**ПРЕДВАРИТЕЛЬНЫЙ ОПРОСНЫЙ ЛИСТ**

**ДЛЯ ОЦЕНКИ СТОИМОСТИ ПРОЕКТА ПО СОЗДАНИЮ/МОДЕРНИЗАЦИИ**

**СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**ОБЩИЕ СВЕДЕНИЯ**

**о \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

 **(наименование организации)**

1. **Общая информация об организации**

**Таблица 1.1.**

| **№ п/п** | **Вопрос** | **Ответ** | **Примечания** |
| --- | --- | --- | --- |
|  | Полное наименование организации(сокращенное наименование организации) |  |  |
|  | Адрес web-сайта организации в сети Интернет |  | Указать, если есть. Если организация является дочерней, то дополнительно необходимо указать web-адрес головной организации |
|  | Виды деятельности организации, связанные с обработкой персональных данных |  |  |
|  | Структура информационной системы (ИС) |  | Автономное АРМ / ЛВС / распределенная ИС |
|  | Трансграничная передача персональных данных (ПДн)[[1]](#footnote-1) |  | Если да, то указать название страны / стран |
|  | Существуют ли базы персональных данных (серверы) за рубежом |  | Если да, то указать название страны, количество баз персональных данных (серверов), состав ПДн в базах (на серверах) |
|  | Наличие лицензий, связанных с деятельностью по защите информации |  | Лицензии ФСТЭК, ФСБ |
|  | Перечень сторонних организаций, с которыми осуществляется информационный обмен сведениями, содержащими ПДн |  | ПФР, ФНС, ФМС и др. |
|  | ФИО и должность лица, ответственного за защиту (обработку) персональных данных |  | Указать участвует ли данное лицо в планируемом проекте по созданию системы защиты персональных данных |
|  | Существуют ли в организации документы по защите персональных данных (ЗПДн) |  | Если да, указать:* какие стадии проекта были выполнены (обследование, техническое проектирование, поставка средств защиты информации (СЗИ), внедрение СЗИ, разработка организационно-распорядительной документации (ОРД), аттестация)
* наименования и количество листов разработанных ОРД
* год, в котором были выполнены работы
 |
|  | Требуется разработка комплекта документов по ЗПДн «с нуля» или доработка существующего комплекта |  |  |
|  | Количество структурных подразделений, участвующих в обработке ПДн |  | Указать наименования и общее количество структурных подразделений, участвующих в обработке ПДн |
|  | Осуществляется ли неавтоматизированная (на бумажных носителях) обработка ПДн в организации |  | Если да, указать процессы, в рамках которых осуществляется неавтоматизированная обработка ПДн |
|  | Является ли организация российской или аффилирована с зарубежной компанией |  | В случае, если организация аффилирована с зарубежной компанией, указать:* страну, где находится головной офис
* порядок управления информационной инфраструктурой (централизованно из головного офиса / локально)
* являются ли все внутренние нормативные документы головного офиса едиными для всех дочерних организаций
 |
|  | Перечень интересующих работ |  | Указать интересуемые работы:* Предпроектное обследование с формированием отчета
* Моделирование угроз
* Техническое проектирование (ТЗ, ТП)
* Поставка СЗИ
* Макетирование
* Внедрение СЗИ
* Разработка эксплуатационной документации
* Разработка ОРД
* Аттестация (не является обязательной)
 |

1. **Перечень информационных систем персональных данных (ИСПДн)**

***ИСПДн - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств***

**Таблица 2.1.**

| **№ п/п** | **Наименование системы[[2]](#footnote-2)** | **Описание и назначения системы** | **Перечень сведений, отнесенных к ПДн[[3]](#footnote-3)** | **Количество обрабатываемых субъектов ПДн[[4]](#footnote-4)** | **Категории субъектов ПДн[[5]](#footnote-5)** | **Нахождение технических средств** **(в пределах РФ/частично за пределами РФ)** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. **Подробное описание территориально разделенных площадок, на которых происходит обработка ПДн
(офисы, филиалы, отделения, удаленные рабочие места и т.п.)**

**Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.**

**Таблица 3.1.**

| **№ п/п** | **Название площадки**  | **Количество рабочих станций** | **Количество серверов[[6]](#footnote-6)** | **ИСПДн на площадке[[7]](#footnote-7)** | **Количество подключений к сети Интернет[[8]](#footnote-8)** | **Обеспечение физической охраны помещений[[9]](#footnote-9)** | **Адрес площадки** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Всего** | **Связанных с обработкой ПДн** | **Всего** | **Связанных с обработкой ПДн** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

1. **Технологическая информация по площадкам**

**Таблица 4.1.**

| **№ п/п** | **Площадка** | **Рабочие станции** | **Серверы** | **Наличие Active Directory (возможно ли расширение)****Количество доменов** | **Средства защиты: состав и количество****(указать наличие сертификата[[10]](#footnote-10) ФСБ/ФСТЭК)** |
| --- | --- | --- | --- | --- | --- |
| **Общесистемное ПО[[11]](#footnote-11)** | **Прикладное ПО [[12]](#footnote-12)** | **Общесистемное ПО[[13]](#footnote-13)** | **Прикладное ПО[[14]](#footnote-14)** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

*При использовании средств виртуализации для обработки ПДн заполнить Таблицу 4.2.[[15]](#footnote-15)*

**Таблица 4.2.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Технология виртуализации сегмента[[16]](#footnote-16)** | **Версия платформы** | **Хосты виртуализации (гипервизоры), входящие в сегмент с обработкой ПДн** | **Количество виртуальных машин с обработкой ПДн** | **Перечень ИСПДн, в которых используется данный сегмент виртуализации** |
| **общее количество** | **суммарное количество процессоров** |
|  | *VMWare (production)* | *5.0 или 5.5 или 6.0…* |  |  |  |  |
|  | *VMWare (test)* | *5.5* |  |  |  |  |
|  | *Hyper-V* | *2012 или 2012 R2* |  |  |  |  |

*При использовании «облачных» сервисов для обработки ПДн заполнить Таблицу 4.3.*

**Таблица 4.3.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование ИСПДн** | **Тип «облака» (частное/публичное)** | **Поставщик «облачного» сервиса (хостинг-провайдер)** | **Место размещения ЦОД хостинг-провайдера (страна)** | **Тип «облачного» сервиса** **(collocation, SaaS, PaaS, IaaS)** | **Наименование «облачного» сервиса[[17]](#footnote-17)** | **Какие ПДн передаются в «облако»** | **Используемые средства защиты, состав и количество[[18]](#footnote-18)** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

1. Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу. [↑](#footnote-ref-1)
2. Примеры типичных ИСПДн: системы кадрового учета, бухгалтерские системы, системы учета клиентов и партнеров / CRM-системы, биллинговые системы, системы, обеспечивающие работу call-центров, cистемы электронного документооборота, содержащего ПДн, автоматизированные банковские системы, скоринговые системы и др.; [↑](#footnote-ref-2)
3. ФИО, дата рождения, место жительства, должность, образование, семейное положение, социально-имущественное положение, профессия, финансы, расовая принадлежность, политические взгляды, религиозные и философские убеждения, состояния здоровья, вопросы интимной жизни и т.п.; [↑](#footnote-ref-3)
4. Общее количество одновременно обрабатываемых записей о субъектах ПДн в данной системе (менее 100 000 субъектов в системе или более); [↑](#footnote-ref-4)
5. Сотрудники организации, клиенты, физ. лица, определенные в законе, на основании которого происходит обработка ПДн. [↑](#footnote-ref-5)
6. Указать количество физических серверов, в том числе количество лезвий блейд-сервера. В данное количество не нужно включать физические серверы, используемы для виртуализации, а также виртуальные серверы. Они указываются в Таблице 4.2; [↑](#footnote-ref-6)
7. Указать какие ИСПДн из п. 2 располагаются на технологической площадке; [↑](#footnote-ref-7)
8. Указать количество входящих каналов связи для площадки; [↑](#footnote-ref-8)
9. Охрана, предусматривающая контроль доступа в здания, помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации, пожарная и охранная сигнализация. [↑](#footnote-ref-9)
10. Наличие лицензии на продукт не означает, что он сертифицирован, необходим сертификат, подтверждающий соответствие продукта требованиям в области информационной безопасности; [↑](#footnote-ref-10)
11. ОС (Windows 95/98/2000/XP/Vista/7, Linux и т.п.); [↑](#footnote-ref-11)
12. 1С Бухгалтерия, 1С Зарплата и Кадры, используемые антивирусы, программные средства защиты и т.п.; [↑](#footnote-ref-12)
13. ОС (Windows Server 2003/2008/2008 R2 и т.п.); [↑](#footnote-ref-13)
14. MS SQL, Firebird, Oracle и т.п.; [↑](#footnote-ref-14)
15. В таблице приведены примеры заполнения; [↑](#footnote-ref-15)
16. Каждый сегмент виртуализации, управляемый, например, своим отдельным VMWare vCenter, отражается отдельной строкой. [↑](#footnote-ref-16)
17. Какая услуга предоставляется; [↑](#footnote-ref-17)
18. Указать наличие сертификата ФСБ/ФСТЭК. [↑](#footnote-ref-18)