|  |  |  |  |
| --- | --- | --- | --- |
|  | **Поле** | **Заполнение** | **Пояснение или пример** |
| **1** | **Организация** | | |
| 1.1 | Наименование организации |  |  |
| 1.2 | Является ли членом холдинга или группы компаний |  | *152-ФЗ не знает понятия «группа компаний». Т.о. передачу ПДн внутри группы компаний нужно оформлять также, как и передачу подрядчикам.* |
| **2** | **Контактное лицо** | | |
| 2.1 | ФИО |  | *Возможно понадобится для уточняющих вопросов* |
| 2.2 | Должность |  |  |
| 2.3 | Телефон |  |  |
| 2.4 | e-mail |  |  |
| **3** | **Описание процессов обработки данных** | | |
| 3.1 | Сфера деятельности организации |  |  |
| 3.2 | Какие процессы требуется привести в соответствие? |  | *В соответствие приводятся не сервера, но бизнес-процессы.*  *Укажите пожалуйста: какие процессы нужно привести в соответствие. Например:*  *- регистрацию и заказы в интернет-магазине;*  *- работу с данными сотрудников подрядчика;*  *- собственное кадровое делопроизводство;* |
| 3.3 | Передаются ли в этих бизнес-процессах данные клиентов подрядчикам?  Какие или зачем? |  | *Например, данные покупателей интернет-магазина курьерам логистической компании* |
| 3.4 | Есть ли сайт организации или приводимого в соответствие процесса? Какой? |  |  |
| **4** | **Описание системы обработки персональных данных** | | |
| 4.1 | Укажите примерный перечень ИТ-систем и серверов, из которых состоит система |  | *Например:*  *- собственное кадровое делопроизводство: 1 терминальный сервер (под Windows) и 1 сервер приложения и БД (Windows + MS SQL)*  *- система обслуживания клиентов: frontend на Linux + NGINX, плюс сервер приложений под Linux плюс кластер БД под My SQL* |

|  |  |  |  |
| --- | --- | --- | --- |
| 4.2 | Какой тип угроз актуален для информационных систем? |  | *Определяется в соответствии с Постановлением Правительства РФ №1119*  *3-й тип угроз позволяет реализовать систему защиты с наименьшими затратами, поэтому обычно, если нет явных и обоснованных внешних требований, то мы считаем актуальным 3-й тип угроз* |
| 4.3 | Какие типы данных обрабатываются? | |  |
| 4.3.1 | Обрабатываются ли Специальные данные? |  | ***Специальные****: медицинские данные, данные о судимостях, данные об интимной жизни, вероисповедании, расовой принадлежности.*  *Да\нет* |
| 4.3.2 | Обрабатываются ли Биометрические данные? |  | ***Биометрические****: данные, используемые с целью биометрической идентификации.*  *Да\нет* |
| 4.3.3 | Обрабатываются ли иные данные? |  | ***Иные****: паспортные данные, номера СНИЛС, ИНН, прав, контактные данные: адрес, телефон и прочее.*  *Да\нет* |
| 4.4 | Количество людей, данные которых обрабатываются |  | *Более 100 000, или менее 100 000* |
| 4.5.1 | Обрабатываются ли данные собственных сотрудников |  | *Да\нет* |
| 4.5.2 | Обрабатываются ли данные прочих субъектов |  | *НЕ сотрудников*  *Да\нет* |
| 4.6 | Необходима ли интеграция с государственной информационной системой (ГИС) |  | *Актуально, преимущественно, для медицинских организаций – в части интеграции с ЕГИСЗ* |
| 4.6.1 | Если необходима интеграция с ГИС – есть ли требования к классу системы |  | *Требования к защите ГИС (17-й приказ ФСТЭК России). Обозначаются как К1\К2\К3* |
| **5** | **Ожидаемые результаты проекта** | | |
| 5.1 | Аудит, разработка рекомендаций и ОРД,  Приведение в соответствие |  | ***Стандартная услуга*** *приведения в соответствие. Подходит большинству заказчиков.*  *Да\нет* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5.2 | Проведение аттестации |  | | *НЕ обязательная мера.*  *Включает проведение испытаний и выдачу аттестата соответствия.*  *Запрещает изменение системы.*  *Да\нет* |
| 5.3 | Иное |  | | *Укажите пожалуйста ваши специальные требования* |
| **6** | **Уже реализованные этапы** | | | |
| 6.1 | Укажите, какие из нижеперечисленных работ уже выполнены в Организации | | | *Если ранее делалась подобный проект* |
| 6.1.1 | Назначены лица, ответственные за организацию обработки персональных данных | |  | *Да\нет* |
| 6.1.2 | Назначены лица, ответственные за обеспечение безопасности персональных данных | |  | *Да\нет* |
| 6.1.3 | Определен перечень обрабатываемых персональных данных | |  | *Да\нет* |
| 6.1.4 | Определен перечень подразделений и лиц, допущенных к работе с персональными данными | |  | *Да\нет* |
| 6.1.5 | Выделены информационные системы персональных данных | |  | *Да\нет* |
| 6.1.6 | Проведена оценка вреда, который может быть причинен субъектам в случае нарушения безопасности их персональных данных | |  | *Да\нет* |
| 6.1.7 | Разработана модель угроз безопасности персональных данных для каждой информационной системы | |  | *Да\нет* |
| 6.1.8 | Определены уровни защищенности для каждой из информационных систем персональных данных | |  | *Да\нет* |
| 6.1.9 | Направлено уведомление об обработке персональных данных в Роскомнадзор | |  | *Да\нет* |
| 6.1.10 | Проведено обучение лиц, осуществляющих обработку персональных данных | |  | *Да\нет* |