# ТЕХНИЧЕСКОЕ ЗАДАНИЕ
# НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

**Содержание**

1 Общие сведения ..... 3
2 Назначение и цели создания СЗПДн ..... 3
2.1 Назначение СЗПДн ..... 3
2.2 Цели создания СЗПДн ..... 3
3 Характеристика объекта защиты ..... 4
3.1 Расположение объекта информатизации ..... 4
3.2 Состав аппаратного и программного обеспечения ИСПДн ..... 5
4 Технические решения по созданию СЗПДн ..... 5
4.1 Этапы создания СЗПДн ..... 5
4.2 Требования к режимам функционирования системы ..... 6
4.3 Требования к надежности ..... 6
4.4 Требования безопасности ..... 6
5 Требования к квалификации Исполнителя ..... 6
6 Состав работ ..... 8
6.1 Проектирование СЗПДн, поставка Оборудования, монтаж Оборудования ..... 8
6.2 Передача прав на использование программного обеспечения, входящего в состав СЗПДн ..... 8
6.3 Пусконаладочные работы, опытная эксплуатацию СЗПДн, аттестация ИСПДн по требованиям безопасности информации. ..... 9
Приложение 1 ..... 11
Приложение 2 ..... 12

# 1 ОБЩИЕ СВЕДЕНИЯ

Настоящее техническое задание (ТЗ) разработано для информационной системы персональных данных ООО «Газпром межрегионгаз Вологда» (ИСПДн) и описывает требования, предъявляемые к построению системы защиты, внедрению системы защиты и передаче прав на использование программного обеспечения с целью создания системы защиты информации в ИСПДн.

Полное наименование и обозначение системы: «Система защиты информации, обрабатываемой в информационной системе персональных данных ООО «Газпром межрегионгаз Вологда».

Сокращенное наименование системы: СЗПДн.

Работы по поставке и пуско-наладке оборудования СЗПДн проводятся на основании данного ТЗ.

Финансирование работ осуществляется из средств бюджета ООО «Газпром межрегионгаз Вологда».

По завершении этапов работ Исполнитель выдает Аттестат соответствия требованиям по безопасности информации ИСПДн.

Порядок оформления и предъявления Заказчику результатов работ определяется на основании действующих стандартов и договорных документов между Заказчиком и Исполнителем.

# 2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СЗПДН

## 2.1 Назначение СЗПДн

Назначением СЗПДн является обеспечение информационной безопасности (ИБ) персональных данных (ПДн), обрабатываемых в ИСПДн.

СЗПДн должна обеспечивать конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн.

## 2.2 Цели создания СЗПДн

Целями создания СЗПДн являются:

– обеспечение защищенности ИСПДн в процессе обработки и хранения ПДн, обеспечение конфиденциальности ПДн при их обработке, а также других необходимых характеристик защищенности информации (целостности, доступности);

– соответствие требованиям обеспечения ИБ при обработке ПДн в ИСПДн, регламентируемых РД ФСТЭК России и ФСБ России.

В результате создания СЗПДн должно быть обеспечено:

– нейтрализация актуальных угроз информационной безопасности ПДн;

– отслеживание действий субъектов информационных отношений.

Критериями оценки достижения поставленных целей по созданию СЗПДн являются:

– соответствие требованиям по обеспечению безопасности ПДн в ИСПДн соответствующего класса, определенным в приказе ФСТЭК России

от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»;

– выполнение требований настоящего ТЗ;

– проведение аттестационных испытаний ИСПДн на соответствие требованиям по безопасности информации и выдача аттестатов соответствия.

## 3 ХАРАКТЕРИСТИКА ОБЪЕКТА ЗАЩИТЫ

Объектом защиты СЗПДн являются персональные данные, обрабатываемые в ИСПДн ООО «Газпром межрегионгаз Вологда».

ИСПДн является территориально – распределенной системой, имеющей в своем составе неоднородные программные и программно-технические средства обработки ПДн.

Рабочие станции пользователей функционируют под управлением ОС Windows XP/7/Vista.

Общее количество АРМ – 110.

Серверы функционируют под управлением ОС Windows 2003 Server, а так же на серверах установлены СУБД MS SQL 2005.

Сеть передачи данных построена на основе коммуникационного оборудования Cisco, 3Com, D-Link. Для подключения удаленных зданий используются выделенные оптоволоконные каналы, предоставляемые операторами связи.

ИСПДн имеет подключения к сетям связи общего пользования и сетям международного информационного обмена.

ИСПДн построены на основе клиент-серверной технологии. Обработка ПДн в ИСПДн осуществляется с использованием средств автоматизации.

По режиму обработки ПДн ИСПДн является многопользовательской, пользователи системы имеют различные права доступа, обрабатываемая информация имеет различный уровень конфиденциальности.

Все технические средства ИС находятся на территории Российской Федерации.

### 3.1 Расположение объекта информатизации

ИСПДн располагается в центральном офисе и удаленных подразделениях ООО «Газпром межрегионгаз Вологда».

Центральный офис ООО «Газпром межрегионгаз Вологда» располагается в трех зданиях по следующими адресам:

- г. Вологда, ул. Октябрьская, д. 51;
- г. Вологда, ул. Благовещенская, д. 36а;
- г. Вологда, ул. Благовещенская, д. 51.

Общее число удаленных подразделений – 9.

### 3.2 Состав аппаратного и программного обеспечения ИСПДн

В состав ИС входят следующие основные компоненты:

- серверы;
- АРМ пользователей;
- коммутационное оборудование:
  - а) активное сетевое оборудование ИСПДн;
  - б) каналы связи;
- программное обеспечение:
  - а) общесистемное программное обеспечение ИСПДн;
  - б) специальное программное обеспечение ИСПДн.

## 4 ТЕХНИЧЕСКИЕ РЕШЕНИЯ ПО СОЗДАНИЮ СЗПДН

СЗПДн в совокупности с механизмом поддержки функциональных подсистем не должна накладывать каких-либо существенных ограничений на информационные технологии, используемые в ИСПДн.

Архитектура СЗПДн должна обеспечивать реализацию функций безопасности на всех технологических этапах эксплуатации ИСПДн, в том числе при проведении технического обслуживания и ремонта.

Эффективность СЗПДн должна достигаться комплексным применением различных средств и методов.

В СЗПДн должны использоваться только средства защиты информации, сертифицированные в установленном порядке на соответствие функциональным требованиям информационной безопасности в системе сертификации ФСТЭК России и ФСБ России.

При использовании средств защиты информации, не сертифицированных по требованиям безопасности информации, Исполнитель должен провести процедуру сертификации.

### 4.1 Этапы создания СЗПДн

Создание СЗПДн проводится в 3 этапа:

1 этап: проектирование СЗПДн, поставка оборудования, входящего в состав средств защиты ПДн (далее - Оборудование), установка Оборудования (Приложение 1).

Исполнитель имеет право корректировать Перечень оборудования (Приложение 1) по согласованию с Заказчиком.

2-й этап: передача прав на использование программного обеспечения, входящего в состав СЗПДн (Приложение 2).

Исполнитель имеет право корректировать перечень программного обеспечения, входящего в состав СЗПДн (Приложение 2) по согласованию с Заказчиком.

3-й этап: пусконаладочные работы, опытная эксплуатация СЗПДн, аттестация ИСПДн по требованиям безопасности информации.

Каждый этап выполняется Исполнителем в соответствии с договором, заключенным с Заказчиком.

Перед выполнением каждого этапа Исполнитель заключает с Заказчиком отдельный договор.

### 4.2 Требования к режимам функционирования системы

При проектировании СЗПДн, установке СЗПДн и выполнении пусконаладочных работ СЗИ должны быть реализованы следующие режимы функционирования:

- режим установки и конфигурирования;
- режим отладки;
- рабочий режим.

Режим конфигурирования предназначен для первичной настройки СЗИ и должен выполняться на этапе пуско-наладочных работ. В этом режиме должно происходить настраивание СЗИ путем создания, редактирования и применения политик, шаблонов, настроек необходимых видов доступа. Режим установки и конфигурирования должен подразумевать работы по установке и начальной настройке установленного программного обеспечения.

Режим отладки предназначен для отладки СЗИ и должен выполняться на этапе ввода в эксплуатацию после режима конфигурирования. В этом режиме должен вестись журнал отработки необходимых компонент СЗИ, настройка видов и методов реагирования компонент на происходящие воздействия.

### 4.3 Требования к надежности

Аппаратно-программные компоненты СЗПДн должны функционировать в режиме круглосуточной работы и позволять осуществлять выполнение процедур резервирования и восстановления системы после сбоев.

### 4.4 Требования безопасности

Конструкция используемого оборудования должна обеспечивать защиту эксплуатирующего персонала от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.003 и ГОСТ 12.2.007.

Размещение оборудования на штатных местах должно обеспечивать его безопасное обслуживание и эксплуатацию.

## 5 ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ ИСПОЛНИТЕЛЯ

Исполнитель должен иметь в штате компании не менее 3 (трех) специалистов, имеющих базовое образование и специализацию в области защиты информации.

Исполнитель должен иметь опыт работ в области оказания услуг по защите информации не менее 10 лет.

Исполнитель должен иметь в структуре компании выделенное подразделение, отвечающее за работы в области информационной безопасности.

Деятельность по защите информации должна быть определена в Уставе (учредительных документах) Исполнителя как основной вид деятельности организации.

Исполнитель должен иметь лицензии ФСТЭК России:

- Лицензия Федеральной службы по техническому и экспортному контролю России на деятельность по технической защите конфиденциальной информации;
- Лицензия Федеральной службы по техническому и экспортному контролю России на деятельность по разработке и (или) производству средств защиты конфиденциальной информации.

Исполнитель должен иметь лицензии ФСБ России:

- Лицензия ФСБ России на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем;
- Лицензия ФСБ России на осуществление технического обслуживания шифровальных (криптографических) средств;
- Лицензия ФСБ России на распространение шифровальных (криптографических) средств;
- Лицензия ФСБ России на осуществление предоставления услуг в области шифрования информации.

Исполнитель должен иметь Аттестаты аккредитации:

- органа по аттестации ФСТЭК России;
- испытательной лаборатории ФСТЭК России.

Исполнитель должен иметь свидетельство СРО о допуске к работам по подготовке проектной документации, которые оказывают влияние на безопасность объектов строительства.

Система менеджмента качества Исполнителя должна быть сертифицирована в соответствии с ГОСТ Р ИСО 9001-2001 (ISO 9001:2000).

Исполнитель должен обладать практическим опытом работы по следующим направлениям:

- проектирование, внедрение и сопровождение средств защиты информации в ИСПДн;
- разработка, внедрение и сопровождение программных средств защиты информации;

- проведение сертификационных испытаний программных и программно-технических средств защиты информации;
- аттестация ИСПДн класса К1;
- оказание услуг по внедрению (применению) криптографических средств защиты информации, электронной цифровой подписи;
- оказание услуг удостоверяющего центра.

## 6 СОСТАВ РАБОТ

### 6.1 Проектирование СЗПДн, поставка Оборудования, монтаж Оборудования

*Проектирование СЗПДн*

Исполнитель должен выполнить работы по разработке технического проекта СЗПДн, состоящего из следующих документов:

- ведомость технического проекта;
- пояснительная записка;
- схема структурная комплекса технических средств;
- ведомость покупных изделий;
- описание организационной структуры.

Также на данном этапе разрабатывается частное техническое задание на внедрение СЗПДн и пакет организационно-распорядительной документации на ИСПДн.

*Поставка Оборудования*

Исполнитель должен осуществить работы по закупке необходимого Оборудования, согласно Приложению 1.

Все поставляемое Оборудование, должно пройти процедуру оценки соответствия требованиям по безопасности информации и иметь сертификат ФСТЭК России или ФСБ России (в соответствии с требованиями нормативно-методических документов).

*Монтаж Оборудования*

Исполнитель должен провести монтаж Оборудования на объектах Заказчика, обеспечить их интеграцию в ЛВС Заказчика:

- монтаж Оборудования, в соответствии с Приложением 1, с учетом технического проекта на СЗПДн.

Если в процессе выполнения работ по монтажу Оборудования возникают какие-либо нештатные ситуации, а также ситуации, которые могут повлечь приостановление вышеуказанных работ, Исполнитель совместно с Заказчиком, принимают все возможные меры по устранению и ликвидации причин, которые привели к таким ситуациям.

### 6.2 Передача прав на использование программного обеспечения, входящего в состав СЗПДн

Все программное обеспечение, права на которое передается заказчику, должно пройти процедуру оценки соответствия требованиям по

безопасности информации и иметь сертификат ФСТЭК России или ФСБ России (в соответствии с требованиями нормативно-методических документов).

### 6.3 Пусконаладочные работы, опытная эксплуатацию СЗПДн, аттестация ИСПДн по требованиям безопасности информации.

*Пусконаладочные работы*

Исполнитель должен провести пусконаладочные работы СЗПДн на объектах Заказчика, обеспечить их интеграцию в ЛВС Заказчика,

Исполнитель должен провести анализ защищенности сетевых сегментов ИСПДн (в пределах ЛВС центрального офиса Заказчика) с использованием средства анализа защищенности.

Если в процессе в процессе выполнения пусконаладочных работ СЗПДн возникают какие-либо нештатные ситуации, а также ситуации, которые могут повлечь приостановление вышеуказанных работ, Исполнитель совместно с Заказчиком, принимают все возможные меры по устранению и ликвидации причин, которые привели к таким ситуациям.

*Опытная эксплуатация*

Опытная эксплуатация включает в себя комплексную проверку готовности СЗПДн. Опытная эксплуатация имеет своей целью проверку алгоритмов, отладку работы СЗПдн и технологического процесса обработки данных при использовании СЗПДн.

*Аттестация ИСПДн*

Состав работ по проведению аттестации ИСПДн включает следующие этапы:

1. Разработка и согласование с Заказчиком «Программы и методики аттестационных испытаний».
2. Проведение аттестационных испытаний ИСПДн на соответствие требованиям по безопасности информации.
3. Выдача заключения по результатам аттестационных испытаний.
4. Выдача аттестата соответствия в случае положительного заключения по результатам аттестационных испытаний.

**Перечень принятых сокращений**

| | | |
|---|---|---|
| АРМ | - | Автоматизированное рабочее место |
| ГОСТ | - | Государственный стандарт |
| ИСПДн | - | Информационная система персональных данных |
| ПДн | - | Персональные данные |
| СЗИ | - | Средства защиты информации |
| СЗПДн | - | Система защиты персональных данных |
| ТЗ | - | Техническое задание |
| ФСБ | - | Федеральная служба безопасности |
| ФСТЭК | - | Федеральная служба технического и экспортного контроля |

Приложение 1

Перечень оборудования, входящего в состав СЗПДн

| **Наименование оборудования** | **Кол-во** |
|---|---|
| Установочный комплект сетевого клиента СЗИ НСД «Блокхост-сеть» (сетевой) | 1 |
| USB-ключ eToken PRO (Java) | 99 |
| СЗИ от НСД «Аккорд-АМДЗ» | 11 |
| АПКШ «Континент» 3.5. ЦУС - Сервер Доступа. Платформа IPC-100 | 1 |
| Установочный комплект. СКЗИ «Континент-АП» версия 3.5 | 9 |
| Cisco IPS 4240 | 1 |
| Аппаратно-программное средство мониторинга и администрирования событий информационной безопасности ПАКАБ | 1 |

Приложение 2

Перечень программ для ЭВМ, входящего в состав СЗПДн

| **Наименование оборудования** | **Кол-во** |
|---|---|
| Лицензия на использование сервера СЗИ НСД «Блокхост-сеть» | 1 |
| Лицензия на использование сетевого клиента СЗИ НСД «Блокхост-сеть» | 99 |
| СЗИ от НСД «Эгида+» | 99 |
| XSpider (128 IP-адреса) | 1 |
| Право на использование Континент АП (1 дополнительное подключение пользователя Континент АП к СД), с правом использования КриптоПро CSP 3.6 | 9 |
| Программное средство мониторинга и администрирования событий информационной безопасности ПАКАБ-СЕРВЕР | 1 |