**УТВЕРЖДАЮ**
Директор

Ильина М.Б.
«28» октября 2025 г.

СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ
ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ
В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
«АБОНЕНТСКИЙ ПУНКТ №13 РЕГИОНАЛЬНОЙ
ИНФОРМАЦИОННОЙ СИСТЕМЫ ЦИФРОВОЕ ОБРАЗОВАНИЕ
ПСКОВСКОЙ ОБЛАСТИ»

# ТЕХНИЧЕСКОЕ ЗАДАНИЕ

1 Общие сведения

1.1 Наименование создаваемой системы защиты информации

Система защиты персональных данных при их обработке в информационной системе персональных данных «Абонентский пункт №13 региональной информационной системы Цифровое образование Псковской области» (далее по тексту – «СЗПДн»).

1.2 Сведения об операторе, обрабатывающем персональные данные:

Наименование: ICL Win-S9HDL204AA9 RAYbook Si1507

Место нахождения: г. Псков, ул. 23 Июля дом 9.

Место установки: Кабинет №19.

1.3 Перечень документов, на основании и в соответствии с которыми создается СЗПДн:

- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

- Постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правыми актами, операторами, являющимися государственными или муниципальными органами.

- 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».

- Нормативно-технический документ. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (утвержден приказом Гостехкомиссии России № 282 от 30.08.2002).

- ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на

автоматизированные системы. Техническое задание на создание автоматизированной системы.

- ГОСТ РО 0043-003-2012 «Защита информации. Аттестации объектов информатизации. Программа и методики аттестационных испытаний».

**2 Назначение и цели создания СЗПДн**

2.1 Назначение СЗПДн

Обеспечение безопасности персональных данных («ПДн») при их обработке в информационной системе персональных данных «Абонентский пункт региональной информационной системы Цифровое образование Псковской области» (далее по тексту - «ИСПДн»).

2.2 Цели создания СЗПДн:

- Принятие необходимых правовых, организационных и технических мер для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий в отношении персональных данных;

- Выполнение требований нормативных правовых актов Российской Федерации, руководящих документов ФСТЭК России, регламентирующих вопросы защиты персональных данных, в том числе требований по обеспечению уровня защищенности персональных данных при их обработке в ИСПДн.

**3 Характеристика и организационная структура ИСПДн, в которой обрабатываются ПДн**

3.1 Характеристика и организационная структура ИСПДн приведены в Акте обследования ИСПДн.

3.2 По структуре ИСПДн представляет собой комплекс, состоящий из автоматизированного рабочего места (АРМ), периферийного оборудования и средств коммуникаций, объединенных в единую информационную систему. По территориальному размещению - локальная ИСПДн, развернутая в пределах одного здания. ИСПДн имеет подключение к сети связи общего пользования.

3.3 По результатам анализа исходных данных и сведений, в соответствии с требованиями к защите персональных данных, утвержденными постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите

персональных данных при их обработке в информационных системах персональных данных», установлена необходимость обеспечения **3–го уровня защищенности** персональных данных при их обработке в ИСПДн.

**4 Требования к СЗПДн**

4.1 Общие положения и требования

4.1.1 СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

4.1.2 Собственные средства защиты не разрабатываются. Должны использоваться существующие, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

4.1.3 Средства защиты информации, входящие в состав СЗПДн, должны быть совместимы с программными, программно-техническими средствами ИСПДн.

4.1.4 Защита информации должна обеспечиваться на всех технологических этапах ее обработки и во всех режимах функционирования СЗПДн, в том числе при проведении ремонтных и регламентных работ по техническому обслуживанию.

4.1.5 Применяемые в составе СЗПДн программные, программно-аппаратные и технические средства защиты информации не должны существенно ухудшать основные функциональные параметры и характеристики существующей ИСПДн.

4.2 Требования для обеспечения уровня защищенности персональных данных при их обработке в ИСПДн

Требования для обеспечения **3-го уровня защищенности** персональных данных при их обработке в ИСПДн должны соответствовать требованиям к защите персональных данных, утвержденным постановлением Правительства от 01.11.2012 № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных», а именно:

а) организация режима обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации для нейтрализации актуальных угроз, определенных в Частной модели угроз.

4.3 Требования к СЗПДн для реализации организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, установленных приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

4.3.1 Организационные и технические меры по обеспечению безопасности персональных данных, необходимые для обеспечения требуемого уровня защищенности, должны соответствовать составу и содержанию мер, утвержденных приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.3.2 Состав и содержание адаптированного базового набора организационных и технических мер по обеспечению безопасности персональных данных (с учетом актуальных угроз безопасности, структурно-функциональных характеристик ИСПДн, особенностей функционирования ИСПДн), которые необходимо реализовать в СЗПДн для обеспечения **3-го уровня защищенности** персональных данных, приведены в таблице 4.1

Таблица 4.1

| Условное обозначение и номер меры | Состав и содержание мер по обеспечению безопасности персональных данных |
|---|---|
| **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 |
| **Управление доступом субъектов доступа к объектам доступа (УПД)** | |
| УПД. 1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями 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, 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.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| **Защита машинных носителей персональных данных (ЗНИ)** | |
| ЗНИ.8 | Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания |
| **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 |
| **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.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ. 2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и 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, в 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 (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 |
| **Требования по обеспечению 3-го уровня защищённости персональных данных при их обработке в информационной системе** | |
| ЗПД.1 | 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 |
| ЗПД.2 | Обеспечение сохранности носителей персональных данных |
| ЗПД.3 | Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей |
| ЗПД.4 | Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в |

| | |
|---|---|
| | случае, когда применение таких средств необходимо для нейтрализации актуальных угроз |

| **Требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимые для обеспечения 3-го уровня защищённости персональных данных (ЗКС)** | |
|---|---|
| ЗКС.1 | Оснащение помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения) входными дверьми с замками, обеспечение постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывание Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений |
| ЗКС.2 | Утверждение правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях |
| ЗКС.3 | Утверждение перечня лиц, имеющих право доступа в Помещения |
| ЗКС.4 | Хранение съёмных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съёмном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов) |
| ЗКС.5 | Поэкземплярный учёт машинных носителей персональных данных, который достигается путём ведения журнала учёта носителей персональных данных с использованием регистрационных (заводских) номеров |
| ЗКС.6 | Применение СКЗИ соответствующего класса, позволяющих обеспечивать безопасность персональных данных при реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых СКЗИ персональных данных или создания условий для этого |

| Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) | |
|---|---|
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных |
| УКФ.3 | 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 |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных |

4.3.3 Для реализации мер по обеспечению безопасности персональных данных должны быть выполнены организационные мероприятия по защите персональных данных, а также выбраны, установлены и проверены технические и программные средства защиты в соответствии с составом и содержанием адаптированного базового набора организационных и технических мер по обеспечению безопасности персональных данных, приведенных в таблице 4.1.

4.3.4 Установка и проверка технических и программных средств защиты должна осуществляться в соответствии с технической и эксплуатационной документацией на эти средства.

4.4 Требование к надежности

Комплекс программно-технических средств СЗПДн должен быть рассчитан для функционирования в режиме круглосуточной работы и позволять осуществлять выполнение процедур резервирования и восстановления системы после сбоев.

4.5 Требования безопасности

В процессе обслуживания и эксплуатации комплекса программно-технических средств СЗПДн должны выполняться требования по обеспечению безопасности обслуживающего персонала, предъявляемые к техническим средствам АРМ в целом.

4.6 Требования к эксплуатации, техническому обслуживанию, ремонту и

хранению компонентов СЗПДн.

4.6.1 Эксплуатация комплекса программно-технических средств СЗПДн должна осуществляться в полном соответствии с эксплуатационной документацией и утвержденной организационно-распорядительной документацией по защите информации (приказов, инструкций и других документов).

4.6.2 Объем, порядок выполнения технического обслуживания, а также ремонта и хранения технических и программных средств СЗПДн должны определяться эксплуатационной документацией.