**ОПРОСНЫЙ ЛИСТ ПО АУДИТУ  
СООТВЕТСТВИЯ ТРЕБОВАНИЯМИ 747-П, 683-П, 719-П**

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

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Цель проведения | | | обязательно |
|  | | | |
| Оценка действующей системы информационной безопасности  Подготовка к проверке регулятора | | | |
| Другое |  | | |
|  | *Указать* | | |
| *- выбрано;*  *- не выбрано* |  | | |
|  |  | | |
|  | | | |
| 1. Участвует ли организация в платёжной системе Банка России? | | | обязательно |
|  | | | |
| АРМ КБР-Н  СБП (быстрые платежи)  ССНП (срочные и несрочные платежи) | | | |
| Иное |  | | |
|  | *Указать* | | |
|  | | | |
| 1. Участвует ли организация в платёжной системе SWIFT Net? | | | обязательно |
|  | | | |
| Да | | Нет | |
|  | | | |
|  | | | |
| 1. Участвует ли организация в платёжных системах пластиковых карт? | | | обязательно |
|  | | | |
| Мир  Visa  JCB  MasterCard  UnionPay | | | |
| Иное |  | | |
|  | *Указать* | | |
|  | | | |
| 1. Если организация участвует в каких-либо других платёжных системах- укажите их | | | |
|  | | | |
|  | | | |
| *Указать* | | | |
|  | | | |
| 1. Имеются ли у организации собственные платёжные системы? | | | |
|  | | | |
| Да | | Нет | |
|  | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Роли проверяемой организации в платежных системах | | | обязательно |
|  | | | |
| Оператор платежной системы  Оператор по переводу денежных средств  Оператор услуг платежной инфраструктуры  Банковский платежный агент  Оператор услуг информационного обмена  Поставщики платежных приложений | | | |
|  | | | |
|  | | | |
| 1. Приложения по переводу денежных средств | | | |
|  | | | |
| **Роль** | | **Наименование** | |
|  | | | |
| АБС |  | | |
|  | | | |
| Интернет-банк (ДБО, веб-приложения) |  | | |
|  | | | |
| Мобильный банк (мобильные приложения) |  | | |
|  | | | |
| Процессинговое ПО |  | | |
|  | | | |
| Приложения сегмента SWIFT |  | | |
|  | | | |
| Иное |  | | |
|  | | | |
|  | | | |
| 1. Укажите количество | | | |
|  | | | |
| Банкоматы/платежные терминалы |  | | |
|  | | | |
| Банковские платёжные агенты |  | | |
|  | | | |
|  | | | |
| 1. Наименование средств защиты информации, применяемых в организации | | | обязательно |
|  | | | |
| Средство защиты от несанкционированного доступа |  | | |
|  | | | |
| Антивирусное программное обеспечение |  | | |
|  | | | |
| Средство межсетевого экранирования |  | | |
|  | | | |
| Средство криптографической защиты информации |  | | |
|  | | | |
| Средство обнаружения и предотвращения вторжений |  | | |
|  | | | |
| Средство контроля защищенности |  | | |
|  | | | |
| Средство мониторинга и анализ событий защиты информации |  | | |
|  | | | |
| Средство предотвращения утечек информации |  | | |
|  | | | |
| Иное |  | | |
|  | | | |
|  | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Дата и балл предыдущей оценки/самооценки | | | | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | | | | |
| **ГОСТ 57580** | | | | | | **Балл** | | | | | **Дата** | | | |
|  | | | | | | | | | | | | | | |
| Внешняя оценка | | | | |  | | | | |  | | | | |
|  | | | | | | | | | | | | | | |
| Самооценка | | | | |  | | | | |  | | | | |
|  | | | | | | | | | | | | | | |
| **382-П** | | | | | |  | | | | |  | | | |
|  | | | | | | | | | | | | | | |
| Внешняя оценка | | | | |  | | | | |  | | | | |
|  | | | | | | | | | | | | | | |
| Самооценка | | | | |  | | | | |  | | | | |
|  | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| 1. Имеется ли собственный отдел разработки ПО? | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| Да | | | | | | Нет | | | | | | | | |
|  | | | | | | | | | | | | | | |
| Если да, то укажите, для каких целей разрабатывается ПО | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| *Указать* | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| 1. Укажите количество человек в штате отдела информационной безопасности, включая филиалы | | | | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | | | | |
| Количество сотрудников ГО | | | | | | |  | | | | | | | |
|  | | | | | | | | | | | | | | |
| Количество в филиалах | | | | | | |  | | | | | | | |
|  | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| 1. Оцените степень документирования процессов ИТ и ИБ от 1 до 10 | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | | 6 | | 7 | 8 | | | 9 | | 10 |
|  | | | | | | | | | | | | | | |
| *1 - не документировано* | | | | | | *10 - документировано в полном объеме* | | | | | | | | |
|  | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| 1. Желаемый перечень работ по Положению 747-П | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| Предварительная оценка соответствия ГОСТ Р 57580.1–2017  Разработка рекомендаций по приведению в соответствие ГОСТ Р 57580.1–2017  Разработка необходимой организационно-распорядительной документации для соответствия ГОСТ Р 57580.1–2017 | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| 1. Желаемый перечень работ по Положению 683-П | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| Предварительная оценка соответствия ГОСТ Р 57580.1–2017  Разработка рекомендаций по приведению в соответствие ГОСТ Р 57580.1–2017  Разработка необходимой организационно-распорядительной документации для соответствия ГОСТ Р 57580.1–2017  Итоговая оценка с подготовкой отчетной документации для Банка России по ГОСТ Р 57580.2–2018  Оценка соответствия общим требованиям 683-П (*ПДн* – 152-ФЗ, постановление Правительства 1119, 21 приказ ФСТЭК, *СКЗИ* – ПКЗ-2005, 378 приказ ФСБ, 63-ФЗ)  Разработка необходимой организационно-распорядительной документации для соответствия общим требованиям 683-П (*ПДн* – 152-ФЗ, постановление Правительства 1119, 21 приказ ФСТЭК, *СКЗИ* – ПКЗ-2005, 378 приказ ФСБ, 63-ФЗ) | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |

|  |  |  |
| --- | --- | --- |
| 1. Желаемый перечень работ по Положению 719-П | | |
|  | | |
| Предварительная оценка соответствия ГОСТ Р 57580.1–2017  Разработка рекомендаций по приведению в соответствие ГОСТ Р 57580.1–2017  Разработка необходимой организационно-распорядительной документации для соответствия ГОСТ Р 57580.1–2017  Итоговая оценка с подготовкой отчетной документации для Банка России по ГОСТ Р 57580.2–2018  Оценка соответствия общим требованиям 719-П (технологические меры защиты информации, применение СКЗИ) | | |
|  | | |
|  | | |
| 1. Желаемый перечень сопутствующих работ | | |
|  | | |
| Проведение тестирования на проникновение и анализа защищенности  Анализ платежного ПО по ОУД4  Разработка модели угроз по новой методике ФСТЭК  Приведение в соответствие требованиям 716-П  Аудит организации в направлении обработки/защиты персональных данных  Независимая внешняя оценка SWIFT | | |
|  | | |
|  | | |
| 1. Желаемый перечень иных работ | | |
|  | | |
| Аудит соответствия требованиям ISO 27001  Аудит степени выполнения 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» | | |
|  | | |
|  | | |
| 1. Желаемая оценка | | обязательно |
|  | | |
| 0,7  0,85  0,95  Фактическая (реальная) | | |
|  | | |
|  | | |
| 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!