Приложение №2

к договору на оказание услуг №_____ от _____2026г.

Техническое задание

Оказание услуг по приведению информационной системы ДСП ФКУ "ПОВОЛЖУПРАВТОДОР" в соответствие с законодательством РФ и проведению аттестации по требованиям безопасности информации в ИС.

1. Основные требования.

1.1. Исполнитель должен иметь все необходимые лицензии на деятельность по технической защите конфиденциальной информации Федеральной службы по техническому и экспортному контролю РФ (ФСТЭК России) и Федеральной службы безопасности РФ (ФСБ России) по соответствующим видам работ и услуг:

1.1.1. Лицензию (и) Федеральной службы по техническому и экспортному контролю РФ (ФСТЭК России) на осуществление деятельности по технической защите конфиденциальной информации по видам работ и услуг предусмотренными подпунктам, а), б), г), д), е) п. 4 «Положения о лицензировании деятельности по технической защите конфиденциальной информации», утвержденного постановлением Правительства Российской Федерации от 03.02.2012 года № 79:

– контроль защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации;

– контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

– аттестационные испытания и аттестация на соответствие требованиям по защите информации средств и систем информатизации;

– проектирование в защищенном исполнении средств и систем информатизации;

– установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

1.1.2. Лицензию Федеральной службы безопасности РФ (ФСБ России), в соответствии с подпунктом 1) пункта 1 статьи 12 Федерального закона Российской Федерации «О лицензировании отдельных видов деятельности» от 04.05.2011 года № 99-ФЗ и Постановлением Правительства РФ от 16.04.2012 года № 313 «О лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), осуществляемой юридическими лицами и индивидуальными предпринимателями», на осуществление деятельности по выполнению и оказанию следующих работ и услуг:

– разработка защищенных с использованием шифровальных (криптографических) средств информационных систем;

– разработка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– производство защищенных с использованием шифровальных (криптографических) средств информационных систем;

– производство защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных

Федеральной службой безопасности Российской Федерации;

– монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;

– монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств информационных систем;

– ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

– работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– передача шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;

– передача защищенных с использованием шифровальных (криптографических) средств информационных систем;

– передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.

1.2. Исполнитель должен оказать услуги и выполнить работы самостоятельно, без привлечения сторонних организаций и третьих лиц.

1.3. Исполнитель должен иметь возможность выполнять работы и оказывать услуги Заказчику непосредственно в офисе Заказчика, (как на период непосредственно выполнения работ и оказания услуг, так и на период последующего сопровождения систем) по адресу: г. Пенза, ул. Кураева, д. 1А.

1.4. Услуги и работы должны быть оказаны и выполнены в соответствии с действующими в РФ руководящими документами по технической защите конфиденциальной информации, а также, в соответствии с требованиями и рекомендациями действующих руководящих документов ФСТЭК России и ФСБ России по технической защите конфиденциальной информации:

1.4.1. Федеральным Законом Российской Федерации от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.4.2. Федеральным Законом Российской Федерации от 27.07.2006 года № 152-ФЗ «О персональных данных».

1.4.3. Указом Президента Российской Федерации от 06.03.1997 года № 188 «О перечне сведений конфиденциального характера».

1.4.4. «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утверждено Постановлением Правительства Российской Федерации от 01.11.2012 года № 1119.

1.4.5. «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждено Постановлением Правительства Российской Федерации от 15.09.2008 года № 687.

1.4.6. Трудовым кодексом Российской Федерации.

1.4.7. Приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

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

1.4.9. «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости», утверждено Приказом ФСБ России от 10.07.2014 года № 378.

2. Объем выполняемых работ и оказываемых услуг.

2.1. Приведению в соответствие с законодательством РФ и аттестации по требованиям безопасности информации подлежит ИС ДСП ФКУ "ПОВОЛЖУПРАВТОДОР" (далее - Заказчик),

расположенной по адресу: г. Пенза, ул. Кураева, дом № 1А.

2.2. ИС состоит из следующих компонентов:

– АРМ пользователей ИС – 1 шт.

2.2.1. Режим обработки информации в ИС – многопользовательский, пользователи имеют различные права доступа к ресурсам ИС.

2.2.2. ИС не имеет подключение к информационно-телекоммуникационным сетям международного информационного обмена.

2.2.3. Компоненты ИС расположены по адресам, указанным в таблице 1:

Таблица 1:

№ п/п	Адрес	Компоненты ИС	
		Сервер ИС	АРМ ИС
1	г. Пенза, ул. Кураева, дом № 1А		1

2.2.4. Обладатель информации (Заказчик) – ФКУ "ПОВОЛЖУПРАВТОДОР.

2.2.5. Оператор ИС – ФКУ "ПОВОЛЖУПРАВТОДОР.

2.2.6. ИС предназначается для обработки, хранения и передачи по каналам связи защищаемой информации (не составляющей государственную тайну), а также общедоступной информации, не содержащей сведений ограниченного распространения.

2.3. Содержание работ, необходимых для приведения ИС в соответствие с законодательством РФ, созданию Системы защиты конфиденциальных данных (СЗКДн) и проведению оценки эффективности принимаемых мер по обеспечению безопасности конфиденциальных данных (КДн), должны включать следующие этапы:

2.3.1. Предпроектное обследование ИС (обследование информационной системы на предмет выполнения требований по защите КДн).

2.3.2. Разработка проекта системы защиты ИС, комплекта документации по обеспечению безопасности КДн при их обработке в ИС и эксплуатации СЗКДн.

2.3.3. Подготовка, установка, настройка и конфигурирование программных, программно-аппаратных комплексов защиты информации в ИС (от несанкционированного доступа (НСД), межсетевых экранов (МЭ), систем обнаружения вторжений (СОВ), систем анализа защищенности (САЗ), средств антивирусной защиты (САВЗ), средств криптографической защиты информации (СКЗИ) и ввод СЗКДн в эксплуатацию.

2.3.4. Проведение оценки соответствия ИС требованиям по безопасности информации: «Аттестация ИС по требованиям безопасности информации».

2.4. На этапе предпроектного обследования, Исполнитель по представленным исходным данным Заказчика осуществляет:

2.4.1. определение необходимости обработки (обсуждения) информации, составляющей предмет защиты в конкретной информационной системе;

2.4.2. определение (уточнение) перечня сведений, подлежащих защите;

2.4.3. определение информационных характеристик и организационных структур ИС;

2.4.4. определение условий расположения ИС относительно границ контролируемой зоны (КЗ);

2.4.5. определение конфигураций и топологий ИС и систем связи в целом и их отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

2.4.6. определение технических средств и систем, предполагаемых к использованию в разрабатываемой (ых), ИС и системах связи, условия их расположения, общесистемные и прикладные программные средства, применяемые в обследуемой системе и предлагаемые к использованию;

2.4.7. определение технологического процесса обработки информации;

2.4.8. определение режимов обработки информации в ИС в целом и в отдельных компонентах;

2.4.9. определение степени участия персонала в обработке (обсуждении, передаче, хранении) информации, характер их взаимодействия между собой.

2.4.10. определение возможных каналов утечки информации и угроз безопасности информации в конкретных условиях функционирования ИС;

2.4.11. определение класса защищенности ИС;

2.4.12. определение уровня защищенности;

2.4.13. разработка модели угроз и нарушителя (частной модели угроз) для ИС в соответствии с

требованиями ФСТЭК России;

2.4.14. разработка модели угроз и нарушителя для ИС в соответствии с требованиями ФСБ России;

2.4.15. определение необходимых организационных и технических мер по обеспечению безопасности данных при их обработке в ИС;

2.4.16. разработка описания технологического процесса обработки информации в ИС.

2.5. На этапе разработки проекта системы защиты ИС, комплекта документации по обеспечению безопасности КДн при их обработке в ИС и эксплуатации СЗКДн, Исполнителем осуществляются:

2.5.1. разработка технического задания на создание системы защиты ИС;

2.5.2. определение перечня и условий применения, предлагаемых к использованию сертифицированных по требованиям безопасности информации средств защиты информации;

2.5.3. определение мероприятий по обеспечению конфиденциальности информации, обрабатываемой в ИС;

2.5.4. разработка технического проекта на создание системы защиты ИС;

2.5.5. разработка технического паспорта на ИС;

2.5.6. разработка инструкции (й) пользователю ИС, администратору (ам) ИС (системному, администратору безопасности и т.п.);

2.5.7. разработка правил разграничения доступа к КДн – разрешительной системы доступа (матрицы доступа) для ИС;

2.5.8. разработка порядка резервирования и восстановления работоспособности технических средств, общесистемного программного обеспечения, прикладного программного обеспечения, СУБД и средств защиты информации;

2.5.9. разработка необходимых журналов (учета работ и т.д.).

2.6. На этапе подготовки, установки, настройки и конфигурировании программных, программно-аппаратных комплексов защиты информации в ИС (от НСД, МЭ, САЗ, САВЗ, СКЗИ) и ввод СЗКДн в эксплуатацию, Исполнитель осуществляет:

2.6.1. приобретение (обновление) средств защиты информации, необходимых для выполнения требований «Технического проекта ИС».

2.6.2. проведение установки средств защиты;

2.6.3. проведение настройки средств защиты;

2.6.4. проведение тестирования и проверки функционирования и работоспособности средств защиты в ИС.

2.7. На этапе проведения оценки соответствия ИС требованиям по безопасности информации в формате: «Аттестация ИС по требованиям безопасности информации». Исполнителем осуществляются:

2.7.1. разработка программы и методики аттестационных испытаний ИС по требованиям безопасности информации;

2.7.2. проведение аттестационных испытаний ИС на соответствие требованиям по безопасности информации;

2.7.3. разработка протоколов аттестационных испытаний ИС по требованиям безопасности информации;

2.7.4. разработка заключений аттестационных испытаний ИС по требованиям безопасности информации;

2.7.5. разработка и выдача «Аттестатов соответствия ИС требованиям безопасности информации».

3. Требования Заказчика к результатам выполненных работ и оказанных услуг.

3.1. По результатам выполненных работ и оказанных услуг Исполнителем должны быть разработаны и согласованы с Заказчиком следующие документы (для каждой ИС, указанной в п. 2.1. настоящего документа разрабатывается отдельный комплект документации):

3.1.1. На этапе предпроектного обследования:

3.1.1.1. Отчет о результатах проведения аудита обеспечения класса защищенности информационной системы Заказчика.

3.1.2. На этапе разработки проекта системы защиты ИС, комплекта документации по обеспечению безопасности КДн при их обработке в ИС и эксплуатации СЗКДн:

3.1.2.1. «Акт определения класса защищенности ИС».

3.1.2.2. «Модель угроз и нарушителя безопасности персональных данных ИС в соответствии с требованиями ФСТЭК России».

3.1.2.3. «Модель угроз и нарушителя безопасности персональных данных ИС в соответствии с требованиями ФСБ России».

3.1.2.4. «Техническое задание на создание системы защиты ИС».

3.1.2.5. «Технический проект на создание системы защиты ИС».

3.1.2.6. «Технический паспорт ИС…».

3.1.2.7. «Описание технологического процесса обработки информации в ИС».

3.1.2.8. «Инструкция пользователю ИС»; «Инструкция (и) администратору (ам) ИС (системному, администратору безопасности ИС и т.п.), «Инструкция по использованию средств антивирусной защиты».

3.1.2.9. «Разрешительная система доступа к ресурсам ИС» («Матрица доступа к ресурсам ИС»).

3.1.2.10. «Порядок резервирования и восстановления работоспособности технических средств, общесистемного программного обеспечения, прикладного программного обеспечения, СУБД и средств защиты информации, персональных данных».

3.1.2.11. «Журнал учёта работ».

3.1.2.12. «Журнал учёта изменений состава АП ИС».

3.1.2.13. «Журнал учёта выдачи приема отчуждаемых накопителей информации».

3.1.2.14. «Журнал по учету мероприятий по контролю состояния защиты КДн»

3.1.3. На этапе подготовки, установки, настройки и конфигурировании программных, программно-аппаратных комплексов защиты информации в ИС (от НСД, МЭ, СОВ, САЗ, САВЗ, СКЗИ) и вводе СЗКДн в эксплуатацию:

3.1.3.1. Акт (ы) установки и конфигурирования программных, программно-аппаратных комплексов защиты информации в ИС (от НСД, МЭ, СОВ, САЗ, САВЗ, СКЗИ.

3.1.4. На этапе проведения оценки соответствия ИС требованиям по безопасности информации в формате: «Аттестация ИС по требованиям безопасности информации» (с Заказчиком не согласовываются):

3.1.4.1. «Программа и методика аттестационных испытаний ИС по требованиям безопасности информации».

3.1.4.2. «Протокол аттестационных испытаний ИС по требованиям безопасности информации».

3.1.4.3. «Заключение по результатам аттестационных испытаний ИС по требованиям безопасности информации».

3.1.4.4. Аттестат соответствия ИС требованиям безопасности информации».

4. Сопровождение СЗКДн и гарантийные обязательства.

4.1. Гарантийный срок на оказанные услуги и на обслуживание и ремонт средств защиты, поставленных Исполнителем (кроме неисправностей, произошедших по вине Заказчика), составляет 12 месяцев.

4.2. В течение гарантийного срока Исполнителем осуществляется сопровождение СЗКДн, в том числе:

- Оказание консультативной помощи по телефону, электронной почте в режиме 5*8 час.
- Гарантийное обслуживание и ремонт проводятся на объектах Заказчика.
- Исполнитель обеспечивает в течение срока гарантийного обслуживания оказание услуг по восстановлению работоспособности СЗКДн (в случае системного сбоя), при этом время реакции не должно превышать 16 рабочих часов.
- Гарантии качества оказанных услуг распространяются на все услуги, оказанные Исполнителем.

5. Требования Заказчика к применяемым в ИС средствам защиты информации.

5.1. В ИС, в качестве средств защиты информации, должны применяться только сертифицированные (ФСТЭК России и (или) ФСБ России) по требованиям безопасности информации средств защиты информации, необходимые для установленного уровня защищенности ИСПДн/класса защищенности ИС.

5.2. Требования к средствам защиты информации для ИС.

Таблица 2

№ п/п	Компонент	Предъявляемые требования	Кол-во
1.	**Аппаратный модуль доверенной загрузки, обеспечивающий защиту от несанкционированного доступа**	**1. Общие требования:** 1) Средства доверенной загрузки (далее – СДЗ) должны представлять собой специализированные встраиваемые аппаратно-программные комплексы средств защиты информации от несанкционированного доступа для рабочих станций и серверов на базе ПЭВМ типа IBM PC, функционирующих под управлением ОС семейств Windows и Linux (32 и 64 бит). 2) СДЗ должны реализовывать механизмы доверенной загрузки ОС и защиты от несанкционированного доступа к компьютеру при многопользовательском режиме эксплуатации рабочих станций. 3) СДЗ должны быть новыми, имеющими торговую марку, комплектующие – от производителей оригинального оборудования и не бывшие в употреблении. 4) СДЗ должно быть серийными, обладать возможностью его технической поддержки в авторизованных производителем сервис-центрах и возможностью доступа к расширенным сервисам по технической поддержке, ремонту и постгарантийному обслуживанию производителя. **2. Требования к функциональности:** СДЗ должно: 1) Использовать для идентификации пользователей персональные идентификаторы (идентификатор iButton типа DS 1993-1996 с брелоком, USB токен). Каналом для работы с персональными идентификаторами является USB порт на материнской плате ПЭВМ. 2) Использовать для аутентификации пользователей пароль длиной от 0 до 12 символов. 3) Блокировать загрузку с отчуждаемых носителей (FDD, CD ROM, ZIP Drive, USB Drive и др.). 4) Обеспечивать хранение в энергонезависимой памяти аппаратной части не менее 1024 записей учетных данных пользователей (или групп пользователей). 5) Блокировать прерывание контрольных процедур, осуществляемых при старте ПЭВМ с клавиатуры. 6) Обеспечивать контроль целостности системных областей жестких дисков, программ и данных, конфигурации технических средств ПЭВМ и ключей системного реестра до загрузки ОС, контроль целостности программной среды компьютера с поддержкой файловых систем FAT16, FAT32, NTFS, Ext2, Ext3, Ext4, ReiserFS. 7) Предоставлять возможность задания временных ограничений на доступ пользователей к ПЭВМ в соответствии с установленным для них режимом работы. 8) Предоставлять возможность блокировки загрузки компьютера при попытке обхода защитных функций АМДЗ на уровне настроек BIOS (механизм сторожевого таймера) без использования дополнительных прерывателей и переходников в системе электропитания ПЭВМ.	**1 шт.**

		9) Осуществлять регистрацию контролируемых событий, в том числе несанкционированных действий пользователей, в энергонезависимом системном журнале, доступ к которому должен предоставляться только администратору безопасности информации. Объем энергонезависимой памяти для хранения журнала событий должен составлять не менее 256 Кб. **3. Требования к составу комплексов СДЗ:** 1) Аппаратная часть СДЗ, должна функционировать в составе ПЭВМ, имеющей шинный интерфейс PCI-express, M.2; 2) Аппаратная часть СДЗ должна включать физический ДСЧ формата M2-PCI-Express. **4. Требования к сертификации** Средство доверенной загрузки должно иметь действующий сертификат ФСТЭК России на соответствие требованиям следующих руководящих документов: – «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) – по 2 уровню доверия. – «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013). «Профиль защиты средства доверенной загрузки уровня платы расширения второго класса защиты. ИТ.СДЗ.ПР2.ПЗ». – Средство доверенной загрузки должно иметь действующий сертификат ФСБ России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки для класса не ниже 2Б. **5. Требования к документации** СДЗ должно поставляться с комплектом эксплуатационной документации (руководством по установке, руководством администратора и руководством пользователя), Формуляром (или Паспортом), Гарантийным талоном Поставщика. Вся документация должна быть на русском языке. Состав и содержание эксплуатационной документации должны быть достаточны для инсталляции и обслуживания СДЗ. **6. Требования к гарантийному обслуживанию** Гарантийный срок на продукцию - не менее 36 месяцев с даты поставки продукции заказчику.	
	Защищенный носитель базового уровня для ключей УКЭП	**Требования к защищенному носителю:** **1. В части возможностей аутентификации владельца:** – наличие двухфакторной аутентификации: по предъявлению самого идентификатора и по предъявлению уникального PIN-кода; – наличие поддержки 3 категорий владельцев: администратор, пользователь, гость; – наличие поддержки 2-х глобальных PIN-кодов: администратора и пользователя; – наличие настраиваемого минимального размера PIN-кода; – наличие индикации факта смены глобальных PIN-кодов с умалчиваемых на оригинальные; – наличие разграничения доступа к файловым объектам в соответствии с уровнем доступа; – наличие ограничения числа попыток ввода PIN-кода. **2. В части файловой системы:** – наличие встроенной файловой структуры по ISO/IEC 7816-4; – число файловых объектов внутри папки — до 255 включительно; – уровень вложенности папок ограничен объемом свободной памяти для файловой системы; – использование File Allocation Table (FAT) для оптимального размещения файловых объектов в памяти;	**2 шт.**

		– использование файлов Elementary File (файл общего назначения, часть файловой системы устройства) для хранения ключевой информации: ключей шифрования, сертификатов и т. п.; – использование предопределенных папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании EF-файлов (Elementary File, файл общего назначения, часть файловой системы устройства); – наличие возможности изменения политики смены PIN-кода пользователя. Смена может быть доступна Пользователю, Администратору или обеим ролям одновременно. **3. В части интерфейсов:** – наличие протокола обмена по ISO 7816-12; – поддержка USB CCID: работа без установки драйверов устройства в современных версиях ОС; – поддержка PC/SC; – наличие поддержки Microsoft Crypto API; – наличие поддержки Microsoft SmartCard API; – наличие PKCS#11. **4. В части встроенного контроля и индикации:** – контроль целостности микропрограммы (прошивки); – контроль целостности системных областей памяти; – проверка целостности EF-файлов перед любым их использованием; – счетчики изменений в файловой структуре и изменений любых PIN-кодов для контроля несанкционированных изменений; – наличие светодиодного индикатора с режимами работы: готовность к работе, выполнение операции, нарушения в системной области памяти. **5. В части общих характеристик:** – наличие современного защищенного микроконтроллера; – наличие идентификации с помощью 32-битного уникального серийного номера; – интерфейс USB 1.1 и выше; – наличие 32-битного уникального серийного номера; – объем памяти для хранения ключевой информации – не менее 128 КБ; – поддержка операционных систем: • Microsoft Windows 11/10/8.1/2019/2016/2012R2/8/2012/7/2008R2/Vista/2008/XP/2003 ; GNU/Linux.	

6. Срок оказания услуг: 31.10.2026 г.