ОБЩАЯ ИНФОРМАЦИЯ О ЗАКАЗЧИКЕ		
1.	Заказчик: (*полное и сокращенное наименование Организации-Заказчика услуг*)	
2.	Сфера деятельности Организации:	
3.	Зарегистрирована ли Организация в качестве оператора персональных данных?	
4.	Официальный web-сайт Организации:	

СВЕДЕНИЯ ОБ ОБЛАСТИ ПРОЕКТА		
Общее описание инфраструктуры и применяемых технологий		
5.	**Технологические площадки и офисы, включая внешние ЦОД** *Количество, типы (офис, ЦОД, …), адрес расположения (город/область)*	
6.	**Серверы** *Количество серверов с указанием типа (физ., вирт.) и места расположения (офис, собственный ЦОД, внешний ЦОД)*	
7.	**Рабочие АРМ работников** *Количество АРМ с указанием адреса площадки (офиса) или указанием статуса удаленного работника*	
8.	**Рабочие АРМ внештатных работников** *Количество АРМ с указанием адреса площадки (офиса) или указанием статуса удаленного работника*	
9.	**Рабочие АРМ разработчиков** *Количество АРМ с указанием адреса площадки (офиса) или указанием статуса удаленного работника*	
10.	**Рабочие АРМ администраторов** *Количество АРМ с указанием адреса площадки (офиса) или указанием статуса удаленного работника*	
11.	**Коммутаторы** *Количество коммутаторов с указанием площадки (офиса)*	
12.	**Каналы связи** *Опишите применяемые технологии. Укажите количество провайдеров и предоставляемую ими производительность*	
13.	**Количество настроенных правил МЭ** *Укажите количество правил настроенных в МЭ*	
14.	**Есть ли обособленное подразделение ИТ, отвечающее за сетевую инфраструктуру** *Да/нет*	
15.	**Есть ли обособленное подразделение ИБ, отвечающее за сетевую инфраструктуру** *Да/нет*	
16.	**Системное программное обеспечение** *Опишите используемое системное ПО*	

17.	**Виртуализация** *Опишите применяемые технологии*	
18.	**Удаленный доступ к ИТ-инфраструктуре работников организации** *В каких случаях лица, не являющиеся работниками организации могут получить доступ к объектам информационной инфраструктуры* *Опишите применяемые технологии для реализации уделенного доступа, его контроля и обеспечения безопасности*	
19.	**Удаленный доступ к ИТ-инфраструктуре лиц, не являющихся работниками** *В каких случаях лица, не являющиеся работниками организации могут получить доступ к объектам информационной инфраструктуры* *Опишите применяемые технологии для реализации уделенного доступа, его контроля и обеспечения безопасности*	
20.	**Мобильные устройства** *Опишите допустимые к применению в работе мобильные устройства, а также применяемые технологии для реализации контроля их применения и обеспечения безопасности*	
21.	**Резервирование** *Опишите применяемые технологии, применяемые меры для контроля и обеспечения безопасности*	
22.	**Резервное копирование и восстановление** *Опишите применяемые технологии, применяемые меры для контроля и обеспечения безопасности*	
Общие сведения об организационной структуре		
23.	**Структурные подразделения внутри компании** *Общее количество структурных подразделений с указанием территориальной площадки, в рамках которой функционирует подразделение, а также типа площадки*	
24.	**Отделы/Службы ИТ и ИБ** *Выделены ли в структуре компании целевые структурные подразделения, реализующие функции ИТ и ИБ, назначены ли руководители и работники внутри подразделений?*	
25.	**Кураторы ИТ и ИБ** *Каким образом осуществляется курирование деятельности ИТ и ИБ направлений, исключен ли конфликт интересов?*	
26.	**Факт назначения на роль ответственного за ИБ представителя руководства** *Назначен ли на роль ответственного за ИБ заместителя руководителя организации?*	
Регламентирование деятельности ИТ и ИБ в компании		
27.	**Документирование ИТ-процессов** *Разработана ли, внедрена ли и контролируется ли выполнение внутренней нормативной документации в области ИТ?*	
28.	**Документирование ИБ-процессов**	

	Разработана ли, внедрена ли и контролируется ли выполнение внутренней нормативной документации в области ИБ?	
29.	**Процедуры внутреннего аудита и контроля** *Каким образом осуществляется контроль деятельности и совершенствование ИТ-процессов?*	
30.	**Процедуры внешнего аудита и контроля** *Каким образом осуществляется контроль деятельности и совершенствование ИБ-процессов?*	
31.	**Наличие внутренних или внешних регуляторных требований в области ИТ и ИБ** *Обязательства по обеспечению соответствия требованиям регламентов и/или стандартов (внутри компании/холдинга/группы), включая отраслевые*	
32.	**Выделение бюджетов для направлений ИТ и ИБ в компании** *Практикуется ли наделение полномочиями и бюджетами направлений ИТ и ИБ*	
Обрабатываемая информация		
33.	**Конфиденциальная информация (информация, отнесенная к какой-либо тайне)** *Осуществляется ли обработка информации ограниченного распространения (разного уровня)?*	
34.	**Категорирование защищаемой информации** *Осуществляется ли категорирование и учет информационных активов и информации, подлежащей защите?*	
35.	**Управление ресурсами и информационными потокам** *Реализованы ли каким-либо образом процессы управления и контроля информационных потоков (в части конфиденциальной информации, отнесенной к коммерческой тайне)?* *Если да, опишите, пожалуйста* *- организационные меры* *- технические меры*	
36.	**Персональные данные** *Реализованы ли каким-либо образом процессы управления и контроля информационных потоков (в части персональных данных)?* *Если да, опишите, пожалуйста* *- организационные меры* *- технические меры*	
37.	**Доступ к информации различных категорий** *Реализованы ли принципы разграничения доступа к информационным ресурсам?* *Если да, опишите, пожалуйста* *- организационные меры* *- технические меры*	

ИНФОРМАЦИЯ ОБ ИНФОРМАЦИОННЫХ СИСТЕМАХ ЗАКАЗЧИКА

38.	*(не обязательно)* Укажите требуемый класс защищенности ИС *Если система является ГИС, укажите реквизиты соответствующего НПА (решение о создании ГИС), а также опишите назначение и цель создания ГИС.*	☐	КЗ-3 (низкий)
		☐	КЗ-2
		☐	КЗ-1 (высокий)
		[подробный комментарий, при необходимости]	
39.	*(не обязательно)* Укажите требуемый уровень защищенности ПДн в ИС	☐	4 уровень защищенности (низкий)
		☐	3 уровень защищенности
		☐	2 уровень защищенности
		☐	1 уровень защищенности (высокий)
		[подробный комментарий, при необходимости]	

ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ПРОЕКТА		
40.	Какие результаты Заказчик ожидает получить по окончанию проекта?	
	☐	Оценка текущего защищенности информационных активов, безопасности информационной инфраструктуры и защищенности объектов информатизации.
	☐	Формирование перечня информационных активов, подлежащих защите.
	☐	Категорирование защищаемых информационных активов, формирование матрицы уровней защищенности.
	☐	Определение перечня законодательных и отраслевых требований, которые необходимы к реализации для защиты тех или иных категорий информационных активов.
	☐	Описание информационных потоков и формирование перечня информационных систем (внутренних и внешних), задействованных в обработки защищаемых информационных активов.
	☐	Оценка актуальных угроз безопасности информации, обрабатываемой в информационных системах, проектирование комплексной системы защиты.
	☐	Создание комплекса регламентов и ОРД, регламентирующих правила обработки информации и обеспечения информационной безопасности информационных активов.
	☐	Комплект внутренних нормативных документов и организационно-распорядительных документов, регламентирующих порядок обеспечения безопасности конфиденциальной информации при осуществлении её обработки в компании.
	☐	Разработка/Актуализация Модели угроз безопасности данных, обрабатываемых в информационной системе и модели нарушителя.
	☐	Разработка/Актуализация Технического задания на создание системы защиты данных
	☐	Разработка/Актуализация пакета организационно-распорядительной документации, обеспечивающего выполнение требований по документационному обеспечению в области обработки и защиты данных
	☐	Разработка/Актуализация Технического проекта системы защиты данных
	☐	Внедрение технических средств защиты информации в соответствии с выбранным проектным решением СЗПДн
	☐	Оценка эффективности реализованных мер в рамках системы защиты персональных данных
	☐	Аттестация информационной системы
	☐	Другое: