

Технические требования
на проектирование, создание и аттестацию системы защиты информации проектируемой информационной системы медико-санитарной части открытого акционерного общества «БЕЛАЗ» – управляющая компания холдинга «БЕЛАЗ-ХОЛДИНГ» (далее – МСЧ ОАО «БЕЛАЗ»)

1. Предмет закупки: выполнение комплекса работ по проектированию, созданию и аттестации системы защиты информации (далее – СЗИ) информационной системы МСЧ ОАО «БЕЛАЗ» в соответствии с требованиями законодательства.

МСЧ ОАО «БЕЛАЗ» включает:

АРМ – 200 шт.;

физических серверов – 2 шт.;

виртуальных серверов – 10 шт.;

количество эксплуатируемых информационных систем – 1 шт.;

2. Источник финансирования: собственные средства.

3. Требования к участникам: участником конкурса может быть любое юридическое лицо, имеющее:

– лицензию 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);

– сертифицированную систему менеджмента качества в соответствии с требованиями СТБ ISO 9001 применительно к проектированию, созданию и аттестации систем защиты информации информационных систем (без привлечения 3 лиц);

– сертифицированную систему менеджмента информационной безопасности в соответствии с требованиями СТБ ISO 27001 применительно к проектированию, созданию и аттестации систем защиты информации информационных систем;

– документально подтвержденный опыт реализации не менее трех проектов по проектированию, созданию и аттестации систем защиты информации в течение последних трех лет (на дату проведения закупки).

Не допускаются к процедуре закупки юридические лица:

– включенные в реестр поставщиков (подрядчиков, исполнителей), временно не допускаемых к закупкам;

- находящихся в процессе ликвидации (прекращения деятельности), реорганизации или признанных в установленном законодательными актами порядке экономически несостоятельными (банкротами), за исключением находящихся в процедуре санации;

- не представивших либо представивших неполную (неточную) информацию о себе и отказавшихся представить соответствующую информацию в приемлемые для ОАО «БЕЛАЗ» сроки;

- не соответствующих требованиям к квалификационным данным, установленным в настоящей процедуре запроса ценового предложения.

4. Перечень выполняемых работ.

Проектирование, создание и аттестация СЗИ МСЧ ОАО «БЕЛАЗ» включает следующие работы:

Обследование МСЧ ОАО «БЕЛАЗ»;

- Разработка технического задания на создание СЗИ МСЧ ОАО «БЕЛАЗ» (далее – техническое задание);

- Выбор средств технической и криптографической защиты информации, удовлетворяющих требованиям технического задания;

- Разработка общей схемы СЗИ МСЧ ОАО «БЕЛАЗ»;

- Разработка спецификации средств технической и криптографической защиты информации;

- Создание СЗИ МСЧ ОАО «БЕЛАЗ»;

- Аттестация СЗИ МСЧ ОАО «БЕЛАЗ».

5. Требования к качеству, техническим характеристикам работ:

5.1 Требования к выполнению работ по проектированию СЗИ МСЧ ОАО «БЕЛАЗ».

- Работы по обследованию МСЧ ОАО «БЕЛАЗ» включают:

- анализ проекта организационной структуры и ИТ-инфраструктуры МСЧ ОАО «БЕЛАЗ», определение состава, границ и мест размещения элементов информационных систем (аппаратных и программных);

- инвентаризацию активов, заложенных в проект, корпоративной ЛВС МСЧ ОАО «БЕЛАЗ»;

- оценку рисков информационной безопасности;

- анализ взаимодействия информационных систем МСЧ ОАО «БЕЛАЗ» с основной информационной системой ОАО «БЕЛАЗ» и их элементов;

- анализ информационных потоков в МСЧ ОАО «БЕЛАЗ»;

- определение и анализ физических и логических границ МСЧ ОАО «БЕЛАЗ»;

– сбор сведений и анализ соблюдения требований, в соответствии с приказом Оперативно-аналитического центра при Президенте Республики Беларусь 10 декабря 2024 г. № 259 «Об изменении приказов Оперативно-аналитического центра при Президенте Республики Беларусь от 28 марта 2014 г. № 26 и от 20 февраля 2020 г. № 66» в зависимости от классов типовых ИС (далее – Приказ 66);

- анализ следующих процессов обеспечения ИБ:
- разграничение доступа пользователей к объектам информационных систем;
- резервирование и уничтожение информации;
- защита от вредоносного программного обеспечения;
- использование съемных носителей информации;
- использование электронной почты;
- парольная политика
- обновление средств защиты информации;
- осуществление контроля (мониторинга) за функционированием информационных систем и систем защиты информации;
- реагирование на события ИБ и ликвидация их последствий;
- управление криптографическими ключами, в том числе их генерацией, распределением, хранением, доступом к ним и их уничтожению;
- обучение (повышение квалификации) пользователей ИС.

По результатам обследования должен быть разработан отчет, содержащий следующие сведения:

- рекомендации с обоснованием по отнесению МСЧ ОАО «БЕЛАЗ» к классам типовых ИС в соответствии с Положением о порядке технической и криптографической защиты информации в информационных системах, распространение и (или) предоставление которой ограничено, утвержденным Приказом № 66;
- отчет о соответствии (несоответствии) СЗИ МСЧ ОАО «БЕЛАЗ» и ЛПА ОАО «БЕЛАЗ» требованиям законодательства Республики Беларусь в области защиты информации и Приказа № 66 в зависимости от классов типовых ИС;
- предложения по совершенствованию организационной структуры обеспечения защиты информации МСЧ ОАО «БЕЛАЗ»;
- техническое задание.

Закупка и внедрение недостающих средств технической и криптографической защиты информации осуществляется ОАО «БЕЛАЗ».

5.2. Требования к выполнению работ по проведению опытной эксплуатации системы защиты информации МСЧ ОАО «БЕЛАЗ».

- Проведение опытной эксплуатации системы защиты информации, проверка работоспособности и совместимости с другими объектами информационной системы.

В процессе опытной эксплуатации информационной системы в установленном порядке осуществляются:

- контроль за соблюдением требований, установленных в нормативных правовых актах, документации на систему защиты информации собственника (владельца) информационной системы;
- контроль за порядком использования объектов информационной системы; мониторинг функционирования системы защиты информации;
- выявление угроз (анализ журналов аудита), которые могут привести к сбоям, нарушению функционирования информационной системы;
- проверка резервного копирования информации, содержащейся в информационной системе; контроль проведения обучения (повышение квалификации) пользователей информационной системы;
- проверка работоспособности и совместимости с другими объектами информационной системы на реально действующей системе защиты информации;

5.3. Работы по аттестации СЗИ МСЧ ОАО «БЕЛАЗ» включают:

- разработка программы и методики аттестации СЗИ МСЧ ОАО «БЕЛАЗ»;
- проверка правильности отнесения информационной системы к классу типовых информационных систем, выбора и применения средств защиты информации;
- установление соответствия реального состава и структуры объектов информационной системы СЗИ МСЧ ОАО «БЕЛАЗ» общей схеме СЗИ;
- анализ разработанной документации на СЗИ собственника (владельца) информационной системы на предмет ее соответствия требованиям законодательства об информации, информатизации и защите информации;
- ознакомление с документацией о распределении функций персонала Заказчика по организации и обеспечению защиты информации Заказчика;
- проведение испытаний системы защиты информации на предмет выполнения установленных законодательством требований по защите информации.
- проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения, о

которых подтверждены изготовителями (разработчиками) этих объектов информационной системы;

- оформление технического отчета и протокола испытаний;
- оформление аттестата соответствия.

5.3.1. Содержание технического отчета:

- сроки проведения испытаний;
- вывод о соответствии (несоответствии) реального состава и структуры объектов информационной системы общей схеме системы защиты информации;
- вывод о выполнении (невыполнении) установленных законодательством требований по защите информации;
- отчет о внешней и внутренней проверке отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно иницированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы.

5.3.2. Программа и методика аттестации.

Программа и методика аттестации разрабатываются на основании исходных данных и должны содержать перечень выполняемых работ, методов проверки требований безопасности, реализованных в системе защиты информации, используемой контрольной аппаратуры и тестовых средств, а также информацию о продолжительности их выполнения.

Программа и методика аттестации разрабатываются исполнителем и согласовывается с заказчиком.

5.3.3. Срок проведения аттестации.

Срок аттестации не может превышать 180 (ста восьмидесяти) календарных дней. В случае выявления в процессе проведения аттестации недостатков исполнитель приостанавливает выполнение работ по договору до устранения недостатков заказчиком.

При подтверждении соответствия системы защиты информации требованиям законодательства об информации, информатизации и защите информации оформляется аттестат соответствующей формы, согласно действующего законодательства.

5.3.4. Аттестат соответствия оформляется сроком на 5 (пять) лет.

6. Требования к отчетной документации

Отчетные документы должны быть представлены в одном экземпляре на бумажном носителе и в одном экземпляре в электронном виде. Электронное представление документов должно соответствовать формату редакторов Microsoft Word.

Исполнитель должен нести ответственность за результаты выполненных работ по комплексной оценке системы защиты информации в реальных условиях эксплуатации информационной системы и гарантировать, что система защиты информации ОАО «БЕЛАЗ» будет соответствовать требованиям законодательства об информации, информатизации и защиты информации на момент составления технического отчета и протокола испытаний в соответствии с договором.

7. Место, условия, сроки выполнения работ, общие сведения: работы проводятся удаленно и на площадках МСЧ ОАО «БЕЛАЗ», расположенных по адресу: Республика Беларусь, Минская обл., г. Жодино, ул. Брестская, 6.

Работы выполняются поэтапно.

8. Форма, сроки и порядок оплаты выполненных работ: оплата осуществляется частями согласно договору в течение 10 (десяти) банковских дней после подписания сторонами акта сдачи-приемки выполненных работ по каждому из этапов.

9. Порядок формирования суммы договора на закупку: стоимость комплекса работ должна включать в себя расходы на транспортировку, страхование, уплату таможенных пошлин, налогов, сборов и других обязательных платежей. Все указанные расходы должны быть отражены в конкурсном предложении участника.

Стоимость предлагаемых работ должна быть неизменна в течение срока действия заключенного по итогам конкурса договора.

10. Критерии оценки предложений: наиболее низкая стоимость, соответствие квалификационным требованиям.

11. Требования к квалификационным данным участников: квалификационными данными участников являются их правоспособность и техническая компетентность.

В подтверждение своих данных участник должен предоставить следующие документы:

копию свидетельства о государственной регистрации;

копию учредительных документов со всеми изменениями и дополнениями, зарегистрированными в установленном порядке (для юридических лиц), копию выписки из торгового регистра страны учреждения нерезидента или иное эквивалентное доказательство юридического статуса в соответствии с законодательством страны его учреждения (для нерезидентов Республики Беларусь);

копию специального разрешения (лицензии), действующего в период выполнения работ, на деятельность по технической и (или) криптографической защите информации в части соответствующих

составляющих данный вид деятельности работ, в соответствии с Приказом № 66;

копию сертификата системы менеджмента качества в соответствии с требованиями СТБ ISO 9001;

копию сертификата система менеджмента информационной безопасности в соответствии с требованиями СТБ ISO 27001;

письмо с указанием организаций и их отзывами о качестве выполненных работ, в которых были успешно реализованы не менее трех проектов по проектированию, созданию и аттестации систем защиты информации в течение последних трех лет.

Начальник ЦКБ



Р.Ю.Якубицкий

Заместитель генерального директора
по безопасности, режиму и кадрам

 И.В.Короткий

02.06.2026