**Техническое задание**

**на выполнение работ по разработке новых модулей для программного обеспечения «Интеграционная шина» для нужд АО «ЭнергосбыТ Плюс»**

1. **ОБЩИЕ ПОЛОЖЕНИЯ**

* 1. Требуется выполнить работы по разработке, тестированию и запуску в эксплуатацию отдельных модулей системы «Интеграционная шина» АО «ЭнергосбыТ Плюс».
  2. Место выполнения работ: работы выполняются дистанционно посредством предоставления удаленного доступа специалистам Исполнителя к средам разработки ПО Заказчика.
  3. Сроки выполнения работ:

Начало выполнения работ – не позднее 5 рабочих дней с даты подписания договора.

Дата окончания выполнения работ – 12 месяцев с начала даты выполнения работ.

1. **ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ РАБОТ**

* 1. В рамках договора на выполнение работ Исполнитель должен:
* организовать координацию работ своих специалистов и специалистов Заказчика в части доработки интеграционного решения, используемого для интеграции существующих и вновь внедряемых Информационных систем Заказчика;
* выполнить работы по анализу и детализации требований Заказчика, разработке, тестированию, документированию и вводу в эксплуатацию компонентов Интеграционного решения Заказчика с целью создания Единой Интеграционной шины, обеспечивающей интеграцию существующих и разрабатываемых Информационных систем (в том числе интеграция со СМЭВ) с требуемой надежностью и быстродействием.

Виды работ в рамках выполнения договора:

- Руководство проектом на стороне подрядчика

- Разработка программного обеспечения

- Аналитика

- Тестирование

- Автоматизированное тестирование

Перечисленные работы должны выполняться с использованием существующих интеграционных решений Заказчика, описание которых приведено в Приложении №1 к настоящему ТЗ.

2.2. **Порядок выполнения работ**:

* + 1. Работы выполняются по задачам АО «ЭнергосбыТ Плюс», направленным специалистами АО «ЭнергосбыТ Плюс» по электронной почте с доменом @esplus.ru, на электронную почту Исполнителя, а также по задачам, поставленным АО «ЭнергосбыТ Плюс» в системе постановки задач, согласованной сторонами в электронной переписке.
    2. По каждой задаче, поставленной Исполнителю Заказчиком в соответствии с п.2.2.1. Стороны предварительно согласовывают способ реализации, срок и объем трудозатрат, которые не могут быть превышены Исполнителем в рамках выполнения работ. В случае, если при уточнении задачи и выявлении дополнительных требований, Исполнитель прогнозирует превышение предварительно согласованного объема трудозатрат, превышения должно быть согласовано сторонами в порядке, описанном в п.2.2.1.

2.3. **Порядок расчета стоимости работ**: стоимость выполненных работ рассчитывается ежемесячно на основании отчета Исполнителя в формате Приложения №5 к Договору о фактически выполненных задачах, исходя из почасовых расценок на работы привлеченных специалистов Исполнителя и фактического количества часов, затраченных на выполнение работ, предварительно согласованных сторонами по каждой задаче. Оплате подлежат только трудозатраты Исполнителя, потраченные на работы по задачам Заказчика, без учета времени простоя.

Задача считается выполненной при следующих условиях:

* + - * Разработка выполнена в полном объеме и оформлена в соответствии с правилами, принятыми у Заказчика
      * Успешно пройдено тестирование
      * Заказчику передан полный объем документации по разработке

1. **ТРЕБОВАНИЯ ПО СРОКАМ И ОБЪЕМАМ ПРЕДОСТАВЛЕНИЯ ГАРАНТИЙ КАЧЕСТВА ВЫПОЛНЕННЫХ РАБОТ**

**Срок предоставления гарантий качества**

Срок предоставления гарантии качества 1 (один) год с даты подписания сторонами Акта сдачи-приемки выполненных работ (в отношении тех доработок, которые закрываются данным Актом сдачи-приемки выполненных работ).

В течение данного периода Исполнитель должен выполнять работы по устранению выявляемых технических ошибок в отношении последних предоставленных Заказчику результатов выполненных работ по доработке модулей системы.

В случае, если в рамках развития модулей "Интеграционной шины", Заказчиком или иной организацией были внесены изменения в результаты выполненных работ Исполнителя по Заявкам на доработку, то такие результаты выполненных работ Исполнителя подпадают под гарантийную поддержку в соответствии с настоящим Техническим заданием только в случае, если Заказчик воспроизводит ошибку в изначальных результатах выполненных работ Исполнителя.

1. **ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ**

Полные требования к информационной безопасности к исполнителю при осуществлении удаленного доступа к инфраструктуре заказчика указаны в приложении №2 к настоящему Техническому заданию.

**Приложения к Техническому заданию:**

Приложение№1 Описание интеграционного решения / Описание инфраструктуры;

Приложение№2 Требования по информационной безопасности.

Приложение №1 к Техническому заданию

1. **Описание интеграционного решения**

* 1. Интеграционное решение построено по микросервисной архитектуре (>150 сервисов).
  2. Стек технологий:
     1. Java Spring Boot;
     2. Apache Camel;
     3. брокер сообщений RabbitMQ;
     4. СУБД PostgreSQL, Tarantool;
     5. Кластер kubernetes.
  3. Используемые версии Java 8, 11, 17.
  4. С внешними системами сервисы взаимодействуют посредством AMQP, SOAP, REST API, а также через прямое подключение к БД в ряде случаев.

1. **Описание инфраструктуры**
   1. Репозитарий – GitLab
   2. Хранение артефактов – Nexus
   3. Процессы CI/CD – Jenkins
   4. Логирование – ELK
   5. Мониторинг – Prometheus + Grafana

Приложение №2 к Техническому заданию

**ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

в части предоставления удаленного доступа третьим лицам, не являющихся работниками Общества (юридические лица, индивидуальные предприниматели, исполнители по договорам ГПХ, в том числе физические лица – плательщики НПД (самозанятые)), выполняющих работу и (или) оказывающих услуги по заказу Общества

1. **Термины и определения**
   1. Исполнитель, третье лицо – лицо, не являющееся работником Общества (юридические лица, индивидуальные предприниматели, исполнители по договорам ГПХ, в том числе физические лица – плательщики НПД (самозанятые)), выполняющее работу и (или) оказывающее услуги по заказу Общества.
   2. Заказчик, Общество - юридическое лицо, входящее в Группу компаний «Т Плюс».
2. **Нормативная база**
   1. Федеральный закон Российской Федерации от 29.07.2004 N 98-ФЗ "О коммерческой тайне".
   2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
   3. Федеральный закон Российской Федерации Ф от 27.07.2006 N 152-ФЗ "О персональных данных".
   4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
   5. Постановление Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
   6. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
   7. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
   8. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности ЗОКИИ».
3. **Общие требования**
   1. Исполнитель при необходимости подключения собственного оборудования к ИТ-инфраструктуре Заказчика обязан предварительно в письменной форме согласовать такое подключение с Заказчиком и соблюсти требования по защите подключаемого оборудования не ниже 3 уровня защищённости персональных данных при их обработке в информационной системе в соответствии с приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
   2. Исполнитель для подключения собственного оборудования к сети Заказчика обязан:
      1. Предоставить аттестат соответствия требованиям защиты информации не ниже 3 уровня защищённости персональных данных при их обработке в информационной системе на подключаемое оборудование, за исключением случаев, когда Исполнителю не требуются административные полномочия на доступ к информационным системам, приложениям и сервисам, а также к любым компонентам устройств в инфраструктуре Заказчика.
      2. Заключить соглашение о неразглашении информации (NDA) для выполнения работ в режиме удаленного доступа.
      3. Направить Заказчику заявку в установленной форме (п 4.4) с перечнем лиц, для которых необходимо предоставить удаленный доступ.
   3. Для выполнения работ Исполнителем в режиме удаленного доступа договор с Исполнителем должен содержать:

оговорку о дистанционном характере выполнения работ;

соглашение о полном соответствии настоящим Требованиям для подключения персонала Исполнителя к ИТ-инфраструктуре Общества.

* 1. Все сведения о составе и характеристиках объектов Заказчика и их компонентах являются конфиденциальной информацией и распространению не подлежат в период действия договорных отношений и после прекращения договорных отношений в течение 10 лет (в случае, если иное не предусмотрено договором).
  2. Исполнитель обязуется:

не проводить противозаконные действия (не ограничиваясь указанным: фальсификация, модификация, блокировка, уничтожение или искажение) по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся у Заказчика;

не осуществлять несанкционированный доступ к информационным ресурсам Заказчика;

не проводить незаконное копирование информации, циркулирующей или хранящейся у Заказчика;

не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;

не внедрять в объекты Заказчика программы-вирусы (загрузочные, файловые и др.);

не устанавливать программные и аппаратные закладные устройства в технические средства Заказчика;

не распространять конфиденциальную информацию о выполняемых работах и полученных результатах;

использовать решения для удаленного доступа, определенные Заказчиком;

использовать удаленный доступ только в целях исполнения договорных обязанностей между Исполнителем и Заказчиком.

* 1. Авторизация работника Исполнителя должна осуществляться под персональными учетными записями, выданными Заказчиком. Использование чужих учетных записей, выданных другим работникам, не допускается.
  2. Работник Исполнителя должен принимать меры по защите предоставленных Заказчиком учетных данных и не допускать неавторизованного доступа других лиц к информационным ресурсам Заказчика.
  3. Исполнитель осуществляет дистанционное подключение к ресурсам Заказчика только с использованием статического IP адреса, согласованного с Заказчиком. Доступ с неизвестных Заказчику IP адресов может блокироваться техническими средствами Заказчика.
  4. Исполнитель обеспечивает выполнение условия, что все ресурсы, с которых осуществляется удаленное подключение, в том числе АРМ пользователя и другие технические средства и информационные сервисы, географически размещены на территории Российской Федерации.
  5. Запрещается подключение работников Исполнителя к ресурсам Заказчика с IP-адресов, расположенных за пределами РФ, (в том числе с использованием VPN-провайдеров, узлов TOR и подсетей хостинговых компаний (VPS/VDS), расположенных на территории РФ).
  6. При осуществлении удаленного подключения персонала Исполнителя к объектам информационной или технологической инфраструктуры Заказчика посредством не принадлежащего Заказчику компьютера или иного средства вычислительной техники (ноутбук, мобильное устройство, далее - Оборудование), если это предусмотрено Техническим заданием на работы, такое оборудование должно соответствовать следующим требованиям:

на Оборудовании должно быть установлено лицензионное общесистемное программное обеспечение, находящееся на поддержке производителя, с установленными актуальными обновлениями, включая обновления безопасности;

на Оборудовании должно быть установлено и функционировать сертифицированное средство антивирусной защиты, включённое в Единый реестр российских программ для ЭВМ и БД, с актуальными антивирусными базами (дата обновления не старше одного дня);

отчет о полной проверке средством антивирусной защиты текущего состояния Оборудования (дата отчета не старше двух дней) не должен содержать событий выявления ВПО или иных событий безопасности.

* 1. Удаленный доступ пользователей к информационным и/или технологическим ресурсам Заказчика, являющихся значимыми объектами критической информационной инфраструктуры (далее - ЗОКИИ), запрещен. В случае необходимости проведения работ на ЗОКИИ, подключение сторонних пользователей к таким объектам и их компонентам допускается только локально (очно) на территории площадок Заказчика.
  2. Исполнитель самостоятельно осуществляет выбор провайдера услуг Интернет, координацию установки оборудования и программного обеспечения, оплату соответствующих тарифов.
  3. Настройка и сопровождение оборудования, с которого осуществляется удалённый доступ к ресурсам Заказчика, а также установленного на оборудовании программного обеспечения, осуществляется Исполнителем.
  4. Запрещается использовать систему удаленного доступа для организации перманентного подключения сторонних сетей, в том числе локальных сетей Исполнителя.
  5. Заказчик с целью защиты своей ИТ-инфраструктуры, репутации и инвестиций, оставляет за собой право принимать любые меры контроля соблюдения Исполнителями настоящих требований по обеспечению необходимого уровня информационной безопасности. Отчет о соответствии указанным в пункте 3.11. требованиям может быть запрошен специалистами, ответственными за обеспечение информационной безопасности в Обществе, в любое время, а также при осуществлении оперативных мероприятий и расследовании инцидентов ИБ.
  6. Заказчик осуществляет контроль использования удаленного доступа к собственной инфраструктуре и может без предупреждения ограничить удаленный доступ в случае выявления нарушений настоящих требований.
  7. В случае компрометации, либо подозрения на компрометацию учетной записи или оборудования Исполнителя, Исполнитель обязан уведомить об этом инциденте Заказчика в кратчайший срок (не более 8 часов) с момента установления такого события.

1. **Порядок оформления**
   1. Нарушение настоящих требований со стороны Исполнителя может влечь за собой в отношении Исполнителя административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации.
   2. Доступ работникам Исполнителя к объектам Заказчика предоставляется при условии выполнения настоящих требований, а также в соответствии с требованиями законодательства РФ.
   3. Доступ предоставляется, только определенному кругу лиц и устройств, которым разрешен удалённый доступ к программным и программно-аппаратным средствам объекта Заказчика.
   4. Форма предоставления сведений о перечне лиц и устройств Исполнителя, которым должен быть предоставлен удалённый доступ к программным и программно-аппаратным средствам:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | ФИО персонала Исполнителя | Статические IP-адреса, с которых будет осуществляться подключение (удаленного устройства). | MAC-адрес устройства, с которого будет осуществляться подключение (удаленного устройства). | Контактные данные (мобильный телефон и электронная почта). | Отметка (подпись и дата) об ознакомлении с мерами безопасности, об ознакомлении с ответственностью, о согласии на обработку персональных данных. | Адрес расположения устройства |
| *1.*  *…* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно  для  заполнения)* | *(Обязательно для заполнения)* |

* 1. Оригиналы заявок на предоставление доступа направляются Исполнителем в печатном и электронном виде Заказчику в рабочее время Заказчика. Заказчик рассматривает заявки в течение 5 рабочих дней со следующего рабочего дня после получения Заказчиком заявки на предоставление удаленного доступа. После рассмотрения заявки Заказчик в течение 3 рабочих дней направляет Исполнителю информацию о рассмотрении заявки.

1. **Порядок надзора за исполнением требований безопасности.** 
   1. Исполнитель обязан в полном объеме и определённые Заказчиком сроки выполнить все требования, направленные на выполнение Исполнителем мероприятий по обеспечению необходимого Заказчику уровня защиты информации. Под необходимыми требованиями понимаются требования, указанные в настоящем документе.
   2. Заказчик для контроля исполнения требований по защите информации имеет право:

использовать имеющиеся у Заказчика средства контроля утечки конфиденциальной информации;

использовать имеющиеся у Заказчика средства контроля действий пользователей;

осуществлять контроль соблюдения Исполнителем требований по защите информации, в т.ч. требовать от Исполнителя предоставить используемую Исполнителем технику для проверки функционирования средств защиты информации в рамках действующих договорных отношений между Заказчиком и Исполнителем.

* 1. Заказчик имеет право в одностороннем порядке приостановить или прекратить предоставление удаленного доступа Исполнителю, а Исполнитель обязан выполнить связанные с этим решением мероприятия в сроки, обозначенные Заказчиком.
  2. Основания для непредоставления, приостановки или прекращения предоставления удаленного доступа:

не предоставление Заказчику оригинала заявки, заполненной надлежащим образом;

не исполнение (в т.ч. нарушение) со стороны Исполнителя требований Заказчика по защите информации, принадлежащей Заказчику, к которой Исполнитель получил доступ и которую он обрабатывал в рамках исполнения договорных отношений с Заказчиком;

прекращение договорных отношений между сторонами;

предписание федерального органа исполнительной власти Российской Федерации, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения, ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности информации Российской Федерации.