**ОПРОСНЫЙ ЛИСТ ПО ОЦЕНКЕ СООТВЕТСТВИЯ ПРИЛОЖЕНИЙ ПО ОУД4**

|  |  |
| --- | --- |
|  | |
| Наименование организации |  |
|  | |
| Контактное лицо |  |
|  | |
| Телефон |  |
|  | |
| Email |  |
|  | |
| Дата заполнения |  |
|  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Общие сведения о программном продукте: | | | | обязательно |
|  | | | | |
| Наименование: |  | | | |
|  | | | | |
| Назначение: |  | | | |
|  | | | | |
| Иная значимая информация на Ваше усмотрение: |  | | | |
|  | | | *Указать* | |
|  | | | | |
| 1. Кем является организация по отношению к программному продукту? | | | | обязательно |
|  | | | | |
| Пользователь | | Разработчик | | |
| *- выбрано;*  *- не выбрано* | |  | | |
|  | | | | |
| 1. Оценка проводится впервые? | | | | обязательно |
|  | | | | |
| Да | | Нет | | |
|  | | | | |
| 1. Имеющаяся документация (отметить, какая имеется): | | | | обязательно |

| **Наименование документа** | **Содержание документа** |
| --- | --- |
|  |  |
| Задание по безопасности | |
|  | * Функциональные требования безопасности * Требования доверия к безопасности |
| Функциональная спецификация | |
|  | * Назначение и методы всех интерфейсов функций безопасности * Перечень и описание всех параметров каждого интерфейса функций безопасности * Перечень и описание всех действий, связанных с каждым интерфейсом функций безопасности * Описание сообщений обо всех непосредственных ошибках, которые могут возникнуть при вызове каждого интерфейса функциональных возможностей безопасности объекта оценки. * Прослеживание функциональных требований безопасности к интерфейсам функциональных возможностей безопасности объекта оценки |
| Проект объекта оценки | |
|  | * Перечень подсистем * Перечень модулей * Описание модулей |
| Описание архитектуры безопасности | |
|  | * Перечень функций безопасности (идентификация, аутентификация и пр.) * Перечень механизмов собственной защиты от вмешательства. * Описание защищённости процесса инициации функций безопасности * Описание невозможности обхода функциональных возможностей, осуществляющих выполнение функциональных требований безопасности |
| Представление реализации (выбранное подмножество реализации) | |
|  | * Определение функциональных возможностей безопасности объекта оценки на таком уровне детализации, что функциональные возможности безопасности объекта оценки могут быть созданы без дополнительных проектных решений. * Демонстрация соответствие между выборкой представления реализации и описанием проекта объекта оценки |
| Руководство пользователя по эксплуатации | |
|  | * Описание доступных пользователям функций, возможных прав и обязанностей, которыми следует управлять в защищенной среде функционирования, а также уместных предупреждений. * Описание принципов безопасной работы с предоставленными в объекте оценки интерфейсами. * Описание доступных для каждой пользовательской роли функций и интерфейсов, особенно всех параметров безопасности под управлением пользователя, с указанием безопасных значений * Для каждой пользовательской роли должно быть представлено четкое представление каждого типа имеющих значение для безопасности событий, связанных с доступными пользователю обязательными для выполнения функциями, включая изменение характеристик безопасности сущностей, находящихся под управлением функциональных возможностей безопасности объекта оценки * Возможные режимы работы объекта оценки (включая операции после сбоев и ошибок эксплуатации), их последствия и участие в обеспечении безопасного функционирования * Для каждой пользовательской роли должно быть описание всех мер безопасности |
| Руководство по подготовительным процедурам | |
|  | * Шаги для безопасной установки * Шаги для безопасной подготовки среды функционирования * Шаги для безопасной приёмки поставленного объекта оценки |
| Документация по управлению конфигурацией | |
|  | • Система управления конфигурацией:   * описание метода, используемого для уникальной идентификации элементов конфигурации (номера версий модулей, контрольные суммы файлов и методика их проверки) * план управления конфигурацией (излагается концепция процесса и реализация средств автоматизации) * описание того, каким образом система управления конфигурацией используется для разработки объекта оценки * описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации как части объекта оценки (тестирование, методика испытаний) * демонстрация соответствия функционирования системы управления конфигурацией с планом управления конфигурацией |
| Описание процедур поставки | |
|  | * Описание всех процедур, необходимых для поддержания безопасности при распространении версий объекта оценки потребителю (описание процедур гарантированной поставки программного обеспечения без изменений (опечатывание, подсчет контрольной суммы или иная проверка целостности)) |
| Документация по безопасности разработки | |
|  | * Описание всех физических, процедурных, организационных и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта объекта оценки и его реализации в среде разработки (используется СКУД, авторизация по логину и паролю, матрица доступа, контроль целостности) |
| Документация определения жизненного цикла | |
|  | * Описание модели, применяемой при разработке и сопровождении объекта оценки (выбрать модель жизненного цикла объекта оценки) * Описание функций контроля по разработке и сопровождению объекта оценки (описание системы ревизий, описание системы отслеживания постановки задачи до ее исполнения (например Atlassian)) |
| Инструментальные средства и методы (описание) | |
|  | * Перечень инструментальных средств разработки (языки программирования и IDE используемые для разработки) * Опции инструментальных средств разработки (настройки средств разработки необходимые для сборки объекта оценки) * Описание языковых конструкций, используемых в реализации (ссылки на документацию к используемым языкам программирования) |
| Свидетельство о покрытии тестами | |
|  | * Демонстрация соответствия между тестами из тестовой документации и интерфейсами из функциональной спецификации * Демонстрация того, что все интерфейсы из функциональной спецификации были подвергнуты тестированию |
| Свидетельство анализа соответствия представлений функций безопасности ОО | |
|  | * Демонстрация соответствия между тестами из тестовой документации подсистемами функций безопасности объекта оценки, а также модулями, выполняющими функциональные требования безопасности (матрица покрытия интерфейсов тестами, однозначную идентификацию между тестами и интерфейсами) * Демонстрация того, что все подсистемы из проекта объекта оценки были подвергнуты тестированию (гистограмма с накоплением, содержащая сведения о числе тестов в отношении каждой из проверяемых подсистем) * Демонстрация того, что осуществляющие выполнение функций безопасности модули из проекта объекта оценки были подвергнуты тестированию (гистограмма с накоплением, содержащая сведения о числе тестов в отношении каждой из проверяемых подсистем) |
| Процедуры тестирования и тестовая документация | |
|  | * Описание плана тестирования, а также ожидаемых и фактических результатов тестирования * Описание тестового окружения объекта оценки * Описание конфигураций объекта оценки * Описание тестов, тестовых наборов, сценариев проведения каждого теста в отношении объекта оценки * Описание фактических и ожидаемых результатов тестирования объекта оценки * Тесты API * Ручные тесты * Автоматизированные тесты * Модульные (юнит) тесты |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. Реализованные функции безопасности: | | | | | | |
|  | | | | | | |
| Идентификация | | | | | | |
| Аутентификация | | | | | | |
| Разграничение доступа | | | | | | |
| Регистрация событий | | | | | | |
| Шифрование данных (собственная разработка) | | | | | | |
| Шифрование данных (сторонние НЕ сертифицированные средства) | | | | | | |
| Шифрование данных (сторонние сертифицированные средства) | | | | | | |
| Фильтрация сетевого потока | | | | | | |
| Защита памяти | | | | | | |
| Контроль целостности | | | | | | |
| Другое | |  | | | | |
|  | *Указать* | | | | | |
|  | | | | | | |
| 1. Применяются ли технологии защиты исходного кода (например, обфускация)? | | | | | | обязательно |
|  | | | | | | |
| Да | | | Нет | | | |
|  | | | | | | |
| 1. Процесс тестирования программного продукта на стороне разработчика: | | | | | | обязательно |
| Автоматизированный | | | | | | |
| Ручной | | | | | | |
| Смешанный (автоматизированный и ручной) | | | | | | |
|  | | | | | | |
| 1. Система отслеживания ошибок: | | | | | | обязательно |
| Не используется | | | | | | |
| Jira | | | | | | |
| Redmine | | | | | | |
| Другое | | | |  | | |
|  | | | | *Указать* | | |
|  | | | | | | |
|  | | | | | | |
| 1. Объем исходных кодов: | | | | | | обязательно |
|  | | | | | | |
| **Язык программирования\*** | | |  | | **Количество строк\*** | |
|  | | | | | | |
|  | | |  | |  | |
|  | | |  | |  | |
|  | | |  | |  | |
|  | | | | | | |
|  | | |  | |  | |
|  | | |  | |  | |
|  | | |  | |  | |
|  | | | | | | |
|  | | |  | |  | |
|  | | |  | |  | |
|  | | |  | |  | |
|  | | | | | | |
|  | | |  | |  | |
|  | | |  | |  | |
|  | | |  | |  | |
|  | | | | | | |
|  | | |  | |  | |
|  | | |  | |  | |
|  | | |  | |  | |
|  | | | | | | |
|  | | | | | | |

|  |  |
| --- | --- |
| 1. Желаемый перечень работ | |
|  | |
| Анализ уязвимостей по ОУД4 по собственному заданию по безопасности;  Анализ уязвимостей по ОУД4 по профилю защиты, рекомендованному Банком России;  Полная оценка соответствия ОУД4 по собственному заданию по безопасности;  Полная оценка соответствия ОУД4 по профилю защиты, рекомендованному Банком России;  Разработка документации на программный продукт | |
|  | |
| Все виды работ проводятся в соответствии с ГОСТ 15408.3 | |
|  | |
|  | |
| 1. Желаемый перечень иных работ | |
|  | |
| Аудит организации в направлении обработки/защиты персональных данных  Разработка модели угроз по новой методике ФСТЭК  Оценка соответствия требованиям 683-П  Оценка соответствия требованиям 757-П  Оценка соответствия требованиям 716-П  Оценка соответствия требованиям 802-П  Оценка соответствия требованиям 719-П  Аудит на соответствие требованиям ГОСТ 57580/Приведение в соответствие требованиям ГОСТ 57580;  Независимая внешняя оценка SWIFT | |
|  | |
|  | |
| 1. Поставка технических решений (ПО, ПАК, оборудование) ИБ/ИТ | |
|  | |
| Планируется ли поставка решений ИБ/ИТ?  Требуется ли консультация по вопросам поставки и внедрения решений ИБ/ИТ? | |
|  | |
| Какие решения по ИБ/ИТ вами рассматриваются? |  |
|  | *Указать* |
|  | |
|  | |

Благодарим за уделенное время!