|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | |
|  |  | | |  |  | | --- | --- | | Приложение № 9 | | | к приказу от \_\_\_\_\_\_ 201\_ № \_\_\_\_\_\_ | | |  |  |  | | |
|  |  | |  |
|  |  | |  |
|  |  | |  |
| ОПИСАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ  при их обработке в информационных системах персональных данных УПРАВЛЕНИЯ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ КРАСНОГОРСКОГО МУНИЦИПАЛЬНОГО РАЙОНА | | | |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |

|  |
| --- |
|  |

Содержание

[Содержание 2](#_Toc414274528)

[Термины и определения 3](#_Toc414274529)

[Сокращения 3](#_Toc414274530)

[1. Общие сведения 4](#_Toc414274531)

[2. Описание ИСПДн 5](#_Toc414274532)

[2.1. Общие сведения 5](#_Toc414274533)

[3. Выбор мер по обеспечению безопасности персональных данных 6](#_Toc414274534)

[3.1. Определение базового набора мер защиты информации 6](#_Toc414274535)

[3.2. Адаптация базового набора мер защиты информации 9](#_Toc414274536)

[3.3. Уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных 10](#_Toc414274537)

[3.4. Дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных 10](#_Toc414274538)

[3.5. Результаты определения состава и содержания мер защиты информации 11](#_Toc414274539)

[4. Структура и функции системы защиты персональных данных 13](#_Toc414274540)

Термины и определения

|  |  |
| --- | --- |
| Информационная система персональных данных | Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств |
| Несанкционированный доступ (несанкционированные действия) | Доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам |
| Обработка персональных данных | Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных |
| Персональные данные | Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) |

Сокращения

|  |  |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| ИСПДн | Информационная система персональных данных |
| НСД | Несанкционированный доступ (несанкционированные действия) |
| ПДн | Персональные данные |
| СЗИ | Средство защиты информации |

1. Общие сведения

Настоящее Описание системы защиты персональных данных при их обработке в ИСПДн Управления образования администрации Красногорского муниципального района (далее - Учреждение) разработано на основании следующих нормативно-методических документов:

* Федеральный закон от 27.07. 2006 года № 152-ФЗ «О персональных данных»;
* постановление Правительства Российской Федерации от 01.11. 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1. Описание ИСПДн
   1. Общие сведения

ИСПДн «ЛВС УО» по структуре являются автоматизированными рабочими местами, имеющими подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Требуемый уровень защищенности персональных данных при их обработке в ИСПДн – четвертый (УЗ 4).

ИСПДн «ЛВС УО» по режиму обработки ПДн относятся к многопользовательским системам без разграничения прав доступа пользователей.

В ИСПДн не предусмотрено использование технологий беспроводного доступа.

В ИСПДн не предусмотрено использование мобильных технических средств.

Взаимодействие с внешними информационными системами не осуществляется.

В ИСПДн не применяется виртуальная инфраструктура.

Передача персональных данных по каналам связи, имеющим выход за пределы контролируемой зоны не осуществляется.

ИСПДн «Сетевой город» по структуре являются Сервером, имеющим подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Требуемый уровень защищенности персональных данных при их обработке в ИСПДн – четвертый (УЗ 4).

ИСПДн «Сетевой город» по режиму обработки ПДн относятся к многопользовательским системам с разграничением прав доступа пользователей.

В ИСПДн не предусмотрено использование технологий беспроводного доступа.

В ИСПДн не предусмотрено использование мобильных технических средств.

Взаимодействие с внешними информационными системами не осуществляется.

В ИСПДн не применяется виртуальная инфраструктура.

Передача персональных данных по каналам связи, имеющим выход за пределы контролируемой зоны не осуществляется.

1. Выбор мер по обеспечению безопасности персональных данных

Выбор мер по обеспечению безопасности ПДн, подлежащих реализации в рамках системы защиты персональных данных в соответствии с приказом ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее - Приказ № 21), включает:

* **определение базового набора мер** защиты информации для установленного уровня защищенности ПДн в соответствии с базовыми наборами мер по обеспечению безопасности ПДн, приведенными в Приказе № 21;
* **адаптацию базового набора мер** по обеспечению безопасности ПДн с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);
* **уточнение адаптированного базового набора мер** по обеспечению безопасности ПДн с учетом не выбранных ранее мер, приведенных в Приказе № 21, в результате чего определяются меры по обеспечению безопасности ПДн, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных;
* **дополнение уточненного адаптированного базового набора мер** по обеспечению безопасности ПДн мерами, обеспечивающими выполнение требований к защите ПДн, установленными иными нормативными правовыми актами в области обеспечения безопасности ПДн и защиты информации.
  1. Определение базового набора мер защиты информации

Базовый набор мер по обеспечению безопасности ПДн, определенный для 4-го уровня защищенности в соответствии с Приказом № 21, приводится в табл. 1.

Таблица 1.

| Индекс меры | Наименование меры |
| --- | --- |
|
|  |
| **Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |
| **Управление доступом субъектов доступа к объектам доступа (УПД)** | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |
| **Регистрация событий безопасности (РСБ)** | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения |
| РСБ.7 | Защита информации о событиях безопасности |
| **Антивирусная защита (АВЗ)** | |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| **Контроль (анализ) защищенности персональных данных (АНЗ)** | |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| **Защита среды виртуализации (ЗСВ)** | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| **Защита технических средств (ЗТС)** | |
| ЗТС.3 | 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 и помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| **Защита информационной системы, ее средств, систем связи и передачи данных (3ИС)** | |
| ЗИС.3 | 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 |

* 1. Адаптация базового набора мер защиты информации

По результатам рассмотрения структурно-функциональных характеристик информационной системы, применяемых информационных технологий и особенностей функционирования информационной системы были внесены изменения в базовый набор мер по обеспечению безопасности ПДн. Перечень внесенных изменений с указанием обоснования приведен в табл. 2.

Таблица 2.

| Индекс меры | Наименование меры | Изменение (добавлена/ исключена) | Обоснование |
| --- | --- | --- | --- |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | исключена | В информационной системе не предусмотрено использование технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | исключена | В информационной системе не предусмотрено использование мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | исключена | Взаимодействие с внешними информационными системами не осуществляется |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | исключена | В информационной системе не применяется виртуальная инфраструктура |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | исключена | В информационной системе не применяется виртуальная инфраструктура |
| ЗИС.3 | 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 | исключена | Передача персональных данных по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи не осуществляется |

* 1. Уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных

По результатам рассмотрения актуальных угроз безопасности ПДн не было выявлено необходимости внесения изменений в адаптированный базовый набор мер по обеспечению безопасности ПДн.

* 1. Дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных

По результатам рассмотрения требований к защите ПДн, установленных нормативными правовыми актами в области обеспечения безопасности ПДн и защиты информации не было выявлено необходимости внесения изменений в уточненный адаптированный базовый набор мер по обеспечению безопасности ПДн.

* 1. Результаты определения состава и содержания мер защиты информации

Результаты определения состава и содержания мер защиты информации, подлежащих реализации в системе защиты персональных данных, приводится в сводной табл. 3.

Таблица 3.

| Индекс меры | Наименование меры |
| --- | --- |
| **Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)** | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |
| **Управление доступом субъектов доступа к объектам доступа (УПД)** | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| **Регистрация событий безопасности (РСБ)** | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения |
| РСБ.7 | Защита информации о событиях безопасности |
| **Антивирусная защита (АВЗ)** | |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| **Контроль (анализ) защищенности информации (АНЗ)** | |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| **Защита технических средств (ЗТС)** | |
| ЗТС.3 | 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 и помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |

1. Структура и функции системы защиты персональных данных

СЗПДн предполагает реализацию организационно-технических мер. В рамках технических мер предполагается установка следующих средств защиты информации на каждое АРМ входящее в состав ИСПДн «ЛВС УО»:



На сервер входящий в состав ИСПДн «Сетевой город» предлагается установить:



Функции защиты, реализуемые средствами защиты информации и наименования средств защиты, приведены в табл. 4.

Таблица 4.

| **№ п/п** | **Тип средства защиты информации** | **Наименование средства защиты информации** | **Реализуемые функции защиты** |
| --- | --- | --- | --- |
|  | Средство защиты от НСД | Secret Net 7 | * ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.5; * УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.13; * РСБ.3, РСБ.7. |
|  | Межсетевой экран | Security Studio Endpoint Protection | * ИАФ.6, УПД.13 |
|  | Средство антивирусной защиты | Security Studio Endpoint Protection | * РСБ.3, РСБ.7; * УПД.3; * АВЗ.1, АВЗ.2. |

Меры по обеспечению безопасности персональных данных РСБ.1, РСБ.2, АНЗ.2, ЗТС.3, ЗТС.4 реализуются путем обеспечения физической защиты и проведения соответствующих организационных мероприятий, рассматриваемых в локальных актах Учреждения.