|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДЕНО |
|  |  | Должность представителя поставщика |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ФИО |
|  |  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

[Наименование органиЗации]

Оценка соответствия реализованных мер по разработке безопасного программного обеспечения в составе цифрового продукта [наименование цифрового продукта]

Страниц \_\_

Москва - 2023 г.

Аннотация

Настоящий документ содержит оценку соответствия реализованных мер
по разработке безопасного программного обеспечения с приложением результатов проведенных испытаний по выявлению уязвимостей в программном обеспечении цифрового продукта [наименование цифрового продукта].

**Обозначения и сокращения**

Используемые в настоящем документе обозначения и сокращения являются понятиями из области автоматизированных систем, которые определены
в ГОСТ Р 59853‑2021. Также в настоящем документе введены следующие обозначения и сокращения на русском и английском языках.

|  |  |
| --- | --- |
| Термин | Определение/Описание |
| Фаззинг-тестирование | FUZZ testing (fuzzing) – это тип тестирования безопасности, который обнаруживает ошибки кодирования и лазейки в программном обеспечении, операционных системах или сетях. Фаззинг включает в себя ввод огромного количества случайных данных, называемых fuzz, в тестируемое программное обеспечение, чтобы заставить его дать сбой или прорвать его защиту |

# Термины и определения

Используемые в настоящем документе термины и определения являются понятиями из области автоматизированных систем, которые определены в ГОСТ Р 59853‑2021. Также в настоящем документе введены следующие понятия на русском языке.

|  |  |
| --- | --- |
| Сокращение | Определение/Описание |
| ПО | Программное обеспечение |
| СУБД | Система управления базой данных |
| ТС | Технические средства |
| ЭВМ | Электронная вычислительная машина |

# Общее описание

Разработчиком [наименование цифрового продукта] (далее – Цифровой продукт) является [наименование организации] (далее Поставщик).

В качестве оценки соответствия для Цифрового продукта предоставляются:

- описание реализации процесса разработки безопасного программного обеспечения Разработчиком в соответствии с требованиями ГОСТ Р 56939-2016 «Разработка безопасного программного обеспечения. Общие требования». приведено в Приложении А к настоящему документу;

- результаты проведенных испытаний по выявлению уязвимостей в программном обеспечении Цифрового продукта. Результаты проведенных испытаний по выявлению уязвимостей в программном обеспечении Цифрового продукта приведены в Приложении Б к настоящему документу.

# Оценка соответствия программного обеспечения Цифрового продукта предъявляемым требованиям

Исследование представленного документа «Описание реализации процесса разработки безопасного программного обеспечения» позволяет сделать заключение, что Поставщиком **реализуются** процессы связанные с созданием безопасного (защищенного) программного обеспечения, а также формированием (поддержанием) среды обеспечения оперативного устранения выявленных ошибок программного обеспечения и уязвимостей в соответствии с требованиями
ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

На основании результатов проведенных испытаний по выявлению уязвимостей в программном обеспечении Цифрового продукта (см.*Наименование документа, содержащего результаты испытаний*) можно сделать вывод, что в в программном обеспечении Цифрового продукта применимых для него уязвимостей **не выявлено.**

**Вывод:** Программное обеспечение Цифрового продукта соответствует требованиям методических рекомендаций «Методические рекомендации
по включению сервисов в единую цифровую платформу Российской Федерации «ГосТех»» в части выполнения п.10.1 требований к защите информации. Процесс разработки программного обеспечения ведется с использованием мер ГОСТ Р 56939 2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

**Приложения:**

## 1. Описание реализации процесса разработки безопасного программного обеспечения

## 2 Результаты проведенных испытаний по выявлению уязвимостей в программном обеспечении цифрового продукта [Наименование цифрового продукта].