

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

1. Наименование, назначение и цели выполняемых работ/оказываемых услуг:

Анализ безопасности систем защиты ПДн. Подготовка проекта доработки и внедрения систем защиты ПДн ОАО «СН-МНГ».

Целью оказываемых услуг является:

- выявление информационных систем персональных данных (ИСПДн) Заказчика;
- уточнение количества рабочих мест в ИСПДн ОАО «СН-МНГ»;
- разработка необходимой проектной и эксплуатационной документации по модернизации существующих средств защиты персональных данных ОАО «СН-МНГ» во исполнение требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» по обеспечению безопасности обрабатываемых персональных данных для исключения или существенного затруднения возможности получения злоумышленниками ПДн, обрабатываемых в информационных системах персональных данных ОАО «СН-МНГ», возможности несанкционированного или непреднамеренного воздействия на ПДн и обрабатывающие их компоненты ИСПДн ОАО «СН-МНГ».

2. Место выполнения работ/оказания услуг с указанием характеристики объекта:

2.1. Место выполнения работ/оказания услуг:

ОАО «СН-МНГ». г.Мегион, Тюменская область, Ханты-Мансийский автономный округ – Югра.

2.2. Характеристика объекта защиты:

В ИСПДн ОАО «СН-МНГ» осуществляется обработка и хранение информации, подлежащей обязательной защите в соответствии с Федеральным Законом «О персональных данных» от 27.07.2006 г. № 152-ФЗ. В ИСПДн ОАО «СН-МНГ». Осуществляется обработка специальной категории (состояние здоровья) персональных данных.

ИСПДн ОАО «СН-МНГ» присвоены классы «К1» и «К2» на соответствие требованиям Приказа ФСТЭК от 5 февраля 2010 г. N 58.

На момент первоначального обследования (2009г) ИСПДн выявлено 250 рабочих мест (60р.м. – «К1» и 190р.м. – «К2»).

Объем обрабатываемых персональных данных в ИСПДн - менее 100000 субъектов.

ИСПДн ОАО «СН-МНГ» являются многопользовательскими клиент-серверной системами, выполненными по двух- и трехзвенной архитектуре.

Технически ИСПДн ОАО «СН-МНГ» реализованы на основе технологий СУБД «Oracle». СУБД «Oracle» установлена на Oracle Exadata Database Machine 2-2.

Вычислительная сеть ОАО «СН-МНГ» построена на основе AD Windows Server 2008R2, клиентские рабочие станции Windows 7/8.

Файловые сервера и сервера приложений на Windows Server 2008/2012 и Linux находятся в виртуальной среде, построенной на VMWare ESXi 5.5.

Для хранения данных используются системы хранения данных EMS Data Domain, EMS VNX, HP EVA, HP StorageWorks.

Основное серверное оборудование находится в Машинном зале Вычислительного центра.

Территориальное размещение – ИСПДн, развернутая в основном в пределах города офисах, некоторые клиенты находятся в цехах, территориально удаленно на несколько сотен или десятков километров от Вычислительного центра.

Наличие соединения с сетями общего пользования - имеющая одноточечный выход в сеть общего пользования.

Трансграничная передача персональных данных отсутствует.

3. Сроки выполнения работ/оказания услуг: 20.11.2015 – 31.12.2015.

4. Условия выполнения работ/оказания услуг: Услуги выполняются в соответствии с предложенным Исполнителем календарным планом. Работы могут быть завершены Исполнителем досрочно по согласованию сторон без изменения стоимости Договора.

5. Требования по выполнению сопутствующих работ, оказания сопутствующих услуг, поставкам необходимых материалов, в том числе оборудования: необходимость оказания сопутствующих услуг отсутствует.

6. Порядок (последовательность, этапы) выполнения работ/оказания услуг:

	Последовательность этапов работ	Отчетные документы по итогам этапов
1.	Обследование существующих информационных систем Общества. Инвентаризация технических и информационных ресурсов ИСПДн ОАО «СН-МНГ». Выявление информационных систем персональных данных	<ul style="list-style-type: none"> - аналитический отчет по проведению обследования информационных систем; - список выявленных ИСПДн; - развернутый перечень ПДн, обрабатываемых в информационных системах Общества; - перечень сотрудников, допущенных к обработке ПДн; - описание входящей и исходящей информации для подразделений, связанных с обработкой ПДн; - описание информационных потоков ПДн между подразделениями; - описание информационных потоков ПДн с третьими лицами; - описание технологических процессов обработки информации в ИСПДн. - описание мер по обеспечению физической безопасности и расположения технических средств охраны; - технологическая информация об используемых информационных подсистемах, обрабатывающих ПДн, в том числе: <ul style="list-style-type: none"> • перечни технических и программных средств, входящих в состав подсистемы; • перечни информационных ресурсов подсистемы; • описание технологии управления подсистемой; • структурная схема топологии информационной системы • технологические сведения об используемых серверах.
2.	Определение в существующих информационных системах подсистем, обрабатывающих персональные данные и уточнение их класса (при необходимости)	<ul style="list-style-type: none"> - проекты актов классификации (определения уровней защищенности) для каждой ИСПДн.
3.	Определение угроз безопасности, формирование модели угроз и модели нарушителя для ИСПДн, формирование и согласование с Заказчиком технических требований к СЗПДн	<ul style="list-style-type: none"> - частная модель угроз безопасности ПДн при их обработке в ИСПДн, включая модель нарушителя; - частное техническое задание на создание системы защиты персональных данных в ИСПДн, содержащее:

		<ul style="list-style-type: none"> • общие сведения о проекте; • назначение и цели проектирования системы защиты; • характеристика объекта защиты; • требования к системе защиты в целом; • функциональные требования к подсистемам; • требования к видам обеспечения; • требования к реализации предложений по оптимизации информационных систем обработки персональных данных; • состав и содержание выполняемых работ по проекту; • порядок контроля и приемки системы защиты; • требования к составу и содержанию работ по подготовке объекта защиты к вводу системы защиты в действие.
4.	Проектирование СЗПДн ИСПДн	<ul style="list-style-type: none"> - технический проект на создание СЗПДн; - пояснительная записка к техническому проекту СЗПДн: • обоснование разработки СЗПДн; • исходные данные на ИСПДн; • ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн; • подтверждение соответствия проектных решений действующим нормам законодательства о ПДн; • конкретизированные мероприятия и требования к СЗПДн (с учетом класса и требований руководящих документов ФСТЭК России и ФСБ России); • перечень предполагаемых к использованию сертифицированных средств защиты информации и схемы их внедрения; • состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн; • пояснительную записку к техническому проекту; • ведомость технического проекта СЗПДн; • программу и методику испытаний СЗПДн; • список мероприятий по защите

		информации.
5.	Разработка и согласование с Заказчиком комплекта организационно-распорядительной документации, регламентирующей процессы обработки и защиты персональных данных	<p>- «Приказ об организации работ в Обществе по защите персональных данных по требованиям информационной безопасности»:</p> <ul style="list-style-type: none"> • Приложение № 1. Положение об обработке персональных данных; • Приложение № 2. Политика оператора в отношении обработки ПДн; • Приложение № 3. Положение о структурном подразделении, отвечающем за защиту персональных данных; • Приложение № 4. Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в ИСПДн. • Приложение № 5. Перечень сотрудников и подразделений, допущенных к обработке персональных данных; • Приложение № 6. Перечень информационных систем персональных данных; • Приложение № 7. Положение о комиссии по защите ПДн; • Приложение № 8. Положение о пропускном и внутриобъектовом режиме; <p>- «Приказ о введение в действие документов, регламентирующих мероприятия по защите персональных данных, обрабатываемых в Обществе»:</p> <p>Приложение № 1. Комплект инструкций:</p> <ul style="list-style-type: none"> • «Инструкция по использованию антивирусных средств»; • «Инструкция по организации парольной защиты»; • «Инструкция по резервному копированию и восстановлению массивов информации»; • «Инструкция по обеспечению безопасности и защиты информации от несанкционированного доступа»; • «Инструкция по организации учета, использования и уничтожения машинных носителей данных, предназначенных для обработки и хранения персональных данных»; • «Инструкция по обработке персональных данных без использования средств автоматизации»;

- «Инструкция администратора безопасности».

Приложение № 2. Комплект регламентов:

- Регламент о предоставлении прав доступа к персональным данным;
- Регламент реагирования на обращения субъектов ПДн и запросы государственных надзорных органов;
- Регламент обмена/выдачи информацией (к договорам между Обществом и сторонними организациями);
- Регламент контроля состава и контроля защищенности ИСПДн;
- Регламент по управлению инцидентами безопасности;
- Регламент резервирования и восстановления работоспособности ИСПДн;
- Регламент организации обращения с защищаемыми носителями ПДн;
- Регламент организации антивирусной защиты;
- Регламент контроля эффективности выполнения требований законодательства РФ по защите ПДн.

Приложение № 3. Комплект журналов:

- Журнал учета СЗИ, эксплуатационной и технической документации к ним;
- Журнал учета открытия/закрытия помещений/мест хранения носителей ПДн;
- Журнал инструктажа пользователей и обслуживающего персонала Общества;
- Журнал учета мероприятий по защите информации в Обществе;
- Журнал учета и выдачи машинных носителей данных, содержащих конфиденциальную информацию Общества;
- Журнал учета ремонтно-восстановительных работ на основных технических средствах Общества;
- Журнал учета выдачи информации на бумажных носителях третьим лицам;
- Журнал учета выдачи персональных ключей.

Приложение №4. Приказы и акты:

- Акт определения уровня

	<p>защищенности;</p> <ul style="list-style-type: none"> • Акт оценки эффективности принимаемых мер по обеспечению безопасности 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 о выполнении мер по безопасности персональных данных; • Приказ о вводе ИСПДн в эксплуатацию. <p>Приложение №5. Пакет документов по СКЗИ:</p> <ul style="list-style-type: none"> • Положение о порядке обеспечения безопасности ПДн с использованием СКЗИ; • Приказ о допуске пользователей к работе с СКЗИ; • Приказ о назначении ответственного пользователя СКЗИ; • Журнал поэкземплярного учета СКЗИ; • Журнал учета хранилищ СКЗИ и ключей к ним; • Заключение о возможности эксплуатации СКЗИ. <p>Приложение №6. Прочее:</p> <ul style="list-style-type: none"> • Описание технологического процесса обработки персональных данных; • Перечень ИСПДн и обрабатываемых в них ПДн; • Матрица доступа субъектов в информационные системы персональных данных; • Проект уточняющего уведомления в Роскомнадзор об обработке персональных данных.
--	---

7. Требования к качеству работ (услуг), в том числе технология производства работ (оказания услуг), методики оказания услуг, организационно-технологическая схема производства работ:

7.1. Общие требования:

СЗПД должна проектироваться в соответствии с требованиями законодательства Российской Федерации, руководящими документами ФСТЭК России, ФСБ и организационно-распорядительными документами ОАО «СН-МНГ»

Технологии защиты информации и применяемые в ее рамках средства защиты должны обеспечить предотвращение несанкционированного доступа к информации и информационным ресурсам, а также изменения штатных режимов функционирования систем и средств информатизации и связи.

Должна быть обеспечена защита, как от внутренних, так и от внешних угроз.

При проектировании СЗПДн должна обеспечиваться минимизация ограничений и объема дополнительных операций, накладываемых на пользователя, осуществляющего санкционированную работу в ИСПДн, при условии выполнения всех необходимых требований информационной безопасности.

7.2. Требования к совместимости:

Планируемые к применению средства защиты информации и режимы их функционирования не должны противоречить утвержденной политике информационной безопасности ОАО «СН-МНГ», установленным средствам защиты, общесистемному и прикладному программному обеспечению в части их касающейся.

7.3. Требования к масштабируемости:

Настройка СЗПДн должна позволять изменять (увеличивать) перечень защищаемых информационных ресурсов, добавление или удаление объектов защиты, не снижая свою функциональность и производительность. Выбранные средства СЗПДн должны обеспечивать масштабируемость - увеличения количества пользователей, узлов и информационных ресурсов ИСПДн.

7.4. Порядок реализации мер по защите персональных данных:

Разработка СЗПДн должна проводиться с соблюдением действующих государственных стандартов в соответствии с областью их распространения.

Порядок реализации мер по защите персональных данных установлен основными регламентирующими документами уполномоченных Федеральных органов по защите информации:

- Федеральному закону РФ от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральному закону РФ от 27.07.2006г. № 152-ФЗ «О персональных данных»;
- Порядок проведения классификации информационных систем персональных данных (Утвержден Постановлением Правительства РФ № 1119 от 1 ноября 2012 года);
- Требования к составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных - Приказ ФСТЭК №21 от 18 февраля 2013 года (Зарегистрирован Министерством Юстиции РФ 14 мая 2013 года);
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54-144;
- «Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России 15.02.2008 г.;
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622.
- Требования к системам обнаружения вторжений, утверждены Приказом ФСТЭК России от 6 декабря 2011 года № 638.

- Требования к средствам антивирусной защиты, утверждены Приказом ФСТЭК России от 20.03.2012 г. № 28.
- Руководящие документы ФСБ (ПКЗ 2005, приказ ФАПСИ №152);
- Постановление Правительства Российской Федерации от 15.09. 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Специальных требований и рекомендаций по технической защите конфиденциальной информации («СТР-К»), утвержденных Приказом Государственной технической комиссии при Президенте Российской Федерации от 30 августа 2002 года № 282;
- ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс Стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».
- а также иных нормативных правовых актов Российской Федерации по защите персональных данных.

7.5. Требования к документированию:

По окончании работ, Заказчику передается следующая документация:

- отчет по результатам проведения обследования информационных систем;
- список выявленных ИСПДн;
- развернутый перечень ПДн, обрабатываемых в информационных системах Общества;
- модель угроз безопасности ПДн при их обработке в ИСПДн, включая модель нарушителя;
- эскизный проект (техническое предложение);
- техническое задание на создание системы защиты персональных данных в ИСПДн в соответствии с разработанным эскизным проектом.

Эскизный проект (техническое предложение) в обязательном порядке должен включать в себя следующие разделы:

- технический проект на создание системы защиты персональных данных;
- пояснительная записка к техническому проекту на создание системы защиты персональных данных;
- ведомость технического проекта СЗПДн;
- программу и методику испытаний СЗПДн.

Пояснительная записка к техническому проекту, в обязательном порядке должна содержать:

- обоснование разработки системы защиты информации;
- исходные данные на ИСПДн;
- ссылку на нормативные документы, с учетом которых будет разрабатываться система защиты информации и приниматься в эксплуатацию ИСПДн;
- конкретизированные мероприятия и требования к СЗПДн (с учетом требований руководящих документов ФСТЭК России и ФСБ России);
- перечень предполагаемых к использованию сертифицированных средств защиты информации и схемы их внедрения;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения системы защиты информации;
- список мероприятий по защите информации.

8. Требования к безопасности выполнения работ/оказания услуг:

Сохранение в тайне целей, задач и результатов работ должно обеспечиваться в соответствии с требованиями законодательных и нормативных актов РФ в области защиты персональных данных и информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

Получение дополнительных сведений об элементах СЗПДн и ИСПДн (в том числе об их составе), предназначенных для обработки персональных данных, должно производиться установленным порядком в соответствии с требованиями законодательных и нормативных актов РФ в области защиты персональных данных и информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, после подписания между сторонами Соглашения о конфиденциальности.

9. Требования к полученным в конечном итоге результатам работ/услуг:

Модернизированная согласно технического проекта СЗПДн должна представлять собой комплекс программно-технических и организационных решений, обеспечивающих выполнение целевых функций ИСПДн.

В состав СЗПДн должны входить следующие подсистемы:

- управления доступом;
- регистрации и учета;
- обеспечения целостности;
- ограничения программной среды;
- антивирусной защиты;
- обнаружения вторжений;
- обеспечения безопасного межсетевого взаимодействия;
- анализа защищенности;
- криптографической защиты информации (при необходимости).

Подсистемы СЗПДн должны соответствовать требованиям, предъявляемым нормативными документами в области безопасности персональных данных применительно к установленному уровню защищенности персональных данных.

Уровень защищенности определяется и согласуется с Заказчиком в соответствии с требованиями Постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Подсистемы СЗПДн должны удовлетворять требованиям Приказа ФСТЭК от 18 февраля 2013 г. N 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» применительно к установленному уровню защищенности персональных данных.

10. Условия привлечения субподрядчиков, субисполнителей:

Субподрядные организации могут привлекаться только по согласованию с Заказчиком.

11. Требования к гарантии на выполненные работы:

Исполнитель гарантирует надлежащее качество оказываемых услуг.

12. Формы, характер и периодичность предоставления отчетов о ходе выполнения работ/оказания услуг:

Ход оказания услуг оформляется общим актом оказанных услуг, направляемым Исполнителем Заказчику по завершении всех этапов работ.

По мере выполнения этапов работ, Исполнитель предоставляет согласно календарному плану отчетные документы, указанные в описании этапа.

13. Контроль за качеством выполняемых работ/оказываемых услуг:

Качество оказанных услуг проверяет инициатор Договора.

14. Требования к проживанию и доставке работников Подрядной организации:

Доставка работников к месту выполнения работ/оказания услуг и проживание работников Подрядной организации должно входить в стоимость предоставляемых услуг по Договору.

15. Необходимость в привлечении техники Заказчика для выполнения работ/оказания услуг:

Привлечение техники Заказчика для выполнения работ/оказания услуг – не требуется.

16. Порядок контроля, приемки и оформления результатов по выполненным работам/оказанным услугам:

16.1. Приемка выполненных обязательств осуществляется в соответствии с Техническим заданием и Календарным планом.

16.2. По завершении выполнения всех обязательств по этапам согласно Календарному плану, Исполнитель направляет Заказчику Акт.

16.3. Заказчик после получения Акта обязан направить Исполнителю подписанный Акт или мотивированный отказ от приемки выполненных работ с перечнем необходимых доработок и сроков их исполнения.

16.4. Исправление замечаний Заказчика производится Исполнителем за свой счет при условии, что они не выходят за рамки Технического задания.

17. Требования к подрядным организациям, которые будут выполнять работы:

Исполнитель должен:

- иметь опыт работ в области оказания услуг по защите информации не менее 5 лет;
- иметь опыт выполнения аналогичных работ;
- обладать материально-техническими и кадровыми ресурсами, необходимыми для своевременного выполнения договора;
- указать количество в штате компании специалистов, имеющих базовое образование и специализацию в области защиты информации;
- указать наличие в штате специалистов, обладающих российскими и международными сертификатами.

Квалификация специалистов Исполнителя подтверждается соответствующими сертификатами (свидетельствами).

Исполнитель должен иметь лицензии:

- ФСТЭК на деятельность по технической защите конфиденциальной информации;
- ФСТЭК на деятельность по разработке и производству средств защиты конфиденциальной информации;
- ФСБ на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Начальник

Вычислительного центра ОАО «СН-МНГ»



С. И. Кошечев

Заместитель начальника ВЦ



Е.С. Глебов