**АНКЕТА ПО ПЕРСОНАЛЬНЫМ ДАННЫМ**

**(НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ 152-ФЗ)**

|  |  |
| --- | --- |
|  | |
| Наименование организации/Банка |  |
|  | |
| Контактное лицо |  |
|  | |
| Телефон |  |
|  | |
| E-mail |  |
|  | |
| Дата заполнения |  |
|  | |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Цель проведения | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Оценка действующей системы информационной безопасности  Подготовка к проверке регулятора  Требования партнеров | | | | | | | | | | | |
| Другое | | | | |  | | | | | | |
|  | | | | | *Указать* | | | | | | |
| *- выбрано;*  *- не выбрано* | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Укажите количество человек в штате отдела информационной безопасности | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| *Указать* | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Назначены ли ответственные за защиту ПДн? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Да | | | | | | Нет | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Укажите количество территорий (зданий, филиалов) в области оценки и их адреса | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| **Территория** | | | | | | **Адрес** | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Определены ли бизнес-процессы, которые задействованы в обработке ПДн? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Да | | | | | | Нет | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Перечень бизнес-процессов, которые задействованы в обработке ПДн | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| *Указать* | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Укажите количество субъектов (сотрудников, клиентов), чьи ПДн обрабатываются | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Количество сотрудников: | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Количество клиентов: | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Какие категории ПДн обрабатываются ? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Общедоступная информация (персональные данные, находящиеся в общедоступных источниках)  Биометрические (внешность, голос)  Специальные (раса, национальность, политические взгляды, состояние здоровья) | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. ПДн каких субъектов обрабатывает Организация? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Сотрудники Организации  Клиенты/контрагенты Организации (лица, с которыми заключен договор ГПХ)  Третьи лица | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Список информационных систем, обрабатывающих ПДн | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| *Указать* | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Функционируют ли в организации государственные информационные системы (ГИС) | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Да | | | | | | Нет | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Список государственных информационных систем, обрабатывающих ПДн | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| *Указать* | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Какие из перечисленных информационных систем находятся за границей (осуществляется ли трансграничная передача ПДн), в каких странах? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| **Информационная система** | | | | | | **Страна** | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Укажите количество серверов, на которых обрабатываются ПДн | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| *Указать (с точностью до порядка)* | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Укажите количество автоматизированных рабочих мест (АРМ), на которых осуществляется обработка ПДн | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| *Указать (с точностью до порядка)* | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Перечень средств защиты (антивирусы, межсетевые экраны, SIEM, DLP, СЗИ от НСД) информации применяются для обеспечения безопасности ПДн | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Антивирусное программное обеспечение: | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Средство защиты от несанкционированного доступа: | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Средство межсетевого экранирования: | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Средство мониторинга и анализ событий защиты информации: | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Средство предотвращение утечек информации (DLP): | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Средство криптографической защиты информации: | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Средство контроля защищенности: | | | | |  | | | | | | |
|  | | | | | | | | | | | |
| Другое: | | | | |  | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Используются ли СКЗИ для защиты ПДн? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Да | | | | | | Нет | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Действует ли в Организации модель угроз ПДн? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Да | | | | | | Нет | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Введена ли в действие политика обработки ПДн, политика защиты ПДн, политика информационной безопасности (ИБ)? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Да | | | | | | Нет | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Действует ли в Организации иная организационно-распорядительная документация в направлении защиты ПДн? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Да | | | | | | Нет | | | | | |
|  | | | | | | | | | | | |
| Если да, то укажите какая | | | | | | | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| *Указать* | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Определён ли уровень защищенности ПДн в информационных системах? | | | | | | | | | | обязательно | |
|  | | | | | | | | | | | |
| Да | | | | | | Нет | | | | | |
|  | | | | | | | | | | | |
|  | | | | | | | | | | | |
| 1. Оцените степень документирования процесса защиты ПДн (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 в направлении защиты ПДн | |
|  | |
| Определение бизнес-процессов, задействованных в процессе обработки ПДн  Правовая оценка системы организации обработки персональных данных  Определение целей обработки, состава обрабатываемых ПДн, порядка обработки ПДн, а также мест и форм хранения ПДн (представленных как на электронном, так и на бумажном носителе) у Заказчика  Обследование реализованных у Заказчика технических и организационных мер защиты ПДн, применяемых при неавтоматизированной обработке ПДн  Разработка рекомендаций по приведению процессов обработки ПДн в соответствие требованиям ФЗ №152, Приказу ФСТЭК России от 18 февраля 2013 г. N 21 и Постановлению Правительства РФ от 1 ноября 2012 г. N 1119  Определение перечня АС, используемых для обработки ПДн в рамках каждого идентифицированного бизнес-процесса  Сбор информации о конфигурации каждой АС, обрабатывающей ПДн, используемых технологиях обработки ПДн, а также топологии сети  Анализ внутренних нормативных документов Заказчика в областях обработки ПДн и информационной безопасности  Обследование реализованных у Заказчика технических и организационных мер защиты ПДн, применяемых при автоматизированной обработке ПДн  Разработка организационно-распорядительной документации в соответствии 152-ФЗ | |
|  | |
|  | |
| 1. Желаемый перечень сопутствующих работ | |
|  | |
| Выстроить систему управления операционными рисками и рисками информационной безопасности в соответствии с требованиями Положения Банка России 716-П  Определение ВНД в рамках обеспечения операционной надежностью в соответствии с требованиями Положения Банка России 787-П (779-П) | |
|  | |
|  | |
| 1. Поставка технических решений (ПО, ПАК) ИБ/ИТ и СУОР | |
|  | |
| Планируется ли поставка решений ИБ/ИТ, СУОР?  Требуется ли консультация по вопросам поставки и внедрения решений ИБ/ИТ, СУОР? | |
|  | |
| Какие решения по ИБ/ИТ, СУОР Вами рассматриваются? |  |
|  | *Указать* |
|  | |
|  | |

Спасибо!

На основании заполненной анкеты сформируем коммерческое предложение и отправим Вам ответным письмом