**Запрос информации по Проекту**

**«Проведение комплексного аудита информационной безопасности и приведение процессов обработки и защиты персональных данных (ПДн) в соответствии с новыми требованиями законодательства для ПАО АФК «Система»»**

**Обзор проекта:**

ПАО АФК «Система» рассматривает возможность реализации проекта **«Проведение комплексного аудита информационной безопасности, процессов обработки и защиты персональных данных (ПДн) в соответствии с новыми требованиями законодательства для АФК «Система»» (далее – «Проект»).**

Требования к составу и содержанию работ указаны в Требованиях (Приложение 2) к настоящему документу.

**Планируемый график реализации Проекта:**

ПАО АФК «Система» планирует начать работы в декабре 2022 года, а завершить их не позднее 1 полугодия 2023 года.

**Предложение и процесс запроса информации:**

Мы ожидаем получить краткое предложение, которое должно включать:

* порядок проведения и описание работ по проведению Проекта в разрезе выполнения основных требований – в формате презентации/пояснительной записки (на выбор);
* предполагаемый объем необходимых работ с оценкой трудозатрат по каждому из этапов (в чел./час.) – в формате Приложения 1, лист «Основные этапы и Ценовое предложение»;
* предложение по цене (в рублях) с учетом применимого НДС, с указанием стоимости по каждому из этапов – в формате Приложения 1, лист «Основные этапы и Ценовое предложение»;
* краткий обзор аналогичных/сопоставимых реализованных проектов;
* данные о ключевых членах предполагаемой проектной команды с указанием их профессионального опыта и функциональных ролей в Проекте – в формате Приложения 1, лист «Команда проекта».

**ВНИМАНИЕ!!!** Подача документов осуществляется Участником в электронном виде через электронно-торговую площадку (далее - «ЭТП») по адресу http://utp.sberbank-ast.ru/VIP/List/PurchaseList/358 в соответствии с регламентом и инструкцией для Участников торговой секции «Закупки и продажи» универсальной торговой платформы «Сбербанк-АСТ», ознакомиться с которыми можно на сайте <http://utp.sberbank-ast.ru/VIP/Notice/752/Information>.

Срок окончания подачи документов на участие и коммерческих предложений «16» ноября 2022г. до 15.00 часов (МСК). **Документы и предложения, поданные после указанного срока, ЭТП не принимаются.**

**Общий объем Аудита:**

Количество площадок, планируемых к обследованию – 2 (г. Москва)

Оценочное количество обследуемой инфраструктуры:

* Внешние IP-адреса – не более 20;
* Пользователи – не более 300;
* Рабочие станции – не более 500.
* Сервера – не более 120.
* ИС – не более 25.

Вы можете направить интересующие Вас вопросы следующим контактным лицам:

|  |  |
| --- | --- |
| **Зайцев Алексей**  ПАО АФК «Система»  Директор по эксплуатации систем информационной безопасности  Тел.: +7 495 692 10 88, доб. 50390  Email: a.zaytsev@sistema.ru |  |

**Важная информация (Disclaimer)**

ПАО АФК «Система» уведомляет, что настоящий запрос информации не должен расцениваться потенциальными исполнителями в качестве публичной оферты ПАО АФК «Система». ПАО АФК «Система» не несет никаких обязательств перед компаниями, принявшими участия в данном запросе информации, и может прекратить проект в любой момент времени.

**Приложения:**

Приложение 1. Анкета участника и форма ценового предложения



Приложение 2. Требования к проведению комплексного аудита информационной безопасности и приведение процессов обработки и защиты персональных данных (ПДн) в соответствии с новыми требованиями законодательства для ПАО АФК «Система»».

**Приложение 2**

**Технические требования**

**к** **проведению комплексного аудита информационной безопасности и приведение процессов обработки и защиты персональных данных (ПДн) в соответствии с новыми требованиями законодательства для ПАО АФК «Система»**

1. **Общие положения**
   1. Наименование работ

Полное наименование: комплексный аудит информационной безопасности и приведение процессов обработки и защиты персональных данных (ПДн) в соответствии с новыми требованиями законодательства для ПАО АФК Система».

* 1. Цели проведения работ

Основными целями реализации Проекта являются:

получение объективной и независимой оценки текущего уровня информационной безопасности (далее – ИБ) информационных систем (далее – ИС) Заказчика, получение рекомендаций по его повышению;

анализ процессов обеспечения информационной безопасности, выявление и практическая верификация киберрисков;

разработка системы защиты персональных данных (СЗПДн) для приведения процессов обработки и защиты персональных данных (ПДн) Заказчика в соответствие требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и требованиям регулирующих органов в области защиты ПДн (Роскомнадзор, ФСТЭК России, ФСБ России).

* 1. Задачи проведения работ по проекту

Достижение указанных целей обеспечивается решением следующих задач:

оценка защищенности внешнего периметра ИТ инфраструктуры от действий внешнего нарушителя;

оценка защищенности беспроводных сетей от действий внешнего нарушителя;

оценка текущего уровня осведомлённости сотрудников Заказчика в вопросах обеспечения информационной безопасности;

оценка защищенности внутренней ИТ инфраструктуры от действий внешнего нарушителя;

сбор и анализ исходных данных об информационных системах, используемых средствах защиты информации и процессах ИБ;

оценка текущего уровня зрелости процессов обеспечения ИБ;

выявление фактов неполного или некорректного выполнения требований законодательства РФ в области обработки ПДн и проведение мероприятий, необходимых для их устранения;

выявление всех ИСПДн Заказчика, определение уровня защищенности ПДн в соответствии с действующим законодательством;

определение возможных нарушителей и угроз безопасности ПДн при их обработке в ИСПДн Заказчика;

разработка технического задания на создание СЗПДн Заказчика;

разработка комплекта проектной документации на создание СЗПДн в объёме, необходимом для успешного внедрения СЗИ и их дальнейшей эксплуатации СЗПДн;

разработка/доработка комплекта организационно-распорядительной документации, необходимой в соответствии с требованиями регулирующих органов (постановлений Правительства, требований Роскомнадзора, приказов ФСТЭК России, ФСБ России).

разработка рекомендаций по повышению уровня ИБ ИС, включая дорожную карту.

1. **Состав и содержание работ**

Работы должны проводиться в три этапа в следующем порядке:

Этап 1. Технический анализ защищенности.

Этап 2. Приведение процессов обработки и защиты персональных данных в соответствии с новыми требованиями законодательства;

Этап 3. Аудит процессов обеспечения информационной безопасности.

обследование ИС, включая интервьюирование владельцев ключевых бизнес‑процессов и сбора свидетельств в части обеспечения защиты информации и оценки рисков;

оценка соответствия текущего уровня зрелости процессов обеспечения ИБ применимым требованиям регуляторов и международным стандартам по информационной безопасности и количественная оценка рисков ключевых бизнес-процессов;

технический анализ защищенности активов ИТ инфраструктуры;

построение карты основных рисков и угроз, их ранжирование по величине потенциального ущерба;

актуализация корпоративного стандарта по информационной безопасности ПАО АФК «Система»;

разработка рекомендаций по повышению уровня ИБ и Стратегии развития ИБ;

перепроверка устранения выявленных в ходе аудита уязвимостей;

анализ исправления недостатков предыдущих аудитов и тестов на проникновение по направлению информационной безопасности

* 1. Этап 1. Технический анализ защищенности

Работы Этапа 1 должны предусматривать следующие работы:

сбор данных и сведений об организации Заказчика из открытых источников;

оценка защищенности внешнего периметра инфраструктуры от действий внешнего нарушителя;

анализ защищенности внутренней инфраструктуры от действий внешнего нарушителя;

оценка защищенности беспроводных сетей от действий внешнего нарушителя;

оценка текущего уровня осведомленности сотрудников в вопросах информационной безопасности;

подготовка рекомендаций по результатам выполнения работ Этапа 1.

Описание работ по каждому этапу приведено ниже.

* + 1. Сбор данных и сведений об организации Заказчика из открытых источников

поиск в общедоступных и закрытых источниках данных (сеть Интернет и др.) информации о скомпрометированных учетных данных для доступа к информационным активам Заказчика;

анализ доступной информации о базах данных Заказчика, размещенных или продаваемых на общедоступных и закрытых источниках (сеть Интернет и др.);

поиск и анализ данных по используемым техническим средствам (в т.ч. по их настройкам и ограничениям) Заказчиком, применяемым для обеспечения работы и защите своей информационной инфраструктуры;

поиск и анализ данных о контрагентах, привлекаемых Заказчиком для поддержки своих ИТ-сервисов, поиск скомпрометированных учетных данных для доступа к информационным активам выявленных контрагентов.

* + 1. Оценка защищенности внешнего периметра инфраструктуры от действий внешнего нарушителя

уточнение объема работ и перечня входящих в область проекта информационных активов на основе анализа информации из открытых источников;

выявление уязвимостей, присутствующих на ресурсах и сервисах, доступных из сети Интернет, разработка и практическое подтверждение возможности их эксплуатации (внешний нарушитель);

в случае успешной компрометации внешнего периметра, по согласованию с Заказчиком, возможно развитие атаки на ресурсы внутренней инфраструктуры;

сбор и обобщение статистических данных по результатам анализа защищенности внешнего периметра.

* + 1. Анализ защищенности внутренней инфраструктуры от действий внешнего нарушителя

анализ инфраструктуры в режиме «черного ящика» – от лица потенциального нарушителя, не имеющего легитимного доступа к сети;

анализ возможности подключения стороннего устройства к корпоративной сети с использованием легко доступных интерфейсов подключения (коридоры, переговорные комнаты и т.п.), изучение и получение доступа к внутренним ресурсам;

попытки получения несанкционированного доступа к конфиденциальной информации и чувствительным компонентам ИТ инфраструктуры, закрепления на внутренних узлах сети.

В рамках данного этапа могут использоваться сведения, полученные в ходе предыдущих этапов.

* + 1. Оценка защищенности беспроводных сетей от действий внешнего нарушителя

проведение атак на беспроводные сети, в том числе защищенные по стандарту WPA2-Enterprise, с целью определения потенциальных точек входа во внутреннюю инфраструктуру;

создание подложных беспроводных сетей с целью перехвата сессий легитимных пользователей по согласованию с Заказчиком;

сбор статистических данных по результатам анализа защищенности беспроводных сетей.

* + 1. Оценка текущего уровня осведомленности сотрудников в вопросах информационной безопасности

подготовка и согласование сценариев атак (социальная инженерия);

подготовка и реализация согласованных атак;

сбор статистических данных по результатам проведенной кампании.

* + 1. Подготовка рекомендаций по результатам выполнения работ Этапа 1

Полученные в результате выполнения работ Этапа 1 данные должны быть представлены в соответствующем разделе Отчета об аудите ИБ и содержать следующую информацию:

общие сведения и описание процесса проведения анализа;

описание методики проведения анализа защищённости;

результаты проведённых проверок;

выводы (как развёрнутые технические, так и более краткие для руководства);

оценку состояния защищённости информационных активов Заказчика как с точки зрения потенциальных векторов проникновения, так и с точки зрения используемых механизмов защиты;

перечень и описание выявленных нарушений защиты информации;

перечень представителей со стороны Заказчика, которые сопровождали исполнителя;

описание хода работ, выявленных уязвимостей, степени потенциальной опасности, вероятности их использования, описание последствий реализации выявленных уязвимостей. Все наблюдения должны быть рассмотрены с точки зрения влияния на бизнес-процессы Заказчика и ранжированы в соответствии с актуальными рисками, выявленными в ходе выполнения работ.

формирование конкретных практических рекомендаций по устранению выявленных уязвимостей, в том числе рекомендации по изменению конфигурации и настроек оборудования, используемых защитных механизмов и программных средств, принятию дополнительных мер и применению дополнительных средств защиты, по установке необходимых обновлений для используемого программного обеспечения;

формирование общих методических рекомендаций по модификации существующих процессов администрирования, разработки и/или аутсорсинга разработки систем Заказчика, их администрирования, направленных на минимизацию количества аналогичных недостатков в дальнейшем;

подготовка рекомендаций по совершенствованию защиты информации;

формирование отчета о найденных уязвимостях, способах их эксплуатации и рекомендации по их устранению, результаты эксплуатации нескольких критически опасных уязвимостей, включая информацию о полученном уровне привилегий в активах на различных этапах тестирования.

* + 1. Ограничения

запрещается проводить атаки на учетные записи легитимных клиентов Заказчика, без согласования с Заказчиком;

без предварительного согласования запрещается проводить атаки на учетные записи администраторов и прочих сотрудников поддержки Заказчика;

тесты, которые могу нарушить доступность систем Заказчика или логику ее функционирования, должны быть согласованы отдельно в устанавливаемом Заказчиком порядке.

* 1. Этап 2. Приведение процессов обработки и защиты персональных данных в соответствии с новыми требованиями законодательства

Работы по созданию системы защиты персональных данных включают следующие под этапы:

проведение обследования ИСПДн и процессов обработки и защиты ПДн;

оценка угроз безопасности ПДн;

формирование требований с СЗПДн;

проектирование СЗПДн;

доработка организационно-распорядительных документов, регламентирующих процессы обработки и защиты ПДн.

Описание работ по каждому этапу приведено ниже.

* + 1. Проведение обследования ИСПДн и процессов обработки и защиты ПДн

На данном этапе проводится обследование ИСПДн. Осуществляется сбор данных о процессах обработки персональных данных в ИСПДн, применяемых методах и средствах защиты в ИСПДн Заказчика, действующих процессах информационной безопасности. Проводимые мероприятия включают:

анализ действующих организационно-распорядительных документов в отношении процессов обработки и обеспечения безопасности ПДн;

проведение серий очных и удаленных интервью с ответственными специалистами со стороны Заказчика в целях выявления полного перечня ПДн, ИСПДн, способов обработки ПДн и используемых технологий и методов защиты информации;

сбор сведений о существующей инфраструктуре Заказчика и функционирующих в ней ИС, технологиях их взаимодействия, организационных и технических мерах по обеспечению информационной безопасности;

выявление всех ИСПДн Заказчика, а также процессов обработки ПДн без использования средств автоматизации на основании данных, полученных на этапе очного обследования на площадке Заказчика;

определение состава системного и прикладного программного обеспечения ИСПДн, мест и форм обработки ПДн;

для каждой ИСПДн определение ее границ, формулирование целей обработки ПДн, объема и состава обрабатываемых ПДн, категорий субъектов ПДн, определение сроков и правовых оснований для обработки ПДн, перечня действий (операций) с ПДн, мест и форм хранения ПДн;

выявление информации о реализованных организационных и технических мерах по защите ПДн Заказчика включая физическую охрану, назначение ответственных лиц, проводимых мероприятиях по защите ПДн, имевших место инцидентах ИБ при обработке ПДн.

Обследование должно проводиться специалистами Исполнителя на основании разработанных опросных форм. Перед началом обследования должно быть проведено согласование списка сотрудников Заказчика, участвующих в интервьюированиях, на основании перечня бизнес-процессов, в рамках которых осуществляется обработка ПДн, а также согласование сроков проведения интервью

На основании анализа всей собранной в процессе обследования информации должна проводиться оценка текущего уровня соответствия процессов обработки и защиты ПДн требованиям актуальных правовых нормативных актов Российской Федерации. Оценка должна проводиться с учетом непосредственно требований нормативно-правовых актов, общедоступных комментариев и разъяснений регуляторов по вопросам обработки и защиты ПДн, а также доступной правоприменительной практики. В рамках оценки соответствия Исполнитель для каждого рассматриваемого процесса обработки ПДн должен провести (в том числе и не ограничиваясь):

оценку соответствия состава, объема, сроков и способов обработки ПДн целям обработки;

анализ возможных условий обработки ПДн в соответствии со ст. 6 152-ФЗ;

оценку необходимости получения согласия на обработку ПДн, его наличия, а также соответствия формы и содержания согласия требованиям 152-ФЗ;

анализ соблюдения условий передачи ПДн третьим лицам;

анализ соблюдения условий поручения обработки ПДн третьим лицам;

анализ реализации режима обработки общедоступных ПДн;

анализ реализации режима обработки специальных категорий ПДн;

анализ реализации режима обработки биометрических ПДн;

анализ реализации режима распространения ПДн;

анализ реализации требований по обработке ПДн в целях продвижения товаров и услуг;

анализ реализации требований по соблюдению прав субъектов при сборе ПДн, в том числе от третьих лиц;

анализ реализации требований по организации трансграничной передачи ПДн;

анализ реализации требований по локализации БД ПДн на территории РФ;

оценку реализации обязанностей, определенных ст. 18.1 152-ФЗ;

оценку реализации обязанностей по защите ПДн, определенных ст. 19 152-ФЗ;

анализ необходимости уведомления уполномоченного органа по защите прав субъектов персональных данных об обработке ПДн, а также самого уведомления (в случае наличия).

Результатом данного этапа будет являться согласованный с Заказчиком аналитический отчет об обследовании процессов обработки и обеспечения безопасности персональных данных. Данный аналитический отчет будет содержать в том числе следующую информацию:

описание организационно-технических мер по обеспечению информационной безопасности;

описание ИСПДн Заказчика, содержащее:

* назначение ИСПДн;
* ключевые характеристики обработки (цель обработки, категория и перечень ПДн, виды субъектов ПДн, правовое обоснование и т.д.);
* архитектура системы и перечень информационных ресурсов;
* описание технологических процессов обработки ПДн (список лиц, допущенных к обработке ПДн, описание процессов сбора, хранения, передачи, уничтожения ПДн, использование съемных носителей и мобильных устройств в процессе обработки ПДн);

описание применяемых средств и технологий защиты информации;

перечень существующих внутренних нормативных документов, регламентирующих порядок обработки ПДн;

перечень выявленных нарушений и мероприятия по их устранению.

* + 1. Оценка угроз безопасности персональных данных

Оценка угроз безопасности ПДн проводится в целях определения угроз безопасности ПДн, реализация (возникновение) которых возможна в ИСПДн и сетях с заданной архитектурой и в условиях их функционирования.

На данном этапе Исполнителем производится:

определение уровней защищенности ПДн;

определение негативных последствий, которые могут наступить от реализации угроз безопасности ПДн;

определение возможных объектов воздействия угроз безопасности ПДн;

определение источников угроз безопасности ПДн;

оценка возможности реализации угроз безопасности ПДн и определение их актуальности.

При моделировании угроз безопасности ПДн Исполнитель использует следующие данные:

общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

описания векторов (шаблоны) компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

документацию на ИСПДн и сети (а именно: технические задания на создание ИСПДн и сетей, частные технические задание на создание систем защиты, программная (конструкторская) и эксплуатационная (руководства, инструкции) документация, содержащая сведения о назначении и функциях, составе и архитектуре ИСПДн и сетей, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах, а также иные документы на ИСПДн и сети, разработка которых предусмотрена требованиями по защите информации (обеспечению безопасности) или национальными стандартами);

договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в случае функционирования ИСПДн и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры);

нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и функционируют ИСПДн и сети, содержащие в том числе описание назначения, задач (функций) ИСПДн и сетей, состав обрабатываемых ПДн и их правовой режим;

технологические, производственные карты или иные документы, содержащие описание управленческих, организационных, производственных и иных основных процессов (бизнес-процессов) в рамках выполнения функций (полномочий) или осуществления видов деятельности Заказчика;

результаты оценки рисков (ущерба), проведенной Заказчиком.

Модель угроз безопасности ПДн представляет собой описательное представление свойств и характеристик угроз безопасности ПДн и содержит краткое описание архитектуры ИСПДн, характеристику источников угроз безопасности ПДн и описание всех угроз безопасности ПДн, актуальных для ПДн.

Исполнитель должен разработать модели угроз и нарушителей для ИСПДн с учетом актуальных методических документов ФСТЭК России и ФСБ России, а также Базы данных угроз (<https://bdu.fstec.ru/>)

Разрабатываемая модель угроз безопасности ПДн содержит следующие разделы:

общие положения;

описание ИСПДн и сетей и их характеристика как объектов защиты;

возможные негативные последствия от реализации угроз безопасности ПДн;

возможные объекты воздействия угроз безопасности ПДн;

источники угроз безопасности ПДн;

способы реализации угроз безопасности ПДн;

актуальные угрозы безопасности ПДн.

Результаты этапа:

согласованные с Заказчиком акты определения уровней защищенности ПДн;

согласованный с Заказчиком документ «Модель угроз безопасности персональных данных».

* + 1. Формирование требований к системе защиты персональных данных

На данном этапе Исполнитель проводит работы по установлению требований к СЗПДн ИСПДн Заказчика.

В ходе данного этапа выполняются следующие работы:

осуществление анализа соответствия требованиям по обеспечению безопасности ПДн;

определение базового набор мер по обеспечению безопасности ПДн на основе установленного уровня защищенности ПДн;

адаптация базового набор мер по обеспечению безопасности ПДн с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы;

уточнение адаптированного базового набора мер по обеспечению безопасности ПДн с учетом не выбранных ранее мер, в результате чего определяются меры по обеспечению безопасности ПДн, направленные на нейтрализацию всех актуальных угроз безопасности ПДн для конкретной ИСПДн Заказчика;

дополнение уточненного адаптированного базового набора мер по обеспечению безопасности ПДн, обеспечивающими выполнение требований к защите ПДн, установленными иными нормативными правовыми актами в области обеспечения безопасности ПДн и защиты информации.

определение компенсирующих мер, обеспечивающих блокирование (нейтрализацию) актуальных угроз безопасности ПДн (при необходимости);

разработка технического задания на создание СЗПДн Заказчика.

Техническое задание разрабатывается с учетом требований ГОСТ 34.602, ГОСТ 34.201.

Техническое задание на СЗПДн должно быть основано на требованиях по защите ПДн, моделях угроз ИСПДн и данных, полученных по результатам обследования.

Техническое задание на СЗПДн должно содержать общие требования к подсистемам и функциональным модулям СЗПДн, а также требования по интеграции и взаимодействию подсистем друг с другом и с существующими устройствами — автоматизированными рабочими местами, серверами, сетевым оборудованием.

Результатом данного этапа будет являться согласованное с Заказчиком техническое задание на создание СЗПДн.

* + 1. Проектирование системы защиты персональных данных

На данном этапе Исполнитель проводит работы по проектированию СЗПДн Заказчика.

На основании согласованного технического задания и модели угроз безопасности ПДн Исполнитель разрабатывает и согласовывает с Заказчиком документацию технического проекта на создание СЗПДн, содержащую описание подходов, технических и организационных решений по обеспечению безопасности ПДн, обрабатываемых в ИСПДн.

Документация технического проекта разрабатываются в соответствии с ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

В рамках проектируемой системы должна учитываться структура и сложность защищаемых ИСПДн, существующая архитектура ИТ-инфраструктуры Заказчика, необходимость организации информационного взаимодействия СЗПДн с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями, а также существующие у Заказчика средства защиты ПДн.

Результатом данного этапа будет являться согласованная с Заказчиком документация технического проекта на создание СЗПДн, которая должна содержать:

ведомость технического проекта;

пояснительная записка;

описание комплекса технических средств;

спецификация оборудования и программного обеспечения;

схема структурная комплекса технических средств;

план расположения оборудования.

* + 1. Доработка организационно-распорядительных документов, регламентирующих процессы обработки и защиты ПДн

На данном этапе Исполнителем производятся работы по разработке/адаптации комплекта организационно-распорядительной документации, соответствующей требованиям законодательства РФ, предъявляемым к документальному обеспечению деятельности операторов ПДн, отражающий внутренние организационные и инфраструктурные особенности процессов обработки ПДн Заказчика. В случае выявленной необходимости проводится доработка существующей организационно-распорядительной документации Заказчика.

При разработке документов должны учитываться имеющиеся у Заказчика документы, а также особенности реализуемых процессов обработки и защиты данных, состав и архитектура существующих ИСПДн, а также требуемые меры защиты ПДн.

Результатом данного этапа будет являться согласованный с Заказчиком комплект организационно-распорядительной документации, удовлетворяющий требованиям законодательства РФ в области защиты ПДн, и включающий в себя следующие документы:

перечень персональных данных, обрабатываемых в информационных системах;

политика обработки ПДн;

положение о комиссии по защите персональных данных;

положение о разграничении прав доступа к обрабатываемым ПДн в информационных системах;

положение об обработке и защите ПДн;

приказ о назначении должностных лиц и определении обязанностей должностных лиц для выполнения требований законодательства Российской Федерации в области обработки и защиты персональных данных;

приказ об упорядочивании доступа к информационным системам;

приказ об утверждении границ контролируемой зоны;

приказ об утверждении документов по защите персональных данных;

приказ об утверждении плана мероприятий и внутренних проверок по защите информации;

регламент контроля состава и контроля защищенности ИСПДн;

регламент по управлению инцидентами безопасности;

регламент реагирования на обращения субъектов ПДн и запросы государственных надзорных органов;

регламент резервирования и восстановления работоспособности ИСПДн;

руководство администратора безопасности ИСПДн;

руководство должностного лица, ответственного за обеспечение безопасности ПДн;

руководство должностного лица, ответственного за организацию обработки ПДн;

руководство пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

руководство системного администратора ИСПДн;

инструкция ответственного пользователя криптосредств;

инструкция по обращению с криптосредствами;

инструкция по организации антивирусной защиты;

инструкция по организации парольной защиты;

инструкция по порядку доступа в защищаемые помещения с размещенными компонентами информационных систем;

инструкция по порядку учета и хранения машинных носителей защищаемой информации;

описание технологического процесса обработки персональных данных;

типовые формы поручений на обработку ПДн;

согласие на обработку ПДн;

согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

* 1. Этап 3. Аудит процессов обеспечения информационной безопасности.

Аудит процессов обеспечения информационной включают следующие под этапы:

разработка и согласование с Заказчиком методики оценки текущего уровня зрелости процессов обеспечения ИБ (результаты оценки должно быть в том числе визуализированы в виде диаграмм/графиков) и оценки рисков;

проведение оценки текущего уровня зрелости процессов обеспечения ИБ и оценки рисков;

разработка рекомендации по повышению уровня ИБ и Стратегии развития ИБ.

Описание работ по каждому этапу приведено ниже.

* + 1. Разработка методики оценки текущего уровня зрелости процессов обеспечения ИБ и оценка текущего уровня зрелости процессов обеспечения ИБ

Разрабатываемая методика должна основываться на лучших российских и международных практиках в области ИБ и учитывать требования регуляторов в области обеспечения информационной безопасности:

Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных»;

Федеральный закон от 29 июля 2004 года №98-ФЗ «О коммерческой тайне»;

Федеральный закон от 26 июля 2006 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Приказ ФСТЭК России от 18 февраля №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСТЭК России от 25 декабря 2017 г. №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

ISO/IEC 27001:2013 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

NIST, SANS, CIS, COBIT, CSF.

Состав нормативной базы, которая будет являться основой для проведения оценки текущего уровня зрелости процессов обеспечения ИБ, должна быть определена Исполнителем и согласована с Заказчиком.

На основании полученных в результате работы данных должны быть выполнены:

оценка выполнения требований законодательства РФ;

оценка эффективности существующих процессов ИБ;

оценка выбора мер защиты информации;

оценка полноты реализации мер защиты информации.

Методика должна учитывать особенности организации Заказчика и позволять демонстрировать динамику изменений текущего уровня зрелости процессов обеспечения ИБ при проведении повторных оценок.

В область работ по количественной оценке ограничена 10 (десятью) ключевыми бизнес-процессами. Перечень процессов, подлежащих анализу, определяется Заказчиком.

Результатом работ является оценка текущего уровня зрелости процессов обеспечения ИБ, которая документируется в соответствующем разделе Отчета об аудите ИБ.

* + 1. Разработка рекомендаций по повышению уровня ИБ и Стратегии развития ИБ

В ходе проведения работ по разработке рекомендаций по повышению уровня ИБ должны быть выполнены работы по анализу результатов обследования, оценки текущего уровня ИБ и анализа киберрисков.

При определении рекомендаций должны быть рассмотрены ключевые процессы ИБ, включая следующие процессы:

управление рисками ИБ;

внутренний аудит ИБ;

организация защиты информации;

управление доступом к информации;

физическая безопасность;

защита от вредоносного ПО;

резервное копирование;

контроль за используемым ПО;

управление уязвимостями;

управление внесением изменений в состав ИС;

мониторинг событий ИБ;

управления инцидентами ИБ.

Рекомендации по повышению уровня ИБ ИС должны включать:

состав мероприятий по повышению уровня ИБ;

рекомендации по приоритетам реализации проектов по ИБ;

бюджетную оценку проектов по ИБ.

По результатам работ должны быть разработаны рекомендации по повышению уровня ИБ, которые документируются в соответствующем разделе Отчета об аудите, а также подготовлена Стратегия ИБ.

Стратегия ИБ должна регламентировать:

цели и задачи развития ИБ;

принципы развития ИБ;

нормативную базу, которая должна являться основой развития ИБ;

ключевые направления развития ИБ (проекты ИБ);

по каждому проекту должны быть определены: состав мероприятий, ожидаемый бизнес-результат от реализации проекта, сроки реализации проекта и бюджетная оценка работ;

предложения по реализации Стратегии ИБ. Этапы дорожной карты должны быть приоритизированы в соответствии с результатами верификации киберрисков.

1. **Требования к документированию**

Работы выполняются Исполнителем поочередно в соответствии с требованиями настоящего ТЗ. По окончании каждой очереди работ Исполнитель сдает Заказчику соответствующие отчетные документы очереди, состав которых определен ТЗ и Договором.

Отчетная документация по выполненным работам в рамках настоящего ТЗ должна быть предоставлена:

* в письменном виде на бумажном носителе в 2 (двух) экземплярах и электронном виде на машинном носителе в 1 (одном) экземпляре (для документов, за исключением комплекта организационно-распорядительной документации);
* в электронном виде на машинном носителе в 1 (одном) экземпляре (для комплекта организационно-распорядительной документации)

Отчетные документы должны разрабатываться с учетом требований Заказчика к оформлению документации.

Все материалы должны быть разработаны на русском языке, допускается использование специализированных терминов и названий систем на английском языке.

Документы, являющиеся результатом выполняемых работ, предоставляются Исполнителем Заказчику в электронном виде в формате программы Microsoft Word («\*.doc», «\*.docx») в одном экземпляре, схемы и другие графические материалы – в формате по согласованию с Заказчиком.

1. **Требования к Исполнителю**

5.1. Исполнитель должен обладать действующей лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации.

5.2. Наличие у Исполнителя подтвержденного опыта по успешному проведению аудитов информационной безопасности и/или обследований информационных систем (не менее 3 проектов за последние 3 года).

5.3. Наличие в штате не менее трех специалистов, имеющих подтвержденную квалификацию (диплом о высшем образовании государственного образца) в области обеспечения информационной безопасности и обладающих опытом выполнения соответствующих проектов или иное высшее образование и стаж работы в области оказываемых услуг не менее 3 лет и прошедшего обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения – не менее 360 аудиторных часов).

Срок деятельности Исполнителя в области оказания услуг по информационной безопасности должен быть не менее 5 лет.

1. **Конфиденциальность**

При взаимодействии между Сторонами подписывается соглашение о неразглашении конфиденциальной информации.

Стороны в полной мере осознают критичность информации, как исходных данных, так и результатов услуг. В ходе оказания услуг специалисты Исполнителя не должны предпринимать каких-либо действий, которые могут привести к уничтожению или блокированию информационных активов Заказчика.