Приложение 1 к документации о закупке

**Техническое задание   
на оказание услуг по сопровождению корпоративной системы   
электронного документооборота АО «ЭнергосбыТ Плюс» на базе платформы Directum**

###### **Общие требования**

* 1. Настоящее Техническое задание определяет объём и перечень услуг Исполнителя по сопровождению Корпоративной системы электронного документооборота АО «ЭнергосбыТ Плюс» на основе платформы Directum 5 (далее «Системы»).
  2. **Заказчиком** услуг является АО «ЭнергосбыТ Плюс».
  3. **Период оказания услуг**: 12 (двенадцать) месяцев с даты подписания договора на оказание услуг.
  4. **Объем услуг:** максимум 520 часов трудозатрат Исполнителя за весь период оказания услуг.
  5. Объем услуг должен оказываться в соответствии с соотношением:

**- 20%** услуг по свободным заявкам Заказчика (максимум 104 ч/часов).

**- 80%** фиксированные услуги в соответствии с Таблицей 1 (максимум 416 ч/часов)

Таблица 1. Перечень фиксированных услуг

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование услуг | Количество (ч/час) | Описание |
| 1 | Работы по повышению скорости работы СЭД Directum 5 (далее «Системы») | 80 | Анализ логов, анализ ресурсоёмких запросов для основной функциональности Системы, анализ индексов БД, рекомендации по повышению производительности работы системы и снижения влияние роста объема данных на скорость работы Системы |
| 2 | Повышение скорости работы интеграции Системы с сервисами ЮЗДО | 72 | Анализ изменения скорости с течением времени (по мере увеличения справочника «Сообщения системы обмена»), выявление ресурсоёмких запросов интеграции с сервисами ЮЗДО (СБИС и Диадок), рекомендации по изменению индексов в БД, поиск иных вариантов повышение скорости работы интеграции Системы с сервисами ЮЗДО |
| 3 | Разработка в Системе в модуле «Канцелярия» функционала «Заявки на выдачу дел из архива» | 184 | (Задача №91746 в Bitrix24)  Содержание работ:  - Разработка справочника заявок на выдачу дел/документов из архива.  - Реализация запуска с обложки модуля «Канцелярия» процесса создания заявки и просмотра журнала заявок.  - Доработка типовой карточки номенклатурного дела.  - Создание новых типовых карточек документов: Карта-заместитель, Акт изъятия документа, Акт о выдаче документа во временное пользование, Акт об утрате документа и разработка шаблонов этих документов.  - Разработка типового маршрута для процесса работы с Заявками.  - Разработка инструкции для пользователей |
| 4 | Анализ ошибок в логах Системы для службы DISI и оценка их влияния на надежность работы службы | 80 | Анализ ошибок логов службы DISI Directum 5:  - «ProcessIncomingMessages|Не удалось импортировать служебные документы»  - «ProcessIncomingMessages|Не удалось определить ИД родительского сообщения на сервисе для ответного сообщения»  - «GetIncomingMessages|NpoComputer.DCX. Common.Exceptions.ServiceException: DCX. Can't get content from url»  - «GetIncomingMessages|NpoComputer.DCX. Common.Exceptions.ServiceException: Неизвестная ошибка при выполнении операции на сервисе обмена ---> Newtonsoft.Json. JsonReaderException: Unexpected character encountered while parsing value: <. Path»  Оценка влияния ошибок на надежность работы службы DISI, поиск проблемы периодического зависания службы. |
|  | **Итого:** | **416** |  |

* 1. Исполнитель должен выделить на выполнение услуг закрепленную команду в количестве не менее 3 сотрудников для возможности постоянных контактов с представителями Заказчика.

1. **Требования к оказанию услуг по сопровождению Системы.**

###### **Термины и определения**

Обращение – зафиксированное обращение потребителя сервиса. В дальнейшем классифицируемое как инцидент, консультация, запрос на обслуживание или запрос на изменение.

**Инцидент** – любое событие, не являющееся частью нормального функционирования информационных систем, которое привело к нарушению их использования.

Взаимодействие – зафиксированный контакт с потребителем сервиса.

Система – корпоративная система электронного документооборота АО «ЭнергосбыТ Плюс» на основе платформы Directum

Заказная разработка – это модификация экземпляра системы у Заказчика, удовлетворяющая его специфические потребности.

Документация к системе – согласованные версии документов: Проектные решения, инструкции пользователей, запросы на изменение, а также документация производителя платформы по используемой версии платформы.

Ошибка системы – под ошибкой понимается несоответствие фактического поведения программного продукта поведению, предусмотренному в документации к системе, воспроизводимое в определенных условиях и не обусловленное неправильными настройками, действиями пользователя или другими внешними факторами.

**Тестовая эксплуатация** – это проверка заказной разработки в тестовой базе Заказчика на предмет соответствия требованиям, зафиксированным в запросе на изменение.

**Опытная эксплуатация** – это проверка заказной разработки в тестовой базе Заказчика на предмет соответствия требованиям, зафиксированным в запросе на изменение, в условиях реальной работы пользователей Заказчика.

Гарантийная поддержка заказной разработки – решение инцидентов в течение определенного срока после завершения периода опытной эксплуатации по запросу на изменение.

**Квартальный отчет** – формализованный отчет по оказанным услугам за отчетный квартал.

Потребитель сервиса – конкретный обратившийся сотрудник Заказчика.

ОСЗ – Ответственный за соглашение со стороны Заказчика, сотрудник, фиксируемый как ответственный за Соглашение со стороны Заказчика. В его обязанности входит регистрация новых потребителей сервиса, согласование ежеквартальных отчетов, согласование и приемка Запросов на изменения, продление Соглашения и т.д. Устанавливается настоящим Соглашением.

ОСИ – Ответственный за соглашение со стороны Исполнителя, сотрудник, фиксируемый как ответственный за Соглашение со стороны Исполнителя. В его обязанности входит подготовка ежеквартальных отчетов, координация всех услуг по инцидентам и запросам на изменение и т.д. Устанавливается настоящим Соглашением.

###### **Регистрация Потребителей сервиса**

Список Потребителей сервиса, взаимодействующих с Исполнителем, является конечным (не более 15 сотрудников Заказчика). Первоначальный список, а также изменения списка Потребителей сервиса направляются Исполнителю Ответственным за Соглашение со стороны Заказчика (ОСЗ).

Для каждого Потребителя сервиса указывается ФИО, должность, контактные данные.

###### В рамках свободных услуг, в соответствии с п.1.5 настоящего ТЗ, Исполнитель должен оказывать следующие **виды услуг по сопровождению Системы**:

* **инцидентная** поддержка (услуги по устранения сбоев и ошибок Системы);
* **консультации** (оказание консультационных услуг по Системе);
* выполнение **запросов на обслуживание**;
* выполнение **запросов на изменение** (проектирование, адаптация, модификация, разработка и тестирование).

Реестр услуг:

| Тип услуги | Наименование |
| --- | --- |
| Инцидент | Диагностика и восстановление работоспособности Системы на пользовательских ПК |
| Инцидент | Диагностика и восстановление работоспособности серверных компонент |
| Инцидент | Исправление дефектов в прикладной разработке |
| Инцидент | Исправление дефектов платформы |
| Консультации | Консультации по системе |
| Запрос на обслуживание | Предоставление дистрибутивов |
| Запрос на обслуживание | Генерация лицензионного ключа |
| Запрос на обслуживание | Установка, настройка, администрирование клиентских компонент |
| Запрос на обслуживание | Установка, настройка, администрирование серверных компонент |
| Запрос на обслуживание | Импорт прикладной разработки |
| Запрос на изменение | Исследование и проектирование настройки и модификаций |
| Запрос на изменение | Администрирование и настройка |
| Запрос на изменение | Прикладная разработка |
| Запрос на изменение | Обновление ПО на новую версию |
| Запрос на изменение | Миграция данных из сторонних систем |
| Запрос на изменение | Разработка/корректировка документации |

###### **Инцидентная поддержка**

Каждому зарегистрированному инциденту службой поддержки Исполнителя должен присваиваться приоритет, в соответствии с которым определяются очередность обработки и стандартные нормы времени реакции. Приоритет инцидента определяется на основании степени воздействия на работу пользователей и частоты проявления.

**Степень воздействия** характеризует меру отклонения от нормального уровня использования программных продуктов, количество и статус пользователей и бизнес-процессов, подвергшихся воздействию в связи с инцидентом.

|  |  |
| --- | --- |
| Степень воздействия | Описание |
| Высокая | Серьезные сбои, при которых становится невозможным выполнение ключевых бизнес-процессов, нарушающие использование всей системы в целом или её отдельных служб. Сбой может охватывать работу как отдельных ключевых пользователей, так и целые группы |
| Средняя | Сбой не останавливает работу системы в целом, но часть функций системы работает некорректно |
| Низкая | Сбой, влияющий на удобство работы с системой, снижающее эффективность ее использования, но не блокирующий выполнение бизнес-процессов |

**Частота** проявления инцидентов определяется следующим образом:

|  |  |
| --- | --- |
| Частота | Описание |
| Высокая | Устойчивое (постоянное) проявление инцидента. |
| Средняя | Частое, но не стабильное проявление инцидента. |
| Низкая | Эпизодическое и не стабильное проявление инцидента. |

**Приоритет** инцидента на основании степени воздействия и частоты проявления определяется в соответствии с таблицей:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Приоритет инцидента | | Степень воздействия | | |
| Высокая | Средняя | Низкая |
| Частота | Высокая | Критический | Высокий | Средний |
| Средняя | Высокий | Средний | Низкий |
| Низкая | Средний | Низкий | Планируемый |

В зависимости от приоритета инцидента должны устанавливаться нормы на время реакции. Под временем реакции понимается количество рабочих часов, прошедших с момента регистрации инцидента, в течение которых назначенный специалист службы поддержки приступает к услуге по его разрешению, и, в зависимости от ситуации, дает первоначальные рекомендации по разрешению инцидента или запрашивает сведения, необходимые для более глубокой диагностики.

Время реакции в зависимости от приоритета инцидента не должно превышать значений, указанных в таблице:

|  |  |
| --- | --- |
| Приоритет инцидента | Максимальное время реакции  (рабочих часов) |
| Критический | 2 |
| Высокий | 4 |
| Средний | 12 |
| Низкий | 24 |
| Планируемый | По отдельной договоренности с Заказчиком |

**Потребитель сервиса** может указать **желаемую срочность** обработки инцидента, которая позволит задать очередность обработки инцидентов среди всех обращений (в том числе с разными приоритетами).

Инцидент считается решенным, если предоставлена рекомендация, позволяющая устранить сбой и восстановить нормальное использование информационных систем. Рекомендация может включать предоставление «обходного пути».

###### **Услуги** **по консультированию**

Консультации оказываются в случае возникновения вопросов от Заказчика по эксплуатации системы, по архитектуре системы и по иным вопросам.

###### **Выполнение запросов на обслуживание**

Под запросом на обслуживание понимается запрос на выполнение какой-либо стандартной процедуры по обслуживанию Системы (например, заведение нового пользователя, сброс пароля пользователя, изменение прав).

###### **Выполнение запросов на изменение**

Запросы на изменение – это запросы от Потребителя сервиса, связанные с изменением функциональности, интерфейсов или способов функционирования системы. Порядок услуг с Запросами на изменения описан в п.4.7.3

###### **Порядок действий по услугам с обращениями Потребителей сервиса**

###### **Регистрация обращения**

К регистрации должны принимаются обращения только от зарегистрированных Потребителей сервиса. При обращении неизвестного Потребителя сервиса Исполнитель должен отказать в регистрации обращения.

Регистрация обращений от Потребителей сервиса должны производиться Исполнителем как минимум следующими способами:

* телефон;
* электронная почта.

Возможны дополнительные способы обращений по предложению Исполнителя.

Прием обращений по телефону должен производиться в рабочие дни в период времени не менее чем с 9-00 до 18-00 по московскому времени.

###### **Классификация обращения**

Каждое обращение должно классифицироваться. При классификации определяется услуга, частота, степень воздействия, приоритет и тип обращения (инцидент, запрос на обслуживание, консультация или запрос на изменение). Потребителю сервиса направляется уведомление по электронной почте.

###### **Обработка** **обращений с типом «инцидент» и «запрос на обслуживание»**

Обращение с типом «инцидент», «консультация» и «запрос на обслуживание» должно без согласования поступать в работу после классификации. В процессе решения обращения сотрудники Исполнителя могут запрашивать дополнительную информацию. В случае отсутствия ответа Потребителя сервиса на запрос информации в течении 5 (трех) рабочих дней, обращение может быть закрыто автоматически.

Если в процессе обработки обращения выявляются вопросы или ошибки, не описанные в исходной формулировке обращения, то они регистрируются отдельными обращениями и отправляются в работу.

После завершения всех услуг по обращению Потребителю сервиса должен отправляется запрос на закрытие обращения, где он отмечает его закрытие и оценивает проведенные по нему услуги. При отказе в закрытии обращения Потребитель сервиса должен указать причину. В том случае, если потребитель не обработает запрос на закрытие в течение 5 (трех) рабочих дней, обращение считается принятым.

По услугам с обращениями с типом «инцидент», «консультация» и «запрос на обслуживание» трудозатраты должны учитываться с точностью до 15 (пятнадцати) минут, при этом должны быть включены все фактические трудозатраты сотрудников Исполнителя, включая исследование причин обращения, взаимодействие с сотрудниками заказчика и т.д.

###### **Обработка «Запросов на изменение»**

После классификации сотрудники Исполнителя должны выполнить предварительное исследование требований, а также возможности и способы реализации, которые согласовываются с Заказчиком. По итогам выполняется детальное проектирование и подготовка документа «Запрос на изменение». Документ содержит описание модификаций и настроек, которые необходимо выполнить, сроки и трудоемкость выполнения данных модификаций и настроек, срок приемки услуг ОСЗ и срок гарантии.

Трудоемкость услуг по Запросу на изменение должна составлять не менее 8 человеко-часов, иначе это обращение необходимо переклассифицировать.

Сроки анализа и последующей реализации Запроса на изменение должны устанавливаться индивидуально по согласованию с Ответственным за соглашение со стороны Заказчика (ОСЗ), но с учетом следующих ограничений:

* сроки выполнения модификации/настройки – определяются индивидуально с учетом трудоемкости услуг и текущей загрузки специалистов Исполнителя и Заказчика;
* сроки приемки услуг Заказчиком при тестовой эксплуатации (на тестовой базе) – не более 10 (десяти) рабочих дней с момента передачи результата услуг Заказчику;
* сроки приемки услуг Заказчиком при опытной эксплуатации (на рабочей базе) – не более 10 (десяти) рабочих дней с момента передачи результата услуг Заказчику;
* сроки гарантийной поддержки – в течение 1 (одного) месяца после приемки услуг Заказчиком, но не более 2 (двух) месяцев с момента передачи выполненной модификации/настройки Заказчику на тестирование.

Заказчик должен согласовать документ «Запрос на изменение», после этого он должен передаваться на реализацию Исполнителю.

Согласование документа «Запрос на изменение» и последующая приемка услуг должна осуществляться сторонами в электронном виде с использованием e-mail или сайта поддержки (при наличии). В случае приемки результатов услуг Заказчик (ОСЗ) направляет Исполнителю соответствующее подтверждение, а в случае отказа от приемки – отказ с перечнем несоответствий для исправления. При отсутствии подтверждения или отказа от приема услуг при истечении срока приемки Заказчиком запрос на изменение считается принятым автоматически.

Трудозатраты Исполнителя на предварительное исследование, способов реализации, детальное проектирование и формирование документа «Запрос на изменение» должны учитываться отдельным пунктом в квартальном отчете и подлежат оплате Заказчиком, даже если Заказчик отказался от реализации Запроса на изменение (после предоставления Исполнителем документа «Запрос на изменение»).

###### **Отчетность**

После окончания отчетного квартала Исполнитель должен в течение 5 рабочих дней предоставить Ежеквартальный отчет, который должен отображать все фактически выполненные услуги за отчетный квартал. В него должны попадать все обращения с типом «инцидент», «консультация» и «запрос на обслуживание», закрытые в отчетный квартал, все Запросы на изменение (вместе с подготовкой документа «Запрос на изменение»), принятые в отчетный квартал, а также все Запросы на изменения, прекращенные в отчетный квартал по инициативе Заказчика.

ОСЗ должен в течение 5 рабочих дней с момента получения квартального отчета отправить подписанную копию или мотивированный отказ Исполнителю. По истечению данного срока отчет считается принятым.

###### При оказании услуг необходимо соблюдать требования по информационной безопасности, указанные в Приложении 1.

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)), 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 услуги 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 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 услуг 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 услуг Исполнителем в режиме удаленного доступа договор с Исполнителем должен содержать:

* оговорку о дистанционном характере выполнения услуг;
* 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 услугах 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 услуги, 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 услуг 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.