Приложение №1 к Приказу
№ 300 от 13.06.2023г.

УТВЕРЖДАЮ

Директор
Государственного бюджетного
общеобразовательного учреждения Липецкой
области "Специальная школа-интернат города
Задонска"
_____Н.И. Левченко
«13» июня 2023г.

Положение о защите персональных данных
на объекте информатизации
«АРМ, подключаемый к федеральной информационной системе
«Федеральный реестр сведений документов об образовании и (или) о квалификации,
документах об обучении»

1. Общие положения

Положение о защите персональных данных на объекте информатизации «АРМ подключаемый к федеральной информационной системе «Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении» (далее – Положение) устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке на объекте информатизации «АРМ подключаемый к федеральной информационной системе «Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении» в ГБОУ "Специальная школа-интернат г.Задонска".

Меры по обеспечению безопасности персональных данных, обрабатываемых на объекте информатизации «АРМ подключаемый к федеральной информационной системе «Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении» (далее – АРМ подключаемый к ФИС «ФРДО»), принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных, обрабатываемых на объекте информатизации АРМ подключаемый к ФИС «ФРДО».

Меры по обеспечению безопасности персональных данных, обрабатываемых на объекте информатизации АРМ, подключаемый к ФИС «ФРДО», реализуются в рамках системы защиты в соответствии с требованиями к защите информации, установленными нормативно-правовыми актами, приведенными в п. 2 настоящего Положения, и направлены на нейтрализацию актуальных угроз безопасности персональных данных, обрабатываемых на объекте информатизации АРМ, подключаемый к ФИС «ФРДО»

Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий защиты ПДн, обрабатываемых на объекте информатизации АРМ, подключаемый к ФИС «ФРДО»

2. Нормативные ссылки

Положение разработано с учетом требований следующих нормативных правовых актов:

– Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной Обработке персональных данных»;

– Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;

– Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России от 18 февраля 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».

При разработке настоящего положения также были учтены утвержденные в ГБОУ "Специальная школа-интернат г.Задонска" Акт об установлении уровня защищенности персональных данных при их обработке на объекте информатизации АРМ подключаемый к ФИС «ФРДО».

3. Описание объекта информатизации АРМ, подключаемый к ФИС «ФРДО»

Объект информатизации АРМ подключаемый к ФИС «ФРДО» располагается по адресу: 399200, Липецкая область, г.Задонск, ул. Крупской, д.13.

Актом об установлении уровня защищенности персональных данных при их обработке на объекте информатизации АРМ подключаемый к ФИС «ФРДО» комиссией ГБОУ "Специальная школа-интернат г.Задонска" был установлен 4-й уровень защищенности персональных данных.

4. Выбор мер по обеспечению безопасности персональных данных, обрабатываемых на объекте информатизации АРМ, подключаемый к ФИС «ФРДО»

В соответствии с Приказом ФСТЭК России от 18 февраля 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» базовый набор мер, необходимых для обеспечения 4-го уровня защищённости, включает в себя меры, приведенные в таблице 1 настоящего Положения.

Таблица 1.

Условное обозначение меры	Содержание мер защиты информации
I. 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)
II. 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) пользователей, администраторов и лиц,

Условное обозначение меры	Содержание мер защиты информации
	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)
V. 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 течение установленного времени хранения
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
XI. 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
XII. 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
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
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

ГБОУ "Специальная школа-интернат г.Задонска" проведена адаптация базового набора мер с учетом структурно-функциональных характеристик ИСПДн, информационных технологий и особенностей функционирования объекта информатизации. Из базового набора мер исключены следующие меры, приведенные в таблице 2.

Таблица 2.

Условное обозначение меры	Содержание мер защиты информации	Причина исключения из базового набора мер
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	В ИСПДн нет внешних пользователей
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Удалённый доступ через внешние информационно-телекоммуникационные сети не осуществляется
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Технологии беспроводного доступа не используются
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Мобильные технические средства не используются
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	В ИСПДн не используется среда виртуализации
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Беспроводной доступ не используется

Для нейтрализации всех актуальных угроз безопасности персональных данных ИСПДн произведено уточнение полученного набора мера путем его дополнения с учетом не выбранных ранее мер.

Для исключения возможности несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированного использования съемных машинных носителей персональных данных добавлены меры по защите машинных носителей персональных данных (ЗНИ.1, ЗНИ.5, ЗНИ.7, ЗНИ.8).

В базовый набор мер входит ряд мер, направленных на сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе. Данный набор дополнен мерой, обеспечивающей возможность просмотра и анализа информации о таких событиях (РСБ.5).

Добавлена мера по ограничению программной среды, регламентирующая установку (инсталляцию) только разрешенного программного обеспечения и (или) его компонентов (ОПС.3).

Увеличено количество мер, направленных на обеспечение контроля (анализа) защищенности персональных данных, в том числе контроля состава и работоспособности технических средств и средств защиты информации, а также реализации правил разграничения доступа к персональным данным (АНЗ.3, АНЗ.4, АНЗ.5).

Добавлена мера по обеспечению целостности ИСПДн (ОЦЛ.3).

С целью снижения риска неработоспособности технических средств и программных средств обработки информации использованы меры: ОДТ.4, ОДТ.5.

Добавлены меры по защите технических средств (ЗТС.2, ЗТС.5), по выявлению инцидентов и реагированию на них (ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, ИНЦ.6), а также по управлению конфигурацией информационной системы и системы защиты персональных данных (УКФ.1, УКФ.2, УКФ.3, УКФ.4).

Дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации, не требуется, в связи с тем, что необходимые и достаточные меры для нейтрализации актуальных угроз безопасности персональных данных в ИСПДн были выбраны на предыдущих этапах.

В состав мер по обеспечению безопасности персональных данных в ИСПДн, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей персональных данных;
- регистрация событий безопасности;
- антивирусная защита;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Более подробное описание выбранных мер по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, а также способ их реализации приведены в таблице 5.

Знаком «+» обозначены меры по обеспечению безопасности персональных данных, которые включены в базовый набор мер для 4-го уровня защищенности.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком «+», были добавлены при уточнении адаптированного базового набора мер.

Таблица 3.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровень защищенности ПДн	Способ реализации мер защиты информации
		4	
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	СЗИ от НСД
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	СЗИ от НСД
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или)	+	Применение организационно-технических мер

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровень защищенности ПДн	Способ реализации мер защиты информации
		4	
	компрометации средств аутентификации		
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	СЗИ от НСД
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	СЗИ от НСД
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	СЗИ от НСД
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	+	СКЗИ
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	СЗИ от НСД
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	СЗИ от НСД
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	СЗИ от НСД
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).	+	СКЗИ
V. Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	СЗИ от НСД
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	СЗИ от НСД
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	СЗИ от НСД
РСБ. 7	Защита информации о событиях безопасности	+	СЗИ от НСД

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровень защищенности ПДн	Способ реализации мер защиты информации
		4	
VI. Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты	+	САВЗ
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	САВЗ
VIII. Контроль (анализ) защищенности информации (АНЗ)			
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	Применение организационных мер
X. Обеспечение доступности персональных данных (ОДТ)			
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных		Применение организационных мер
ОДТ. 5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала		Применение организационных мер
XII. 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, в помещения и сооружения, в которых они установлены	+	Применение организационно-технических мер
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	Применение организационных мер
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.3	Обеспечение защиты персональных данных 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	+	СКЗИ

В соответствии с постановлением Правительства РФ от 01 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных» состав и содержание мер, по обеспечению безопасности необходимых для обеспечения 4-го уровня защищённости ПДн, обрабатываемых на объекте информатизации «АРМ подключаемый к федеральной информационной системе «Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении», включает в себя меры, приведенные в таблице 4 настоящего Положения.

Таблица 4.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Способ реализации мер защиты информации
1119.а	Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	Принятие организационных мер
1119.б	Обеспечение сохранности носителей персональных данных	Принятие организационных мер
1119.в	Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	Принятие организационных мер
1119.г	Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	Принятие организационных мер

5. Реализация мер по обеспечению безопасности персональных данных в ИСПДн

3.1. Для реализации технических мер по обеспечению безопасности персональных данных в ИСПДн необходимо осуществить выбор, установку и настройку средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, в соответствии с установленным уровнем защищенности персональных данных и с учетом типа актуальных угроз.

3.2. Организационные меры по обеспечению безопасности персональных данных в ИСПД необходимо реализовать путем утверждения инструкций, регламентирующих функции, задачи и обязанности ответственных лиц и иных пользователей, инструкций, определяющих правила и процедуры управления системой защиты информации информационной системы, выявления инцидентов безопасности обработки персональных данных, осуществления резервного копирования информации, содержащей персональные данные, а также определения правил разграничения доступа субъектов доступа к объектам доступа.

3.3. Для контроля за соблюдением мер по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, необходимо разработать документы, определяющие правила и процедуры проведения внутреннего контроля (анализа) защищенности персональных данных, в том числе контроля за обеспечением уровня защищенности персональных данных, содержащихся в ИСПДн.