*Приложение 1 к закупочной процедуре*

**Техническое задание**

**на оказание услуг по сопровождению информационной системы «ЕКС»   
на платформе 1С:Предприятие 8 для нужд АО «ЭнергосбыТ Плюс»**

**Перечень терминов, сокращений и обозначений**

Используемые в настоящем документе сокращения, определения и основные понятия области автоматизированных систем определены в ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения». Также в тексте настоящего документа введены специальные термины и обозначения, указанные ниже:

|  |  |
| --- | --- |
| **Термин / Сокращение** | **Определение** |
| БД | * База данных |
| ГОСТ | * Государственный стандарт |
| ПО | * Программное обеспечение |
| СУБД | * Система управления базами данных |
| ТЗ | * Техническое задание |
| СЗИ | * средство защиты информации |
| СЗИ от НСД | * средство защиты информации от несанкционированного доступа |
| СУБД | * система управления базами данных |
| ФСБ России | * Федеральная служба безопасности Российской Федерации |
| ФСТЭК России | * Федеральная служба по техническому и экспортному контролю Российской Федерации |
| Отчетный период | * Календарный месяц |

1. **ОБЩИЕ СВЕДЕНИЯ**

## Полное наименование системы – «Единая кассовая информационная система для нужд АО «ЭнергосбыТ Плюс». Условное обозначение системы – ЕКС, Система.

## Полное наименование услуг: Сопровождение и поддержка единой кассовой информационной системы для нужд АО «ЭнергосбыТ Плюс».

## Заказчиком услуг является АО «ЭнергосбыТ Плюс». Система работает в следующих регионах:

* Оренбургская область (Оренбургский филиал АО «ЭнергосбыТ Плюс»);
* Кировская область (Кировский филиал АО «ЭнергосбыТ Плюс»);
* Ивановская область (Ивановский филиал АО «ЭнергосбыТ Плюс»);
* Удмуртская республика (Удмуртский филиал АО «ЭнергосбыТ Плюс»);
* Свердловская область (Свердловский филиал АО «ЭнергосбыТ Плюс»);
* Нижегородская область (Нижегородский филиал АО «ЭнергосбыТ Плюс»);
* Владимирская область (Владимирский филиал АО «ЭнергосбыТ Плюс»).

Общее количество пользователей системы до 500, количество обслуживаемых касс до 460.

## Срок оказания услуг: с момента подписания договора по 31.12.2026 г.

## Порядок оформления и предъявления Заказчику результатов выполнения работ по сопровождению системы. Результаты выполнения работ передаются Заказчику на основании Актов, Товарных накладных (универсальных передаточных документов). Текстовые документы, передаваемые на машиночитаемых носителях, должны быть представлены в форматах \*.docx и \*.pdf.

Все материалы передаются с сопроводительными письмами Исполнителя.

## **УСЛОВИЯ И ПОРЯДОК ОКАЗАНИЯ УСЛУГ**

Исполнитель должен обеспечить качественную и высококвалифицированную техническую поддержку ЕКС для выполнения следующих работ:

* Поддержка пользователей
* Адаптация функционала ЕКС
* Модификация ЕКС

Исполнитель обязуется исполнять «Требования по информационной безопасности» в части предоставления удаленного доступа третьим лицам, не являющимся работниками Заказчика (юридические лица, индивидуальные предприниматели, исполнители по договорам ГПХ), в редакции Приложения 1.

Заявка в техническую поддержку Заказчика подается посредством системы регистрации заявок Заказчика, к которой имеют доступ специалисты поддержки Исполнителя.

График работы технической поддержки с 06.00 до 19.00 по Московскому времени (понедельник-пятница) и с 06.00 до 16.00 по Московскому времени (суббота).

После получения заявки Исполнитель обязуется консультировать специалистов Заказчика по техническим вопросам, связанными с эксплуатацией ЕКС. Максимальное время реакции на заявку пользователей зависит от типа обращения: Обращение по проблеме, не позволяющий работать большому количеству касс – 2 часа. Обращение по проблеме, не позволяющий работать одной кассе – 4 часа. Другие виды работ – 8 часов.

Для указанных видов обращений время реакции должно составлять 1 час:

- Не открывается кассовая смена в ЕКС

- Не закрывается кассовая смена в ЕКС

- Не пробивается чек на ККТ

Допускается производить сопровождение удаленно.

Специалисты Исполнителя должны обладать специальными знаниями по вопросам эксплуатации, настройки и установки подключения всех программных продуктов и кассового оборудования, входящих в состав модулей ЕКС. Исполнитель должен обеспечить проведение ежемесячного анализа обращений специалистов Заказчика и по запросу предоставить его Заказчику в виде журнала обращений пользователей системы.

Исполнитель должен обеспечить устранение сбоев в базе данных автоматизированных систем по мере обращения Заказчика в течение 3-х рабочих дней с момента получения заявки Заказчика, при условии наличия резервных копий системы;

Исполнитель должен обеспечить установку новых релизов программного продукта «1С:Розница 2.3». Установка новых релизов осуществляется по мере необходимости для поддержания работоспособности системы, обновление выполняется по согласованию времени обновления с Заказчиком

Исполнитель должен обеспечить предоставление доступа для новых пользователей ЕКС в течение 4 – х часов с момента подачи заявки, настройка прав доступа. с момента подтверждения заявки пользователя ответственным от Заказчика лицом.

Исполнитель обеспечивает взаимодействие с разработчиком - Фирмой “1С” по вопросам исправления ошибок и расширению типового функционала программного продукта.

Исполнитель должен обеспечить настройку в Системе следующего торгового оборудования: сканера штрихкодов, фискального регистратора и подключаемого банковского терминала, подключенного к компьютеру кассира. Драйвера для банковского терминала предоставляет банк.

Исполнитель должен обеспечить выполнение услуг по адаптации и развитию функциональности программного обеспечения (Доработки типового функционала) на основании оценки дополнительных работ и частного технического задания. Оценка работ производится в срок - 24 часов для доработок, требующих не более 30 часов работ и 56 часов для доработок, требующих от 30 до 70 часов работ.

## В рамках оказания услуг адаптации и модификации Исполнитель обязан производить доработки функционала (программирование, дизайн, верстка) Системы по запросам на изменение, поступающим от Заказчика, в согласованном объёме 30 часов в месяц. При этом в случае, если указанное количество часов не будет выбрано Заказчиком в течение отчётного месяца, то остаток невыбранных часов переносится на следующий месяц, но не более, чем за 2 месяца, в рамках одного календарного квартала. При отсутствии необходимости в услугах по адаптации и модификации в течение более 2 месяцев, перенос объема работ согласуется Сторонами по срокам и объёму.

После выполнения обращения Исполнитель должен проинформировать Заказчика через согласованные каналы поступления обращений о завершении выполнения.

В случае если Заказчик отменяет или приостанавливает выполнения работ по обращению, принятому в обработку Исполнителем более чем на 1 (Один) месяц, он должен письменно проинформировать Исполнителя (менеджера сопровождения) об отмене или приостановлении. В указанном выше случае приостановки или отмены обращения Заказчика Исполнитель предъявляет Заказчику фактический результат оказанных услуг уполномоченному представителю Заказчика, а Заказчик со своей стороны обязан принять такой результат. При возобновлении работ по отмененному или приостановленному обращению время решения может быть пересмотрено Исполнителем в одностороннем порядке.

В случае если дать плановую оценку по обращениям не представляется возможным Исполнитель должен уведомить Заказчика и согласовать закрытие обращения по фактическим часам и согласованным с Заказчиком этапам работ.

## **ИСТОЧНИКИ РАЗРАБОТКИ ТЕХНИЧЕСКОГО ЗАДАНИЯ**

1. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
3. Федеральным законом от 06 апреля 2011 №63-ФЗ «Об электронной подписи»;
4. Постановление Правительства Российской Федерации от 06 июля 2015 г. №676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации»;
5. Постановление Правительства Российской Федерации от 01.11. 2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
6. Постановление Правительства РФ от 16.11.2015 №1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»;
7. Постановление Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
8. Постановление Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
9. Приказ ФСТЭК России №17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
10. Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении требований состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
11. Приказ ФСБ России от 10.07.2014 №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
12. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания" (утв. постановлением Госстандарта СССР от 29 декабря 1990 г. N3469);
13. ГОСТ 34.602-89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы" (утв. постановлением Госстандарта СССР от 24 марта 1989 г. N661);
14. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положение»;
15. ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»;
16. ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»;
17. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения»;
18. ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
19. ГОСТ 19.101-77-82 «Единая система программной документации. Виды программ и программных документов»;
20. ГОСТ 19.103-77 «Единая система программной документации. Обозначения программ и программных документов»;
21. ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем»;
22. ГОСТ 7.32-2017 «Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления»;
23. Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России от 11 февраля 2014 г.;
24. ГОСТ 2.051-2006. Единая система конструкторской документации. Электронные документы. Общие положения;
25. ГОСТ 2.105-95. Единая система конструкторской документации. Общие требования к текстовым документам;
26. ГОСТ 2.301-68. Единая система конструкторской документации. Форматы;
27. ГОСТ 6.10.4-84. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники;
28. ГОСТ Р 6.30-2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов;
29. ГОСТ 19781-90. Обеспечение систем обработки информации программное. Термины и определения;
30. ГОСТ 19.101-77-82. Единая система программной документации. Виды программ и программных документов;
31. ГОСТ 19.201-78-82. Единая система программной документации. Техническое задание. Требования к содержанию и оформлению;
32. ГОСТ Р ИСО/МЭК 14764-2002 «Информационная технология. Сопровождение программных средств» (Постановление Госстандарта России от 25 июня 2002 г №248-ст.);
33. РД 50-680-88. Автоматизированные системы. Основные положения;
34. РД 50-34.698-90. Автоматизированные системы. Требования к содержанию документов;
35. СанПиН 2.2.24.548-96. Физические факторы производственной среды. Гигиенические требования к микроклимату производственных помещений;
36. СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы.

Приложение 1 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 № 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 № 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 № 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 класса защищенности 1Г в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
   2. Исполнитель для подключения собственного оборудования к сети Заказчика обязан:
      1. Предоставить аттестат соответствия требованиям защиты информации по классу не ниже «1Г» на подключаемое оборудование.
      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.
  8. Исполнителем должна обеспечиваться регистрация событий безопасности, связанных с действиями пользователей при осуществлении удаленного доступа к ИТ-инфраструктуре Заказчика. Срок хранения таких событий должен составлять не менее 1 (одного) года.

Регистрации подлежат:

* для операционной системы Windows все события безопасности, содержащиеся по умолчанию в журнале «Безопасность»;
* для операционных систем семейства Linux все события безопасности, фиксируемые модулями аудита (например, auditd).
  1. В случае возникновения инцидента информационной безопасности, в том числе связанного с ИТ-инфраструктурой Исполнителя, Исполнитель по запросу Заказчика обязан предоставить журналы регистрации событий, указанных в пункте 3.19.
  2. Подключение к ИТ-инфраструктуре Заказчика осуществляется только в рабочие часы Заказчика. Удаленное подключение вне указанного временного интервала допускается при наличии обоснования необходимости такого подключения в соответствии с условиями договора.
  3. Доступ к ИТ-инфраструктуре Заказчика должен осуществляться со средств вычислительной техники, которые не используются в целях, не связанных с исполнением договорных или трудовых обязанностей Исполнителя, и соответствуют настоящим Требованиям.
  4. Для организации безопасного взаимодействия при удаленном доступе к ИТ-инфраструктуре Заказчика Исполнителем должен реализовываться базовый набор мер по информационной безопасности в соответствии с Приложением № 1 к настоящим Требованиям.

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 | Обоснование необходимости удаленного подключения к ИТ-инфраструктуре вне рабочие часы Заказчика\* (ссылка на пункт договора, временной интервал доступа) |
| *1.*  *…* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно  для  заполнения)* | *(Обязательно для заполнения)* | *(заполняется при необходимости)* |

*\*указывается пункт договора, являющийся обоснованием предоставления удаленного доступа вне рабочие часы Заказчика, и временной интервал такого доступа.*

* 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;
* при необходимости производить периодические проверки с предварительным согласованием Исполнителя на предмет возникновения нештатных ситуаций или инцидентов информационной безопасности путем имитации указанных событий (проведение тренировок);
* в случае необходимости запрашивать у Исполнителя политику информационной безопасности, результаты внутренних (внешних) аудитов информационной безопасности, результаты тестирования на проникновение ИТ-инфраструктуры Исполнителя, план реагирования на компьютерные инциденты, а также регламент действий работников Исполнителя в случае нештатных ситуаций.
  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.

1. **Контактные лица для оперативного взаимодействия**
   1. При подозрении на возникновение инцидента информационной безопасности, связанного с удаленным доступом к ИТ-инфраструктуре Заказчика, взаимодействие между Заказчиком и Исполнителем должно осуществляться путем информирования ответственных лиц способами, приведенными в таблице № 1.

Таблица № 1 – Контактные данные для взаимодействия

| **Должность ответственного лица** | **Фамилия, имя, отчество** | **Телефон** | **E-mail:** |
| --- | --- | --- | --- |
| **Заказчик** | | | |
| Руководитель центра информационной безопасности | Демидов Денис Олегович | +7 (937) 214 63 02 | [soc@tplusgroup.ru](mailto:soc@tplusgroup.ru) |
| Начальник отдела мониторинга и реагирования на инциденты информационной безопасности центра информационной безопасности | Билюкович Юрий Вадимович | +7 (937) 185 82 20 | [soc@tplusgroup.ru](mailto:soc@tplusgroup.ru) |
| **Исполнитель** | | | |
| *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* | *(Обязательно для заполнения)* |

* 1. Заказчик и Исполнитель в течение 5 рабочих дней со дня Дополнительного соглашения осуществляют обмен контактными данными для взаимодействия в рамках реагирования на инциденты.
  2. Уведомление, содержащее контактные данные, направляется Исполнителем ответственному лицу со стороны Заказчика.
  3. В случае изменения контактных данных Заказчик и Исполнитель обязаны проинформировать друг друга о произошедших изменениях в течение 5 рабочих дней после их наступления.

Приложение № 1

к Требованиям 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) оказывающее услуги по заказу Общества)

Перечень базовых мер

по информационной безопасности

В целях организации безопасного взаимодействия при наличии удаленного доступа к ИТ-инфраструктуре Группы «Т Плюс» организациям, оказывающим услуги в рамках заключенных договоров, необходимо обеспечить реализацию следующих базовых мер по информационной безопасности в собственной инфраструктуре:

1. Двухфакторная аутентификация пользователей.
2. Антивирусная защита автоматизированных рабочих мест и серверов.
3. Защита почтовых сервисов от фишинга.
4. Защищенный обмен файлами и информацией через файловое хранилище.
5. Обеспечение процесса управления уязвимостями.
6. Реализация парольной политики, соответствующей следующим требованиям:

* длина пароля должна быть не менее 10 символов;
* пароль должен содержать буквы верхнего и нижнего регистра (А-Я, A-Z, а-я, a-z), специальные символы (!, », №, %, \*, /);
* в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов);
* пароли от учетной записи для доступа к собственной инфраструктуре и учетной записи, созданной для доступа к ИТ-инфраструктуре Группы «Т Плюс», должны отличаться.