р.П.	1	Пройден
Б-L4.1	14.12.22	Никаноров Р.П.	1	Пройден
Б-L4.2	14.12.22	Никаноров Р.П.	1	Пройден
Б-L5	14.12.22	Никаноров Р.П.	1	Пройден
Б-L6	14.12.22	Никаноров Р.П.	1	Пройден
Б-L7	14.12.22	Никаноров Р.П.	1	Пройден
Б-L8	14.12.22	Никаноров Р.П.	1	Пройден
Б-L9	14.12.22	Никаноров Р.П.	1	Пройден
Б-L10	14.12.22	Никаноров Р.П.	1	Пройден
Б-L11.1	14.12.22	Никаноров Р.П.	1	Пройден
Б-L11.2	14.12.22	Никаноров Р.П.	1	Пройден
Б-L12.1	14.12.22	Никаноров Р.П.	1	Пройден
Б-L12.2	14.12.22	Никаноров Р.П.	1	Пройден
Б-L13.1	14.12.22	Никаноров Р.П.	1	Пройден
Б-L13.2	14.12.22	Никаноров Р.П.	1	Пройден
Б-L13.3	14.12.22	Никаноров Р.П.	1	Пройден
Б-L14	14.12.22	Никаноров Р.П.	1	Пройден

Таблица 136: Журнал блочного тестирования

## 6.2 Интеграционное тестирование

№ теста	Дата	Тестирующий	Попытка	Результат
И-DL1	14.12.22	Никаноров Р.П.	1	Пройден
И-DL2.1	14.12.22	Никаноров Р.П.	1	Пройден
И-DL2.2	14.12.22	Никаноров Р.П.	1	Пройден
И-DL3.1	14.12.22	Никаноров Р.П.	1	Пройден
И-DL3.2	14.12.22	Никаноров Р.П.	1	Пройден
И-DL4.1	14.12.22	Никаноров Р.П.	1	Пройден
И-DL4.2	14.12.22	Никаноров Р.П.	1	Пройден
И-DL5	14.12.22	Никаноров Р.П.	1	Пройден
И-DL6	14.12.22	Никаноров Р.П.	1	Пройден
И-DL7	14.12.22	Никаноров Р.П.	1	Пройден
И-DL8.1	14.12.22	Никаноров Р.П.	1	Пройден
И-DL8.2	14.12.22	Никаноров Р.П.	1	Пройден
И-DC1	14.12.22	Никаноров Р.П.	1	Пройден
И-DC2	14.12.22	Никаноров Р.П.	1	Пройден
И-DC3	14.12.22	Никаноров Р.П.	1	Пройден
И-DC4	14.12.22	Никаноров Р.П.	1	Пройден
И-DC5	14.12.22	Никаноров Р.П.	1	Пройден
И-DR1	14.12.22	Никаноров Р.П.	1	Пройден
И-DR2	14.12.22	Никаноров Р.П.	1	Пройден
И-CR1	14.12.22	Никаноров Р.П.	1	Пройден
И-CR2	14.12.22	Никаноров Р.П.	1	Пройден
И-CR3	14.12.22	Никаноров Р.П.	1	Пройден
И-LR1	14.12.22	Никаноров Р.П.	1	Пройден
И-LR2	14.12.22	Никаноров Р.П.	1	Пройден
И-A1	14.12.22	Никаноров Р.П.	1	Пройден
И-A2	14.12.22	Никаноров Р.П.	1	Пройден
И-A3	14.12.22	Никаноров Р.П.	1	Пройден
И-A4	14.12.22	Никаноров Р.П.	1	Пройден
И-A5	14.12.22	Никаноров Р.П.	1	Пройден

Таблица 137: Журнал интеграционного тестирования

### 6.3 Аттестационное тестирование

№ теста	Дата	Тестирующий	Попытка	Результат
A-1	12.12.22	Никаноров Р.П.	1	Пройден
A-2.1	12.12.22	Никаноров Р.П.	1	Пройден
A-2.2	12.12.22	Никаноров Р.П.	1	Пройден
A-2.3	12.12.22	Никаноров Р.П.	1	Пройден
A-2.4	12.12.22	Никаноров Р.П.	1	Пройден
A-2.5	12.12.22	Никаноров Р.П.	1	Пройден
A-2.6	12.12.22	Никаноров Р.П.	1	Пройден
A-2.7	12.12.22	Никаноров Р.П.	1	Пройден
A-3	12.12.22	Никаноров Р.П.	1	Пройден
A-4	12.12.22	Никаноров Р.П.	1	Пройден
A-5.1	12.12.22	Никаноров Р.П.	1	Пройден
A-5.2	12.12.22	Никаноров Р.П.	1	Пройден
A-5.3	12.12.22	Никаноров Р.П.	1	Пройден
A-5.4	12.12.22	Никаноров Р.П.	1	Пройден
A-5.5	12.12.22	Никаноров Р.П.	1	Пройден
A-6	12.12.22	Никаноров Р.П.	1	Пройден
A-7.1	12.12.22	Никаноров Р.П.	1	Пройден
A-7.2	12.12.22	Никаноров Р.П.	1	Пройден
A-7.3	12.12.22	Никаноров Р.П.	1	Пройден
A-8.1	12.12.22	Никаноров Р.П.	1	Пройден
A-8.2	12.12.22	Никаноров Р.П.	1	Пройден
A-8.3	12.12.22	Никаноров Р.П.	1	Пройден
A-8.4	12.12.22	Никаноров Р.П.	1	Пройден
A-9	12.12.22	Никаноров Р.П.	1	Пройден
A-10.1	12.12.22	Никаноров Р.П.	1	Пройден
A-10.2	12.12.22	Никаноров Р.П.	1	Пройден
A-10.3	12.12.22	Никаноров Р.П.	1	Пройден
A-11.1	12.12.22	Никаноров Р.П.	1	Пройден
A-11.2	12.12.22	Никаноров Р.П.	1	Пройден
A-12	12.12.22	Никаноров Р.П.	1	Пройден

Таблица 138: Журнал аттестационного тестирования

### 6.4 Специальное тестирование

№ теста	Дата	Тестирующий	Попытка	Результат
S-1	15.12.22	Никаноров Р.П.	1	Пройден
S-2	15.12.22	Никаноров Р.П.	1	Пройден
S-3	15.12.22	Никаноров Р.П.	1	Пройден
S-4	15.12.22	Никаноров Р.П.	1	Пройден
S-5	15.12.22	Никаноров Р.П.	1	Пройден
S-6	15.12.22	Никаноров Р.П.	1	Пройден

Таблица 139: Журнал специального тестирования

## 7 Результаты

В рамках дисциплины «Верификация программного обеспечения» была протестирована криптосистема и написано 135 тестов: 70 блочных, 29 интеграционных, 30 аттестационных и 6 специальных. Данные тесты помогут в будущем с быстрой проверкой системы после её модификации. Общее покрытие тестами достигло 80%.

На этапах тестирования не было выявлено критических ошибок в работе тестируемых модулей, но были выявлены недостатки архитектуры, которые могут быть рассмотрены и исправлены в будущем.