**ОПРОСНЫЙ ЛИСТ ПО АУДИТУ  
системы обеспечения операционной   
надежности для Кредитных и некредитных финансовых организаций**

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. Тип организации | | | | | | |
|  | | | | | | |
| Кредитная банковская организация  Некредитная финансовая организация | | | | | | |
| *- выбрано;*  *- не выбрано* | | | | | | |
|  | | | | | | |
|  | | | | | | |
| 1. Цель проведения | | | | | | |
|  | | | | | | |
| Соответствие 787-П / 779-П | | | | | | |
| Другое |  | | | | | |
|  | *Указать* | | | | | |
|  | | | | | | |
|  | | | | | | |
| 1. Проведены ли работы по категорированию КИИ (187-ФЗ)? | | | | | обязательно | |
|  | | | | | | |
| Да, значимые объекты имеются  Да, значимые объекты отсутствуют  Нет, не проведены | | | | | | |
|  | | | | | | |
|  | | | | | | |
| 1. Проведена ли классификация операционных рисков? | | | | обязательно | | |
|  | | | | | | |
| Да, в соответствии с 716-П  Да, по иной методике  Нет | | | | | | |
|  | | | | | | |
|  | | | | | | |
| 1. Укажите, какие процедуры по опернадежности реализованы? | | | | обязательно | | |
|  | | | | | | |
| **Процедура** | | **Реализация** | | | | |
|  | | | | | | |
| Фиксация простоев | | | Да | | | Нет |
|  | | | | | | |
| Установлены пороговые значения для простоев | | | Да | | | Нет |
|  | | | | | | |
| Определение и возмещение потерь по простоям | | | Да | | | Нет |
|  | | | | | | |
| Ведётся учет технологических процессов | | | Да | | | Нет |
|  | | | | | | |
| Сформулированы и контролируются целевые показатели опернадежности | | | Да | | | Нет |
|  | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Укажите количество: | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Информационных систем | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Офисов | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Физических серверов | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Виртуальных серверов | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Облачных решений | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Штат сотрудников IT | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Штат сотрудников ИБ | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Какой уровень защиты информации реализуете? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Усиленный  Стандартный  Минимальный  Никакой | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Ведется ли работа с рисками ИБ? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Да, в соответствии с 716-П  Да, по иной методике  Нет | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Оцените степень документирования процессов управления операционными рисками | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | | 6 | 7 | 8 | 9 | | 10 |
|  | | | | | | | | | | | |
| *1 - не документировано* | | | | | | *10 - документировано в полном объеме* | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Оцените степень документирования процессов системы обеспечения операционной надежности | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | | 6 | 7 | 8 | 9 | | 10 |
|  | | | | | | | | | | | |
| *1 - не документировано* | | | | | | *10 - документировано в полном объеме* | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Кто из персонала вовлечен в работу с рисками и опернадежностью? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Высшее руководство  Руководство подразделений  Сотрудники профильного подразделения  Все сотрудники (хотя бы в части обнаружения событий) | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Наличие внутренних документов | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Политика управления операционными рискам  Процедуры управления операционными рисками  План ОНиВД  Политика ИС  Политика ИБС  Классификатор бизнес-процессов организации  Классификатор технологических процессов организации  Задействованная информационная инфраструктура  Положение по обеспечению качества данных в информационных системах  Модель угроз критичной архитектуры  Модель угроз информационной безопасности  Порядок обеспечения информационной безопасности структуры виртуализации  Регламент мониторинга событий информационной безопасности  Регламент обеспечения защиты вычислительной сети  Регламент поиска и устранения уязвимостей, проведения контроля целостности ресурсов в информационной инфраструктуре | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Проводилось ли категорирование и проектирование объектов КИИ (критической информационной инфраструктуры) | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Да, в соответствии с Постановлением правительства №127  Нет, организация не относится к объектам КИИ  Нет | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Желаемый перечень работ по Положению 787-П / 779-П | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Аудит соответствия требованиям 787-П / 779-П  Разработка рекомендаций по приведению в соответствие 787-П / 779-П  Разработка необходимой организационно-распорядительной документации для соответствия 787-П / 779-П  Определение бизнес-процессов  Определение технологических процессов  Разработка модели угроз по новой методике ФСТЭК  Аудит организации в направлении обработки/защиты персональных данных  Тестирование на проникновение и анализа защищенности (пентест внешний/внутренний) | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Желаемый перечень сопутствующих работ | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Проведение тестирования на проникновение и анализа защищенности  Анализ платежного ПО по ОУД4  Разработка модели угроз по новой методике ФСТЭК  Аудит на соответствие требованиям 716-П, 719-П, 683-П, 802-П, иных источников требований ЦБ  Приведение в соответствие требованиям 716-П, 719-П, 683-П, 802-П, иных источников требований ЦБ  Аудит на соответствие требованиям ГОСТ 57580  Приведение в соответствие требованиям ГОСТ 57580  Полный цикл обследования объектов КИИ, помощь в категорировании и составление актов категорирования. | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Желаемый перечень иных работ | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Аудит организации в направлении обработки/защиты персональных данных  Аудит степени выполнения 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»  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!