УТВЕРЖДАЮ

Председатель Счетной палаты

города Барнаула

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.М.Магель

«12» апреля 2017 г.

**Описание системы защиты персональных данных**

**Счетной палаты города Барнаула**

Содержание

[1. Общие сведения 3](#_Toc488825842)

[1.1 Основание для разработки 3](#_Toc488825843)

[1.2 Список используемых сокращений 3](#_Toc488825844)

[1.3 Законодательная и нормативно-методическая база 3](#_Toc488825845)

[2. Цели и задачи создания системы 4](#_Toc488825846)

[2.1 Цель создания системы 4](#_Toc488825847)

[2.2 Задачи создания системы 5](#_Toc488825848)

[3. Требования к СЗПДн 5](#_Toc488825849)

[3.1 Общие требования к техническим средствам защиты информации 5](#_Toc488825850)

[3.2 Требования к подсистеме управления доступом 5](#_Toc488825851)

[3.3 Требования к подсистеме регистрации и учета 5](#_Toc488825852)

[3.4 Требования к подсистеме обеспечения целостности 6](#_Toc488825853)

[3.5 Требования к подсистеме антивирусной защиты 6](#_Toc488825854)

[3.6 Требования к подсистеме безопасного межсетевого взаимодействия 6](#_Toc488825855)

[4. Угрозы безопасности ИСПДн 7](#_Toc488825856)

[5. Построение системы защиты персональных данных 7](#_Toc488825857)

[6. Основные технические решения 7](#_Toc488825858)

[6.1 Решения по защите от НСД 7](#_Toc488825859)

[6.2 Решения по антивирусной защите 7](#_Toc488825860)

[6.3 Решения по защите межсетевого взаимодействия 8](#_Toc488825861)

[7. Организационные мероприятия по защите ПДн в ИСПДн 8](#_Toc488825862)

[7.1 Общие требования 8](#_Toc488825863)

[7.2 Описание организационных мероприятий 8](#_Toc488825864)

# 1. Общие сведения

## 1.1 Основание для разработки

В настоящем Описании представлены основные технические решения по созданию системы защиты персональных данных, обрабатываемых с использованием средств автоматизации, для информационных систем персональных данных Счетной палаты города Барнаула (далее – Счетная палата).

## 1.2 Список используемых сокращений

ИС – информационная система

ИСПДн – информационная система персональных данных

МЭ – межсетевой экран

НДВ – недекларированные возможности

НСД – несанкционированный доступ

ОИ – объект информатизации

ПДн – персональные данные

РД – руководящий документ

СВТ – средство вычислительной техники

СЗИ – средство защиты информации

СЗИ НСД – средство защиты информации от несанкционированного доступа

СЗПДн – система защиты персональных данных

СКЗИ – средство криптографической защиты информации

СКН – средства контроля съемных носителей информации

СОВ – средства обнаружения вторжений

ПК – персональный компьютер

ПО – программное обеспечение

## 1.3 Законодательная и нормативно-методическая база

* Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных», устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн;
* Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30.08.2002 №282;
* ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
* ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования;
* постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* постановление Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
* постановление Правительства РФ от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
* приказ Федеральной службы по техническому и экспортному контролю от 05.02.2010 №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»;
* руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992);
* руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 25.07.1997);
* руководящий документ Защита от несанкционированного доступа к информации. Термины и определения (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992);
* руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992);
* руководящий документ. Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утв. решением Государственной технической комиссии при Президенте РФ от 04.06.1999 №114);
* другие нормативно-методические документы по обеспечению защиты информации.

# 2. Цели и задачи создания системы

## 2.1 Цель создания системы

Назначением СЗПДн является обеспечение информационной безопасности персональных данных, обрабатываемых в ИСПДн Счетной палаты.

Основной целью проведения работ является приведение порядка обработки персональных данных в Счетной палате в соответствие с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», нормативных правовых документов, в том числе в части требований к технической защите автоматизированных систем, обрабатывающих персональные данные.

Целью создания СЗПДн является исключение или существенное затруднение получения злоумышленником защищаемой информации, обрабатываемой в ИСПДн, а также исключение или существенное затруднение несанкционированного и/или непреднамеренного воздействия на защищаемую информацию и ее носители.

## 2.2 Задачи создания системы

Создаваемая СЗПДн должна обеспечивать эффективное решение следующих задач:

* защиту от вмешательства в процесс функционирования ОИ посторонних лиц (возможность использования ОИ и доступ к его ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
* разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ОИ;
* регистрацию действий пользователей при использовании защищаемых ресурсов ОИ Счетной палаты в системных журналах и периодический контроль корректности действий пользователей ОИ путем анализа содержимого этих журналов;
* контроль целостности среды исполнения программ;
* защиту от внедрения несанкционированных программ, включая компьютерные вирусы;
* обеспечение безопасного межсетевого взаимодействия;
* защиту конфиденциальной информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
* обнаружение вторжений.

# 3. Требования к СЗПДн

## 3.1 Общие требования к техническим средствам защиты информации

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

СЗПДн должна включать в себя следующие подсистемы:

* подсистема управления доступом;
* подсистема регистрации и учета;
* подсистема обеспечения целостности;
* подсистема антивирусной защиты;
* подсистема безопасного межсетевого взаимодействия;
* подсистема анализа защищённости;
* подсистема обнаружения вторжений.

## 3.2 Требования к подсистеме управления доступом

Подсистема управления доступом должна обеспечивать выполнение следующих требований: идентификация и проверка подлинности пользователя при входе в систему информационной системы по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

##

## 3.3 Требования к подсистеме регистрации и учета

Подсистема регистрации и учета должна обеспечивать выполнение следующих требований:

* регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. В параметрах регистрации указываются: дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы;
* учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета.

## 3.4 Требования к подсистеме обеспечения целостности

Подсистема обеспечения целостности должна обеспечивать выполнение следующих требований:

* обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. Целостность обеспечивается отсутствием в информационной системе средств разработки и отладки программ;
* физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;
* выполнение резервного копирования защищаемой информации.

##

## 3.5 Требования к подсистеме антивирусной защиты

Предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов).

## 3.6 Требования к подсистеме безопасного межсетевого взаимодействия

Подсистема безопасного межсетевого взаимодействия должна обеспечивать выполнение следующих требований:

* фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
* фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
* идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю;
* контроль целостности своей программной и информационной части;
* восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
* фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
* фильтрация с учетом любых значимых полей сетевых пакетов.

# 4. Угрозы безопасности ИСПДн

Актуальными угрозами безопасности в ИСПДн Счетной палаты являются угрозы несанкционированного доступа к информации:

* несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ;
* установка ПО, не связанного с исполнением служебных обязанностей;
* утрата ключей и атрибутов доступа;
* разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

# 5. Построение системы защиты персональных данных

Для обеспечения безопасности ПДн в ИСПДн Счетной палаты осуществляется:

* защита ПДн, обращающихся на СВТ, входящих в ИСПДн, от несанкционированного доступа с использованием СЗИ от НСД;
* защита ПДн, передаваемых по каналам связи;
* защита от утечки по техническим каналам;
* защита ПДн от вирусных угроз.

СЗПДн при выполнении организационно-режимных мероприятий по обеспечению безопасности информации в ИС обеспечивает выполнение требований, предъявленных к СЗПДн в разделе 4 данного документа, а также обеспечивает противодействие угрозам безопасности, описанным в разделе 5.

Построение СЗПДн в ИС заключается в применении сертифицированных средств защиты информации и обеспечении организационно-режимных мероприятий по защите информации в зависимости от структуры объекта, актуальности и показателя опасности угроз информационной безопасности на данном объекте.

# 6. Основные технические решения

## 6.1 Решения по защите от НСД

В качестве СЗИ от НСД для защиты персональных данных в ИСПДн применяется ПО «Secret Net Studio 8- С», Dallas Lock 8.0-K.

ПО «Secret Net Studio 8- С» имеет сертификат: ФСТЭК России как средство защиты информации на соответствие РД МЭ по 2 классу, РД СВТ по 3 классу и РД НДВ по 2 уровню.

ПО Dallas Lock 8.0-K имеет сертификат: ФСТЭК России №2720 от 25.09.2012 на соответствие 4 уровню контроля отсутствия НДВ, 5 классу защищенности от НСД, 3 классу защищенности МЭ, 4 классу защиты СОВ, 4 классу защиты СКН.

## 6.2 Решения по антивирусной защите

Для защиты от угроз внедрения вредоносных программ (вирусов) на защищаемых ПК установлена сертифицированная версия лицензионного ПО «Kaspersky Endpoint Security 10 для бизнеса».

Для защиты от угроз внедрения вредоносных программ (вирусов) на защищаемых серверах установлена сертифицированная версия лицензионного ПО ПО «Kaspersky Endpoint Security 10 для бизнеса».

## 6.3 Решения по защите межсетевого взаимодействия

Для защиты межсетевого взаимодействия и организации защищенных каналов связи на ПК пользователей ИСПДн применяется ПО «Secret Net Studio 8- С».

ПО «Secret Net Studio 8- С» имеет сертификат: ФСТЭК России как средство защиты информации на соответствие РД МЭ по 2 классу, РД СВТ по 3 классу и РД НДВ по 2 уровню.

Для защиты межсетевого взаимодействия в месте подключения внутренней сети Счетной палаты к сетям общего пользования а так же к сети Интернет на границе контролируемой зоны установлены программно-аппаратные комплексы межсетевого экранирования «ViPNet Coordinator HW1000».

# 7. Организационные мероприятия по защите ПДн в ИСПДн

## 7.1 Общие требования

В разделе описываются организационные (организационно-режимные, организационно-технические, кадровые) мероприятия по обеспечению информационной безопасности, по организации деятельности персонала, порядку эксплуатации технических средств системы в помещениях, систематическому выполнению мер по недопущению вывода системы из строя и контроля утечки защищаемой информации.

## 7.2 Описание организационных мероприятий

Проведенные организационные меры по защите ПДн включают:

* описание технологического процесса обработки информации;
* утверждение политики информационной безопасности;
* назначение ответственных за обеспечение безопасности ПДн;
* назначение ответственных за организацию обработки ПДн;
* назначение ответственных за организацию обработки ПДн с использованием средств криптографической защиты;
* создание перечня сотрудников, имеющих доступ к ПДн, обрабатываемым в ИСПДн;
* создание перечня сотрудников, работающих со средствами криптографической защиты;
* определение перечня помещений ограниченного доступа, в которых обрабатываются ПДн;
* сотрудники, имеющие доступ к ПДн, ознакомлены с имеющимися нормативными актами и организационно-распорядительными документами и инструкциями;
* сотрудники, работающие со средствами криптографической защиты, согласно программе обучения изучают техническую документацию к используемым средствам защиты, знакомятся с существующими нормативными правовыми актами и принятыми организационно-распорядительными документами;
* со всех сотрудников, имеющих доступ к ПДн, взято обязательство о неразглашении сведений конфиденциального характера;
* установка и настройка программного обеспечения СЗИ произведена в соответствии с требованиями технической и эксплуатационной документации к этим СЗИ;
* реализованы меры, обеспечивающие резервное копирование и восстановление информационных ресурсов ИСПДн. Утвержден регламент резервного копирования. В соответствии с регламентом ведется журнал резервного копирования;
* регламентирован порядок ремонта и технического обслуживания технических средств ИСПДн;
* в целях организации работы с носителями информации, содержащими ПДн, введен журнал учета электронных носителей информации;
* при хранении материальных носителей соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.