**ОПРОСНЫЙ ЛИСТ ПО АНАЛИЗУ УЯЗВИМОСТЕЙ  
ПРИЛОЖЕНИЙ ПО ОУД 4**

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

|  |  |  |
| --- | --- | --- |
| 1. Цель проведения | | |
|  | | |
| Оценка действующей системы информационной безопасности  Подготовка к проверке регулятора  Требования партнеров | | |
| Другое |  | |
|  | *Указать* | |
| *- выбрано;*  *- не выбрано* | | |
|  | | |
|  | | |
| 1. Общие сведения о программном продукте | | |
|  | | |
| Наименование |  | |
|  | | |
| Назначение |  | |
|  | | |
| Иная значимая информация на Ваше усмотрение |  | |
|  | | |
|  | | |
| 1. Кем является организация по отношению к программному продукту? | | |
|  | | |
| Пользователь | | Разработчик |
|  | | |
|  | | |
| 1. Оценка проводится впервые? | | |
|  | | |
| Да | | Нет |
|  | | |
|  | | |

|  |  |
| --- | --- |
| 1. Имеющаяся документация (отметить, какая имеется) | |
|  | |
| **Наименование документа** | **Содержание** |
|  | |
| 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 |
|  | |
| Инструментальные средства и методы (описание) | • Перечень инструментальных средств разработки  • Опции инструментальных средств разработки  • Описание языковых конструкций, используемых в реализации |
|  | |

|  |  |  |  |
| --- | --- | --- | --- |
| 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)? | | | |
|  | | | |
| Да | | | Нет |
|  | | | |
|  | | | |
| 1. Дата и балл предыдущей оценки/самооценки | | | |
|  | | | |
| **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 747-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!