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

[Наименование органиЗации]

Документация по разработке безопасного программного обеспечения

Страниц \_\_\_

Москва

2023 г.

Аннотация

Настоящий документ содержит документацию по разработке безопасного программного обеспечения принятые в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (далее – Поставщик). Процессы, описанные в нем, направлены на обеспечение необходимого уровня защиты информации, посредством реализации мер, минимизирующих количество уязвимостей и недостатков программ на всех этапах жизненного цикла ПО и ведутся с использованием мер ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

**1.** **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.

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

# 2. 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.

|  |  |
| --- | --- |
| 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 |

# 3. Введение

|  |  |
| --- | --- |
| Наименование документа | Документация по разработке безопасного программного обеспечения |
| Версия документа | Версия 1.0 |

# 4. Общие положения

Целью создания безопасного ПО является снижение вероятности возникновения в ПО уязвимостей и иных недостатков, ведущих к нарушению его свойств безопасности или невозможности выполнения ПО возложенных на него функций.

Указанная цель достигается:

- реализацией мер по разработке безопасного ПО в среде разработки ПО;

- умелым распределением ролей и обязанностей, связанных с реализацией мер по разработке безопасного ПО, между работниками;

- качественной разработкой документации Поставщика, связанной
с - реализацией мер по разработке безопасного ПО;

- организацией и проведением внутренних проверок выполнения мер
по - разработке безопасного ПО;

- реализацией действий, направленных на улучшение процессов, связанных с разработкой безопасного ПО.

**5. Меры безопасности**

## 5.1. Меры по разработке безопасного программного обеспечения

### 5.1.1. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении конструирования и комплексирования программного обеспечения

При выполнении конструирования и комплексирования ПО Поставщиком реализуются следующие меры:

- использование при разработке ПО идентифицированных инструментальных средств;

- статический анализ исходного кода программы (по результатам проведения статического анализа может проводиться доработка разрабатываемого ПО;

- экспертиза исходного кода программы.

Статический анализ исходного кода программы выполняют Поставщики или сторонние организации, обладающие компетенцией в области выявления уязвимостей программ.

Статический анализ выполняется при каждой сборке.

Экспертизу исходного кода программы выполняет специалист Поставщика, отвечающий за безопасность разрабатываемого ПО, или сторонние организации, обладающие компетенцией в области выявления уязвимостей программ.

В результате успешной реализации мер должны быть выполнены следующие мероприятия:

- при создании ПО используются только идентифицированные Поставщиком инструментальные средства с определенными опциями (настройками);

- в исходном коде ПО выявляются и устраняются недостатки (потенциально уязвимые конструкции).

### 5.1.2. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении квалификационного тестирования программного обеспечения

При выполнении квалификационного тестирования ПО Поставщиком реализуется функциональное тестирование программы.

Тесты, выполняемые в рамках квалификационного тестирования программы, разрабатываются с учетом:

- результатов статического анализа исходного кода программы (перечень выявленных потенциально уязвимых конструкций в исходном коде программы);

- результатов экспертизы исходного кода программы (перечень выявленных потенциально уязвимых конструкций в исходном коде программы).

По результатам выполненных работ может проводиться доработка программы.

В результате успешной реализации мер проводится:

- тестирование ПО, документальное оформление результатов
и формирование списка выявленных несоответствий требованиям безопасности и (или) уязвимостей программы (при наличии);

- доработка программы, направленная на устранение выявленных несоответствий требованиям безопасности и (или) уязвимостей программы.

### 5.1.3. Меры по разработке безопасного программного обеспечения, реализуемые при выполнении инсталляции программы и поддержки приемки программного обеспечения

При выполнении инсталляции программы и поддержки приемки разработанного ПО Поставщиком реализуются следующие меры:

- обеспечение защиты ПО от угроз безопасности информации, связанных с нарушением целостности, в процессе его передачи пользователю (где такое применимо);

- поставка пользователю эксплуатационных документов.

### 5.1.4. Меры по разработке безопасного программного обеспечения, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации

В процессе сопровождения эксплуатации разработанного ПО Поставщик реализует следующие меры:

- обеспечение процесса приема информации о недостатках и уязвимостях ПО;

- обеспечение процесса поиска ошибок ПО и уязвимостей программы.

Процедура устранения уязвимостей обеспечивает возможность обновления разработанного ПО для устранения актуальных уязвимостей функционирования. Устранение уязвимостей производится с использованием организационно-технических процедур, представленных ниже.

Поставщик проводит поиск известных (подтвержденных) уязвимостей
в общедоступных источниках информации об уязвимостях.

Поставщик должен осуществлять прием и обработку сообщений
от пользователей об ошибках и уязвимостях в разработанном ПО и запросов
на их устранение.

Поставщик при выявлении или получении информации об уязвимости или недостатках в разработанном ПО проводит анализ выявленных уязвимостей.

При выявлении уязвимости(ей) в разработанном ПО, заявитель должен оповестить потребителя о необходимости установки обновлений ПО.

В случае отсутствия на момент проверки информации по выявленной уязвимости доступных обновлений с устраненной уязвимостью Поставщик доводит до потребителя инструкцию по проведению организационно-технических мероприятий, направленных на недопущение попыток эксплуатации выявленной уязвимости злоумышленником (-ами).

### 5.1.5. Меры по разработке безопасного программного обеспечения, реализуемые в процессе менеджмента документации и конфигурации программы

В рамках менеджмента документации и конфигурации программы Поставщик ПО реализует следующие меры:

- реализация и использование процедуры уникальной маркировки каждой версии ПО;

- использование системы управления конфигурацией ПО.

### 5.1.6. Меры по разработке безопасного программного обеспечения, реализуемые в процессе менеджмента инфраструктуры среды разработки программного обеспечения

В рамках менеджмента инфраструктуры среды разработки ПО Поставщик ПО реализует следующие меры:

- защита от несанкционированного доступа к элементам конфигурации;

- резервное копирование элементов конфигурации;

- регистрация событий, связанных с фактами изменения элементов конфигурации.

Среда разработки ПО размещается в границах контролируемой зоны, куда доступ посторонних лиц запрещен.

### 5.1.7. Меры по разработке безопасного программного обеспечения, реализуемые в процессе менеджмента людских ресурсов

В процессе менеджмента персонала Поставщик ПО проводит периодическое обучение сотрудников;

К проведению обучения сотрудников могут привлекаться сторонние организации.

## 6. Свидетельство соблюдения мер безопасности

Описанные выше меры безопасности отражены в правилах внутреннего трудового распорядка, должностных инструкциях и других внутренних нормативных документах, с которыми персонал разработки, тестирования
и производства ознакомлены под подпись.

Указанные меры позволяют обеспечить снижение вероятности возникновения в разработанном ПО уязвимостей и иных недостатков, ведущих к нарушению его свойств безопасности или невозможности выполнения возложенных на него функций.

**Лист согласования**

|  |  |  |
| --- | --- | --- |
| **№** | **Раздел документа (выполняемые меры)** | **Участники процесса разработки** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

 «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 202\_\_ г.