Содержание

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 комитета по образованию города Барнаула (далее - Комитет).

1.2 Список используемых сокращений

АП - абонентский пункт
АРМ - автоматизированное рабочее место
АС - автоматизированная система
ИБ - информационная безопасность
ИС - информационная система
ИСПДн - информационная система персональных данных
КЗ - контролируемая зона
ЛВС - локальная вычислительная сеть
МЭ - межсетевой экран
НСД - несанкционированный доступ
ОИ - объект информатизации
ОПО - общесистемное программное обеспечение
ПДн - персональные данные
ППО - прикладное программное обеспечение
РД - руководящий документ
СВТ - средство вычислительной техники
СЗИ - средство защиты информации
СЗИ НСД - средство защиты информации от несанкционированного доступа
СКЗИ - средство криптографической защиты информации
ТЗ - техническое задание
ПО - программное обеспечение
ЭЦП - электронная цифровая подпись

1.3 Законодательная и нормативно-методическая база

- Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее - 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), утверждены приказом Гостехкомиссии России от 30.08.2002 г. №282.
- Извещение о корректировке Специальных требований и рекомендаций по технической защите конфиденциальной информации 2006, 2008.
- Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим калам, 2002.
- ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении.
- ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.

- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные постановлением Правительства РФ от 1 ноября 2012г. №1119.

- «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. №687.

- «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.

- Приказ Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. № 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 марта 1992 г.).

- 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 июля 1997 г.).

- Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.).

- 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 марта 1992 г.).

- Руководящий документ. Защита от несанкционированного доступа к информации Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей (утв. решением Государственной технической комиссии при Президенте РФ от 4 июня 1999 г. N 114).

- и 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 Комитета.

Основной целью проведения работ является приведение порядка обработки персональных данных в Комитете в соответствие с требованиями Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», нормативно-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 установленным порядком пользователи);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ОИ;
- регистрацию действий пользователей при использовании защищаемых ресурсов ОИ Комитета 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.

3.1 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, установленным порядком 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 проверки 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

4.1 Перечень актуальных угроз безопасности в ИСПДн

Актуальными угрозами безопасности в ИСПДн Комитета являются:

Угрозы несанкционированного доступа к информации.

— Кража ключей и атрибутов доступа.
— Кража, модификация, уничтожение 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.
— Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке.
— Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

Угрозы утечки по видовым каналам.

— Угроза подсматривания конфиденциальной информации с мониторов ПК.

Угрозы несанкционированного доступа по каналам связи. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:

— Перехват в пределах контролируемой зоны внутренними нарушителями.
— Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.
— Угрозы выявления паролей по сети.
— Угрозы удаленного запуска приложений.
— Угрозы внедрения по сети вредоносных программ.

5. ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для обеспечения безопасности ПДн в ИСПДн Комитета 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 сертифицированное программное обеспечение.

6.2 Решения по защите от утечки ПДн за счет ПЭМИН

В информационных системах для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники. Угрозы утечки по каналам ПЭМИН не актуальны.

6.3 Решения по защите от утечки ПДн по видовому каналу

Для защиты от утечки ПДн по видовому каналу ПК устанавливаются таким образом, чтобы исключить возможность просмотра посторонними лицами текстовой и графической информации, содержащей персональные данные с монитора компьютера.

6.4 Решения по антивирусной защите

Для защиты от угроз внедрения вредоносных программ (вирусов) на защищаемых ПК установлена сертифицированная версия лицензионного ПО.

6.5 Решения по защите межсетевого взаимодействия

Для защиты межсетевого взаимодействия и организации защищенных каналов связи на ПК пользователей ИСПДн применяется межсетевой экран.

ПО имеет сертификаты:

- ФСБ России как средство межсетевого экранирования 4 класса защищенности;
- ФСБ России как средство криптографической защиты информации (шифрование файлов, данных, содержащихся в областях оперативной памяти,

и IP-трафика, вычисление имитовставки для файлов, данных содержащихся в оперативной памяти и 1Р-трафика, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти).

Таким образом, ПО полностью соответствует всем требованиям безопасности, предъявляемым в части обеспечении безопасности межсетевого экранирования, а так же выполняет функции клиентского криптографического клиента для подключения к защищенной сети передачи данных.

Для защиты межсетевого взаимодействия в месте подключения внутренней сети Комитета к сетям общего пользования а так же к сети Интернет на границе контролируемой зоны установлены программно-аппаратные комплексы межсетевого экранирования. Схема подключения приведена на рисунке 1.

На схеме введены следующие обозначения:

LAN - внутренняя сеть Администрации
КСПД - корпоративная сеть администрации Алтайского края

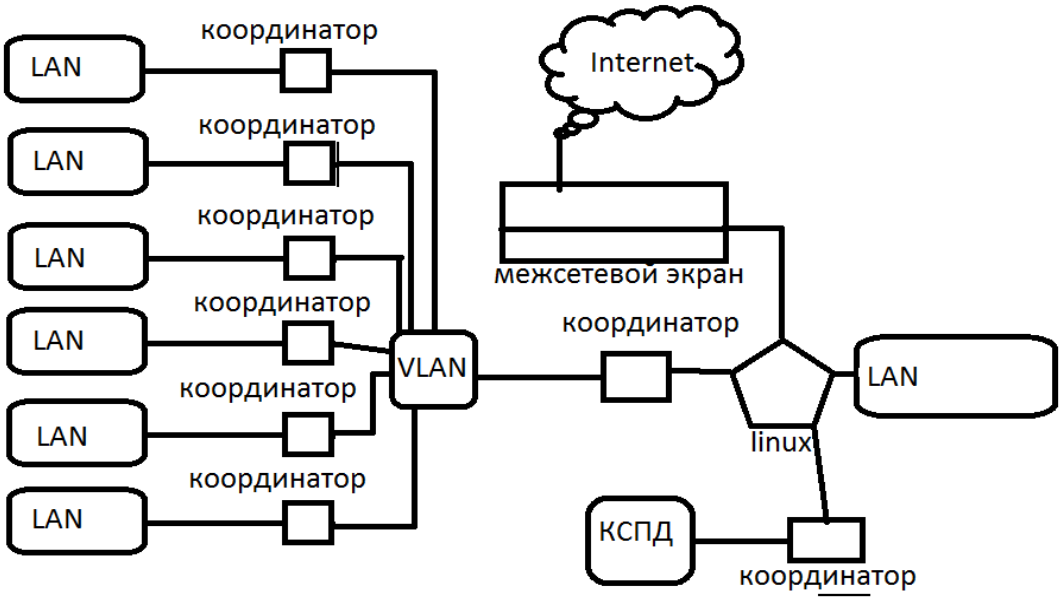

Рисунок 1

7. ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИДИ 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;
- 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 нормативно-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 требования технической и эксплуатационной документацией 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 обслуживание технических средств ИСПДн;
- в целях организации работы с носителями информации, содержащими ПДн введены журналы учета НЖМД и учета съемных носителей информации;
- при хранении, материальных носителей соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.