ООО «ГСКС «ПРОФИ»

ИНН 4826040935 КПП 482601001
Юр. адрес: 398001, г.Липецк, ул. М. Горького, д.19
Почтовый адрес: 398001, г.Липецк, ул. М. Горького, д.19
Тел/Факс: +7 (4742) 515-888, e-mail: info@profy48.ru

Конфиденциально
Экз. № 2

СОГЛАСОВАНО
Директор
Государственного областного
бюджетного профессионального
образовательного учреждения
«Липецкий колледж строительства,
архитектуры и отраслевых
технологий»
_____ М.В. Дворникова
«06» октября 2023 г.

УТВЕРЖДАЮ
Генеральный директор
ООО «ГСКС «Профи»
_____ Р.С. Бесчеревных
"06" октября 2023 г.

ПРОГРАММА И МЕТОДИКА

оценки эффективности
реализованных, в рамках защиты персональных данных, мер по обеспечению безопасности персональных данных на объекте информатизации -
АРМ, подключаемый к Федеральной информационной системе «Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении»
Государственного областного бюджетного профессионального образовательного учреждения «Липецкий колледж строительства, архитектуры и отраслевых технологий»

2023 г.

Рег. № 23-3383 от 06.10.2023 г.

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

Информационная система – это взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации для достижения цели управления.

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или посещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Средство вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Автоматизированное рабочее место – объект вычислительной техники, созданный на базе автономных средств вычислительной техники с необходимым для решения конкретных задач периферийным оборудованием.

Локальная информационная система – совокупность автоматизированных рабочих мест и (или) отдельных средств вычислительной техники, объединенных между собой в единую систему посредством линий передачи данных, не выходящих за пределы контролируемой зоны.

Распределенная информационная система – комплекс автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа.

АРМ –	Автоматизированное рабочее место
ФИС -	Федеральная информационная система
НСД -	Несанкционированный доступ
ОТСС -	Основные технические средства и системы
ОИ -	Объект информатизации
СВТ-	Средство вычислительной техники
СЗИ-	Средство защиты информации

1. Общие положения

1.1. Характеристика объекта информатизации

Настоящий документ определяет цели, задачи, методы, условия, объем, порядок и методику проведения оценки эффективности реализованных, в рамках защиты персональных данных, мер (далее – оценка эффективности) объекта информатизации - АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении" (далее – ОИ), Государственного областного бюджетного профессионального образовательного учреждения «Липецкий колледж строительства, архитектуры и отраслевых технологий» по адресу: 398058, Липецкая область, г Липецк, Студенческий г-к, д. 1.

1.2. Перечень информации обрабатываемой на объекте информатизации

ПДн, обрабатываемые в ФИС «Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении»:

Фамилия; Имя; Отчество; Дата рождения; Пол; Адрес проживания; Реквизиты документа, удостоверяющего личность; Образовательное учреждение; Форма обучения; Профильные предметы; Номер класса; Данные о сдаче экзаменов (Категория участника ЕГЭ, Перечень общеобразовательных предметов, выбранных для сдачи ЕГЭ); Код регистрации; Регион сдачи ЕГЭ.

В соответствии с Актом определения уровня защищенности персональных данных на объекте информатизации «АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении" (от 31.08.2023 г.) для ОИ определены характеристики, указанные в Таблице 1 и установлен **4-й уровень защищенности ПДн.**

Таблица 1. Характеристика ОИ 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»

Критерий	Характеристика
Категория обрабатываемых персональных данных	Иные
Субъект персональных данных	Субъекты не являются сотрудниками «Оператора»
Объем обрабатываемых персональных данных	менее 100 000
Тип актуальных угроз	Угрозы 3-го типа

1.3. Сведения о комиссии по оценке эффективности

Комиссия по оценке эффективности назначена приказом генерального директора ООО «ГСКС «Профи» №1 от 31.01.2023 г. (лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации от 07.08.2014 г., серия КИ 0299, № 015032, рег. № 2362; лицензия ФСТЭК России на деятельность по разработке и (или) производству средств защиты конфиденциальной информации от 11.05.2016 г., серия КИ 0272, № 013669, рег. № 1550) из числа штатных сотрудников.

Приказом Генерального директора ООО «ГСКС «Профи» в состав комиссии назначены:

	Должность исполнителя	Фамилия, имя, отчество
Председатель комиссии	Начальник отдела	Р.Ю. Борисенко
Член комиссии	Руководитель направления	П.Ю. Кобозев
Член комиссии	Специалист по защите информации	И.В. Ананьева

1.4. Цель проведения оценки эффективности мер, реализованных в рамах системы защиты персональных данных, и используемая нормативная документация

Целью проведения оценки эффективности является определение соответствия ОИ организации требованиям безопасности персональных данных (далее – ПДн). Оценка эффективности проводится на соответствие положениям и требованиям действующих нормативных правовых актов (далее – НПА), методических документов и национальных стандартов в области защиты ПДн:

Наименование и реквизиты документов, устанавливающих требования по защите информации, на соответствие которым проводится оценка эффективности системы защиты ПДн объекта информатизации.

Оценка эффективности проводится на соответствие положениям и требованиям действующих нормативных правовых актов, методических документов и национальных стандартов в области защиты информации:

– Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

– Федеральный закон от 4 мая 2011 г. №99-ФЗ «О лицензировании отдельных видов деятельности»;

– Приказ ФСБ России от 10.07.2014 г. №378 «Об утверждении Состава 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»;

– «Положение о сертификации средств защиты информации», утвержденное постановлением Правительства Российской Федерации от 26 июня 1995 г. №608;

– «Требования к средствам антивирусной защиты», утвержденные приказом ФСТЭК России №28 от 20.03.2012 г;

– «Требования к системам обнаружения вторжений», утвержденные приказом ФСТЭК России №638 от 06.12.2011 г;

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

– Постановление Правительства РФ от 31 мая 2021 г. N 825 «О федеральной информационной системе «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении»;

– Информационное сообщение об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных от 20 ноября 2012 г. №240/24/4669;

– 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»;

– Информационное сообщение по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и Приказа 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» от 15 июля 2013 г. №240/22/2637;

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

– Руководящий документ. Защита от НСД Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей;

– «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (Утверждены руководством 8 Центра ФСБ России 21.02.2008 г.);

– Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (Утверждены руководством 8 Центра ФСБ России 21.02.2008 г.);

– Приказ ФСТЭК России от 29.04.2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну.

1.5. Данные о моделировании угроз безопасности для объекта информатизации

Оценка угроз безопасности персональных данных при их обработке в информационных системах персональных данных объекта информатизации – АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении" утверждена Директором Государственного областного бюджетного профессионального образовательного учреждения «Липецкий колледж строительства, архитектуры и отраслевых технологий» от 04.10.2023 г.

2. Программа и методика оценки эффективности мер, реализованных в рамках системы защиты персональных данных

2.1. Испытания и перечень работ для оценки эффективности

Оценка эффективности ОИ проводится в соответствии с программой, включающей следующий перечень работ и порядок их проведения:

2.1.1 Идентификация объекта информатизации.

2.1.2 Проверка ОИ на соответствие организационным требованиям по защите ПДн.

2.1.3 Анализ уязвимостей объекта информатизации

2.1.4 Проверка соответствия использованных мер и средств защиты ОИ требуемому уровню защищенности ПДн на ОИ.

2.2. Ответственные за проведение работ

Ответственными за проведение работ по оценки эффективности на объекте информатизации - АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении" назначены следующие эксперты ООО «ГСКС «Профи»:

- при проведении мероприятий и работ, предусмотренных п.п. 2.1.1, 2.1.2 и 2.1.4 настоящей Программы и методики – Начальник отдела Борисенко Р.Ю., специалист по защите информации Ананьева И.В.;
- при проведении мероприятий и работ, предусмотренных п.п. 2.1.3 настоящей программы и методики – Руководитель направления Кобозев П.Ю.

2.3. Методы проверок

При проведении оценки эффективности используют следующие методы проверок:

Экспертно-документальный метод - при проведении мероприятий и работ, предусмотренных п.п. 2.1.1, 2.1.2 и 2.1.4 настоящей Программы и методики, – оценка эффективности системы защиты ПДн объекта информатизации требованиям по защите ПДн на основе анализа экспертами органа по оценке эффективности документов, предусмотренных законодательством РФ в области защиты ПДн;

Инструментально-расчетный метод – испытания системы защиты информации путем осуществления тестирования ее функций безопасности (функциональное тестирование), анализ уязвимостей с использованием средств контроля эффективности защиты ПДн от несанкционированного доступа, а также испытания системы защиты ПДн путем осуществления попыток несанкционированного доступа (воздействия) в обход системы защиты ПДн с использованием средств тестирования.

Используемые средства измерения и инструментальные средства контроля эффективности защиты ПДн указаны в таблице 2.

Таблица 2. Средства измерения и инструментального контроля

№	Наименование	Назначение	Сведения о сертификации	Знак соответствия
1	Программный комплекс «Сканер-ВС-Инспектор»	– формирование модели системы разграничения доступа пользователей к информационным ресурсам; – проведение автоматизированной проверки соответствия модели разграничения доступа реальным настройкам прав доступа пользователей;	Сертификат соответствия ФСТЭК № 2204 от 13.11.2010 г., срок действия до 13.11.2024 г.	Регистрационный номер 006061.21.2362

		– проведение проверки механизмов гарантированного уничтожения информации с носителей и из оперативной памяти в автоматизированном режиме; – фиксация и контроль исходного состояния файлов и папок по контрольным суммам; – инвентаризация программных и аппаратных средств; – функция контроля изменений; – поиск по ключевым словам и встроенным словарям, возможность создания собственных словарей		

2.4. Сроки проведения проверок и испытаний

Продолжительность работ по пунктам «Программы и методики оценки эффективности» составляет:

- по 2.1.1, 2.1.2, 2.1.4 – до 15 рабочих дней;
- по 2.1.3 – до 10 рабочих дней.

2.5. Условия проведения испытаний

Оценка эффективности проводятся до полного завершения работ вне зависимости от промежуточных результатов.

Оценка эффективности проводится в нормальных климатических условиях эксплуатации ОИ (ГОСТ 21552-84), а также в условиях тестовых режимов работы технических средств и воздействия тестирующих средств, предусмотренных настоящим документом. Проверки и испытания должны проводиться при нормальной работе технических средств ОИ, без имитации отказов и сбоев ОИ, а также без изменения (повышения, понижения) и отключения напряжения сети питания.

Меры безопасности обслуживающего персонала и членов комиссии при проведении оценки эффективности должны соответствовать требованиям ГОСТ 21552-84.

Испытания могут быть прерваны или прекращены при:

- несоответствии представленных исходных данных ОИ, на котором проводится оценка эффективности, либо непредставлении требуемых исходных данных;
- неработоспособности представленных для испытаний технических средств;
- не укомплектованности технических средств необходимым программным обеспечением.

3. Методики оценки эффективности системы защиты ПДн на объекте информатизации

Настоящие методики предназначены для проведения оценки эффективности реализованных в рамках системы защиты информации ПДн мер по обеспечению безопасности ПДн на ОИ.

3.1. Идентификация ОИ включает следующие проверки

3.1.1. Проверку соответствия серийных номеров тех средств, представленных на оценку эффективности, заявленным в Техническом паспорте объекта информатизации.

3.1.2. Проверку соответствия программных средств, представленных на оценку эффективности, заявленным в Техническом паспорте объекта информатизации. Проверку соответствия размещения ОТСС относительно границ контролируемой зоны, заявленным в ОРД.

Комиссии по оценке эффективности должны быть предоставлены следующие документы:

- Технический паспорт ОИ;
- Приказ об организации режима безопасности помещений;

3.1.3. Проверка считается успешной если состав, номенклатура, структура программно-технических средств и их размещение полностью соответствует представленной документации.

3.2. Проверка ОИ на соответствие организационным требованиям по защите информации

3.2.1. Проверка достаточности представленных исходных документов и соответствие их содержания требованиям стандартам и иным руководящим документам ФСТЭК России.

Оператором ОИ, комиссии по оценке эффективности должны быть предоставлены следующие документы:

- Приказ о назначении администратора безопасности;
- Приказ о создании комиссии для установления уровня защищённости;
- Приказ о назначении лица, ответственного за организацию обработки ПДн;
- Акт определения уровня защищенности персональных данных;
- Акт оценки вреда;
- Приказ об утверждении Положения о защите информации;
- Положение о защите информации;
- Приказ об организации режима безопасности помещений;
- Перечень лиц, имеющих право доступа в помещения, в которых размещены компоненты информационных систем, в том числе используемые СКЗИ, носители ключевой, аутентифицирующей и парольной информации СКЗИ;
- Порядок доступа работников в помещения, в которых ведется обработка персональных данных;
- Приказ об утверждении инструкций по обеспечению безопасности информации;
- Приказ об определении системы доступа к информационным ресурсам;
- Положение о разрешительной системе доступа к информационным ресурсам;
- Матрица доступа;
- Перечень сотрудников, доступ которых к персональным данным необходим для выполнения ими трудовых обязанностей;
- Приказ об организации контроля (анализа) защищенности информации;
- Приказ о порядке хранения и эксплуатации средств криптографической защиты информации;
- Перечень сотрудников, допущенных к работе с СКЗИ;
- Инструкция по обращению со средствами криптографической защиты информации;
- Инструкция ответственного пользователя средств криптографической защиты информации;
- Журнал поэкземплярного учёта средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов;
- Технический (аппаратный) журнал;

- Инструкция администратора безопасности;
- Инструкция ответственного за организацию обработки персональных данных;
- Инструкция по организации парольной защиты;
- Инструкция по организации учета, использования и уничтожения машинных носителей;
- Инструкция по применению средств антивирусной защиты;
- Инструкция по регистрации, выявлению и реагированию на инциденты;
- Инструкция по резервному копированию;
- Инструкция пользователя;
- Журнал инструктажа пользователей;
- Журнал учёта выдачи паролей;
- Журнал учёта инцидентов;
- Журнал учёта конфиденциальной информации;
- Журнал учёта машинных носителей;
- Журнал учета СЗИ;
- Журнал учета хранилищ, ключей и оттисков печатей.

Добавить блок СКЗИ (инструкция, инструкция по обращению с скзи, журнал)

3.2.2. Проверка правильности определения уровня значимости ПДн на ОИ.

Комиссии по оценке эффективности должны быть предоставлены следующие документы:

- Акт определения уровня защищенности ПДн;

3.2.3. Проверка наличия сертификатов соответствия на применяемые средства защиты информации.

Применяемые средства защиты информации должны быть сертифицированы по требованиям безопасности информации.

Проверяется наличие сертификатов соответствия на средства защиты информации, подтверждающие возможность применения этих средств для защиты информации. Сертификаты должны быть выданы уполномоченными федеральными органами исполнительной власти и подтверждены знаками соответствия. На момент проведения оценки эффективности действие сертификатов не должно быть просрочено, либо производитель должен оказывать техническую поддержку средства защиты информации, информация о которой должна содержаться в реестре сертифицированных средств защиты информации уполномоченного федерального органа исполнительной власти.

Средства защиты информации должны удовлетворять требованиям по уровню доверия, классу криптозащиты по соответствующему уровню защищенности ПДн.

В информационных системах 4-го уровня защищенности ПДн должны применяться средства защиты информации 6 класса и 6 уровня доверия, а также средства вычислительной техники не ниже 6 класса.

Проверка считается успешной если применяемые на ОИ средства защиты информации удовлетворяют требованиям по уровню доверия, классу криптозащиты по соответствующему уровню защищенности ПДн и имеют сертификаты по требованиям безопасности информации.

Состав средств защиты информации должен соответствовать требованиям по обеспечению безопасности ПДн 4-го уровня защищенности.

3.3. Анализ уязвимостей включает:

3.3.1. Проверку отсутствия известных уязвимостей средств защиты информации, технических средств и программного обеспечения.

Комиссия по оценке эффективности проводит сканирование инфраструктуры объекта информатизации.

3.3.2. Проверка правильности установки и настройки средств защиты.

Комиссия по оценке эффективности проверяет корректность работы установленных СЗИ на ОИ.

Корректность настройки проверяется в соответствии с Техническим проектом на систему защиты информации.

3.4. Проверка соответствия использованных мер и средств защиты ОИ установленному на объекте информатизации уровню защищенности ПДн.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
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»		
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	На ОИ должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора. Проверяется реализация многофакторной аутентификации для локального и удаленного доступа привилегированных и непривилегированных пользователей ОИ
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	На ОИ должны быть регламентированы правила и процедуры управления идентификаторами, сроки блокировки идентификатора, сроки неиспользования, заблокированного идентификатора. Проверяется наличие в ОРД пунктов о правилах повторного использования и блокировке 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	На ОИ должны быть регламентированы правила выдачи идентификатора пользователю, определены длина, сложность и срок действия пароля. Проверяется регламентация правил выдачи пароля пользователю и его характеристики (длина пароля, алфавит пароля, максимальное количество неуспешных попыток аутентификации)
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	На ОИ должна осуществляться защита аутентификационной информации в процессе ее ввода путем исключения ее отображения для пользователя. Вводимые символы

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
		пароля могут отображаться условными знаками ("*", " • "). Проверяется путем ввода пароля в предназначенное для этого поля и его визуальное отображение
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	На ОИ должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей. Проверяется регламентация правил и процедур идентификации и аутентификации в ОРД
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	На ОИ должна использоваться автоматизированная система управления учетными записями, реализована автоматическая блокировка неиспользуемых учетных записей. На ОИ должны быть регламентированы правила и процедуры управления учётными записями
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	На ОИ правила разграничения доступа регламентируются в организационно-распорядительных документах оператора по защите информации. В документах должны быть зафиксированы типы и правила доступа для каждого субъекта к каждому объекту
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	На ОИ должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы. Проверяется наличие СЗИ, реализующих передачу информации между устройствами и сегментами в рамках ОИ
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	На ОИ должно быть обеспечено разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
		обязанностями. Проверяется фиксирование в ОРД по защите информации полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	На ОИ должно быть реализовано назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей. Проверяется наличие в ОРД по защите информации назначение прав и привилегий администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	На ОИ обеспечивается автоматическое блокирование устройства, с которого предпринимаются попытки доступа, и учетной записи пользователя при превышении ограничения количества неуспешных попыток входа в информационную систему за установленный период времени с возможностью разблокирования только администратором или иным лицом, имеющим соответствующие полномочия. Проверяется наличие в ОРД по защите информации разрешенное количество неуспешных попыток входа в ИС
IV. Защита машинных носителей персональных данных (ЗНИ)		
ЗНИ.1	Учет машинных носителей персональных данных	На ОИ должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации. Проверяется наличие и ведение журнала учёта машинных носителей информации, а также правила их учёта
V. Регистрация событий безопасности (РСБ)		

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	На ОИ должны быть определены события безопасности в информационной системе, подлежащие регистрации, и сроки их хранения. Проверяется наличие пересмотра перечня событий безопасности в плане внутренних проверок, регламентация в ОРД сроков хранения информации о событиях безопасности
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	На ОИ должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации. Проверяется наличие в ОРД перечня событий, подлежащих регистрации, информации о них и журнал учёта событий безопасности
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	На ОИ должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности. Проверяется журналирование в СЗИ
РСБ.7	Защита информации о событиях безопасности	На ОИ должна обеспечиваться защита информации о событиях безопасности. Проверяется настройка СЗИ, в части резервного копирования записей аудита
VI. Антивирусная защита (АВЗ)		
АВЗ.1	Реализация антивирусной защиты	На ОИ должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации. Проверяется наличие САВЗ на объекте информатизации и предоставление прав администрирования САВЗ администратору ИБ

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	На ОИ должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ. Проверяется регламентация правил и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) в ОРД
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)		
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	На ОИ должен осуществляться контроль установки обновлений ПО, включая ПО СЗИ и ПО базовой системы ввода-вывода. Проверяется наличие в ОРД правил и процедур установки ПО, и установленной периодичности установки обновлений ПО
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	На ОИ должны обеспечиваться контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СЗИ и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены. Проверяется наличие перечня лиц/должностей, допущенных к техническим средствам, а так же перечень лиц/должностей, допущенных в помещение, где расположен ОИ, перечень лиц/должностей, допущенных к СЗИ
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	На ОИ должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр. Проверяется размещение устройств вывода, условия должны удовлетворять требова-

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
		нию, исключающему несанкционированный просмотр информации
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	На ОИ должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны. Проверяется наличие соответствующих СЗИ
Требования для обеспечения 4-го уровня защищенности ПДн, установленные Постановлением Правительства РФ от 01 ноября 2012 г. №1119		
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		Проверяется организация режима обеспечения безопасности помещений ОИ, наличие актуальных перечней лиц/должностей, допущенных в эти помещения
Обеспечение сохранности носителей персональных данных		Проверяется наличие и ведение журнала учета машинных носителей информации, доступ к машинным носителям
Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей		Проверяется наличие перечня лиц/должностей, доступ которых к ПДн, обрабатываемым в ИС, необходим для выполнения ими трудовых обязанностей
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		Проверяется наличие сертификатов соответствия ФСТЭК и/или ФСБ России на применяемые средства защиты информации.

Для проверки выполнения Требований для обеспечения 4-го уровня защищенности ПДн, установленные Постановлением Правительства РФ от 01 ноября 2012 г. №1119 использовать Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава 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».

Проверка считается успешной, если все меры защиты реализованы, имеются все необходимые СЗИ, и выполнены все требования для обеспечения 4-го уровня защищенности ПДн.

4. Методика испытаний объекта информатизации по защите информации от несанкционированного доступа

4.1. Испытания подсистемы управления доступом

Испытания подсистемы управления доступом включают в себя:

4.1.1 Проверку подсистемы идентификации и аутентификации субъектов доступа.

Проверяется правильность идентификации субъектов доступа путем обращения субъектов доступа ОИ к объектам доступа при помощи штатных средств.

При обращении должна проводиться проверка принадлежности предъявленного субъектом идентификатора множеству всех зарегистрированных на ОИ идентификаторов. Если субъект доступа предъявляет идентификатор, не известный подсистеме идентификации, то средства управления должны прекращать процесс предоставления доступа.

4.1.2. Проверку наличия и надежности подсистемы аутентификации

Проверяют правильность аутентификации субъекта доступа. Если субъект доступа предъявляет пароль, не соответствующий идентификатору субъекта, то средства управления должны прекращать процесс предоставления доступа.

Проверяют возможность компрометации пароля методом его подбора. Для ОИ, где подсистема аутентификации предусматривает средства, обеспечивающие блокировку подбора пароля. Проверку осуществляют следующим образом. Выполняют неоднократные попытки ввода неверного пароля. При превышении предельного числа попыток ввода информации идентификации/аутентификации, установленного политикой безопасности, подсистема управления доступом должна полностью блокировать ввод информации идентификации/аутентификации субъекта доступа. Правом снятия блокировки должен обладать исключительно администратор (служба) защиты информации на ОИ.

4.1.3. Проверку отсутствия условий компрометации подсистемы идентификации и аутентификации

Проверяют условия хранения, выдачи, использования устройств и информации об идентификации и аутентификации. Организационные и технические мероприятия на ОИ должны надежно препятствовать несанкционированному получению или хищению устройств и информации об идентификации и аутентификации.

Проверяют возможность несанкционированного изменения информации об идентификации и аутентификации. Доступ субъектов на ОИ к файлам, содержащим информацию об идентификации и аутентификации, должен быть полностью закрыт для прикладных программ. На СВТ, входящих в состав на ОИ, должны отсутствовать прикладные программные средства прямого доступа к устройствам и оперативной памяти, средства разработки и отладки программ.

4.1.4. Проверку времени действия пароля.

На АРМ производят перевод системного времени вперед, при этом не превышая установленного политикой безопасности времени действия пароля. Затем осуществляют попытку входа пользователя в систему. Подсистема идентификации и аутентификации должна разрешить вход пользователя в систему, но соответствующим сообщением предупредить его о необходимости замены пароля.

На АРМ производят перевод системного времени вперед на интервал, больший установленного политикой безопасности времени действия пароля. Затем осуществляют попытку входа пользователя в систему. Подсистема идентификации и аутентификации должна блокировать вход пользователя в систему.

После проведения испытаний на АРМ устанавливают текущее время.

4.1.5. Проверку длины пароля

Подсистема контроля доступа должна предусматривать средства, обеспечивающие установку минимальной длины пароля. Проверку осуществляют попыткой смены длины пароля субъектом доступа. Проверка считается успешной, если подсистема контроля доступа отказала субъекту в замене пароля.

Право установки минимальной размерности пароля должно предоставляться администратору ОИ.

4.2. Проверка подсистемы идентификации объектов доступа.

4.2.1. Проверка идентификации аппаратурных объектов доступа:

Идентификация внешних устройств АРМ должна осуществляться по одному из нижеперечисленных типов идентификаторов:

- по логическим адресам (номерам);
- по логическим именам;
- по логическим именам и (или) адресам;
- по физическим адресам (номерам);
- по уникальным встроенным устройствам.

Проверка считается успешной, если во время работы со средствами контроля защищенности ОИ от НСД не выявлены неизвестные (неидентифицированные) объекты доступа.

4.2.2. Проверка идентификации информационных объектов доступа.

Проверяется механизм подсистемы контроля доступа, обеспечивающий проверку идентификации программ, томов, каталогов, файлов, записей, полей записей по именам.

С помощью средств контроля защищенности ОИ от НСД проводится сканирование ресурсов файловой системы ОИ (логических дисков, каталогов, файлов), доступных для пользователя. Перед началом сканирования в настройках комплекса необходимо задать поиск неизвестных устройств.

Проверка считается успешной, если в выходном отчете комплексов средств контроля не будут указаны неизвестные (не идентифицированные) объекты доступа.

4.3. Испытания подсистемы регистрации и учета

Испытания подсистемы регистрации и учета включают в себя:

4.3.1. Проверку регистрации начала и окончания работ.

Проверка осуществляется штатными средствами ОИ

Проводится загрузка операционной системы и запуск программных комплексов на ОИ, предусмотренных технологией инициализации ОИ.

Осуществляются попытки входа в систему по неверному идентификатору доступа, по верному идентификатору доступа и неверному паролю, по идентификатору и паролю легитимного субъекта доступа.

Производится программный останов ОИ.

Производится загрузка операционной системы, запуск программных комплексона ОИ, предусмотренных технологией инициализации ОИ, вход в систему с правами администратора защиты и исследование журнала регистрации доступа.

Проверка считается успешной, если организационными и техническими мероприятиями, проводимыми в соответствии с политикой безопасности ОИ, обеспечивается ведение журнала регистрации доступа (аппаратного журнала), в котором фиксируется регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. При этом регистрационные записи для каждого события должны содержать:

– дату и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

– результат попытки входа: успешная или неуспешная - несанкционированная;

– идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа.

4.3.2. Проверку регистрации выдачи документов на «твердую» копию.

В соответствии с принятой на ОИ технологией проводится выдача документа на «твердую» копию. Во время операции вывода документа на «твердую» копию проводится принудительное отключение электропитания устройства вывода и выполняются действия, предусмотренные документацией ОИ для внештатных ситуаций.

Проверка считается успешной, если организационными и техническими мероприятиями, проводимыми в соответствии с политикой безопасности ОИ, обеспечивается регистрация выдачи документов на «твердую» копию. При этом регистрационные записи для каждого события должны содержать:

– дату и время выдачи документа (обращения к подсистеме вывода документа);

– спецификацию устройства выдачи (логическое имя внешнего устройства);

– краткое содержание (наименование, вид, шифр, код) документа;

– идентификатор субъекта доступа, запросившего документ;

4.3.3. Проверку учета защищаемых носителей информации.

Проверяется выполнение организационных и технических мероприятий по учету защищаемых носителей информации.

Проверка считается успешной, если организационно-технические мероприятия, проводимые в соответствии с политикой безопасности ОИ, обеспечивают:

– учет всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал (учетную карточку);

– учет защищаемых носителей в журнале (картотеке) регистрации их выдачи / приема;

– дополнительный (дублирующий) учет защищаемых носителей информации с регистрацией их выдачи/приема.

4.3.4. Проверку очистки освобождаемых областей памяти.

Проверяются сертификаты (при необходимости – эксплуатационная документация) СЗИ на предмет подтверждения соответствия используемых методов очистки (обнуления, обезличивания) освобождаемых (перераспределяемых) областей оперативной памяти и внешних носителей требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также требованиям документов по стандартизации в области защиты информации.

Проверка считается успешной, если сертификаты и эксплуатационная документация СЗИ подтверждают возможность выполнения очистки (обнуления, обезличивания) освобождаемых (перераспределяемых) областей оперативной памяти и внешних носителей двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Проверку очистки внешней памяти при ее освобождении (перераспределении). Объектами исследований являются накопители на гибких и жестких магнитных дисках. Поиск

задают или по всему физическому диску, или в пределах логического диска. Область применения охватывает операционные среды MS Windows.

Проверка считается успешной:

– если контекст контрольной информации не был обнаружен на внешнем носителе;

– если сектора, которые ранее содержали контекст контрольной информации, заполнены маскирующей информацией.

4.4. Испытание подсистемы обеспечения целостности

Испытание подсистемы обеспечения целостности, включает в себя:

4.4.1. Проверку организационно-штатных мероприятий по защите информации.

Проверяется организационно-штатная структура и нормативная документация ОИ на предмет организации службы защиты информации.

Методом выборочного опроса проверяют знание должностными лицами службы защиты информации их функциональных обязанностей и оценивают уровень их профессиональной подготовки.

Проверка считается успешной:

– если организационно-штатная структура ОИ предусматривает наличие службы (администратора) защиты информации;

– если уровень профессиональной подготовки должностных лиц службы защиты информации обеспечивает выполнение требований безопасности информации на ОИ;

– если деятельность службы защиты информации регламентирована организационно-распорядительными документами ОИ.

4.4.2. Проверку средств контроля целостности программных компонентов СЗИ от НСД.

Перед проведением проверки штатными средствами ОИ осуществляется резервное копирование программных компонентов СЗИ от НСД.

Производится моделирование несанкционированных действий по нарушению целостности программных компонентов СЗИ от НСД. Производится удаление либо переименование определенных программных модулей СЗИ от НСД.

Производится перезагрузка системы. По завершении инициализации СЗИ от НСД анализируется реакция средств подсистемы обеспечения целостности.

Проверка считается успешной, если СЗИ от НСД зафиксировали изменения в составе программных компонентов.

4.4.3. Проверку тестирования функций СЗИ от НСД.

Проверяется наличие средств тестирования функций СЗИ от НСД, в частности настройка и использование средств диагностики СЗИ от НСД.

Проверяется периодичность проведения тестирования всех функций СЗИ от НСД. Проверка осуществляется методом экспертизы эксплуатационной документации и журналов регистрации событий СЗИ от НСД.

Проверка считается успешной, если средства тестирования всех функций СЗИ от НСД и периодичность проверок соответствуют требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также требованиям документов по стандартизации в области защиты информации.

4.4.4. Проверку средств восстановления СЗИ от НСД.

Исследуется организационно-распорядительная документация ОИ, определяющая порядок проведения резервного копирования СЗИ от НСД, используемого на ОИ.

Проверяется периодичность обновления и контроля работоспособности копий. Проверка осуществляется методом экспертизы эксплуатационной документации и журналов регистрации событий СЗИ от НСД.

Проверка считается успешной, если на ОИ осуществляется ведение двух копий программных СЗИ от НСД, а также производится периодическое обновление и контроль работоспособности копий.

4.4.5. Проверку обеспечения целостности (неизменности) программной среды.

Исследуется технология внесения новых программных средств в операционную среду ОИ. Технология должна содержать:

– процедуры экспертной оценки и верификации новых программных средств на предмет выявления потенциально опасных для СЗИ программных функций;

– критерии санкционирования ввода программ в операционную среду;

– критерии допуска определенных категорий пользователей к этим программам;

– порядок проведения антивирусного контроля программных комплексона ОИ.

Проверяется наличие и работоспособность средств и мер предотвращения несанкционированного ввода программ в операционную среду, средств антивирусного контроля.

Проверяется наличие установленных антивирусных средств на ОИ, а также их работоспособность, наличие механизма обновления и актуальность антивирусных баз, параметры их функционирования, наличие доверенного канала получения обновлений антивирусных баз.

Проводится экспертиза программного обеспечения ОИ на отсутствие:

– средств модификации объектного кода программ;

– средств разработки и отладки программ;

– программ, использование которых не требует трансляции с языков высокого уровня.

Проверка считается успешной, если принятые на ОИ меры обеспечения целостности (неизменности) программной среды соответствуют требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также требованиям документов по стандартизации в области защиты информации.

4.5. Испытания подсистемы межсетевого экранирования

Испытания подсистемы межсетевого экранирования, включают в себя:

Проверку подсистемы межсетевого экранирования проводится системой анализа программного и аппаратного обеспечения TCP/IP сетей. Проверка считается успешной, если критических уязвимостей обнаружено не было.

4.6. Испытания подсистемы криптографической защиты

Испытания подсистемы криптографической защиты (при ее наличии), включает в себя

4.6.1. Проверку наличия установленных СКЗИ

Проверяется наличие установленных СКЗИ на рабочих местах пользователей, посредством средства инвентаризации программных и аппаратных средств, наличие установленных программно-аппаратных комплексов, в серверных помещениях на ОИ.

Проверка считается успешной, если все используемые средства СКЗИ на ОИ установлены и отражены в отчете инвентаризации

4.6.2. Проверку шифрования сетевого трафика.

Проверка проводится путем запуска telnet и Wireshark, производится подключение по протоколу telnet при этом сканируется и записывается сетевой трафик.

Проверка считается успешной если весь сетевой трафик при анализе в Wireshark будет зашифрован.

5. Подготовка отчетной документации и оценка результатов оценки эффективности объекта информатизации

5.1. Оформление протокола оценки эффективности

Результаты испытаний, предусмотренных п. 2 настоящей Программы и методики оценки эффективности реализованных, в рамках защиты персональных данных, мер по обеспечению безопасности персональных данных, оформляются Протоколом оценки эффективности, содержащим:

- наименование испытания в соответствии с Программой и методикой оценки эффективности;
- дату утверждения Программы и методик оценки эффективности реализованных, в рамках защиты персональных данных, мер по обеспечению безопасности персональных данных;
- дату и место проведения испытаний;
- критерии выполнения требований по защите информации, в отношении которых проводились испытания;
- условия и исходные данные для проведения испытаний;
- применяемые при проведении испытаний средства контроля эффективности защиты информации от несанкционированного доступа, а также контрольно-измерительное и испытательное оборудование;
- описание порядка испытаний по оценке критериев выполнения требований по защите информации;
- результаты испытаний по каждому оцениваемому критериев выполнения требований по защите информации.

Протокол оценки эффективности на соответствие объекта информатизации требованиям по защите ПДн от несанкционированного доступа оформляется отдельным документом в соответствии с п. 19 Приказа ФСТЭК России № 77 от 29.04.2021 г.

5.2. Оформление заключения по результатам оценки эффективности

По результатам оценки эффективности оформляется Заключение по результатам оценки эффективности, включающее следующие сведения:

- наименование ОИ и его назначение, состав технических средств и средств защиты информации;
- уровень защищенности ПДн;
- фамилии, имена, отчества (при наличии), должности экспертов ООО «ГСКС «Профи», проводивших оценку эффективности;
- дату утверждения Программы и методик оценки эффективности реализованных, в рамках защиты персональных данных, мер по обеспечению безопасности персональных данных;
- срок проведения оценки эффективности;
- наименования и реквизиты документов, устанавливающих требования по защите информации, на соответствие которым проводилась оценка эффективности;
- результаты испытаний с описанием состава проведенных работ и испытаний в соответствии с Программой и методикой оценки эффективности, указанием сроков вы-

полнения каждого испытания и экспертов ООО «ГСКС «Профи», ответственных за проведение каждого испытания, используемых экспертами при испытаниях средств, а также заключение о соответствии (несоответствии) требованиям по защите информации по каждой проведенной работе и испытанию;

- рекомендации по устранению несоответствий системы защиты информации ОИ требованиям по защите информации в случае их выявления при проведении оценки эффективности;
- вывод об оценке эффективности оценки эффективности реализованных, в рамках защиты персональных данных, мер по обеспечению безопасности персональных данных.

6. Периодичность оценки эффективности

Оценка эффективности реализованных, в рамках защиты персональных данных, мер по обеспечению безопасности персональных данных проводится не реже одного раза в 3 года в соответствии с п. 6 Приказа 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».

К оценке эффективности привлекаются сотрудники, ответственные за обработку ПДн и при необходимости сотрудники организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

В ходе проведения оценки эффективности осуществляются следующие мероприятия:

– в соответствии с п.3 на основе анализа материалов испытаний проверяется неизменность состояния защищенности ПДн;

– в соответствии с п. 4 проверяется выполнение требований по защите информации от несанкционированного доступа.

Материалы по оценки эффективности организацией, осуществляющей работы по оценке эффективности, в виде протокола и заключения по результатам контроля защищенности ПДн и выдаются собственнику проверяемого ОИ.

Разработчик:
Специалист по защите информации Ананьева И.В.