|  |
| --- |
| УТВЕРЖДАЮ |
| Директор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2018 г. |

Государственная информационная система

наименование вида

ГИС «**{ИМЯ\_ИС}**»

наименование ИС

ТЕХНИЧЕСКИЙ ПРОЕКТ

на создание системы защиты государственной информационной системы

на \_\_\_\_\_листах

Действует с \_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| СОГЛАСОВАНО |
| Специалист по технической защите |
| информации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2018 г. |
|  |

Хабаровск

2018

# Термины и определения

**Автоматизированное рабочее место** – программно-технический комплекс, предназначенный для автоматизированной деятельности определенного вида.

**Администратор автоматизированной системы** – лицо, ответственное за функционирование автоматизированной информационной системы в установленном штатном режиме работы.

**Администратор защиты (безопасности) информации** – лицо, ответственное за защиту автоматизированной информационной системы от несанкционированного доступа к информации.

**Аутентификация** – проверка принадлежности субъекту доступа предъявленного им идентификатора.

**Безопасность персональных данных –** состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ к информации** – возможность получения информации и ее использования.

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Объект защиты информации** - информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Пользователь информационной системы персональных данных** – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Система – совокупность взаимосвязанных и взаимодействующих элементов.**

**Средства защиты информации** – технические, программные средства, вещества и (или) материал, предназначенные или используемые для защиты информации.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Средства криптографической защиты информации** – аппаратные, программные и программно-аппаратные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

**Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п

**Угроза безопасности информации** – совокупность условий и факторов, создающих потенциальную или реальную существующую опасность, связанную с утечкой информации и/или непреднамеренными воздействиями на нее.

**Учетная запись пользователя** – набор данных, однозначно идентифицирующих пользователя в системе, совокупность прав и привилегий доступа к объектам и набор квот системных ресурсов.

**Специальные категории персональных данных** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

# Принятые сокращения

|  |  |  |
| --- | --- | --- |
| АРМ | – | автоматизированное рабочее место |
| АС | – | автоматизированная система |
| ГОСТ | – | государственный стандарт |
| ИБ | – | информационная безопасность |
| ИТ | – | информационные технологии |
| КЗ | – | контролируемая зона |
| ЛВС | – | локальная вычислительная сеть |
| НСД | – | несанкционированный доступ |
| ОС | – | операционная система |
| ОТСС | – | основные технические средства и системы |
| ПДн | – | персональные данные |
| ПО | – | программное обеспечение |
| РД | – | руководящий документ |
| СВТ | – | средства вычислительной техники |
| СЗИ | – | система защиты информации |
| СЗГИС | – | система защиты государственной информационной системы |
| СКЗИ | – | средства криптографической защиты информации |
| СрЗИ | – | средства защиты информации |
| ТЗ | – | техническое задание |
| ТС | – | технические средства |
| ТП | – | технический проект |
| ФСБ | – | Федеральная служба безопасности |
| ФСТЭК | – | Федеральная служба технического и экспортного контроля |

# 1 Общие положения

## 1.1 Наименование разработки

Наименование работы: «Разработка технического проекта на создание системы защиты государственной информационной системы».

## 1.2 Основание для разработки

Основанием для разработки изделия послужили:

## 1.3 Организации, участвующие в разработке

### 1.3.1 Цель работы

Целью работы является разработка технического проекта, позволяющего осуществить проектирование системы защиты информационной системы, обрабатывающей информацию ограниченного доступа в ГИС «**{ИМЯ\_ИС}**».

### 1.3.2 Назначение

Основным назначением работы является разработка технического проекта на создание комплексной системы защиты государственной информационной системы, обрабатывающей информацию ограниченного характера, в соответствии с нормами и требованиями законодательства РФ в области обеспечения безопасности информации при ее обработке в информационных системах, и технической защиты конфиденциальной информации.

### 1.3.3 Область использования результатов разработки

Результаты работы ориентированы на применение средств защиты для исключения НСД к информации в ГИС «**{ИМЯ\_ИС}**».

## 1.4 Нормативно-методическая документация, используемая при разработке проекта системы защиты ГИС

При разработке СЗГИС использовались следующие нормативно-методические документы:

* Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
* Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282;
* «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.;
* ГОСТ РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов», утверждены постановлением Госстандарта СССР от 27.12.1990 № 3380;
* ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», утверждено постановлением Госстандарта СССР от 29 декабря 1990 г. № 3469;
* ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» утверждено постановлением Госстандарта СССР от 24 марта 1989 г. №664;
* ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения» утверждено постановлением Госстандарта СССР от 27 декабря 1990 г. № 3399.
* «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утверждено приказом ФСТЭК России от 18.02.2013 № 21.
* «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утверждено постановлением Правительства РФ от 01.11.2012 № 1119
* ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».
* Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
* ГОСТ Р 51583-2000 "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения";
* ГОСТ 34.603 "Информационная технология. Виды испытаний автоматизированных систем".

## 1.5 Объемы выполнения работ

В процессе выполнения работ по созданию проекта системы защиты государственной информационной системы, обрабатывающей информацию ограниченного доступа, разработан комплект организационно-распорядительных и технологических документов, определенных в ТЗ на создание системы защиты ГИС «**{ИМЯ\_ИС}**».

# 2 Описание объекта информатизации

* 1. 2.1 Информационная характеристика

В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными Приказом ФСТЭК России от 11 февраля 2013г. № 17, масштабом информационной системы, определенными степенями ущерба для свойств безопасности информации, в ГИС «**{ИМЯ\_ИС}**» установлен **{КЗ}-й класс защищенности.**

## 2.2 Характеристика комплекса ОТСС и ВТСС, программного обеспечения, режима обработки, технологического процесса обработки информации ГИС

### 2.2.1 Характеристика комплекса ОТСС

### 2.2.2 Характеристика комплекса ВТСС

### 2.2.3 Состав программного обеспечения ГИС «{ИМЯ\_ИС}»

### 2.2.4 Режим обработки информации

В ГИС «**{ИМЯ\_ИС}**» обработка информации осуществляется в многопользовательском режиме с разграничением прав доступа.

Обработка информации ограниченного доступа предусматривает следующие действия: сбор, систематизацию, накопление, хранение, уточнение (обновление), использование, блокирование, уничтожение информации.

## 2.3 Физические лица, имеющие доступ к ресурсам и (или) в помещения, в которых располагаются ТС ГИС

### 2.4 Технологический процесс обработки информации

Технологический процесс обработки информации в ГИС включает в себя:

* загрузку операционной системы;
* запуск офисных приложений;
* разработку текстовых документов;
* формирование и печать документов.
  + 1. Порядок обработки информации ограниченного доступа

В ГИС «**{ИМЯ\_ИС}**» установлен следующий порядок обработки информации:

## 2.5 Структурно-функциональные характеристики ГИС

Структурно-функциональные характеристики ГИС «**{ИМЯ\_ИС}**», представлены в таблице 2.1.

Таблица 2.1 – Характеристики ГИС «{ИМЯ\_ИС}»

{SFH}

## 2.6 Характеристики и состав аппаратного и программного обеспечения

### 2.6.1 Компоненты ГИС

В состав ГИС входят следующие основные компоненты:

1. АРМ пользователей, допущенных к обработке информации ограниченного доступа;
2. программное обеспечение:
   1. общесистемное ПО;
   2. специальное ПО;
   3. прикладное ПО.

## 2.7 Информация, обрабатываемая в ГИС

В ГИС «**{ИМЯ\_ИС}**» обрабатывается информация ограниченного доступа, которая включает:

## 2.8 Организационные мероприятия, реализованные в ГИС «**{ИМЯ\_ИС}**»

В ГИС «**{ИМЯ\_ИС}**» введены следующие организационные меры защиты:

# 3 Меры по обеспечению безопасности информации

В СЗГИС должны использоваться только средства защиты информации, сертифицированные в установленном порядке на соответствие требованиям информационной безопасности, установленные требованиями ФСТЭК России или (и) ФСБ России.

В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11.02.2013 № 17, структурно-функциональными характеристиками ГИС, применяемыми информационными технологиями, актуальными угрозами и выполнением требований к защите информации ограниченного доступа **{КЗ}-го класса защищенности**, в СЗГИС необходимо реализовать следующие меры:

* идентификацию и аутентификацию субъектов доступа и объектов доступа;
* управление доступом субъектов доступа к объектам доступа;
* ограничение программной среды;
* защиту машинных носителей информации;
* регистрацию событий безопасности;
* антивирусную защиту;
* обнаружение вторжений;
* контроль (анализ) защищенности информации;
* обеспечение целостности информационной системы и персональных данных;
* обеспечение доступности персональных данных;
* защиту технических средств;
* защиту информационной системы, ее средств, систем связи и передачи данных
* выявление инцидентов и реагирование на них
* управление конфигурацией информационной системы и СЗГИС.

.

### 3.1 Меры по идентификации и аутентификации субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Данные меры включают в себя:

* идентификацию и аутентификацию пользователей, являющихся работниками оператора;
* Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных;
* управление идентификаторами, в том числе создание, присвоение и уничтожение;
* управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
* защита обратной связи при вводе аутентификационной информации:

### 3.2 Меры по управлению доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа обеспечивают управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивают контроль соблюдения этих правил.

Данные меры включают в себя:

* управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
* реализация необходимых методов (дискреционных, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа);
* управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, а также между информационными системами;
* разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
* назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
* ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе;
* блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
* разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
* регламентация и контроль использования в информационной системе мобильных технических средств;
* управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);
* обеспечение доверенной загрузки средств вычислительной техники;

### 3.3 Меры по ограничению программной среды

Меры по ограничению программной среды обеспечивают установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска, запрещенного к использованию в информационной системе программного обеспечения.

Данные меры включают в себя:

* управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения;
* управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения;
* установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.

### 3.4 Меры по защите машинных носителей информации

Меры по защите машинных носителей информации (средств обработки (хранения), съемных машинных носителей информации) исключают возможность несанкционированного доступа к машинным носителям и хранящей на них информации, а также несанкционированное использование съемных машинных информации.

Данные меры включают в себя:

* учет машинных носителей информции;
* управление доступом к машинным носителям информации;
* контроль перемещения машинных носителей информации за пределы контролируемой зоны;
* контроль ввода (вывода) информации на машинные носители информации;
* контроль подключения машинных носителей информации;
* уничтожение (стирание) или обезличивание информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания.

### 3.5 Меры по регистрации событий безопасности

Меры по регистрации событий безопасности обеспечивают сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Данные меры включают в себя:

* определение событий безопасности, подлежащих регистрации и сроков их хранения;
* определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
* сбор, запись, хранение информации о событиях безопасности в течение установленного времени хранения;
* реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;
* мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
* защита информации о событиях безопасности;

### 3.6 Меры по антивирусной защите

Меры по антивирусной защите обеспечивают обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Данные меры включают в себя:

* реализация антивирусной защиты;
* обновление баз данных признаков вредоносных компьютерных программ (вирусов).

### 3.7 Меры по контролю (анализу) защищенности информации

Меры по контролю (анализу) защищенности персональных данных обеспечивают контроль класса защищенности информации, обрабатываемой в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности СЗГИС.

Данные меры включают в себя:

* выявления, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;
* контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
* контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
* контроль состава технических средств, программного обеспечения и средств защиты информации;
* контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе.

### 3.8 Меры по обеспечению целостности информационной системы и информации

Меры по обеспечению целостности информационной системы и информации обеспечивают обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней информации, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

Данные меры включают в себя:

* контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
* обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама);
* контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях.

### 3.9 Меры по обеспечению доступности информации

Меры по обеспечению доступности информации обеспечивают авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

Данные меры включают в себя:

* использование отказоустойчивых технических средств;
* контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование;
* периодическое резервное копирование информации на резервные машинные носители информации;
* обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала.

### 3.10 Меры по защите технических средств

Меры по защите технических средств исключают несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий.

Данные меры включают в себя:

* организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования;
* контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;
* размещение устройств вывода (отображение) информации, исключающие ее несанкционированный просмотр;
* защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

### 3.11 Меры по защите информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности информации.

Данные меры включают в себя:

* разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы;
* обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;
* подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам;
* обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов;
* защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации;
* разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы.

### 3.12 Меры по выявлению инцидентов и реагированию на них

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

Данные меры включают в себя:

* определение лиц, ответственных за выявление инцидентов и реагирование на них;
* обнаружение, идентификация и регистрация инцидентов;
* своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;
* анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
* принятие мер по устранению последствий инцидентов;
* планирование и принятие мер по предотвращению повторного возникновения инцидентов.

### 3.13 Меры по управлению конфигурациями информационной системы и системы защиты персональных данных

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных обеспечивают управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Данные меры включают в себя:

* определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных;
* управление изменениями конфигурации информационной системы и системы защиты персональных данных;
* анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных;
* документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных.

### 3.14 Базовый набор мер

В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11.02.2013 г., базовый набор мер, применяемых для обеспечения **{КЗ}-го класса защищенности** ГИС представлен в таблице 3.1

Таблица 3.1 – Содержание базового набора мер

{BASIC}

### 3.15 Адаптация базового набора мер

При адаптации из базового набора мер защиты информации исключаются меры, непосредственно связанные с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе. Перечень исключаемых мер приведен в таблице 3.2.

Таблица 3.2 – Содержание исключаемых из базового набора мер

{ADAPTIVE}

### 3.16 Уточнение адаптированного базового набора мер

При уточнении базового набора мер добавляются меры, не выбранные ранее, нейтрализующие все актуальные угрозы безопасности персональных данных в соответствии с Моделью нарушителя и угроз безопасности персональных данных при их обработке в ГИС «{название ИС}». Перечень мер, нейтрализующих актуальные УБИ, приведен в таблице 3.3. Перечень добавленных мер представлен в таблице 3.4.

Таблица 3.3 – Перечень мер, нейтрализующих актуальные УБИ

{THR-MEAS}

Таблица 3.4 – Перечень добавляемых мер при уточнении

{Add-Meas}

### 3.17 Итоговый перечень мер защиты информации

В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК от 11.02.2013 № 17, «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18.02.2013 № 21 сформирован перечень мер защиты информации, применяемый с целью установления **{КЗ}-го класса защищенности** ГИС. Содержание итогового перечня мер защиты информации представлено в таблице 3.5.

Таблица 3.5 – Итоговый перечень мер защиты информации

{FINAL}

# 4 Предлагаемые средства защиты информации

СЗГИС реализуется с использованием как штатных (операционные системы), так и встроенных средств защиты информации, формирующих функциональные подсистемы СЗГИС.

Применяемые СрЗИ в совокупности образуют комплексную систему защиты информации, обеспечивающую безопасность их обработки на всех узлах рассматриваемой ГИС. СрЗИ, используемые в составе комплексной СЗГИС, общесистемные программные и технические средства защиты обеспечивают время восстановления:

* для отказов, не требующих замены или ремонта компонентов системы – не более 6 часов;
* для отказов, требующих внешнего вмешательства для замены или ремонта компонента системы – не более 96 часов.

Применяемые в составе СЗГИС средства защиты должны обеспечивать масштабируемость по количеству пользователей на объекте внедрения. Состав необходимых к внедрению программных и программно-аппаратных сертифицированных технических средств защиты информации представлен в таблице 4.1. Перечень реализуемых технических мер предлагаемыми средствами защиты информации приведен в таблице 4.2.

Таблица 4.1 – Состав предлагаемых сертифицированных СЗИ

{SZIs}

Таблица 4.2 – Реализация технических мер предлагаемыми СЗИ

{Meas-SZIs}

# 6 Организационные мероприятия по защите персональных данных в ГИС

## 6.1 Общие требования

Организационные (организационно-режимные, организационно-технические, кадровые) мероприятия по обеспечению информационной безопасности являются мероприятиями по организации деятельности персонала, порядку эксплуатации ТС системы в помещениях, систематическому выполнению мер по недопущению вывода системы из строя и контроля утечки защищаемой информации.

Мероприятия по защите ПДн при автоматизированной обработке должны выполняться в соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных» и другими требованиями ФСТЭК и ФСБ России.

## 6.2 Организационные меры по размещению ТС

Организационные меры по размещению ТС включают в себя:

* размещение ТС ГИС в помещениях, расположенных в пределах КЗ;
* размещение ТС должно препятствовать несанкционированному просмотру информации на дисплее;
* должны быть предусмотрены организационные меры, препятствующие несанкционированному доступу к ТС ГИС (режим доступа в помещения, порядок допуска к работе с ТС, опечатывание корпусов и мест подключения периферийных устройств (в случае запрещения пользования съёмными носителями информации) к основным техническим средствам обработки информации);
* должны быть предусмотрены организационные меры, препятствующие несанкционированному доступу к АРМ (режим доступа в помещения, порядок допуска к работе с АРМ);
* должны быть предусмотрены организационные меры, препятствующие несанкционированному доступу к техническим средствам защиты информации (определен порядок допуска к работе с СрЗИ, определен порядок их эксплуатации);
* при размещении ТС, использующих СрЗИ, следует руководствоваться рекомендациями документации на данные средства;
* размещение ТС, предназначенных для вывода защищаемой информации на печать, необходимо проводить с учетом максимального затруднения визуального просмотра информации лицами, не имеющими санкционированного допуска к обрабатываемой информации.

## 6.3 Организационные меры по работе со съемными носителями информации

При работе со съемными носителями информации:

* должны быть реализованы организационные меры по учету носителей;
* должен быть внедрен порядок использования и хранения съемных носителей, препятствующий краже, утере носителей;
* должен быть внедрен порядок учета, использования и хранения съемных носителей, препятствующего несанкционированному доступу к ним;
* должно осуществляться уничтожение выведенных из употребления носителей.

## 6.4 Организация работ по защите информации от НСД

При эксплуатации ГИС:

* должны быть изданы правила и процедуры для администратора безопасности по защите от НСД к системе, разработанные на базе руководящих документов, а также настоящего технического проекта;
* должен быть назначен ответственный за обеспечение безопасности ПДн в ГИС - администратор безопасности ГИС;
* каждый исполнитель работ должен быть зарегистрирован в ГИС у администратора безопасности;
* при установке программного обеспечения СрЗИ следует руководствоваться эксплуатационной документацией на данные средства;
* должны быть реализованы меры, обеспечивающие восстановление информационных ресурсов и СЗГИС:
  1. создание резервных копий баз данных и информационных массивов в территориально-удаленных от основных технических средств обработки местах с ограниченным контролируемым доступом;
  2. должно быть обеспечено бесперебойное электропитание серверного оборудования;
  3. в случае необходимости должно быть предусмотрено резервирование технических средств ГИС;
  4. должно быть организовано ведение двух копий программных средств СЗГИС, их периодическое обновление и контроль работоспособности;
* обращение с ключевыми носителями должно осуществляться в соответствии с требованиями и рекомендациями ФСБ России.

## 6.5 Организация работы администратора безопасности

Администратор безопасности должен владеть информацией по настройке и эксплуатации средств защиты информации, применяемых в СЗГИС, в соответствии с поставляемой с ними эксплуатационной документацией, а также предписаниями и выписками из заключений, определяющими порядок их эксплуатации в ГИС.

Администратор безопасности осуществляет локальное и удаленное управление всеми СрЗИ из состава СЗГИС.

Администратор безопасности ведет журналы учета идентификаторов и паролей доступа пользователей к ТС, идентификаторов и паролей доступа администратора к ТС, регламентных работ с СЗГИС, учета неисправностей СЗГИС.

В случае лишения пользователя прав доступа (например, в связи со сменой работы или деятельности) его пароли и аутентифицирующая информация должны ликвидироваться администратором безопасности.

Оператором должен быть определен порядок смены атрибутов безопасности пользователей ГИС (в случае компрометации ключевой информации пользователей, в случае истечения срока действия паролей пользователей и т.п.).

Перед установкой программного обеспечения ГИС администратор безопасности должен провести его антивирусную проверку (проверку дистрибутивов устанавливаемого программного обеспечения).

Факты и попытки НСД к ПДн, а также случаи утечки обрабатываемых с использованием средств автоматизации ПДн регистрируются администратором безопасности в предназначенном для данных записей журнала, после чего им проводятся служебные расследования по выявленным фактам и попыткам НСД и случаям утечки защищаемой информации.

Администратор безопасности должен проводить:

* периодическое тестирование функций СЗГИС при изменении программной среды и пользователей информационной системы с помощью тест-программы анализа защищенности, имитирующей попытки НСД.
* регламентное тестирование реализации политики безопасности, в том числе: процесса идентификации и аутентификации пользователей и администраторов, в том числе процесса идентификации и аутентификации администратора СрЗИ, процесса регистрации действий администратора СрЗИ, процесса выполнения контроля целостности.

# 7 Порядок ввода СЗГИС в эксплуатацию

При создании СЗГИС в соответствии с предлагаемым техническим проектом должны выполняться следующие этапы работ.

## 7.1 Адаптация технических решений

### 7.1.1 Обследование объектов

Исполнитель должен провести инспекцию объекта информатизации Заказчика, с целью оценки степени готовности объекта к проведению работ по установке СЗИ, включая определение состава ИТ-инфраструктуры и количественных показателей, оценку актуальности угроз безопасности.

Заказчик должен предоставить доступ в помещения, где расположено сетевое оборудование, и к рабочим местам пользователей, подлежащих защите.

Заказчик должен предоставить техническую документацию на объект информатизации, включая документацию на инфраструктурные и прикладные сервисы, физические и логические схемы сетей, схемы коммутации и матрицы доступов и т.д.

Заказчик должен предоставить идентификационную и аутентификационную информацию, с уровнями привилегий, достаточными для выполнения работ по установке технических средств защиты информации.

Заказчик должен предоставить технические средства, находящиеся в исправном состоянии, с исправно функционирующим и лицензионным общесистемным и прикладным программным обеспечением.

По результатам инспекции объектов информатизации Исполнитель может сделать предложения по доработке информационных подсистем Заказчика на соответствие требованиям, предъявляемым настоящим проектом.

### 7.1.2 Предложения по доработке подсистем

С целью реализации оптимальной структуры СЗИ и контроля использования информационно-вычислительных ресурсов, Исполнитель должен проанализировать реализованные на объектах Заказчика схемы коммутации, маршрутизации и фильтрации сетевого трафика, схемы прохождения и обработки информационных потоков, а также разработать методику, позволяющую подготовить, настроить и интегрировать технические средства защиты информации в инфраструктуру Заказчика и согласовать её с Заказчиком в установленный срок.

Исполнитель должен подготовить предложения (дополнения к техническим решениям) по реализации оптимальных схем включения технических средств СЗИ в состав вычислительных сетей Заказчика и интеграции, развернутых на них программных сервисов.

## 7.2 Материальные затраты на приобретение средств защиты

Стоимость предлагаемых к использованию сертифицированных средств защиты представлена в таблице 7.2.1.

Таблица 7.2.1 – Стоимость сертифицированных технических средств защиты для основной конфигурации СЗГИС

|  |  |  |  |
| --- | --- | --- | --- |
| Продукт | Кол-во | Цена розничная, 1 шт., рублей | Общая стоимость, рублей |
| Dallas Lock 8.0-K с модулями «Межсетевой экран» и «Средство обнаружения и предотвращения вторжений». Право на использование (СЗИ НСД, СКН, МЭ, СОВ). | 8 | 10000 | 80000 |
| Kaspersky Endpoint Security 10 для Windows – электронная лицензия на 1 год | 8 | 1653 | 13224 |
| Средство анализа защищенности «Сканер-ВС» | 1 | 5000 | 5000 |
| Права на программы для ЭВМ Лицензия на использование программы «Сканер-ВС» на 8 IP-адресов на 1 год | 1 | 10000 | 10000 |
| Электронный идентификатор «Rutoken 4», защищённая память 64КБ | 8 | 1175 | 9400 |
| Средство доверенной загрузки ПАК «Dallas Lock» | 8 | 5000 | 40000 |
| Acronis Backup & Recovery 11 Server for Windows, лицензия на 1 год | 1 | 16900 | 16900 |
| Шлюз безопасности ViPNet Coordinator HW50 v4 | 1 | 73000 | 73000 |
| **Итого:** | **247 524** | | |

## 7.3 Поставка оборудования и программного обеспечения

Заказчик должен осуществить работы по закупке необходимых технических средств защиты информации, согласно ведомости покупных изделий, включая оборудование и программное обеспечение.

## 7.4 Ввод в действие

### 7.4.1 Установка и документирование СЗИ

Исполнитель должен провести монтаж и установку технических средств защиты информации на объект Заказчика, провести подключение поставленных технических средств защиты информации и технических средств Заказчика, а также обеспечить их интеграцию в ЛВС Заказчика.

Исполнитель должен документировать проделанные работы, по итогам которых должен представить Заказчику отчет, содержащий сведения, необходимые для работы технических служб.

Если в процессе проведения работ по установке и настройке СЗИ возникают какие-либо нештатные ситуации, а также ситуации, которые могут повлечь приостановление вышеуказанных работ, Исполнитель совместно с Заказчиком, принимает все возможные меры по устранению и ликвидации причин, которые привели к таким ситуациям.

### 7.4.2 Выполнение мероприятий по подготовке персонала

Подсистемы, входящие в СЗИ, обладают самым разнообразным функционалом, предназначенным для защиты информации. Для управления всем функционалом СЗГИС должны привлекаться специалисты, имеющие необходимую квалификацию в области защиты информации и администрирования установленных технических средств защиты информации.

Для обеспечения рационального подхода по комплектации кадров организации предлагается рассмотреть возможность направления специалиста на соответствующие курсы повышения квалификации в области информационной безопасности, а также технические курсы по соответствующим подсистемам защиты.

Для администратора безопасности Заказчика предлагается пройти учебный курс по защите персональных данных.

### 7.4.3 Организация необходимых подразделений и рабочих мест

Для обеспечения выполнения требований законодательства по защите информации, а также эффективного функционирования СЗИ, необходимо наличие штатного специалиста, ответственного за защиту информации. Согласно Положению «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» от 15.09.1993 г. № 912-51 и «Требованиям к защите персональных данных при их обработке в информационных системах персональных данных», утвержденным постановлением Правительства РФ от 01.11.2012 № 1119 Указанные подразделения (штатные специалисты) подчиняются непосредственно руководителю предприятия или его заместителю.

Таким образом, для обеспечения выполнения требований законодательства по защите информации, а также эффективного функционирования технических средств защиты информации, необходимо наличие штатного специалиста по защите информации, ответственного за защиту информации. Специалист по защите информации, будет управлять и контролировать работу СЗИ ГИС.

Специалист по защите информации (администратор безопасности) для выполнения своих функций будет иметь возможность осуществлять необходимые действия с любого рабочего места в организации, при наличии необходимых прав доступа.

### 7.4.4 Приемо-сдаточные испытания

В установленные сроки после окончания этапа работ по опытной эксплуатации Исполнитель должен разработать программу и методику приёмочных испытаний и согласовать её с Заказчиком.

Исполнитель совместно с Заказчиком должен провести работы, согласно разработанной Исполнителем программе и методике приемочных испытаний.

После окончания работ по приёмо-сдаточным испытаниям Заказчик совместно с Исполнителем должны подписать акт о проведении приёмо-сдаточных испытаний.

### 7.4.5 Предложения по доработке и развитию технических средств защиты информации

После окончания предыдущих этапов работ Исполнитель может сделать предложения Заказчику по развитию и доработке технических средств защиты информации, а также «обособленных» технических средств, функционирующих на площадках Заказчика на соответствие требованиям информационной безопасности и по защите персональных данных.

# Заключение

Результатом проектирования СЗГИС является создание программно-технического решения, представляющего собой совокупность взаимосвязано функционирующих подсистем, реализуемых как встроенными в операционные системы, так и наложенными СрЗИ, образующими единую СЗГИС, которая выполняет требования технического задания и нормативных документов в области обеспечения защиты информации.

Совокупность предложенных механизмов защиты информации, а также реализация организационно-режимных мероприятий позволит создать эффективную систему обеспечения безопасности информации в информационных системах, исключающую реализацию угроз информационной безопасности, перечисленных в документе «Модель угроз безопасности персональных данных при их обработке в государственной информационной системе «{ИМЯ\_ИС}».

ТП ГИС «{ИМЯ\_ИС}»

код ТП

СОСТАВИЛ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование организации предприятия | Должность исполнителя | Фамилия, имя, отчество | Подпись | Дата |
| ДВГУПС | студент | Королев И.А. |  |  |

СОГЛАСОВАНО

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование организации предприятия | Должность | Фамилия, имя, отчество | Подпись | Дата |
| ДВГУПС | Директор ДВУНЦ | Никитин В.В. |  |  |

# Лист регистрации изменений

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номера листов | | | | | Всего листов в доку- менте | Номер документа | Входящий № сопроводительного документа и дата | Подпись | Дата |
| Изм. | Измененных | Замененных | Новых | Аннулированных |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |