

УТВЕРЖДАЮ

Директор

Ильина М.Б.

«28» октября 2025 г.



ПРОГРАММА И МЕТОДИКИ

оценки эффективности реализованных мер по обеспечению безопасности
персональных данных в информационной системе персональных данных
«Абонентский пункт №13 региональной информационной системы Цифровое
образование Псковской области»

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ	3
1. ОБЩИЕ ПОЛОЖЕНИЯ	4
1.1. Объект оценки	4
1.2. Состав комиссии по оценке	4
1.3. Цель и задачи испытаний	4
2. ПРОГРАММА ИСПЫТАНИЙ	5
2.1. Перечень проверок и испытаний и их последовательность	5
2.2. Подготовка отчётной документации и оценка результатов испытаний	6
2.3. Контроль соответствия СЗПДн требованиям безопасности информации в процессе эксплуатации	Ошибка! Закладка не определена.
3. МЕТОДИКА ИСПЫТАНИЙ	6
3.1. Проверка структуры, состава и условий эксплуатации информационной системы ..	6
3.2. Проверка состояния организации работ и выполнения требований по защите информации	8
3.3. Проверка информационной системы на соответствие требованиям безопасности информации	8
3.4. Проведение испытаний информационной системы на соответствие требованиям по защите информации от несанкционированного доступа	9
ПРИЛОЖЕНИЕ А	10

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	– автоматизированное рабочее место;
ГОСТ	– национальный стандарт Российской Федерации;
ИСПДн	– информационная система персональных данных;
ОТСС	– основные технические средства и системы;
СВТ	– средства вычислительной техники;
ФСБ России	– Федеральная служба безопасности Российской Федерации;
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Объект оценки

Объектом оценки эффективности, принимаемых в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных является информационная система персональных данных «Абонентский пункт **№13** региональной информационной системы Цифровое образование Псковской области» (далее – ИСПДн «АП РИС ЦОПО») с созданной системой защиты персональных данных, для которой установлена необходимость обеспечения 3-го уровня защищённости персональных данных (УЗЗ).

Оценка эффективности реализованных мер по обеспечению безопасности персональных данных проводится в виде комплексных испытаний ИСПДн «АП РИС ЦОПО» (далее – испытания) на соответствие положениям и требованиям действующих нормативных правовых актов, методических документов и национальных стандартов в области защиты информации (Приложение А).

1.2. Состав комиссии по оценке

1.2.1. Комиссия по оценке эффективности реализованных мер по обеспечению безопасности персональных данных назначается [] из числа штатных сотрудников.

1.2.2. В соответствии с приказом [] в состав комиссии включены:

	Должность	Наименование организации	Фамилия, имя, отчество
Председатель	Директор	Муниципальное бюджетное общеобразовательное учреждение «Средняя общеобразовательная школа № 18 имени Героя Советского Союза генерала армии В.Ф.Маргелова»	Ильина М.Б.
Члены комиссии:	Учитель информатики		Косаржевская К.С.
	Завуч по учебно-воспитательной работе		Абабкова Ю.В.
	Завуч по учебно-воспитательной работе		Павлова О.В.

1.3. Цель и задачи испытаний

1.3.1. Целью испытаний является оценка эффективности реализованных мер по обеспечению безопасности персональных данных ИСПДн «АП РИС ЦОПО» в муниципальном бюджетном общеобразовательном учреждение «Средняя общеобразовательная школа № 18 имени Героя Советского Союза генерала армии В.Ф.Маргелова».

1.3.2. Задачей испытаний является оценка соответствия системы защиты персональных данных информационной системы персональных данных «Абонентский пункт **№13** региональной информационной системы Цифровое образование Псковской области» (далее – СЗПДн) требованиям безопасности информации, выполнение которых обеспечивает

защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. ПРОГРАММА ИСПЫТАНИЙ

2.1. Перечень проверок и испытаний и их последовательность

2.1.1. Испытания проводятся в следующей последовательности:

1) Проверка структуры, состава и условий эксплуатации ИСПДн «АП РИС ЦОПО», включающая:

- анализ полноты исходных данных и проверку их соответствия реальным условиям размещения, монтажа и эксплуатации информационной системы;
- исследование технологического процесса обработки, хранения и передачи информации;
- анализ информационных потоков;
- определение состава используемых для обработки, хранения и передачи ОТСС.

2) Проверка состояния организации работ и выполнения требований по защите информации, включающая:

- оценку правильности определения уровня защищенности персональных данных при их обработке в ИСПДн «АП РИС ЦОПО»;
- оценки полноты разработки организационно-распорядительной и технической документации;
- проверку наличия распределения ответственности пользователей ИСПДн «АП РИС ЦОПО» за выполнение требований безопасности информации.

3) Проверка ИСПДн «АП РИС ЦОПО» на соответствие требованиям безопасности информации, включающая:

- проверку наличия необходимых документов и соответствия их содержания установленным требованиям;
- проверку наличия сертификатов на средства защиты информации, выполнения правил их эксплуатации;
- проверка обеспечения сохранности носителей персональных данных;
- проверку выполнения требований безопасности информации к помещениям, в которых проводятся обработка информации.

4) Проведение испытаний ИСПДн «АП РИС ЦОПО» на соответствие требованиям по защите информации от несанкционированного доступа:

- проверку выполнения требований, утвержденных постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», предъявляемых к информационным системам персональных данных, для которых установлена необходимость обеспечения 3-го уровня защищенности персональных данных;
- проверку выполнения требований, 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», необходимых для обеспечения 3-го уровня защищённости персональных данных;

- проверку выполнения требований по обеспечению безопасности персональных данных, установленных приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости», необходимых для обеспечения 3-го уровня защищённости персональных данных.

5) Подготовка отчётной документации и оценка результатов испытаний информационной системы.

2.2. Подготовка отчётной документации и оценка результатов испытаний

2.2.1. Результаты проведения испытаний ИСПДн «АП РИС ЦОПО» на соответствие требованиям по защите информации отражаются в Акте проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных в ИСПДн «АП РИС ЦОПО» (Акт оценки), который подписывается членами комиссии, проводившими испытания.

2.2.2. Акт оценки должен содержать:

- наименование объекта информатизации;
- цель испытаний;
- перечень использованных нормативных документов и методик испытаний;
- описание проверок;
- результаты испытаний.

2.2.3. На основании Акта оценки составляется заключение по результатам оценки реализованных принимаемых мер по обеспечению безопасности персональных данных в ИСПДн «АП РИС ЦОПО», включающее:

- оценку соответствия ИСПДн «АП РИС ЦОПО» требованиям безопасности информации;
- перечень выявленных недостатков и нарушений;
- рекомендации по устранению выявленных недостатков и нарушений;
- заключение по результатам оценки эффективности реализованных мер по обеспечению безопасности персональных данных.

3. МЕТОДИКА ИСПЫТАНИЙ

3.1. Проверка структуры, состава и условий эксплуатации информационной системы

3.1.1. Анализ полноты исходных данных и проверка их соответствия реальным условиям размещения, монтажа и эксплуатации ИСПДн «АП РИС ЦОПО»

Комиссии по оценке должны быть предоставлены:

- модель угроз безопасности информации ИСПДн «АП РИС ЦОПО»;
- техническое задание на создание системы защиты персональных данных;
- акт определения уровня защищённости персональных данных при их обработке в ИСПДн «АП РИС ЦОПО»;
- оформленный технический паспорт на ИСПДн «АП РИС ЦОПО»;

- сертификаты соответствия требованиям по безопасности информации на используемые средства защиты информации;
- организационно-распорядительная документация, разработанная в целях реализации мер и выполнения требований нормативных актов по обеспечению безопасности персональных данных;
- эксплуатационная документация на используемые средства защиты информации.

Приведённый перечень исходных данных и документации при необходимости может уточняться по результатам анализа и проверки в зависимости от особенностей ИСПДн «АП РИС ЦОПО» по согласованию с комиссией по оценке.

3.1.2. Исследование технологического процесса обработки, хранения и передачи информации

Комиссии по оценке предоставляется описание технологического процесса обработки информации в ИСПДн «АП РИС ЦОПО»:

- перечень объектов и субъектов доступа;
- перечень штатных средств доступа к информации;
- перечень средств защиты информации;
- описание реализованных правил разграничения доступа;
- описание информационных потоков.

При исследовании технологического процесса автоматизированной обработки и хранения информации проверяют объекты доступа, используемые в технологическом процессе обработки информации и субъекты доступа, посредством которых осуществляется доступ к объектам доступа.

Проверяют соответствие описания технологического процесса обработки, хранения и передачи защищаемой информации реальному технологическому процессу обработки.

3.1.3. Анализ информационных потоков

Используя разрешительную систему доступа пользователей к защищаемым информационным ресурсам ИСПДн «АП РИС ЦОПО» и данные по обработке и передаче защищаемой информации, анализируют обобщённую технологическую схему ИСПДн «АП РИС ЦОПО» с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации.

3.1.4. Определение состава используемых для обработки, хранения и передачи ОТСС

Проверяют паспортные (исходные) данные на ИСПДн «АП РИС ЦОПО».

С представленной документацией сверяют состав и структуру программно-технических средств ИСПДн «АП РИС ЦОПО» (типы, заводские номера, места размещения и т.д.), включённых в реальный технологический процесс обработки информации.

С использованием стандартных средств операционной системы фиксируют перечень программных средств и сверяют его с приведённым в техническом паспорте, документах разрешительной системы доступа и описании технологического процесса обработки защищаемой информации.

Проверка считается успешной, если состав, номенклатура, структура программных средств ИСПДн «АП РИС ЦОПО» и их размещение полностью соответствует представленной документации на информационную систему.

3.2. Проверка состояния организации работ и выполнения требований по защите информации

3.2.1. Оценка правильности определения уровня защищенности персональных данных

Производится проверка правильности определения уровня защищенности персональных данных при их обработке в ИСПДн «АП РИС ЦОПО» в соответствии с Требованиями к защите персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

Проверка считается успешной, если уровень защищенности персональных данных при их обработке в ИСПДн «АП РИС ЦОПО» соответствует представленному на испытания Акту определения уровня защищенности персональных данных при их обработке в ИСПДн «АП РИС ЦОПО».

3.2.2. Оценка полноты разработки организационно-распорядительной и технической документации

Проверяют соответствие предоставленной на испытания организационно-распорядительной и технической документации требованиям нормативных правовых актов и методических документов в области защиты информации.

Проверка считается успешной, если представленные документы соответствуют требуемому составу, не содержат противоречивых сведений и оформлены в соответствии с установленными требованиями.

3.2.3. Проверка наличия распределения ответственности пользователей информационной системы за выполнение требований безопасности информации

Проверку проводят на основе анализа предоставленной на испытания документации, устанавливающей распределение ответственности различных категорий пользователей ИСПДн «АП № 1 РИС ЦОПО» за выполнение требований безопасности информации.

Проверку считают успешной, если представленные документы содержат сведения о распределении ответственности пользователей ИСПДн «АП РИС ЦОПО» за выполнение требований безопасности информации.

3.3. Проверка информационной системы на соответствие требованиям безопасности информации

3.3.1. Проверка наличия необходимых документов и соответствия их содержания установленным требованиям

Проверяют соответствие предоставленных на испытания документов требованиям нормативных правовых актов и методических документов в области защиты информации.

Проверка считается успешной, если представленные документы соответствуют требуемому составу, не содержат противоречивых сведений и оформлены в соответствии с установленными требованиями.

3.3.2. Проверка наличия сертификатов на средства защиты информации, выполнения правил их эксплуатации

Проверяют соответствие представленных сертификатов установленным (используемым) в ИСПДн «АП РИС ЦОПО» средствам защиты информации.

Проверка считается успешной:

- если на все используемые в ИСПДн «АП РИС ЦОПО» средства защиты информации представлены сертификаты соответствия требованиям по безопасности информации;

- если используемые средства защиты информации соответствуют уровню защищенности персональных данных, обрабатываемых в ИСПДн «АП РИС ЦОПО» и используемой технологии обработки информации;
- если функции безопасности средств защиты информации, сертифицированных по требованиям, указанным в технических условиях (заданиях безопасности), обеспечивают реализацию мер защиты информации;

3.3.3. Проверка выполнения требований безопасности информации к помещениям, в которых проводятся обработка информации

Внешним осмотром проверяют соответствие помещений ИСПДн «АП РИС ЦОПО» установленным к ним требованиям.

Проверяют выполнение установленных требований по условиям размещения ОТСС внутри помещений. Размещение ОТСС должно исключать возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-вывода информации лицами, не имеющими права доступа к обрабатываемой информации.

Проверка считается успешной при выполнении всех установленных требований.

3.4. Проведение испытаний информационной системы на соответствие требованиям по защите информации от несанкционированного доступа

3.4.1. Проверка организации 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.

Проверяется наличие утверждённых организационно-распорядительных документов, регламентирующих режим обеспечения безопасности помещений и наличие физической охраны помещений, в которых размещена ИСПДн «АП РИС ЦОПО».

3.4.2. Проверка обеспечения сохранности носителей персональных данных

Проверяется наличие физической охраны помещений и оборудование помещений и хранилищ носителей информации необходимыми защитными средствами.

3.4.3. Проверка утверждения руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей

Проверяется наличие приказа (распоряжения), определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей.

3.4.4. Проверка использования 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

Проверяется наличие сертификатов соответствия требованиям безопасности информации на средства защиты информации, используемые в составе системы защиты персональных данных для нейтрализации актуальных угроз безопасности персональных данных.

ПРИЛОЖЕНИЕ А

к Программе и методикам оценки эффективности реализованных мер по обеспечению безопасности персональных данных в ИСПДн «АП РИС ЦОПО»

ПЕРЕЧЕНЬ

действующих нормативных правовых актов, методических документов и национальных стандартов в области защиты информации на соответствие положениям и требованиям которых проводятся испытания

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. 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».
5. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
6. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методика аттестационных испытаний.