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

УТВЕРЖДАЮ

Генеральный директор
ООО «ГСКС «Профи»

_____ Р.С. Бесчеревных
"23" октября 2023 г.

ПРОТОКОЛ

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. № 23-3386 от 23.10.2023 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», расположенного 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

2. Сведения о Программе и методиках оценки эффективности и периоде проведения оценки эффективности

2.1. Сведения о Программе и методике оценки эффективности

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"» утверждена от 06.10.2023 г. (Рег. № 23-3383)

2.2. Период проведения оценки эффективности на объекте информатизации

Мероприятий и работы по оценке эффективности, предусмотренные п.п. 2.1.1, 2.1.2 и 2.1.4 Программы и методик оценки эффективности проводились на объекте информатизации в срок с 09.10.2023 г. по 13.10.2023 г.

Мероприятий и работы по оценке эффективности, предусмотренные п.п. 2.1.3 Программой и методиками оценки эффективности проводились на объекте информатизации в срок с 11.10.2023 г. по 20.10.2023 г.

Ответственные за проведения испытаний работ, предусмотренных п.п. 2.1.1, 2.1.2 и 2.1.4 Программы и методик оценки эффективности – Начальник отдела Борисенко Р.Ю., специалист по защите информации Ананьева И.В.

Ответственный за проведения испытаний работ, предусмотренных п.п. 2.1.3 Программы и методик оценки эффективности – Руководитель направления Кобозев П.Ю.

3. Оценка эффективности, а также, критерии выполнения требований по защите ПДн, в отношении которых проводились испытания в соответствии с программой и методикой

3.1. Испытания подсистемы управления доступом

3.1.1. Проверка подсистемы идентификации и аутентификации субъектов доступа.

При обращении должна проводиться проверка принадлежности предъявленного субъектом идентификатора множеству всех зарегистрированных на ОИ идентификаторов.

Критерий: проводится проверка принадлежности предъявленного субъектом идентификатора множеству всех зарегистрированных на ОИ идентификаторов.

Проверка считается успешной, если при предъявлении субъектом доступа идентификатора, неизвестного подсистеме идентификации, средства управления прекратили процесс предоставления доступа.

3.1.2. Проверка наличия и надежности подсистемы аутентификации

Выполняют неоднократные попытки ввода неверного пароля.

Критерий: 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.

Проверка считается успешной, если субъект доступа предъявляет пароль, не соответствующий идентификатору субъекта, то средства управления должны прекращать процесс предоставления доступа. Правом снятия блокировки должен обладать исключительно администратор (служба) защиты информации на ОИ.

3.1.3. Проверка отсутствия условий компрометации подсистемы идентификации и аутентификации.

Выполняется проверка условий хранения, выдачи, использования устройств и информации об идентификации и аутентификации, а также возможность несанкционированного изменения информации об идентификации и аутентификации

Критерий: организационные и технические мероприятия на ОИ должны надежно препятствовать несанкционированному получению или хищению устройств и информации об идентификации и аутентификации.

Проверка считается успешной, если доступ субъектов на ОИ к файлам, содержащим информацию об идентификации и аутентификации, полностью закрыт для прикладных программ. На СВТ, входящих в состав на ОИ, отсутствуют прикладные программные средства прямого доступа к устройствам и оперативной памяти, средства разработки и отладки программ.

3.1.4. Проверка 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.

Критерий: подсистема идентификации и аутентификации должна разрешить вход пользователя в систему, но соответствующим сообщением предупредить его о необходимости замены пароля.

Проверка считается успешной, если был осуществлен вход в систему с соответствующим сообщением

На АРМ производят перевод системного времени вперед на интервал, больший установленного политикой безопасности времени действия пароля. Затем осуществляют попытку входа пользователя в систему.

Критерий: идентификации и аутентификации должна блокировать вход пользователя в систему.

Проверка считается успешной, если вход пользователя в систему заблокирован.

3.1.5. Проверка длины пароля

Проверку осуществляют попыткой смены длины пароля субъектом доступа.

Критерий: подсистема контроля доступа должна предусматривать средства, обеспечивающие установку минимальной длины пароля.

Проверка считается успешной, если подсистема контроля доступа отказала субъекту в замене пароля.

3.2. Проверка подсистемы идентификации объектов доступа.

3.2.1. Проверка идентификации аппаратурных объектов доступа.

Критерии: 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 (не идентифицированные) объекты доступа.

3.2.2. Проверка идентификации информационных объектов доступа.

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

Критерии: 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.

3.3. Испытания подсистемы регистрации и учета

3.3.1. Проверка регистрации начала и окончания работ штатными средствами ОИ.

Критерии: 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 программная остановка ОИ.

Производится загрузка операционной системы, запуск программных комплексов на 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.

3.3.2. Проверка регистрации выдачи документов на «твердую» копию.

В соответствии с принятой на ОИ технологией проводится выдача документа на «твердую» копию.

Критерии: 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.

3.3.3. Проверка учета защищаемых носителей информации.

Критерии: 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.

3.3.4. Проверка очистки освобождаемых областей памяти.

Критерии: производится проверка сертификатов, а также эксплуатационной документации 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).

3.4. Испытание подсистемы обеспечения целостности.

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

Критерии: 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.

3.4.2. Проверка средств контроля целостности программных компонентов СЗИ от НСД.

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

Критерии: 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.

3.4.3. Проверка тестирования функций СЗИ от НСД.

Критерии: 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.

3.4.4. Проверка средств восстановления СЗИ от НСД.

Критерии: 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.

3.4.5. Проверка обеспечения целостности (неизменности) программной среды.

Исследуется технология внесения новых программных средств в операционную среду ОИ.

Критерии: 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.

3.5. Испытания подсистемы межсетевого экранирования.

3.5.1. Проверка организационно-штатных мероприятий по защите информации.

Критерии: проверяется подсистема межсетевого экранирования проводится системой анализа программного и аппаратного обеспечения TCP/IP сетей.

Проверка считается успешной, если критических уязвимостей обнаружено не было

3.6. Испытания подсистемы криптографической защиты

3.6.1. Проверку наличия установленных СКЗИ

Критерии: 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

3.6.2. Проверка шифрования сетевого трафика.

Критерии: 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.

4. Контроль эффективности защиты информации от несанкционированного доступа, а также контрольно-измерительное и испытательное оборудование

4.1. Методы проверок

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

4.2. Используемые средства контроля

4.2.1. Используемые средства измерения и инструментальные средства контроля эффективности защиты информации 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 раз-	Сертификат соответствия ФСТЭК № 2204 от 13.11.2010 г., срок действия до 13.11.2024 г.	Регистрационный номер 006061.21.2362

		граничения доступа реальным настройкам прав доступа пользователей; – 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		

Испытания ОИ проводятся до полного их завершения вне зависимости от промежуточных результатов.

Испытания проводятся 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.

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

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.

5. Порядок испытаний по каждому оцениваемому критерию выполнения требований по защите информации

5.1. Результаты испытаний на ОИ, приведения в таблице 3 – 8:

Таблица 3. Результаты испытания подсистемы управления доступом.

Условия и исходные данные для проведения испытаний	Критерий	Результат
1. Испытания подсистемы управления доступом.		
1.1.Проверка подсистемы идентификации и аутентификации субъектов доступа.		
	При обращении должна проводиться проверка принадлежности предъявленного субъектом иден-	Проверка успешна. При предъявлении субъектом доступа идентификатора, неизвестного подсистеме идентификации,

Условия и исходные данные для проведения испытаний	Критерий	Результат
	тификатора множеству всех зарегистрированных на ОИ идентификаторов	средства управления прекратили процесс предоставления доступа.
1.2. Проверка наличия и надежности подсистемы аутентификации		
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	Проверка успешна. При предъявлении пароля субъектом доступа, не соответствующего идентификатору субъекта, средства управления прекратили процесс предоставления доступа. Правом снятия блокировки обладает исключительно администратор защиты информации на ОИ
1.3. Проверка отсутствия условий компрометации подсистемы идентификации и аутентификации.		
Выполняется проверка условий хранения, выдачи, использования устройств и информации об идентификации и аутентификации, а также возможность несанкционированного изменения 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	Проверка успешна. Доступ субъектов на ОИ к файлам, содержащим информацию об идентификации и аутентификации, полностью закрыт для прикладных программ. На СВТ, входящих в состав на ОИ, отсутствуют прикладные программные средства прямого доступа к устройствам и оперативной памяти, средства разработки и отладки программ.
1.4.Проверка 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.	Проверка успешна. После осуществления входа в систему отобразилось соответствующее сообщение, о необходимости замены пароля.
На АРМ производят перевод системного времени вперед на интервал, больший	Идентификации и аутентификации должна блокировать вход пользователя в систему.	Проверка успешна. Вход пользователя в систему заблокирован.

Условия и исходные данные для проведения испытаний	Критерий	Результат
установленного политикой безопасности времени действия пароля. Затем осуществляют попытку входа пользователя в систему.		
1.5.Проверка длины пароля		
Проверку осуществляют попыткой смены длины пароля субъектом доступа.	Подсистема контроля доступа должна предусматривать средства, обеспечивающие установку минимальной длины пароля.	Проверка успешна. Подсистема контроля доступа отказала субъекту в замене пароля.

Таблица 4. Результаты испытания подсистемы идентификации объектов доступа.

Условия и исходные данные для проведения испытаний	Критерий	Результат
2. Проверка подсистемы идентификации объектов доступа.		
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 успешна. Во время работы со средствами контроля защищенности ОИ от НСД не выявлены неизвестные (не идентифицированные) объекты доступа.
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 успешна. в выходном отчете комплексов средств контроля не указаны неизвестные (не идентифицированные) объекты доступа.

Таблица 5. Результаты Испытания подсистемы регистрации и учета.

Условия и исходные данные для проведения испытаний	Критерий	Результат
3. Испытания подсистемы регистрации и учета.		
3.1.Проверка регистрации начала и окончания работ 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 программная остановка ОИ. Производится загрузка операционной системы, запуск программных комплексов на ОИ, предусмотренных технологией инициализации ОИ, вход в систему с правами администратора защиты и исследование журнала регистрации доступа.	Проверка успешна. 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.
3.2.Проверка 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 успешна. 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

Условия и исходные данные для проведения испытаний	Критерий	Результат
		подсистеме вывода документа); – спецификацию устройства выдачи (логическое имя внешнего устройства); – краткое содержание (наименование, вид, шифр, код) документа; – идентификатор субъекта доступа, запросившего документ.
	Проверяется выполнение организационных и технических мероприятий по учету защищаемых носителей информации.	Проверка успешна. 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.
3.3.Проверка очистки освобождаемых областей памяти		
	Производится проверка сертификатов, а также эксплуатационной документации 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 успешна. 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)

Таблица 6. Результаты испытаний подсистемы обеспечения целостности

Условия и исходные данные для проведения испытаний	Критерий	Результат
4. Испытание подсистемы обеспечения целостности.		
4.1. 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 успешна. – 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.
4.2.Проверка 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 успешна. СЗИ от НСД зафиксировали изменения в составе программных компонентов.
4.3.Проверка 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 успешна. 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.

Условия и исходные данные для проведения испытаний	Критерий	Результат
4.4.Проверка 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 успешна. На ОИ осуществляется ведение двух копий программных СЗИ от НСД, а также производится периодическое обновление и контроль работоспособности копий.
4.5. Проверка обеспечения целостности (неизменности) программной среды.		
Исследуется технология внесения новых программных средств в операционную среду 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 успешна. 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.

Таблица 7. Результаты испытаний подсистемы межсетевого экранирования

Условия и исходные данные для проведения испытаний	Критерий	Результат

5. Испытания подсистемы межсетевого экранирования.		
5.1. Проверка организационно-штатных мероприятий по защите информации.		
	проверяется подсистема межсетевого экранирования проводится системой анализа программного и аппаратного обеспечения TCP/IP сетей.	Проверка успешна. Критических уязвимостей обнаружено не было

Таблица 8. Результаты испытаний подсистемы криптографической защиты

Условия и исходные данные для проведения испытаний	**Критерий**	**Результат**
6. Испытания подсистемы криптографической защиты		
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 успешна. Все используемые средства СКЗИ на ОИ установлены и отражены в отчете инвентаризации
6.2.Проверка шифрования сетевого трафика.		
	Проверка проводится путем запуска telnet и Wireshark, производится подключение по протоколу telnet при этом сканируется и записывается сетевой трафик.	Проверка успешна. весь сетевой трафик при анализе в Wireshark оказался зашифрован.

5.2. Выводы

Результаты проведенных испытаний и работ для оценки эффективности показали, что объект информатизации - **АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении"**, что выполненные требования для обеспечения **4-го уровня защищенности** персональных данных при их обработке в информационной системе и реализованные организационные и технические меры по обеспечению безопасности персональных данных соответствуют требованиям и мерам, установленным нормативными правовыми актами Российской Федерации в области защиты персональных данных.

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

Рег. № 23-3386 дсп
Отп. 1 экз. на 9 л., без черновика
Экз.___ – в адрес;
Исп. и отп. Ананьева И.В.
от 23.10.2023 г.
Тел. 515-888