УТВЕРЖДАЮ
Заместитель генерального директора
_____Т.И. Мельникович
«__» _____2026 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на закупку услуг по проектированию, созданию и аттестации системы защиты информации Могилевского РУП «Фармация»

1. **Предмет закупки:** услуга по созданию и аттестации системы защиты информации Могилевского РУП «Фармация» (далее – Предприятие) (код ОКРБ 007-2012 62.01.12.000).

2. **Описание объекта:**

Информационная система Предприятия представляет собой совокупность активного и пассивного серверного, сетевого оборудования, вычислительных средств, информационных ресурсов, комплексов программно-технических средств и средств защиты информации.

Контур: управление Предприятия и аптека №1 г.Могилева, (г. Могилев, ул. Первомайская, 59), Белыничская ЦРА №41 (г.п. Белыничи, ул. Энгельса, 3Б).

Эксплуатируется около 100 ПЭВМ, 4 единицы серверного оборудования (развернут кластер VMware на основе гипервизоров VMware 6.7.0 – обслуживается 12 виртуальных машин

3. **Основные понятия:**

Система защиты информации (далее - СЗИ) - комплекс организационных, технических и технологических средств, методов и мер, препятствующих несанкционированному доступу к информации.

4. **Требования к предмету закупки:**

4.1 Этапы создания и аттестации СЗИ:

№	Наименование услуг	Результаты работ (услуг) - отчетные документы	Срок выполнения работ
Этап 2. Создание СЗИ.			
2.1	Корректировка структурной и логической схем информационной системы (при необходимости);	Актуализированные: Логическая схема СЗИ. Структурная схема ИС (Описание активов Структуры информационной сети).	Количество рабочих дней
2.2	Разработка документации на СЗИ по перечню, определенному в техническом задании.	Документация на СЗИ по перечню, определенному в техническом задании на СЗИ.	
2.3	Корректировка проектов политики информационной безопасности и иных локальных правовых актов и других организационно-распорядительных документов;	Актуализированные документы	

2.4	Закупка дополнительных средств технической и криптографической защиты информации (при необходимости, осуществляется Заказчиком).	Подготовка ТЗ (заказчик совместно с исполнителем)	
2.5	Исполнитель совместно с заказчиком: Монтаж и наладка средств технической и криптографической защиты информации в соответствии с документацией на СЗИ, рекомендациями изготовителя, требованиями по совместимости средств криптографической защиты информации и ограничениями, указанными в сертификате соответствия. На данном этапе осуществляется реализация мер по технической и криптографической защите информации, в том числе: внедрение технических и криптографических средств защиты, их монтаж и наладку; проверка работоспособности и совместимости средств защиты с активами ИС; проверку корректности выполнения средствами защиты информации требований по защите информации в реальных условиях эксплуатации и во взаимодействии с активами информационной системы; маркировку всех физических линий связи согласно структурной схеме информационной системы; обеспечение выполнения технических условий внутри своей ИТ-инфраструктуры, необходимых для проведения со стороны Исполнителя удалённого сканирования на наличие уязвимостей.	Акт проверки работоспособности и совместимости с другими объектами информационной сети и средств технической и криптографической защиты информации.	
2.6	Смена реквизитов доступа к функциям управления и настройкам, установленным по умолчанию, либо блокировка учетных записей, не предусматривающих смену указанных реквизитов (осуществляется Заказчиком, при необходимости Исполнителем при условии заключения соответствующего дополнительного соглашения).		
2.7	Проведение предварительных испытаний СЗИ с оформлением соответствующего акта.	Акт проведения предварительных испытаний СЗИ.	

2.8	Проверка корректности выполнения средствами защиты информации требований безопасности в реальных условиях эксплуатации и во взаимодействии с другими объектами информационной системы.	Отчет о результатах проверки корректности выполнения средствами защиты информации требований безопасности в реальных условиях эксплуатации.	
2.9	Проведение обследования и подготовка предложений по реализации организационных мер по защите информации.	Отчет о достаточности организационных мер по защите информации в информационной системе.	
2.10	Подготовка исходных данных на СЗИ Предприятия для проведения аттестации СЗИ в соответствии с приказом оперативно- аналитического центра при Президенте Республики Беларусь от 20.02.2020 №66.		
2.11	Иные документы.	Иная документация на СЗИ, предусмотренная законодательством для этапа создания системы защиты информации (при необходимости). Акт сдачи-приемки оказанных услуг.	
2.12	Разработка ЛПА, регулирующих деятельность системы защиты информации (перечень указанных актов согласовывается с Заказчиком на этапе проектирования).	Локальные правовые акты на СЗИ и её деятельность.	
2.13	Проведение сканирования на уязвимости (устранение уязвимостей при необходимости)	Отчет по сканированию.	
2.14	Услуга по настройке системы защиты информации Сегментирование сети (создание VLAN, настройка интерфейсов сетевого оборудования) и настройка правил маршрутизации и перенаправления трафика; Настройка средства межсетевого экранирования; Настройка синхронизации временных меток на сетевом оборудовании (межсетевой экран, коммутаторы), средствах защиты информации, в среде виртуализации, ОС серверов с единым источником времени; Настройка ОС серверов;	Готовность системы к аттестации	На протяжении выполнения всех этапов

	Установка и настройка контроллера домена (Active Directory) с обеспечением подключения к нему сетевого оборудования; Установка и настройка ПО среды виртуализации и средства управления средой виртуализации (любой, имеющейся у заказчика) Установка и настройка ОС виртуальных машин, развернутых в среде виртуализации; Установка и настройка программного обеспечения для централизованного управления учетными записями пользователей и администраторов, разграничения доступа их к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации; Установка и настройка программного обеспечения для централизованного мониторинга за объектами информационной системы, для контроля за работоспособностью, параметрами настроек, правильностью функционирования и составом средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации; Установка и настройка средства централизованного менеджмента и сбора событий информационной безопасности для объектов ИС; Установка и настройка средства защиты от вредоносного программного обеспечения (сервер управления и настройка типового агента) для объектов ИС; Установка и настройка программного обеспечения для резервного копирования; Настройка систем хранения и резервного копирования данных; Настройка парольной политики на объектах ИС учреждения; Настройка контроля съёмных носителей; Внедрение средства криптографической защиты информации (BelVPN Gate, S-Crypto VPN), настройка и подключение (при необходимости); Настройка контроля использования съемных носителей. Консультации ИТ-персонала учреждения		

	по работе и сопровождению с созданной СЗИ ИС, первоначальное обучение и техническая поддержка		
Этап 3. Аттестация СЗИ			
3.1	Разработка программы и методики аттестации.	Программа и методика аттестации.	Количество рабочих дней
3.2	Установление соответствия реального состава и структуры объектов информационной системы общей схемы СЗИ.	Заключения по проведенным проверкам.	
3.3	Проверка правильности отнесения информационной системы к классу типовых информационных систем, выбора и применения средств защиты информации.		
3.4	Анализ разработанной документации на СЗИ собственника (владельца) информационной системы на предмет ее соответствия требованиям законодательства об информации, информатизации и защите информации. Актуализация локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации на предмет соответствия законодательству об информации, информатизации и защите информации (осуществляется Исполнителем совместно с Заказчиком);		
3.5	Ознакомление с документацией о распределении функций персонала по организации и обеспечению защиты информации.		
3.6	Проведение испытаний СЗИ на предмет установленных законодательством требований по защите информации. (включая сканирование уязвимостей, тестирование на проникновение) с применением средств оценки эффективности защищённости (сетевой сканер, сканер уязвимостей, сканер уязвимостей веб-приложений и др.) (осуществляется Исполнителем совместно с Заказчиком);	Протокол испытаний.	

3.7	Проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств аппаратных, программных и программно-аппаратных средств, которые могут быть инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы.	Технический отчет.	
3.8	Оформление и выдача аттестата соответствия.	Аттестат соответствия.	
3.9	Иные документы.	Иная документация на СЗИ, предусмотренная законодательством для этапа аттестации системы защиты информации (при необходимости). Акт сдачи-приемки оказанных услуг.	

4.2. Локальные правовые акты на СЗИ, внедрение средств технической и криптографической защиты информации, реализация организационных мер по ЗИ осуществляются согласно актуальным требованиям Оперативно-аналитического центра при Президенте Республики Беларусь.

4.3. Сроки могут измениться в зависимости от необходимости Заказчика в приобретении технических средств, сертификации средств защиты информации и иных факторов, влияющих на проведение работ по созданию и аттестации системы защиты информации информационных систем.

5. Квалификационные требования к исполнителю работ

К исполнителю работ предъявляются следующие требования:

– наличие лицензии Оперативно-аналитического центра при Президенте Республики Беларусь на право осуществления деятельности по технической и (или) криптографической защите информации (проектирование, создание, аттестация систем защиты информации информационных систем, предназначенных для обработки информации, распространение и(или) предоставление которой ограничено, не отнесенной к государственным секретам);

– наличие сертифицированной системы менеджмента информационной безопасности на соответствие требованиям СТБ ISO/IEC 27001:2016 или СТБ ISO/IEC 27001:2024 применительно к проектированию, созданию и аттестации систем защиты информации информационных систем и (или) наличие сертифицированной системы менеджмента качества в соответствии с требованиями СТБ ISO 9001:2015 применительно к проектированию, созданию и аттестации систем защиты информации информационных систем;

– наличие в штате не менее 3 специалистов для выполнения работ собственными силами без привлечения субподрядчиков;

– документально подтвержденный положительный опыт выполнения работ по проектированию СЗИ ИС (не менее двух отзывов).

Исполнитель обязан осуществить актуализацию всех документов, необходимых для создания и аттестации СЗИ ИС, в том числе документы, которые должны быть разработаны и утверждены от имени собственника (владельца) информационной системы (информационного ресурса).

6. Требования по гарантии:

Гарантийный срок на оказанные Услуги исчисляются с даты подписания акта выполненных работ (оказанных услуг) и должен составлять не менее 12 месяцев.

В случае изменения в течение гарантийного срока требований законодательства Республики Беларусь об информации, информатизации и защите информации, на основании которого было выполнено проектирование СЗИ отдельных элементов Предприятия, Исполнитель дорабатывает проект в соответствии с новыми требованиями за свой счет, если в законодательстве не будет оговорено, что аттестация СЗИ для таких информационных систем осуществляется в соответствии с законодательством, действующим до вступления в силу нового законодательства.

7. Оплата стоимости услуг по каждому этапу производится Заказчиком на расчетный счет Исполнителя в течение 10 (десяти) банковских дней со дня подписания Акта сдачи-приемки оказанных услуг.

8. Источник финансирования закупки - собственные средства.

9. Коммерческое предложение должно содержать цену, представленную в белорусских рублях.

10. Срок выполнения работ - **90 календарных дней без учета работ, выполняемых Заказчиком.**

11. Коммерческое предложение на выполнение работ (оказание услуг) по созданию и аттестации системы защиты информации Предприятия предоставить **до 15.07.2026 года по форме Приложение 1, e-mail zakupka_it@mogpharm.by.**

Подача альтернативных предложений не допускается. Участник в праве предоставить только одно коммерческое предложение.

12. Контактные лица:

(80222) 62-96-67 Тризонова Елена Валерьевна, начальник отдела информационных технологий, Козик Виталий Викторович, ведущий инженер-системотехник отдела информационных технологий.

Информация 1-го этапа проектирования ТЗИ предоставляется участнику-победителю по письменному запросу:

– политика информационной безопасности;
– техническое задание информационной безопасности;
– технический отчет;
– отчет обследования;
– перечень средств защиты информации;
– логическая и структурная схема.

Информация поступившего предложения будет использована для определения ориентировочной стоимости предмета закупки и иных условий, и не влечет за собой возникновение каких-либо обязательств между Заказчиком и потенциальным поставщиком (подрядчиком, исполнителем).

Ведущий инженер-системотехник В.В. Козик

Начальник отдела информационных технологий Е.В. Тризонова

Приложение 1

Форма коммерческого предложения участника

На официальном бланке

КОММЕРЧЕСКОЕ ПРЕДЛОЖЕНИЕ

1. Сведения об участнике:

1.1.Полное наименование: _____

1.2.Место нахождения: _____

1.3.Почтовый адрес: _____

1.4.Электронный адрес: _____

1.5.Сайт: _____

1.6.Телефон: _____ , телефон/факс_____

1.7.Контактное лицо: _____

1.8.Расчетный счет: _____

1.9.Дополнительные сведения: _____

Предмет закупки: услуга по проектированию информационной системы защиты информации Могилевского РУП «Фармация» (далее – Предприятие) (код ОКРБ 007-2012 62.01.12.000).

Система защиты информации (далее - СЗИ) - комплекс организационных, технических и технологических средств, методов и мер, препятствующих несанкционированному доступу к информации.

2. Требования к предмету закупки:

№	Наименование услуг	Результаты работ (услуг) - отчетные документы	Срок выполнения работ
Этап 2. Создание СЗИ.			
2.1	Корректировка структурной и логической схем информационной системы (при необходимости);	Актуализированные: Логическая схема СЗИ. Структурная схема ИС (Описание активов Структуры информационной сети).	Количество рабочих дней
2.2	Разработка документации на СЗИ по перечню, определенному в техническом задании.	Документация на СЗИ по перечню, определенному в техническом задании на СЗИ.	
2.3	Корректировка проектов политики информационной безопасности и иных локальных правовых актов и других организационно-распорядительных документов;	Актуализированные документы	

2.4	Закупка дополнительных средств технической и криптографической защиты информации (при необходимости, осуществляется Заказчиком).	Подготовка ТЗ (заказчик совместно с исполнителем)
2.5	Исполнитель совместно с заказчиком: Монтаж и наладка средств технической и криптографической защиты информации в соответствии с документацией на СЗИ, рекомендациями изготовителя, требованиями по совместимости средств криптографической защиты информации и ограничениями, указанными в сертификате соответствия. На данном этапе осуществляется реализация мер по технической и криптографической защите информации, в том числе: внедрение технических и криптографических средств защиты, их монтаж и наладку; проверка работоспособности и совместимости средств защиты с активами ИС; проверку корректности выполнения средствами защиты информации требований по защите информации в реальных условиях эксплуатации и во взаимодействии с активами информационной системы; маркировку всех физических линий связи согласно структурной схеме информационной системы; обеспечение выполнения технических условий внутри своей ИТ-инфраструктуры, необходимых для проведения со стороны Исполнителя удалённого сканирования на наличие уязвимостей.	Акт проверки работоспособности и совместимости с другими объектами информационной сети и средств технической и криптографической защиты информации.
2.6	Смена реквизитов доступа к функциям управления и настройкам, установленным по умолчанию, либо блокировка учетных записей, не предусматривающих смену указанных реквизитов (осуществляется	

	Заказчиком, при необходимости Исполнителем при условии заключения соответствующего дополнительного соглашения).		
2.7	Проведение предварительных испытаний СЗИ с оформлением соответствующего акта.	Акт проведения предварительных испытаний СЗИ.	
2.8	Проверка корректности выполнения средствами защиты информации требований безопасности в реальных условиях эксплуатации и во взаимодействии с другими объектами информационной системы.	Отчет о результатах проверки корректности выполнения средствами защиты информации требований безопасности в реальных условиях эксплуатации.	
2.9	Проведение обследования и подготовка предложений по реализации организационных мер по защите информации.	Отчет о достаточности организационных мер по защите информации в информационной системе.	
2.10	Подготовка исходных данных на СЗИ Предприятия для проведения аттестации СЗИ в соответствии с приказом оперативно- аналитического центра при Президенте Республики Беларусь от 20.02.2020 №66.		
2.11	Иные документы.	Иная документация на СЗИ, предусмотренная законодательством для этапа создания системы защиты информации (при необходимости). Акт сдачи-приемки оказанных услуг.	
2.12	Разработка ЛПА, регулирующих деятельность системы защиты информации (перечень указанных актов согласовывается с Заказчиком на этапе проектирования).	Локальные правовые акты на СЗИ и её деятельность.	
2.13	Проведение сканирования на уязвимости (устранение уязвимостей при необходимости)	Отчет по сканированию.	
2.14	Услуга по настройке системы защиты информации	Готовность системы к аттестации	На протяжении выполнения всех этапов

	Сегментирование сети (создание VLAN, настройка интерфейсов сетевого оборудования) и настройка правил маршрутизации и перенаправления трафика; Настройка средства межсетевого экранирования; Настройка синхронизации временных меток на сетевом оборудовании (межсетевой экран, коммутаторы), средствах защиты информации, в среде виртуализации, ОС серверов с единым источником времени; Настройка ОС серверов; Установка и настройка контроллера домена (Active Directory) с обеспечением подключения к нему сетевого оборудования; Установка и настройка ПО среды виртуализации и средства управления средой виртуализации (любой, имеющейся у заказчика) Установка и настройка ОС виртуальных машин, развернутых в среде виртуализации; Установка и настройка программного обеспечения для централизованного управления учетными записями пользователей и администраторов, разграничения доступа их к средствам вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации; Установка и настройка программного обеспечения для централизованного мониторинга за объектами информационной системы, для контроля за работоспособностью, параметрами настроек, правильностью функционирования и составом средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации; Установка и настройка средства		

	централизованного менеджмента и сбора событий информационной безопасности для объектов ИС; Установка и настройка средства защиты от вредоносного программного обеспечения (сервер управления и настройка типового агента) для объектов ИС; Установка и настройка программного обеспечения для резервного копирования; Настройка систем хранения и резервного копирования данных; Настройка парольной политики на объектах ИС учреждения; Настройка контроля съёмных носителей; Внедрение средства криптографической защиты информации (BelVPN Gate, S-Crypto VPN), настройка и подключение (при необходимости); Настройка контроля использования съемных носителей. Консультации ИТ-персонала учреждения по работе и сопровождению с созданной СЗИ ИС, первоначальное обучение и техническая поддержка		
Этап 3. Аттестация СЗИ			
3.1	Разработка программы и методики аттестации.	Программа и методика аттестации.	Количество рабочих дней
3.2	Установление соответствия реального состава и структуры объектов информационной системы общей схемы СЗИ.	Заключения по проведенным проверкам.	
3.3	Проверка правильности отнесения информационной системы к классу типовых информационных систем, выбора и применения средств защиты информации.		
3.4	Анализ разработанной документации на СЗИ собственника (владельца) информационной системы на предмет ее соответствия требованиям законодательства об информации, информатизации и защите информации.		

	Актуализация локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации на предмет соответствия законодательству об информации, информатизации и защите информации (осуществляется Исполнителем совместно с Заказчиком);		
3.5	Ознакомление с документацией о распределении функций персонала по организации и обеспечению защиты информации.		
3.6	Проведение испытаний СЗИ на предмет установленных законодательством требований по защите информации. (включая сканирование уязвимостей, тестирование на проникновение) с применением средств оценки эффективности защищённости (сетевой сканер, сканер уязвимостей, сканер уязвимостей веб-приложений и др.) (осуществляется Исполнителем совместно с Заказчиком);	Протокол испытаний.	
3.7	Проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств аппаратных, программных и программно-аппаратных средств, которые могут быть инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы.	Технический отчет.	
3.8	Оформление и выдача аттестата соответствия.	Аттестат соответствия.	
3.9	Иные документы.	Иная документация на СЗИ, предусмотренная законодательством для этапа аттестации системы защиты информации (при необходимости).	

		Акт сдачи-приемки оказанных услуг.	

3. Цена предложения: _____ бел. рублей,
в том числе НДС _____ бел. рублей;
Если цена без НДС, то указать обоснование освобождения от НДС.

4. Требования по гарантии:
Гарантийный срок: _____ месяцев.

Срок выполнения работ при возникновении гарантийного случая не более _____ календарных дней.

5. Требования к качеству: в случае изменения в течение гарантийного срока требований законодательства Республики Беларусь об информации, информатизации и защите информации, на основании которого было выполнено проектирование СЗИ отдельных элементов Предприятия, Исполнитель дорабатывает проект в соответствии с новыми требованиями за свой счет, если в законодательстве не будет оговорено, что аттестация СЗИ для таких информационных систем осуществляется в соответствии с законодательством, действующим до вступления в силу нового законодательства.

6. Место оказания услуг: г. Могилев, ул. Первомайская, 59.

7. Оплата стоимости услуг производится Заказчиком на расчетный счет Поставщика в течение 10 (десяти) банковских дней со дня подписания акта выполненных работ.

8. Порядок формирования суммы договора на закупку с учетом расходов на доставку, страхование, уплату таможенных пошлин, налогов, сборов и других обязательных платежей.

9. Предложение содержит цену, представленную в белорусских рублях. Цена предложения содержит расходы на доставку, страхование, уплату таможенных пошлин, налогов, сборов и других обязательных платежей. Цена остается фиксированной в течение всего срока выполнения договора.

10. Настоящее коммерческое предложение действительно на протяжении не менее _____ календарных дней с момента окончательного срока представления ценовых предложений.

11. Наличие лицензии Оперативно-аналитического центра при Президенте Республики Беларусь на право осуществления деятельности по технической и (или) криптографической защите информации (проектирование, создание, аттестация систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам) на ___ л. в 1 экз.

12. Заверенные копии сертификатов систем менеджмента СТБ ISO 9001 и СТБ ISO 27001 (система менеджмента информационной безопасности) применительно к проектированию, созданию и аттестации систем защиты информации информационных систем.

13. наличие в штате не менее ___ специалистов для выполнения работ собственными силами без привлечения субподрядчиков;

14. положительный опыт выполнения работ по созданию и аттестации СЗИ ИС _____ шт (документально подтвержденных не менее двух отзывов).

Ф.И.О. руководителя предприятия подпись печать (при наличии)