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
"24" октября 2023 г.

ЗАКЛЮЧЕНИЕ

по результатам 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. № 23-3387 от 24.10.2023 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
ПО-	Программное обеспечение
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. Кабинет № 301.

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. Нормативно-правовая база

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.

2. Состав программно-технических, программных средств и средств защиты информации

2.1. Перечень программно-технических средств

Перечень программно-технических средств, входящих в состав объекта информатизации - "АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении"

№ п.п.	Тип технического средства	Наименование, модель	Серийный/инвентарный номер
	АРМ – 1 Кабинет № 301		
1.	Монитор	Samsung SM173	DE17H9NL403887A
2.	Системный блок	ПК helios VLX310	0061740002
3.	Клавиатура	Microsoft	б/н
4.	Мышь	Aceline	б/н

2.2. Перечень программных средств

Перечень программных средств, входящих в состав объекта информатизации - "АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении"

№ п/п	Тип программного обеспечения	Наименование, версия	Серийный/инвентарный номер
	АРМ – 1 Кабинет № 301		
1.	Операционная система	Microsoft Windows 7 Pro	55041-005-5928524-86546
2.	Офис	Microsoft Office 2013	00216-40000-00000-AA528
3.	СЗИ от НСД	Secret Net Studio 8	1A84DF
4.	МЭ	Модуль персонального межсетевого экрана "Secret Net Studio" 8	1A84DE

2.3. Перечень средств защиты информации

Перечень средств защиты информации, входящих в состав объекта информатизации «АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении"»

№ п/п	Тип средства защиты информации	Наименование	Серийный номер и знак соответствия
1.	СКЗИ	ПО ViPNet Client 4.x (версия 4.5)	КлКС2-4-302664 / 782-303639
2.	СЗИ от НСД	СЗИ от НСД "Secret Net Studio"	L3ZJGFBH / П 721659
3.	САВЗ	Kaspersky Endpoint Security 11 for Windows"	СМП8067-38253, П 306331

№ п/п	Тип средства защиты информации	Наименование	Серийный номер и знак соответствия
4.	САЗ	ПК "Средство анализа защищенности "Сканер-ВС"	0060601.22.0711, П949985

Сведения о комиссии по оценке эффективности и проведенных испытаниях

2.4. Сведения о комиссии

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

2.5. Сведения о проведенных испытаниях по оценке эффективности

Испытания по оценке эффективности проводятся в соответствии с Программой и методикой 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" утвержденной 06.10.2023 г. (Рег. №23-3383).

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 Программы и методики оценки эффективности –Начальник отдела безопасности и защиты информации Борисенко Р.Ю., Специалист по защите информации Ананьева И.В. Сроки проведения мероприятий и работ: с «09» октября 2023 г. по «13» октября 2023 г.

- при проведении мероприятий и работ, предусмотренных п.п. 2.1.3 Программы и методики оценки эффективности – Руководитель направления Кобозев П.Ю. Сроки проведения мероприятий и работ: с «11» октября 2023 г. по «20» октября 2023 г.

3. Результаты аттестационных испытаний

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.

Комиссия по оценке эффективности проверила соответствие серийных номеров технических средств, представленных в Техническом паспорте объекта информатизации -

АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении".

Проверка показала соответствие серийных номеров технических средств на ОИ, представленным в техническом паспорте.

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 предоставлены следующие документы:

– Технический паспорт объекта информатизации - АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении"

– Приказ об определении границ контролируемой зоны объекта информатизации.

По результатам проверки было установлено что состав, программных средств и размещение ОТСС 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 предоставлены следующие документы:

Наименование документа	Реквизиты документа
Акт определения УЗ	«31» августа 2023 г.
Акт оценки вреда	«31» августа 2023 г.
Приказ о назначении администратора безопасности	«31» августа 2023 г. № 244/1-О
Приказ о создании комиссии для установления уровня защищенности	«31» августа 2023 г. № 245/1-О
Приказ об утверждении Положения о защите информации	«31» августа 2023 г. № 246/1-О
Приказ об организации режима безопасности помещений	«31» августа 2023 г. № 247/1-О
Приказ об утверждении инструкций по обеспечению безопасности информации и функционированию информационных систем	«31» августа 2023 г. № 248/1-О
Приказ об определении системы доступа к информационным ресурсам	«31» августа 2023 г. № 249/1-О
Приказ об организации контроля (анализа) защищенности информации	«31» августа 2023 г. № 250/1-О
Приказ о порядке хранения и эксплуатации средств криптографической защиты информации	«31» августа 2023 г. № 251/1-О
Приказ о назначении лица, ответственного за организацию обработки персональных данных	«31» августа 2023 г. № 252/1-О

Проведенная проверка показала достаточность и соответствие их содержания требованиям стандартам и иным руководящим документам ФСТЭК России.

3.2.2. Проверка правильности определения уровня значимости ПДн на ОИ.

Комиссии по оценке эффективности предоставлены следующие документы:

– Акт определения уровня защищенности ПДн – «31» августа 2023 г.;

Проведенная проверка показала соответствие акта определения уровня защищенности ПДн требованиям Постановления Правительства РФ №1119 от 01.11.2012 г.

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

Применяемые средства защиты информации сертифицированы по требованиям безопасности информации.

ПО ViPNet Client 4.x имеет сертификат соответствия ФСБ России № СФ/124-4062 (действительный до 18.05.2024г.), удостоверяющий, что изделие «Программный комплекс «ViPNet Client 4»(версия 4.5) (исполнения 1, 2, 3) в комплектации согласно формуляру ФРКЕ-00116-05 30 01 ФО соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1, КС2, КС3 для исполнений 1, 2, 3, соответственно, Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КС1, КС2, КС3 для исполнений 1, 2, 3, соответственно, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, и IP-трафика, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, и IP трафика, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63 ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Kaspersky Endpoint Security 11 for Windows имеет сертификат ФСТЭК России № 4068 (до 22.01.2024 г.). Соответствует требованиям документов: Требования доверия(2), Требования к САВЗ, Профиль защиты САВЗ(Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ), Профиль защиты САВЗ(В второго класса защиты. ИТ.САВЗ.В2.ПЗ), Профиль защиты САВЗ(Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ), ЗБ.

СЗИ от НСД "Secret Net Studio" имеет сертификат соответствия ФСТЭК России № 3745 (до 16.05.2025г.). Соответствует требованиям документов: Требования доверия(4), Требования к МЭ, Профиль защиты МЭ(В четвертого класса защиты. ИТ.МЭ.В4.ПЗ), Требования к САВЗ, Профиль защиты САВЗ(А четвертого класса защиты. ИТ.САВЗ.А4.ПЗ), Профиль защиты САВЗ(Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ), Профиль защиты САВЗ(В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ), Профиль защиты САВЗ(Г четвертого класса защиты. ИТ.САВЗ.Г4.ПЗ), Требования к СКН, Профиль защиты СКН(контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ), Требования к СОВ, Профили защиты СОВ(узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ), ЗБ, РД СВТ(5).

ПК "Средство анализа защищенности "Сканер-ВС" имеет сертификат соответствия ФСТЭК России № 2204 (до 13.11.2024 г.), который подтверждает соответствие требованиям документов: Требования доверия(4), ТУ.

Проверка показала, что состав средств защиты информации соответствует требованиям по обеспечению безопасности ПДн 4-го уровня защищенности, средства защиты информации удовлетворяют требованиям по уровню доверия и классу средства защиты, классу криптозащиты по соответствующему классу информационной системы. Все используемые средства защиты сертифицированы по требованиям безопасности информации.

3.3. Анализ уязвимостей включает:

Корректность настройки проверяется в соответствии с формуляром на средство 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		

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
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 обеспечивается идентификация и аутентификация пользователей, являющихся работниками оператора. Проверена реализация многофакторной аутентификации для локального и удаленного доступа привилегированных и непривилегированных пользователей ИС. Аутентификация реализуется с использованием СЗИ от НСД "Secret Net Studio"
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	На ОИ регламентированы правила и процедуры управления идентификаторами, сроки блокировки идентификатора, сроки неиспользования, заблокированного идентификатора. Проверено 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 регламентированы правила выдачи идентификатора пользователю, определены длина, сложность и срок действия пароля. Проверена 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 осуществляться защита аутентификационной информации в процессе ее ввода путем исключения ее отображения для пользователя. Вводимые символы 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 осуществляется однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей. Проверена регламентация правил и процедур идентификации и аутентификации в ОРД
II. Управление доступом субъектов доступа к объектам доступа (УПД)		

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	На ОИ используется автоматизированная система управления учетными записями, реализована автоматическая блокировка неиспользуемых учетных записей. На ОИ регламентированы правила и процедуры управления учётными записями. Мера реализована с использованием СЗИ от НСД "Secret Net Studio"
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 регламентированы в организационно-распорядительных документах оператора по защите информации. В документах зафиксированы типы и правила доступа для каждого субъекта к каждому объекту. Мера реализована с использованием СЗИ от НСД "Secret Net Studio"
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 осуществляется управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы. Проверено наличие СЗИ, реализующих передачу информации между устройствами в рамках ОИ. Мера реализована с использованием ПО ViPNet Client 4.x (версия 4.5)
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	На ОИ обеспечено разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями. Проверено фиксирование в ОРД по защите информации полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы. Мера реализована с использованием СЗИ от НСД "Secret Net Studio"
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	На ОИ 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. Проверено наличие в ОРД по защите информации назначение прав и привилегий

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
		администраторам и лицам, обеспечивающим функционирование информационной системы. Мера реализована с использованием СЗИ от НСД "Secret Net Studio"
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. Проверено наличие в ОРД по защите информации разрешенное количество неуспешных попыток входа в ИС. Мера реализована с использованием СЗИ от НСД "Secret Net Studio"
IV. Защита машинных носителей персональных данных (ЗНИ)		
ЗНИ.1	Учет машинных носителей персональных данных	На ОИ обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации. Проверено наличие и ведение журнала учёта машинных носителей информации, а также правила их учёта. Мера реализована с использованием СЗИ от НСД "Secret Net Studio"
V. Регистрация событий безопасности (РСБ)		
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	На ОИ определены события безопасности в информационной системе, подлежащие регистрации, и сроки их хранения. Проверена регламентация в ОРД сроков хранения информации о событиях безопасности, осуществляется пересмотр перечня событий безопасности в плане внутренних проверок. Мера реализована с использованием СЗИ от НСД "Secret Net Studio"
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	На ОИ осуществляется реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти. Проверена реакция на

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
		переполнение журнала в СЗИ от НСД "Secret Net Studio".
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	На ОИ осуществляется мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них. Проверено ведение журнала регистрации событий безопасности, а также регламентация правил и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них. Мера реализована с использованием СЗИ от НСД "Secret Net Studio"
РСБ.7	Защита информации о событиях безопасности	На ОИ обеспечивается защита информации о событиях безопасности. Проверена настройка СЗИ, в части резервного копирования записей аудита. Мера реализована с использованием СЗИ от НСД "Secret Net Studio"
VI. Антивирусная защита (АВЗ)		
АВЗ.1	Реализация антивирусной защиты	На ОИ обеспечивается 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. Проверено наличие САВЗ на объекте информатизации. Мера реализована с использованием Kaspersky Endpoint Security 11 for Windows
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	На ОИ обеспечено обновление базы данных признаков вредоносных компьютерных программ. Проверена регламентация правил и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) в ОРД. Мера реализована с использованием Kaspersky Endpoint Security 11 for Windows
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)		
АНЗ.2	Контроль установки обновлений программного обеспечения, включая	На ОИ осуществляется контроль установки обновлений ПО, включая ПО СЗИ и ПО базовой системы ввода-

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
	обновление программного обеспечения средств защиты информации	вывода. Проверено 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 обеспечивается 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. Проверены наличие перечня лиц/должностей, допущенных к техническим средствам, а также 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 осуществляется размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр. Проверено размещение устройств вывода, условия должны удовлетворять требованию, 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 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. Проверено наличие соответствующих СЗИ. Мера реализована с использованием ПО ViPNet Client 4.x (версия 4.5)
Требования для обеспечения 4-го уровня защищенности ПДн, установленные Постановлением Правительства РФ от 01 ноября 2012 г. №1119		

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Проверка выполнения меры
	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	Проверено наличие Перечня сотрудников, имеющих право доступа в помещение и Правила доступа в помещение в рабочее и не рабочее время. Помещение оборудовано входными дверьми с замками, обеспечено постоянного закрытия дверей помещения на замок и их открытия только для санкционированного прохода,
	Обеспечение сохранности носителей персональных данных	На ОИ ведется поэкземплярный учет машинных носителей ПДн, который реализован путем ведения журнала учета носителей ПДн с использованием регистрационных (заводских) номеров.
	Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	Проверено наличие документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым на ОИ, необходим для выполнения ими служебных (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	На ОИ применяется СКЗИ класса КС2, что удовлетворяет требованиям по защите ПДн 4-го УЗ. ПО ViPNet Client 4.х (версия 4.5) сертифицирован по требованиям ФСТЭК и ФСБ.

Проверка показала полноту реализованных мер защиты информации, имеются все необходимые для обеспечения 4-го уровня защищенности ПДн.

4. Выводы аттестационной комиссии по результатам испытаний

Результаты оценки эффективности объекта информатизации - **АРМ, подключаемый к Федеральной информационной системе "Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении"** показали, что выполненные требования для обеспечения **4-го уровня** защищенности персональных данных при их обработке на объекте информатизации **Государственное областное бюджетное профессиональное образовательное учреждение «Липецкий колледж строительства, архитектуры и отраслевых технологий»**, реализованные организационные и технические меры по обеспечению безопасности ПДн соответствуют требованиям и мерам, установленным нормативными правовыми актами Российской Федерации в области защиты ПДн.

Оценка эффективности реализованных, в рамках защиты персональных данных, мер по обеспечению безопасности персональных данных на объекте информатизации проводится не реже одного раза в 3 года.

	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. № 23-3387
Отп. 1 экз. на 9 л., без черновика
Экз. ед. – в адрес;
Исп. Ананьева И.В.
Отп. Ананьева И.В.
От 24.10.2023 г. г.
тел. 515-888