

УТВЕРЖДАЮ
Дубининко Д.П.
02-10 2026

ЗАДАНИЕ

на закупку работ по проектированию, созданию, внедрению и аттестации систем защиты информации

1. Общие положения

1.1. Работы по проектированию, созданию, внедрению и аттестации систем защиты информации (далее – СЗИ) информационных систем (далее – ИС) ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и информационной системы ИС ИС-4-ДСП выполняются исполнителем в целях обеспечения конфиденциальности, целостности, доступности и сохранности информации, обрабатываемой в ИС Открытого акционерного общества «Дорожно-строительный трест № 5» (далее – заказчик).

1.2. Все этапы выполнения работ по проектированию, созданию, внедрению и аттестации СЗИ ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП выполняются согласно с графику выполнения работ, являющимся неотъемлемой частью договора, а также в соответствии с требованиями нижеуказанных документов:

Законом Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

Законом Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»;

Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»;

Указом Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации»;

Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (в редакции приказа от 10.12.2024 № 259) (далее – Приказ ОАЦ № 66);

иными нормативными правовыми актами Республики Беларусь, стандартами и иными техническими нормативными правовыми актами в области защиты информации.

1.3. Предварительная информация:

ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ отнесены к классам типовых ИС – 3-ин, 3-спец, 3-юл;

ИС ИС-4-ДСП отнесена к классу типовых ИС – 4-дсп.

1.4. ИС ИС-4-ДСП представляет собой отдельно установленную рабочую станцию, установленную в головном офисе, не подключенную к сети, с использованием которой у заказчика обрабатывается служебная информация ограниченного распространения.

ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ представляет собой набор сетевого оборудования (15шт~), физических серверов (5шт~), рабочих станций (350шт~), антивирусного ПО (350шт~ из них 5шт~ сертифицированных) виртуальных машин (10шт~), средств защиты информации, прикладного и системного программного обеспечения, которые в совокупности осуществляют обеспечение функционирования и защиту информационных ресурсов и систем, эксплуатируемых у заказчика.

В дополнение: все элементы за исключением серверов и отдельного ОП распределены по филиалам, адреса которых указаны в пункте 1.5. В том числе есть сотрудники, работающие удаленно.

1.5. Примерный список адресов и названий городов по расположению офисов и производственных баз ОАО “ДСТ № 5”:

1.5.1. ул. Лукьяновича, 4-253, 220113, г. Минск (Головной офис).

1.5.1. Щомыслицкий сельсовет (Озерцо).

1.5.1. Минская обл., Молодечненский р-н, г.Молодечно, ул. Замковая, 33.

1.5.1. Минская обл., Вилейский р-н, г.Вилейка, ул. 1 Мая, 64.

1.5.1. Минская обл., Березинский р-н, г.Березино, ул.Зеленая, 22/3.

1.5.1. Минская обл., Слуцкий р-н, Исернский с/с, 5, 1180м севернее от д.Великая Слива, ул.Центральная, 28.

1.5.1. г.Фаниполь.

1.5.1. г.Заславль.

1.6. Работы включают в себя:

1.6.1. Проектирование СЗИ;

- 1.6.2. Создание СЗИ;
- 1.6.3. Внедрение СЗИ;
- 1.6.4. Аттестация СЗИ.

1.7. Заказчик: Открытое акционерное общество «Дорожно-строительный трест № 5», УНП 100219908, ул. Лукьяновича, 4-253, 220113, г. Минск.

2. Требования к проектированию СЗИ

2.1. В процессе проектирования СЗИ ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП должны быть проведены следующие мероприятия:

2.1.1. анализ структуры ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП и информационных потоков (внутренних и внешних) в целях определения состава, количества и мест размещения элементов ИС (аппаратных и программных), её физических и логических границ;

2.1.2. анализ взаимодействия информационных систем, входящих в состав ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП, и их элементов;

2.1.3. разработка (корректировка) Политики информационной безопасности;

2.1.4. разработка структурной и логической схем ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП;

2.1.5. разработка технического задания на создание системы защиты информации ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП (далее – техническое задание);

2.1.6. выбор средств криптографической защиты информации, удовлетворяющих требованиям ОАЦ;

2.1.7. разработка проектов локальных нормативных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации;

2.1.8. издание иной документации, предусмотренной техническим заданием и Положениями;

2.1.9. прочие мероприятия, направленные на подготовку информационной инфраструктуры заказчика к созданию СЗИ ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП в организационном и техническом плане: консультирование заказчика по выбору и настройке сетевого, серверного оборудования, средств вычислительной техники, программного обеспечения, средств защиты информации, иных активов ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП.

2.2. Поскольку для ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ документация по защите информации отсутствует, проектирование СЗИ выполняется в полном объеме. Для ИС ИС-4-ДСП имеется ранее разработанная документация, проектирование СЗИ выполняется с её актуализацией и доработкой по результатам обследования.

3. Требования к созданию СЗИ

3.1. В процессе создания СЗИ ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП должны быть проведены следующие мероприятия (в соответствии с Положениями):

3.1.1. Реализация (внедрение) мер защиты информации, предусмотренных проектом СЗИ;

3.1.2. корректировка (при необходимости) разработанных на этапе проектирования системы защиты информации структурной и логической схем информационной системы. При корректировке разработанных на этапе проектирования системы защиты информации проектов локальных нормативных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации учитываются результаты внедрения средств технической и криптографической защиты информации, проверки их работоспособности и совместимости с активами ИС.

4. Требования к внедрению СЗИ

4.1. В процессе внедрения СЗИ ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП должны быть проведены следующие мероприятия:

4.1.1. установка и настройка средств технической и криптографической защиты информации, предусмотренных проектом СЗИ;

4.1.2. проверка работоспособности и совместимости средств защиты информации с активами ИС;

4.1.3. реализация организационных мер защиты информации, предусмотренных проектом СЗИ;

4.1.4. проверка функционирования СЗИ в реальных условиях эксплуатации;

4.1.5. корректировка (при необходимости) структурной и логической схем ИС, локальных нормативных правовых актов и других организационно-распорядительных документов по результатам внедрения;

5. Требования к аттестации СЗИ

5.1. На этапе аттестации должна быть дана комплексная оценка СЗИ ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП в реальных условиях эксплуатации.

Данный этап работ в соответствии с Положениями включает:

5.1.1. разработку программы и методики аттестации СЗИ ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП;

5.1.2. установление соответствия фактического состава активов ИС структурной и логической схемам ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП;

5.1.3. проверку правильности отнесения ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП к классу (классам) типовых информационных систем;

5.1.4. проверку достаточности реализованных в СЗИ мер по защите информации, в том числе анализ локальных нормативных правовых актов и других организационно-распорядительных документов по вопросам применения СЗИ на предмет их соответствия требованиям законодательства об информации, информатизации и защите информации;

5.1.5. проведение испытаний СЗИ на предмет выполнения установленных законодательством требований по защите информации;

5.1.6. внешнюю и внутреннюю проверку отсутствия либо невозможности использования нарушителем свойств активов ИС, средств защиты информации, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих активов ИС, СЗИ;

5.1.7. оформление технического отчёта и протокола испытаний;

5.1.8. оформление аттестата соответствия.

5.2. Отчётные документы по аттестации СЗИ ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП должны быть представлены исполнителем заказчику в одном экземпляре на бумажном носителе и в одном экземпляре в электронном виде на съёмном носителе (USB-накопителе) (в части, касающейся проектирования СЗИ). Электронное представление документов должно соответствовать форматам документов Microsoft Word и PDF.

6. Срок выполнения работ

6.1. Срок выполнения работ по проектированию, созданию и аттестации СЗИ ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП – в соответствии с графиком выполнения работ, являющимся неотъемлемой частью договора.

7. Квалификационные требования к исполнителю

7.1. Работы по проектированию, созданию, внедрению и аттестации СЗИ ИС ИС-3-ИН, ИС-3-СПЕЦ, ИС-3-ЮЛ и ИС ИС-4-ДСП выполняются исполнителем (организацией) при соблюдении следующих требований:

7.1.1. наличие у исполнителя действующей 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 отнесённой к государственным секретам).

8. Обеспечение конфиденциальности

8.1. Исполнитель должен гарантировать сохранение конфиденциальности документации, параметров настройки сетевого оборудования, средств защиты информации, исходных кодов компьютерных программ, персональных данных и иных сведений, которые не являются общедоступными, полученных от заказчика в рамках выполнения работ.

8.2. Исполнитель должен принять все необходимые меры для того, чтобы предотвратить полное или частичное разглашение информации или ознакомление с ней третьих лиц без письменного согласия заказчика.

9. Дополнительные условия

9.1. Расходы на приобретение дополнительного оборудования и программного обеспечения, необходимого для устранения замечаний регулятора, несёт заказчик.

Ориентировочная стоимость закупки: 15 000,00 бел. руб.

Способ закупки: проведение процедуры запроса ценовых предложений.

Ответственное лицо за рассмотрение предложений: ведущий системный администратор А.М. Артюшевский, тел. +375 (25) 540-41-07.

Ведущий системный администратор

А.М. Артюшевский