|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДЕНО |
|  |  | Генеральный директор  Центра сертификации ФГУП НИИ «Восход» |
|  |  | \_\_\_\_\_\_\_\_\_\_\_ В.В. Петров |
|  |  | “\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2024 г. |
|  |  |  |

Программный комплекс «Программа»

**Протокол испытаний № 2**

643.22222222.11111-01 51 01- ЛУ

Листов 13

|  |  |  |
| --- | --- | --- |
|  |  | Ответственный исполнитель |
|  |  |  |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Васьков А.В. |
|  |  | “\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_2024 г. |
|  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Санкт-Петербург

2024

ОГЛАВЛЕНИЕ

[1 Контроль состава и содержания документации 3](#_Toc188548576)

[2 Контроль исходного состояния ПО 3](#_Toc188548577)

[3 Контроль полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне файлов 4](#_Toc188548578)

[4 Контроль соответствия исходных текстов ПО его загрузочному коду 5](#_Toc188548579)

[5 Контроль связей функциональных объектов по управлению 5](#_Toc188548580)

[6 Контроль связей функциональных объектов по информации 6](#_Toc188548581)

[7 Контроль информационных объектов 7](#_Toc188548582)

[8 Формирования перечня маршрутов выполнения функциональных объектов 8](#_Toc188548583)

[9 Контроль выполнения функциональных объектов 10](#_Toc188548584)

[10 Сопоставления фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа 12](#_Toc188548585)

[11 Интегральная оценка проведённых испытаний 13](#_Toc188548586)

# 1 Контроль состава и содержания документации

Перечень программной документации, предоставленной Разработчиком при проведении испытаний:

1. Руководство по эксплуатации ПО «Программа»:   
   643.33333333.22222-01 91 01.
2. Спецификация ПО «Программа»: 643.33333333.22222-01 10 01.
3. Описание программы ПО «Программа»: 643.33333333.22222-01 13 01.
4. Текст программы ПО «Программа»: 643.33333333.22222-01 12 01.
5. Пояснительная записка ПО «Программа»: 643.33333333.22222-01 81 01.

Данный перечень программной документации полностью совпадает с заявленным на проведение испытаний перечнем документов.

Проверка программной документации, предоставленной Разработчиком при проведении испытаний:

1. Спецификация ПО «Программа»: 643.33333333.22222-01 10 01 соответствует требованиям к содержанию и оформлению ГОСТ 19.202-78.
2. Описание программы ПО «Программа»: 643.33333333.22222-01 13 01 соответствует требованиям к содержанию и оформлению ГОСТ 19.402-78.
3. Текст программы ПО «Программа»: 643.33333333.22222-01 12 01 соответствует требованиям к содержанию и оформлению ГОСТ 19.401-78.
4. Пояснительная записка ПО «Программа»: 643.33333333.22222-01 81 01 соответствует требованиям к содержанию и оформлению ГОСТ 19.404-79.

В ходе испытаний было заключено, что состав и содержание полностью соответствует РД, на основе которого проводятся испытания.

**Испытание пройдено успешно.**

# 2 Контроль исходного состояния ПО

Были рассчитаны хэш-суммы представленного исходного программного продукта и хэш-суммы продукта, представленного на испытания (хеш-сумма MD5 рассчитывается с помощью программного средства фиксации и контроля исходного состояния «hashtab»).

Расчет уникальных значений контрольных сумм загрузочных модулей и исходных текстов программ, входящих в состав ПО:

|  |  |  |  |
| --- | --- | --- | --- |
| Файл | Рассчитанное в ходе испытаний hash-значение | Hash-значение, указанное в описание программы | Эталонный образец разработчика |
| Lab\_3.cpp | f7c3e9a1d5b6478c8b2e4f31a6d29bcc | f7c3e9a1d5b6478c8b2e4f31a6d29bcc | f7c3e9a1d5b6478c8b2e4f31a6d29bcc |
| Lab\_3.exe | d3f1a8b6e3c2499b9e7f4fcb1d85a2bc | d3f1a8b6e3c2499b9e7f4fcb1d85a2bc | d3f1a8b6e3c2499b9e7f4fcb1d85a2bc |

Требуемые КС исследуемого ПО полностью совпадают:

**Испытание пройдено успешно.**

# 3 Контроль полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне файлов

Перечень исходных текстов (файлов), необходимых и достаточных для корректной сборки исследуемого ПО, предъявляемый заявителем:

|  |  |
| --- | --- |
| **Дистрибутив** | **Исходные файлы** |
| Lab\_3 | Lab\_3.cpp |
| Lab\_3 | Lab\_3.exe |

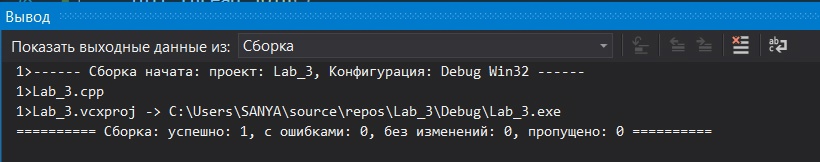


Рис.1 Сборка всех файлов и компиляция ПО

Полнота представленных исходных текстов на уровне файлов ПО подтверждается фактом успешной компиляции и сборки исследуемого ПО.

Избыточность представленных исходных текстов на уровне файлов ПО подтверждается фактом отсутствия файлов, которые не используются при выполнении функциональных требований ПО.

**Испытание пройдено успешно.**

# 4 Контроль соответствия исходных текстов ПО его загрузочному коду

|  |  |  |
| --- | --- | --- |
| **Файл** | **Данные о КС, предъявляемые заявителем** | **Контроль, проведённый в рамках текущего испытания** |
| Lab\_3.exe | d3f1a8b6e3c2499b9e7f4fcb1d85a2bc | d3f1a8b6e3c2499b9e7f4fcb1d85a2bc |

Требуемые КС исследуемого ПО полностью совпадают:

**Испытание пройдено успешно.**

# 5 Контроль связей функциональных объектов по управлению

Таблица 1. Связи функциональных объектов по управлению

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **generate\_key\_pair** | initialize\_key\_pairs | xor\_hash | create\_signatures | verify\_signatures | main |
| **generate\_key\_pair** |  | + |  |  |  |  |
| initialize\_key\_pairs | + |  |  |  |  | + |
| **xor\_hash** |  | + |  | + |  |  |
| **create\_signatures** |  |  | + |  |  |  |
| **verify\_signatures** |  |  | + | + |  |  |
| **main** |  |  |  |  | + |  |

Все установленные связи функциональных объектов по управлению полностью соответствуют логике работы тестового ПО, заявленного в документации (пояснительной записке).

**Испытание пройдено успешно.**

# 6 Контроль связей функциональных объектов по информации

Таблица 2. Связи функциональных объектов по информации

|  |  |  |  |
| --- | --- | --- | --- |
| **Функциональный Объект** | **Имя ИО** | **Тип ИО** | **Вид ИО** |
| **generate\_key\_pair** | private\_key | int | локальная |
| **generate\_key\_pair** | public\_key | int | локальная |
| initialize\_key\_pairs | num\_keys | int | локальная |
| initialize\_key\_pairs  create\_signatures  verify\_signatures  main | key\_pairs | vector<KeyPair> | локальная |
| xor\_hash | data | string | локальная |
| xor\_hash | key | int | локальная |
| xor\_hash | hash | string | локальная |
| create\_signatures  verify\_signatures  main | document\_hash | string | локальная |
| create\_signatures  verify\_signatures  main | signatures | vector<string> | локальная |
| create\_signatures  verify\_signatures | current\_signature | string | локальная |
| verify\_signatures | current\_signature | string | локальная |
| main | document | string | локальная |

Исходя из анализа связей функциональных объектов по информации, установлено, что глобальные и локальные переменные соответствуют логике работы тестового ПО, заявленной в документации (пояснительной записке), а также не нарушает принципы безопасности критических переменных.

**Испытание пройдено успешно.**

# 7 Контроль информационных объектов

Таблица 3. Информационные объекты

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Имя ИО** | **Тип ИО** | **Граничные значения** | | | **Вид ИО** |
| Минимальное значение | Максимальное значение | | локальная |
| 1 | private\_key | int | 1 | | 255 | локальная |
| 2 | public\_key | int | 10 000 | | 2 550 000 | локальная |
| 3 | num\_keys | int | 2 | | 5 | локальная |
| 4 | key\_pairs | vector<KeyPair> | 0 (пустой вектор) | | зависит от доступной памяти | локальная |
| 5 | data | string | Пустая строка | | зависит от доступной памяти | локальная |
| 6 | key | int | 1 | | 255 | локальная |
| 7 | hash | string | Пустая строка | | зависит от доступной памяти | локальная |
| 8 | document\_hash | string | Пустая строка | | зависит от доступной памяти | локальная |
| 9 | signatures | string | Пустая строка | | зависит от доступной памяти | локальная |
| 10 | current\_signature | string | Пустая строка | | зависит от доступной памяти | локальная |
| 11 | document | string | Пустая строка | | зависит от доступной памяти | локальная |

В процессе тестирования было выявлено, что изменена логика программы и значение открытого ключа public\_key увеличилось до диапазона 10,000–2,550,000 (вместо 2–510), хотя значения не выходят за пределы допустимого диапазона для типа данных int (−2,147,483,648 до 2,147,483,647, 4 байта), но такое увеличение приводит к проблемам при выполнении арифметических операций, включая XOR-хэширование. В результате наблюдается искажение данных, которое нарушает корректность вычислений и делает невозможной успешную проверку подписей. Это уязвимость классифицируется как нарушение целостности вычислений (CWE-682: Неверные вычисления).

**Испытание не пройдено.**

# 8 Формирования перечня маршрутов выполнения функциональных объектов

На основе предыдущих пунктов был построен граф, отражающий маршруты выполнения функциональных объектов.

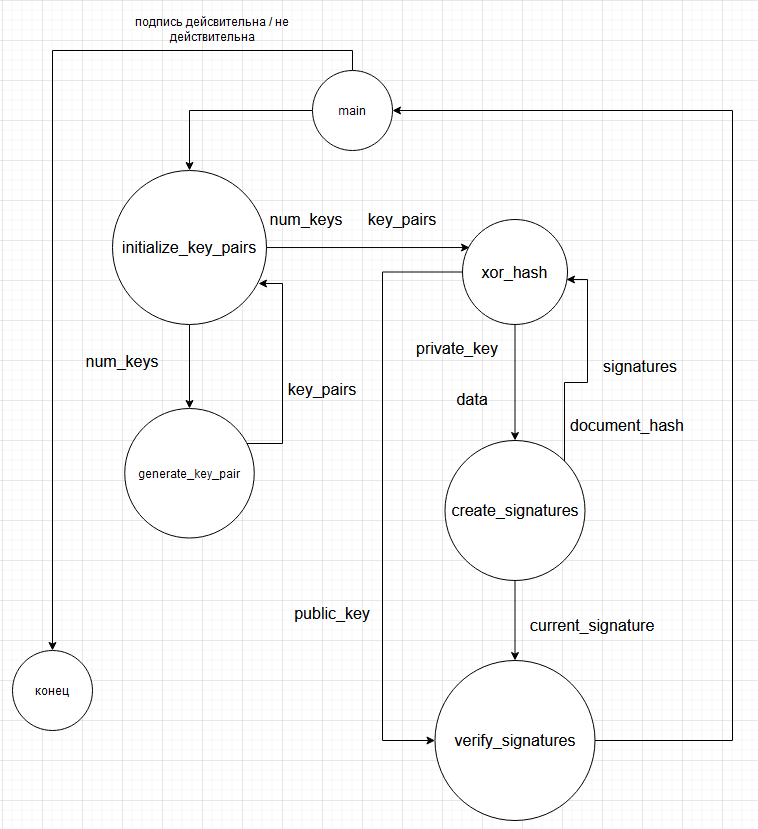


Рис.2 Граф маршрутов трасс ПО

В ходе анализа маршрутов выполнения функциональных объектов было заключено, что статические маршруты вызовов функциональных объектов, а также их порядок и последовательность соответствуют логике работы тестового ПО, заявленной в документации (пояснительной записке).

**Испытание пройдено успешно.**

# 9 Контроль выполнения функциональных объектов

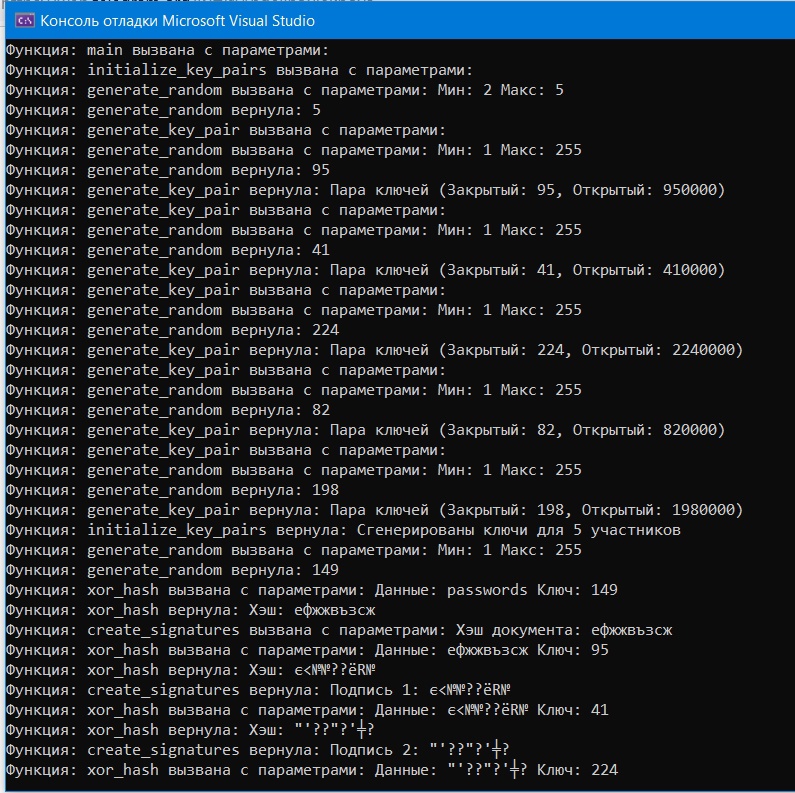


Рисунок 3 – Проверка выполнения функциональных объектов

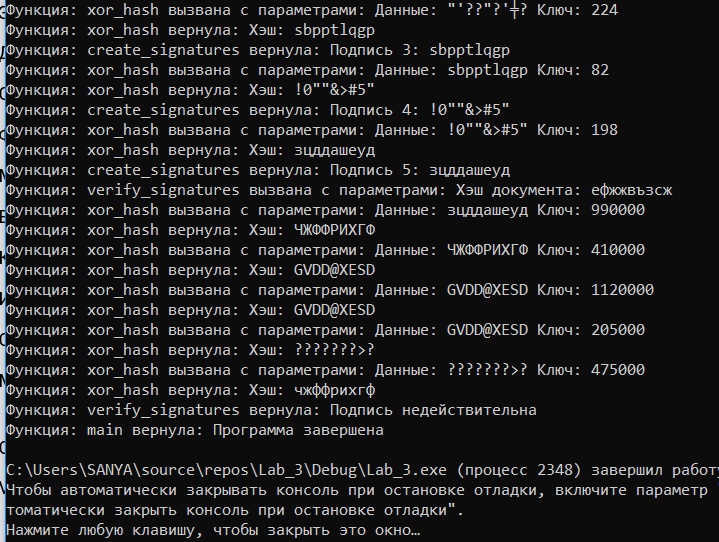


Рисунок 4 – Проверка выполнения функциональных объектов

Было выявлено, что ПО не выполняет необходимых функций. При выполнении программы возникает ошибка целочисленного переполнения в блоке генерации ключей. В результате значения открытых ключей становятся некорректными, что приводит к нарушению логики работы следующих функциональных блоков.

Подписи, созданные на основе некорректных данных, не проходят верификацию на этапе проверки. Программа не завершает работу аварийно, однако приводит к сбою выполнения основной функции: подтверждение подлинности подписей невозможно. Это классифицируется как нарушение целостности вычислений (CWE-682: Неверные вычисления).

**Испытание не пройдено.**

# 10 Сопоставления фактических маршрутов выполнения функциональных объектов и маршрутов, построенных в процессе проведения статического анализа

**На основании п.8 и п.9 установлено, что построенные фактические маршруты выполнения соответствуют маршрутам, построенным в процессе проведения статического анализа.**

**Однако выявлено, что некорректное состояние данных из-за уязвимости (целочисленного переполнения) приводит к недостижению основной функциональной цели программы (верификация подписей). Это указывает на расхождение не в маршрутах выполнения, а в корректности выполнения функций.**

**Испытание не пройдено.**

# 11 Интегральная оценка проведённых испытаний

|  |  |
| --- | --- |
| **Испытание** | **Результат** |
| Контроль состава и содержания документации | успешно |
| Контроля исходного состояния ПО | успешно |
| Контроля полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне файлов | успешно |
| Контроля соответствия исходных текстов ПО его загрузочному коду. | успешно |
| Контроля полноты и отсутствия избыточности исходных текстов контролируемого ПО на уровне функциональных объектов (процедур) | успешно |
| Контроля связей функциональных объектов по управлению | успешно |
| Контроля связей функциональных объектов по информации | успешно |
| Контроля информационных объектов различных типов (например, локальных переменных, глобальных переменных, внешних переменных и т.п.) | Испытание не пройдено |
| Формирования перечня маршрутов выполнения функциональных объектов | успешно |
| Контроля выполнения функциональных объектов | Испытание не пройдено |
| Сопоставления фактических маршрутов выполнения функциональных объектов (процедур, функций) и маршрутов, построенных в процессе проведения статического анализа. | Испытание не пройдено |

Некоторые испытания ПО «Программа» на контроль отсутствия НДВ согласно РД не пройдены. Исследуемое ПО не может соответствовать 3-му уровню контроля отсутствия НДВ согласно РД «Защита от НСД к информации. Часть 1. ПО СЗИ. Классификация по уровню контроля отсутствия НДВ».