БТК

Міністэрства сувязі і інфарматызацыі
Рэспублікі Беларусь
**Рэспубліканскае унітарнае
прадпрыемства электрасувязі
«БЕЛТЭЛЕКАМ»
(РУП «БЕЛТЭЛЕКАМ»)**
вул. Энгельса, 6, 220030, г. Мінск
тэл. (017) 217 10 06, факс (017) 327 44 22
e-mail: info@main.beltelecom.by, http://www.beltelecom.by
Р.р. BY05 AKBB3012 1002 7001 8550 0000
у ААТ «ААБ Беларусбанк» г. Мінска, код AKBBBY2X, УНП 101007741

Министерство связи и информатизации
Республики Беларусь
**Республиканское унитарное
предприятие электросвязи
«БЕЛТЕЛЕКОМ»
(РУП «БЕЛТЕЛЕКОМ»)**
ул. Энгельса, 6, 220030, г. Минск
тел. (017) 217 10 06, факс (017) 327 44 22
e-mail: info@main.beltelecom.by, http://www.beltelecom.by
Р.с. BY05 AKBB3012 1002 7001 8550 0000
в ОАО «АСБ Беларусбанк» г. Минска, код AKBBBY2X, УНП 101007741

СТБ ISO 9001

2024

03.04.26 №25-8/3080
На № _____ ад _____

Всем заинтересованным

ПРИГЛАШЕНИЕ
НА УЧАСТИЕ В ЗАКУПКЕ

по проектированию, созданию и аттестации системы защиты информации АПК «Мой Белтелеком», в том числе услуги по проектированию и созданию системы информационной безопасности критически важного объекта информатизации

Республиканское унитарное предприятие электросвязи «Белтелеком» (далее по тексту именуемое «Заказчик») приняло решение о закупке услуги по проектированию, созданию и аттестации системы защиты информации АПК «Мой Белтелеком», в том числе услуги по проектированию и созданию системы информационной безопасности критически важного объекта информатизации (далее – Услуга) и приглашает заинтересованные организации (далее – Участники) принять участие в процедуре оформления конкурентного листа и подготовить соответствующим образом оформленное коммерческое предложение на поставку.

Требования к Услуге указаны в Приложении 1.

Ориентировочная стоимость закупки – до **1 000 базовых величин (44 900,00 BYN)**.

Критерием оценки предложений является:

- цена предложения – **100%,** при условии полного соответствия требованиям закупки.

Предложение в обязательном порядке должно содержать / соответствовать:

1. Наименование, юридический и почтовый адрес, банковские реквизиты участника.
2. Стоимость, которая должна быть выражена в **белорусских рублях**, и дана с учётом таможенных пошлин, налогов на импорт, других налогов и сборов, применяемых в Республике Беларусь.
3. Техническое описание предлагаемой Услуги.
4. Место выполнения работ (предоставления услуги): г.Минск, ул.Захарова,55.
5. Наличие специального разрешения (лицензии) на проектирование и создание систем информационной безопасности критически важных объектов информатизации.
6. Наличие специального разрешения (лицензии) на проектирование,

создание, аттестацию систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесённой к государственным секретам.

7. Предоставление гарантийных обязательств о корректировке сведений в предоставляемом комплекте документации на период 18 (восемнадцать) месяцев с момента подписания Акта выполненных работ.

8. Внесение изменений и дополнений в комплект документации, в период гарантийных обязательств, в случае такой необходимости (по результатам опытной и иной эксплуатации системы защиты информации).

9. Условия оплаты – 100% по факту подписания Акта выполненных работ (оказанных услуг) в течение 30 (тридцати) календарных дней с оплатой в белорусских рублях.

10. Срок реализации проекта: 140 календарных дней.

11. Срок действия Предложений должен составлять **30** (тридцать) календарных дней с Даты подачи Предложений.

12. С учетом вышесказанного, Предложение должно быть подано не позднее **12:00** 10 **апреля 2026 года** в запечатанном конверте, в виде, позволяющем установить достоверность доставки к назначенному сроку по адресу: г.Минск, ул.Энгельса,6 РУП «Белтелеком», Отдел конкурсных закупок Служба материально-технического обеспечения, с пометкой:

"Предложение на закупку услуги по проектированию, созданию и аттестации системы защиты информации АПК «Мой Белтелеком», в том числе услуги по проектированию и созданию системы информационной безопасности критически важного объекта информатизации
не вскрывать до 12:00 «10» апреля 2026 года
От: наименование Участника"

Все, что не предусмотрено настоящим письмом, регламентируется Положением о порядке выбора поставщика (подрядчика, исполнителя) при осуществлении закупок товаров (работ, услуг) за счет собственных средств РУП «Белтелеком», утвержденного приказом РУП «Белтелеком» от 20.06.2022 №512 и Гражданским кодексом Республики Беларусь.

Заказчик оставляет за собой право на прекращение всего процесса процедуры закупки на любой его стадии. В случае реализации данного права, Заказчик не несет никакой ответственности перед Участником за причинённые действия.

Дополнительная информация может быть получена:
Габрусёнок Татьяна Александровна, тел. (017) 217 1184, Лопатко Павел Сергеевич (017) 217 11 24 (по техническим вопросам);
Стельмах Яна Дмитриевна, тел. (017) 217 1403, факс (017) 217 1494 (по процедурным вопросам).

Заместитель Генерального директора
по техническим вопросам
РУП «Белтелеком» А.Р.Жаркевич

25-2 Стельмах 217 1403

Приложение 1

Требования к проектированию,
созданию и аттестации системы защиты информации
АПК «Мой Белтелеком», в том числе СИБ КВОИ

1. Назначение информационной системы.

АПК «Мой Белтелеком» РУП «Белтелеком» – это интернет-ресурс, предоставляющий пользователям возможность удалённого самообслуживания, подключения, изменения услуг и информационно-справочной информации из различных информационных систем РУП «Белтелеком», на основе единообразного доступа, тем самым минимизируя необходимость клиенту посещать офисы продаж РУП «Белтелеком». Основной задачей АПК «Мой Белтелеком» является обеспечение работоспособности пользовательских приложений web, Android и iOS версий, которое позволяет:

- управлять услугами (подключение и отключение услуг, смена тарифного плана, подключение дополнительных услуг, просмотр статистики пользования);
- проводить оплаты за оказанные услуги;
- оказывать техническую поддержку (звонок в службу поддержки, онлайн-чат со специалистом службы поддержки);
- предоставлять последние новости РУП «Белетелеком», сообщения о работах на сетях, акционные предложения.

АПК «Мой Белтелеком» отнесён к КВОИ и классам типовых информационных систем: 3-ин; 3-юл. На основании вышеуказанного в техническом задании должны быть определены требования, предъявляемые к системе защиты информации, в том числе СИБ КВОИ, в соответствии Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 (в ред. от 10.12.2024 № 259).

2. Технические требования должны быть разработаны с учётом следующих нормативных правовых актов:

Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»(в ред. от 10.10.2022 № 209-З);

Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 (в ред. от 22.06.2023 № 178) «О некоторых мерах по совершенствованию защиты информации»;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 (в ред. от 10.12.2024 № 259);

Постановление Совета Министров Республики Беларусь от 12 августа 2014 № 783 «О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну»;

Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утверждённый постановлением Совета Министров

Республики Беларусь от 15.05.2013 № 375 (в ред. от 12.03.2020 №145).

3. В рамках проектирования Системы защиты информации Исполнитель должен осуществить:

3.1. Обследование объекта информационной инфраструктуры (далее – ОИИ) – АПК «Мой Белтелеком»;

3.2. Разработку (корректировку) политики информационной безопасности;

3.3. Разработку структурной и логической схем информационной системы;

3.4. Разработку технического задания на создание системы защиты информации;

3.5. Разработку проектов локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации.

4. В процессе обследования ОИИ (АПК «Мой Белтелеком») Исполнитель должен обеспечить:

4.1. Обследование АПК «Мой Белтелеком». Основанием для проведения обследования является заключённое Соглашение о конфиденциальности. Результаты обследования оформляются документально;

4.2. Анализ состава и структуры комплекса технических средств и программного обеспечения АПК «Мой Белтелеком», информационных потоков, технологического оборудования и существующих средств защиты информации (далее – СрЗИ), рассмотреть возможность и целесообразность использования существующих СрЗИ;

4.3. Подготовку предложений по сегментации АПК «Мой Белтелеком», с возможностью межсегментного взаимодействия через СрЗИ и, при необходимости, средства криптографической защиты информации (далее – СКЗИ);

4.4. Анализ локальных актов предприятия, определяющих порядок функционирования АПК «Мой Белтелеком», работу пользователей с АПК «Мой Белтелеком» и порядок применения пользователями СрЗИ.

5. При разработке технического задания на создание системы защиты информации Исполнитель должен выполнить следующие требования:

5.1. Разработать техническое задание на создание системы защиты информации, которое должно содержать:

5.1.1. Наименование информационной системы с указанием присвоенных ей классов типовых информационных систем, рассмотреть корректность действующего акта отнесения;

5.1.2. Требования к системе защиты информации в зависимости от используемых технологий и классов типовых информационных систем на основе действующих нормативных правовых актов Республики Беларусь;

5.1.3. Требования к средствам технической и криптографической защиты информации на основе перечня государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность»

(ТР 2013/027/BY), утверждённым постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375;

5.1.4. В случае необходимости приобретения (обновления) оборудования и (или) программного обеспечения для реализации системы защиты информации – разработать Перечни оборудования (средства вычислительной техники, сетевого оборудования, СрЗИ), а также системного и прикладного программного обеспечения для нужд сегментации и последующей аттестации СЗИ АПК «Мой Белтелеком» с указанием основных технических характеристик (для оборудования) и назначения/основных функций (для программного обеспечения). Указанные перечни включаются в ТЗ и оформляются в виде таблиц (таблица 1 и таблица 2);

Таблица 1 – Перечень оборудования

№ п/п	Наименование/тип оборудования	Основные технические характеристики	Количество единиц	Предлагаемый производитель, модель
1	2	3	4	5

Таблица 2 – Перечень системного и прикладного программного обеспечения

№ п/п	Наименование ПО (системное/ прикладное)	Назначение/основные функции	Количество единиц (лицензий)	Предлагаемый производитель, продукт
1	2	3	4	5

5.1.5. Описание распределения функций, обязанностей и ответственности по общему руководству информационной безопасностью, технической эксплуатации, обслуживанию, администрированию и мониторингу информационной системы и системы защиты информации между должностями (подразделениями) с указанием ролей и рекомендуемого количества специалистов по каждой роли, определяемого Исполнителем исходя из объемов работ по обеспечению выполнения выше указанных функций и периодичности их выполнения, а также с учетом необходимости исключения конфликта интересов (разделение функций администрирования, эксплуатации, контроля и оценки эффективности СЗИ между различными должностями/подразделениями). Для оформления указанной информации в ТЗ должна быть предусмотрена таблица 3;

Таблица 3 – Распределение функций между специалистами

№ п/п	Должность (роль) специалиста	Перечень выполняемых работ/функций	Периодичность выполнения работ/функций
1	2	3	

5.2. Исполнитель обязан предусмотреть:

5.2.1. Наличие файрвола веб-приложений (WAF);

5.2.2. Наличие на сетевом оборудовании функционала Port security;

5.2.3. Использование при организации удалённого доступа пользователей к СрЗИ двухфакторной авторизации;

5.2.4. Использование механизма AAA;

5.2.5. Резервирование средств защиты;

5.2.6. Использование СрЗИ, имеющих подтверждение соответствия требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY);

5.2.7. Размещение используемого в АПК «Мой Белтелеком» оборудования на территории Республики Беларусь;

5.2.8. Предоставление доступа к настройкам СрЗИ (межсетевого экранирования, активного сетевого оборудования, антивирусного программного обеспечения и др.) специалистам Заказчика согласно Таблице 3;

6. При создании системы защиты информации Исполнитель должен выполнить следующие работы:

6.1. Внедрение средств защиты информации, проверка их работоспособности и совместимости с активами информационной системы (осуществляется совместно с Заказчиком);

6.2. Корректировка (при необходимости) разработанных на этапе проектирования системы защиты информации структурной и логической схем информационной системы;

6.3. Корректировка (при необходимости) разработанных на этапе проектирования системы защиты информации проектов локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации.

7. При аттестации системы защиты информации Исполнитель должен выполнить следующие работы:

7.1. Разработка программы аттестации;

7.2. Разработка методики аттестации;

7.3. Проверка правильности отнесения информационной системы к классу (классам) типовых информационных систем;

7.4. Установление соответствия фактического состава активов информационной системы структурной и логической схемам информационной системы;

7.5. Проверка достаточности реализованных в системе защиты информации мер по защите информации;

7.6. Анализ локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации на предмет их соответствия требованиям законодательства об информации, информатизации и защите информации;

7.7. Проведение испытаний системы защиты информации на предмет выполнения установленных законодательством требований по защите информации;

7.8. Внешняя и внутренняя проверка отсутствия либо невозможности использования нарушителем свойств активов информационной системы, 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 информационной системы, средств защиты информации;

7.9. Оформление технического отчета;

7.10. Оформление протокола испытаний;

7.11. Оформление аттестата соответствия (в случае положительного результата проведения испытаний системы защиты информации, в противном случае – отказ в выдаче аттестата соответствия).

8. При проектировании СИБ КВОИ Исполнитель должен выполнить следующие работы:

8.1. Определение внутренних (организационная структура, информационные системы, информационные потоки и процессы) и внешних (взаимосвязи с контрагентами и другое) границ, оказывающих влияние на обеспечение информационной безопасности критически важного объекта информатизации;

8.2. Определение целей обеспечения информационной безопасности критически важного объекта информатизации, совместимых с процессами деятельности владельца критически важного объекта информатизации и прогнозными документами организации (осуществляется Заказчиком);

8.3. Инвентаризация (выявление и учёт), а также определение степени важности для основной деятельности критически важного объекта информатизации (исходя из конфиденциальности, целостности и доступности) следующих активов критически важного объекта информатизации: программно-аппаратных средств и физических устройств; программного обеспечения (прикладного и системного); СрЗИ; информационных систем и информационных сетей; средств обработки информации (потоков информации), средств коммуникации, администрирования и конфигурирования;

8.4. Определение физических и логических границ области применения системы информационной безопасности (формуляр критически важного объекта информатизации) с использованием структурной и логической схем критически важного объекта информатизации. При этом структурная схема должна содержать расположение физических устройств с номерами портов, а также физических линий связи, соединяющих физические интерфейсы технических, программно-аппаратных средств обработки информации, средств защиты информации, автоматизированных рабочих мест администратора (оператора). В логической схеме должны быть отображены информационные системы, направления потоков данных, а также спецификация используемых технологий и протоколов, списки VLAN, IP-адреса устройств;

8.5. Определение угроз информационной безопасности критически

важного объекта информатизации;

8.6. Разработка либо корректировка методологии (методики) оценки рисков информационной безопасности критически важного объекта информатизации и оценка таких рисков;

8.7. Определение требований к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, по обеспечению информационной безопасности критически важного объекта информатизации, блокированию (нейтрализации) угроз информационной безопасности критически важного объекта информатизации;

8.8. Определение средств управления, необходимых для реализации выбранного варианта обработки рисков информационной безопасности критически важного объекта информатизации (план обработки рисков).

9. При создании СИБ КВОИ Исполнитель должен выполнить следующие работы:

9.1. Разработка политики информационной безопасности критически важного объекта информатизации;

9.2. Разработка локальных правовых актов, содержащих следующие инструкции и регламенты:

9.2.1. идентификация и аутентификация:

– определение политик и процедур идентификации и аутентификации;

– идентификация и аутентификация пользователей и инициируемых ими процессов;

– инвентаризация и контроль за активами критически важного объекта информатизации;

9.2.2. управление доступом к активам критически важного объекта информатизации:

– определение политик и процедур управления доступом;

– разделение прав доступа пользователей;

– управление учётными записями и паролями пользователей;

– управление привилегированными правами доступа;

– ограничение неуспешных попыток доступа к активам критически важного объекта информатизации;

– оповещение пользователя при входе о предыдущем доступе к активам критически важного объекта информатизации;

– ограничение числа параллельных сеансов доступа;

– блокирование сеанса доступа пользователя при неактивности;

– ограничение защищенного удаленного доступа к активам критически важного объекта информатизации;

– контроль доступа из внешних информационных (автоматизированных) систем;

– использование выделенного автоматизированного рабочего места для администрирования, требующего привилегированного доступа, не имеющего доступа к внешним информационным сетям;

–управление запуском, установкой (инсталляцией) компонентов программного обеспечения (приложений);

9.2.3. обращение с носителями информации:

– определение политик и процедур обращения со съемными носителями информации;

– учет съемных носителей информации;

– управление физическим доступом к съемным носителям информации;

– контроль за перемещением контролируемой зоны;

– съемных носителей информации за пределы ограничение ввода (вывода) информации на периферийные устройства, в том числе съемные носители информации;

– регистрация и контроль за подключением съемных носителей информации;

– уничтожение (удаление) информации со съемных носителей информации;

9.2.4. аудит информационной безопасности:

– определение политик и процедур аудита информационной безопасности;

– поиск уязвимостей активов критически важного объекта информатизации и их устранение;

– генерирование временных меток и (или) синхронизация системного времени;

– защита информации о событиях информационной безопасности;

– аудит информации о действиях пользователей;

– регистрация и мониторинг событий информационной безопасности;

– хранение результатов аудита безопасности;

9.2.5. защита от вредоносного программного обеспечения:

– определение политик и процедур защиты от вредоносного программного обеспечения;

– реализация защиты от вредоносного программного обеспечения;

– обновление механизмов сканирования и базы данных сигнатур вредоносного программного обеспечения;

– регистрация событий обнаружения вредоносных программ;

9.2.6. управление процедурами резервирования:

– определение политик и процедур резервирования;

– резервирование программных и программно-аппаратных средств и систем;

–резервное копирование информации, программного обеспечения и обеспечение возможности восстановления из резервных копий;

– резервное копирование конфигурационных файлов и журналов аудита;

– обеспечение защиты резервных копий;

9.2.7. обеспечение информационной безопасности критически важного объекта информатизации и его элементов:

– определение политик и процедур защиты информационной (автоматизированной) системы и ее элементов;

– разделение функций по управлению активами критически важного объекта информатизации с другими функциями;

– сегментирование сети критически важного объекта информатизации;

– управление сетевыми потоками;
– использование межсетевых экранов;
– сокрытие архитектуры и конфигурации критически важного объекта информатизации;
– управление безопасной настройкой сетевых устройств (средств защиты информации);
– отключение беспроводных соединений и интерфейсов;
– исключение доступа через общие ресурсы;
– защита от угроз отказа в обслуживании;
– ограничение использования мобильных устройств;
– управление перемещением виртуальных машин и обрабатываемых на них данных;

9.2.8. управление конфигурацией:
– определение политик и процедур управления конфигурацией информационной
– (автоматизированной) системы;
– идентификация объектов управления конфигурацией;
– управление изменениями конфигурации;
–установка (инсталляция) только разрешенного к использованию программного обеспечения;
– контроль за действиями по изменению конфигурации;

9.2.9. обновление программного обеспечения:
– определение политик и процедур управления обновлениями программного обеспечения;
– обновление программного обеспечения из доверенного источника;

9.2.10. планирование мероприятий по обеспечению информационной безопасности критически важного объекта информатизации:
–определение политик и процедур планирования мероприятий по обеспечению информационной безопасности критически важного объекта информатизации;
– разработка, утверждение и актуализация плана мероприятий по обеспечению информационной безопасности критически важного объекта информатизации;
– контроль за выполнением мероприятий по обеспечению информационной безопасности критически важного объекта информатизации;

9.2.11. реагирование на события информационной безопасности критически важного объекта информатизации и управление ими:
– разработка плана реагирования на события информационной безопасности;
– определение периодичности проведения мероприятий по оповещению и отработке действий работников в случае реализации угроз информационной безопасности критически важного объекта информатизации в соответствии с планом реагирования;
– разработка и внедрение методологии реагирования на события информационной безопасности, обеспечивающей реагирование в сроки,

определенные эксплуатационной документацией на критически важный объект информатизации и локальными правовыми актами, в целях исключения (снижения до приемлемого уровня) вероятного ущерба;

– создание альтернативных мест хранения и обработки информации в случае возникновения событий информационной безопасности;

– анализ возникших событий информационной безопасности и принятие мер по недопущению их повторного возникновения;

9.2.12. информирование и обучение персонала:

– определение политик и процедур информирования и обучения персонала, ответственности за нарушение требований по информационной безопасности критически важного объекта информатизации;

– информирование персонала об угрозах информационной безопасности критически важного объекта информатизации, правилах безопасной работы с активами критически важного объекта информатизации.

9.3. Реализация организационных и технических мер согласно разработанным локальным правовым актам осуществляется Заказчиком (Исполнитель оказывает техническую поддержку при реализации организационных и технических мер).

10. Техническое задание на создание системы защиты информации должно быть разработано Исполнителем и утверждено уполномоченным лицом Заказчика.

11. Исполнитель обязан осуществить разработку (корректировку) всех документов, необходимых для проектирования, создания и аттестации СЗИ ИС Заказчика, а также для проектирования, создания и аудита СИБ КВОИ.

12. В случае обнаружения (выявления) недостатков в утверждённом проекте и комплекте документации СЗИ, после даты подписания Акта выполненных работ, Исполнитель в течение 18 (восемнадцати) месяцев за свой счёт обеспечивает внесение изменений и дополнений для их устранения.

13. Заказчику должны быть переданы Исполнителем два экземпляра разработанных документов на бумажном носителе и в электронном виде в формате текстового редактора Microsoft Word, схемы в формате Microsoft Visio и .drawio.

14. Требования к сдаче-приемке работ:

14.1. По окончании выполнения работ по каждому этапу должен быть предоставлен акт сдачи-приёмки выполненных работ (далее – Акт), а также по окончании выполнения всего комплекса работ – Акт, на основании которого будет произведена оплата.

Заказчик в течение 5 (пяти) рабочих дней после получения Акта по соответствующему этапу должен осуществить приёмку выполненных работ и подписать Акт либо предоставить мотивированный отказ от его подписания.