«УТВЕРЖДАЮ»

Исполнительный директор –

Председатель ЗК

ПАО «Ставропольэнергосбыт»

\_\_\_\_\_\_\_\_\_\_\_\_\_И. Б. Салпагаров

«30» апреля 2025 года

**ОТКРЫТЫЙ ЗАПРОС ПРЕДЛОЖЕНИЙ**

**НА ПРАВО ЗАКЛЮЧЕНИЯ ДОГОВОРА**

**на оказание услуг по мониторингу и реагированию**

**на инциденты информационной безопасности и организацию**

**информационного взаимодействия с ГосСОПКА**

**для нужд**

**ПАО «Ставропольэнергосбыт»**

**в 2025г.**

г. Ессентуки 2025г.

**1. Общие положения**

1. **Общие сведения о процедуре запроса предложений**
2. ПАО «Ставропольэнергосбыт», Юридический адрес: (357633, Ставропольский край, г. Ессентуки, ул. Большевистская, 59а), (Далее — Организатор, Заказчик), извещением о проведении открытого запроса предложений, размещенном на официальном сайте ПАО «Ставропольэнергосбыт» на сайте www.staves.ru в разделе закупки/текущие закупки/2025/проведение процедур закупок в 2025г., приглашает юридических лиц и индивидуальных предпринимателей (далее — исполнители) к участию в открытом запросе предложений на право заключения договора на оказание услуг по мониторингу и реагированию на инциденты информационной безопасности и организацию информационного взаимодействия с ГосСопка для нужд ПАО «Ставропольэнергосбыт» в 2025г. (далее — услуги).
3. Открытый запрос предложений проводится на основании Приказа ПАО «Ставропольэнергосбыт» № 177 от 30.04.2025 г. Дата начала приема заявок 10:00 30.04.2025г., дата окончания приема заявок 10:00 (время московское) 14.05.2025г.
4. Для справок обращаться: начальник ОМТС Ветлицкий Станислав Юрьевич, т/ф. 8(87934) 4-26-84, эл. почта: s.vetlitskiy@staves.ru
5. Подробные требования к оказываемым услугам изложены в разделе 2 (здесь и далее ссылки относятся к настоящей Документации по открытому запросу предложений). Порядок проведения запроса предложений и участия в нем, а также инструкции по подготовке Предложений, приведены в разделе 3. Проект договора в разделе 4. Информационная карта запроса предложений в разделе 5. Форма письма о подаче оферты в разделе 6. Порядок, критерии оценки и сопоставления заявок в разделе 7.
6. **Правовой статус процедур и документов**

1.2.1 Данная процедура открытого запроса предложений не является конкурсом, и ее проведение не регулируется статьями 447—449 части первой Гражданского кодекса Российской Федерации. Данная процедура открытого запроса предложений также не является публичным конкурсом и не регулируется статьями 1057— 1061 части второй Гражданского кодекса Российской Федерации. Таким образом, процедура запроса предложений не накладывает на Заказчика соответствующего объема гражданско-правовых обязательств.

1. Извещение к участию в открытом запросе предложений вместе с настоящей Документацией по запросу предложений, являющейся его неотъемлемым приложением, являются приглашением делать оферты и должны рассматриваться Участниками в соответствии с этим.
2. Предложение Участника имеет правовой статус оферты и будет рассматриваться Заказчиком в соответствии с этим.
3. Заключенный по результатам запроса предложений Договор фиксирует все достигнутые сторонами договоренности.
4. При определении условий Договора с Победителем используются следующие документы с соблюдением указанной иерархии (в случае их противоречия):
   1. Протоколы преддоговорных переговоров между Заказчиком и Победителем (по условиям, не оговоренным ни в настоящей Документации по запросу предложений, ни в Предложении Победителя);
   2. Извещение к участию в открытом запросе предложений и настоящая Документация по запросу предложений по всем проведенным этапам со всеми дополнениями и разъяснениями;
   3. Предложение Победителя со всеми дополнениями и разъяснениями, соответствующими требованиям Заказчика.
5. Иные документы Заказчика и Участников не определяют права и обязанности сторон в связи с данным запросом предложений.
6. Во всем, что не урегулировано извещением к участию в открытом запросе предложений и настоящей Документации по запросу предложений стороны руководствуются Гражданским кодексом Российской Федерации.

**1.3 Обжалование**

1.3.1 До заключения договора разногласия направляются в закупочную комиссию ПАО «Ставропольэнергосбыт». О получении заявления о рассмотрении разногласий ответственный секретарь ЗК незамедлительно уведомляет председателя комиссии, проводящей закупку. На время рассмотрения разногласий в ЗК процедура проведения закупки приостанавливается до вынесения решения, если к тому нет явных препятствий юридического или экономического характера.

1. Если разногласия не разрешены по взаимному согласию представившего их участника и лиц, производивших закупку, ЗК заказчика в течение 10 дней со дня получения таких разногласий выносит письменное решение, которое должно содержать:
   1. обоснование мотивов принятия решения;
   2. меры, направленные на удовлетворение изложенных требований, в случае полного или частичного разрешения разногласий.
2. ЗК вправе принять одно или несколько из следующих решений:
   1. при разногласиях по завершившимся закупкам — предложить руководству принять решение о возмещении убытков, понесенных участником в результате незаконного действия, решения либо использования незаконной процедуры. Если оговорка об одностороннем расторжении договора, в случае обнаружения нарушений процедуры его заключения, включена в договор, ЗК вправе предложить руководству принять решение об одностороннем расторжении договора после его заключения;
   2. признать заявление участника необоснованным.
3. Все споры и разногласия, возникающие в связи с проведением запроса предложений, в том числе касающиеся исполнения Организатором и Участниками запроса предложений своих обязательств, не урегулированные путем претензионного порядка, обращения в ЗК заказчика, могут разрешаться путем обращения в Центральную Конкурсную Комиссию (ЦКК) общества.
4. Вышеизложенное не ограничивает права сторон на обращение в суд в соответствии с действующим законодательством РФ.

**1.4 Прочие положения**

1. Исполнитель самостоятельно несет все расходы, связанные с подготовкой и подачей Предложения.
2. Заказчик обеспечивает разумную конфиденциальность относительно всех полученных от Участников сведений, в том числе содержащихся в Предложениях.

**2. ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на оказание услуг по мониторингу и реагированию**

**на инциденты информационной безопасности и организацию информационного взаимодействия с ГосСОПКА**

**для нужд ПАО «Ставропольэнергосбыт» в 2025г.**

**1. ОБЛАСТЬ ПРИМЕНЕНИЯ**

**1.1** Данное техническое задание определяет необходимый объем и уровень оказания услуг по мониторингу и реагированию на инциденты информационной безопасности и организацию информационного взаимодействия с ГосСОПКА для ПАО «Ставропольэнергосбыт» (далее — Заказчик), оказываемых организацией, взявшей на себя обязательства по исполнениюе указанных услуг (далее — Исполнитель).

**2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

* 1. **Информационная безопасность (ИБ)** – сохранение конфиденциальности, целостности и доступности информации.
  2. **Событие ИБ** – выявленное состояние системы, услуги или сети Заказчика, указывающее на возможное нарушение политики обеспечения ИБ или сбой мер обеспечения ИБ, или ранее неизвестная ситуация, которая может иметь отношение к вопросам ИБ.
  3. **ИИС** – информационные инфраструктурные сервисы
  4. **Security operation center (SOC)** –центр оперативного мониторинга событий ИБ Исполнителя, реализующий Услугу.
  5. **Инцидент ИБ** – срабатывание одного или нескольких правил корреляции, не сопровождаемых наличием связных событий ИБ, достоверно указывающих на ложное срабатывание, или подозрительная активность, замеченная сотрудниками SOC в процессе работы.
  6. **Система SOC** –программное обеспечение и/или аппаратно-программный комплекс SOC, предназначенные для автоматизированного сбора событий ИБ, обнаружения и регистрации инцидентов ИБ и последующего реагирования на них.
  7. **Правило корреляции** – соотнесение между собой в Системе SOC событий ИБ, удовлетворяющих определенным условиям с целью обнаружения инцидентов ИБ. Правила корреляции являются коммерческой тайной Исполнителя.
  8. **Услуга** – услуга по мониторингу и реагированию на инциденты ИБ, представляющая собой обеспечение круглосуточного мониторинга событий ИБ, проведения их анализа, своевременного обнаружения и разрешение инцидентов ИБ, а также организацию информационного взаимодействия Заказчика с ГосСОПКА через КЦ ГосСОПКА.
  9. **ГосСОПКА** – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
  10. **КЦ ГосСОПКА** – корпоративный центр ГосСОПКА Исполнителя, являющийся частью Системы SOC.
  11. **НКЦКИ** –Национальный координационный центр по компьютерным инцидентам.
  12. **Реагирование на инцидент ИБ** – структурированная совокупность действий Исполнителя, направленная на установление деталей инцидента ИБ и информирование о нем Заказчика.
  13. **СЗИ** – средства защиты информации Заказчика.
  14. **БД** – база данных.
  15. **ИР** – информационные ресурсы.
  16. **Хост источника** – оконечные устройства Заказчика, на которых настроена отправка событий ИБ в Систему SOC (например, конкретный сервер или приложение).
  17. **Системы-источники** – совокупность хостов-источников (серверов, приложений), объединённых по функциональному назначению, например, Система антивирусной защиты (может состоять из нескольких серверов БД), Система документооборота (может состоять из нескольких серверов-приложений).
  18. **Коллектор** – централизованный сервер, аккумулирующий события ИБ с различных систем-источников, расположенный в инфраструктуре Заказчика и сопровождаемый силами Заказчика.
  19. **Личный кабинет SOC (ЛК SOC)** – информационный портал Исполнителя, предназначенный для взаимодействия Заказчика и SOC, предоставления аналитической и отчетной информации, а также взаимодействия Заказчика с ГосСОПКА, являющийся частью Системы SOC.
  20. **Event per second (EPS)** – события ИБ в секунду, передаваемые в Систему SOC.
  21. **Технологическое окно** – запланированный период времени для проведения технических работ, в течение которого ЛК SOC будет недоступен.
  22. **Простой** – недоступность ЛК SOC для Заказчика.
  23. **Заказ** – выбираемый Заказчиком набор параметров и опций Услуги, содержащий информацию об оказываемой Услуге, включающий её стоимость и срок действия (период оказания). Заказ является неотъемлемой частью Договора.
  24. **Отчётный период** – период с первого по последнее число соответствующего календарного месяца, в котором были оказаны Услуги.
  25. **Информационная инфраструктура (ИИ)** – информационная инфраструктура Заказчика.
  26. **ОИИ** – объект информационной инфраструктуры Заказчика.
  27. **Критическая информационная инфраструктура (КИИ)** – объекты критической информационной инфраструктуры Заказчика, а также сети электросвязи, используемые для организации взаимодействия таких объектов.
  28. **Объект критической информационной инфраструктуры (ОКИИ)** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления КИИ Заказчика.
  29. **Компьютерная атака (КА)** – целенаправленное воздействие программных и (или) программно-аппаратных средств на ОКИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.
  30. **Компьютерный инцидент (КИ)** – факт нарушения и (или) прекращения функционирования ОКИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате КА.
  31. **ЦЗИиСС** – Центр защиты информации и специальной связи Федеральной службы безопасности Российской Федерации.
  32. **Virtual private network (VPN)** – технология, позволяющая обеспечить одно или несколько сетевых соединений поверх другой сети, с повышенным уровнем защиты благодаря использованию средств криптографии.
  33. **Demilitarized Zone (DMZ)** – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных.

**3. ОБЩИЕ ПОЛОЖЕНИЯ**

* 1. Услуга по мониторингу и реагированию на инциденты ИБ представляет собой обеспечение круглосуточного мониторинга событий ИБ, проведения их анализа, своевременного обнаружения и разрешение инцидентов ИБ, а также организацию информационного взаимодействия Заказчика с ГосСОПКА через КЦ ГосСОПКА.
  2. В рамках оказываемой Услуги Исполнитель осуществляет:
  3. совместно с Заказчиком подключение систем-источников событий ИБ к Системе SOC и профилирование их активности;
  4. мониторинг и реагирование на инциденты ИБ, зарегистрированные в подключенных системах-источниках. Данная услуга предполагает подключение в качестве источников событий ИБ следующих элементов ИИС Заказчика:
* межсетевые экраны, маршрутизаторы;
* прокси-серверы;
* DHCP-серверы;
* система обнаружения/предупреждения вторжений;
* контроллеры домена;
* почтовые серверы;
* прикладные, файловые, терминальные серверы, серверы баз данных;
* АРМ критичных пользователей;
* антивирусное ПО;
* системы и серверы виртуализации;
* элементы объектов критической информационной инфраструктуры (по согласованию Исполнителя и Заказчика);
* другие источники по запросу Заказчика.
  1. организацию совместно с Заказчиком и в соответствии с Приложением № 1 информационного взаимодействия Заказчика с ГосСОПКА через КЦ ГосСОПКА.

**4. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ**

* 1. Взаимодействие Сторон в рамках оказываемой Услуги осуществляется через ЛК SOC (преимущественно) и/или способом из Матрицы контактов, указанной в пункте 4.4.
  2. Внесение изменений в Матрицу контактов, указанную пункте 4.4, а также запрос на предоставление нового доступа в ЛК SOC осуществляется путем обращения через ЛК SOC или по электронной почте.
  3. Контактное лицо Заказчика оповещается при выявлении инцидента ИБ в нерабочее время посредством телефона при указании данного параметра в Матрице контактов из пункта 4.4.
  4. Матрица контактов Сторон:

Контакты Исполнителя

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Уровень обращения** | **Контактное лицо** | **Адрес электронной почты** | **Телефон** |
| 1 | Взаимодействие по инцидентам ИБ | Дежурная смена SOC |  |  |

Контакты Заказчика

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **ФИО/наименование группы рассылки** | **Направление (зона ответствен-ности)** | **Адрес электронной почты** | **Телефон** | **Оповещение в нерабочее время по телефону**  **(да/нет)** | **Доступ к ЛК SOC**  **(да/нет)** |
| 1 | Отдел ИБ | ИБ |  |  | нет | да |

Уровень критичности инцидентов ИБ для оповещения по контактному телефону в нерабочее время: *(****высокая****/*средняя/*низкая/не оповещать)*

**4.5** Обеспечение работоспособности ЛК SOC:

|  |  |  |
| --- | --- | --- |
| Период работы и обслуживания | Период работы | 24\*7 |
| Количество технологических окон за месяц | не более 1 |
| Уведомление о технологическом окне | за 3 рабочих дня |
| Максимальная длительность технологического окна | не более 6 часов |
| Уведомление о простоях | в течении 60 минут |

1. **ПАРАМЕТРЫ ОКАЗАНИЯ УСЛУГИ**
   1. При подготовке к запуску Услуги Заказчик заполняет Перечень систем-источников, подключаемых к Системе SOC.
   2. Исполнитель обязуется осуществлять мониторинг и реагирование на инциденты ИБ, зафиксированные в подключенных системах-источниках.
   3. Параметры Услуги:

| **Наименование параметра** | **Значение параметра** | |
| --- | --- | --- |
| Обработка и анализ поступающих событий ИБ | Анализ событий ИБ в реальном времени в соответствие с правилами корреляции | |
| Длительность хранения собранных событий ИБ с момента их фиксации в Системе SOC | 3 месяца | |
| Максимальное количество EPS (среднее значение за месяц). Превышение данного лимита оплачиваются отдельно. | 400 EPS | |
| SIEM-платформа | Kaspersky KUMA | |
| **Дежурная смена**  *Обеспечение мониторинга и реагирования на регистрируемые в Системе SOC инциденты ИБ силами Исполнителя* | | |
| Период предоставления Услуги | 24\*7 | |
| Предоставление первичных рекомендаций по инциденту с момента его фиксации в Системе SOC | 20 минут | |
| Время реагирования на инцидент ИБ с момента его фиксации в Системе SOC | Высокая критичность | 60 минут |
| Средняя критичность | 90 минут |
| Низкая критичность | 120 минут |
| **Изменение профиля Услуги** | | |
| Время выполнения работ по подключению новых систем-источников | | 20 рабочих дней/1 источник |
| Кол-во подключаемых новых систем-источников по запросу Заказчика | | не более 1-го в месяц |
| Время выполнения запроса на разработку правил обнаружения инцидентов ИБ | | 10 рабочих дней/1 правило |
| Кол-во разрабатываемых правил обнаружения инцидентов ИБ по запросу Заказчика | | не более 3-х в год |
| Расширенный экспертный анализ по инцидентам ИБ | | не более 3-х в год |

* 1. Услуга не включает в себя оказание консультаций и обучения по работе с СЗИ и системами-источниками.
  2. Услуга не включает в себя проведение аудита инфраструктуры Заказчика.

1. **ПОДКЛЮЧЕНИЕ ЗАКАЗЧИКА К СИСТЕМЕ SOC**
   1. Процесс оказания Услуги включает в себя процедуру подключения инфраструктуры Заказчика к Системе SOC, предоставление Заказчику доступа в ЛК SOC для взаимодействия Заказчика с НКЦКИ и осуществления мониторинга и реагирования на зафиксированные инциденты ИБ в Системе SOC с поэтапным отчетным периодом.

Подключение систем-источников, настройка отчетности, профилирование активности, настройка автоматических уведомлений о возникающих инцидентах осуществляются в течение 20 (двадцати) рабочих дней с момента подписания Договора, при своевременном выполнении работ со стороны Заказчика, а также при наличии у Заказчика необходимых технических возможностей (оборудование для организации и организация туннеля доступа к системам-источникам (равнозначно также, «VPN», «VPN–канал», организуемого Заказчиком, серверного оборудования и т.д.).

* 1. В рамках подключения к Услуге Исполнитель:
* согласовывает итоговый перечень подключаемых систем-источников. Для систем-источников должно быть готовое правило корреляции (перечень правил доступен в ЛК SOC либо предоставляется по запросу);
* совместно с Заказчиком подключается по организованному и предоставленному Заказчиком туннелю доступа к коллекторам, настраивает защищённое соединение между коллекторами и Системой SOC с целью передачи событий ИБ с систем-источников на коллекторы и с них в Систему SOC в режиме реального времени. При настройке соединения за основу берётся схема, представленная на рисунке 1:

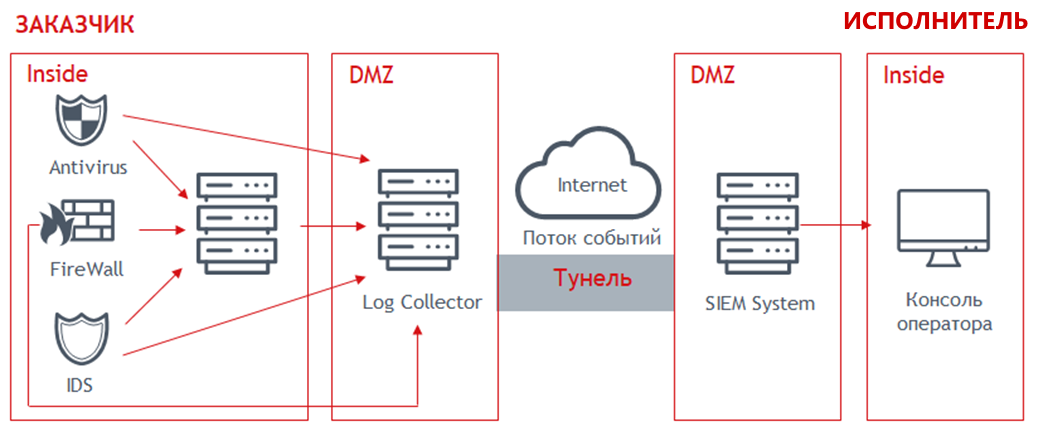


Рисунок 1. Схема взаимодействия

* направляет в адрес сотрудников Заказчика, указанных в Матрице контактов из пункта 4.4, инструкции по настройке сбора событий ИБ на соответствующих ИТ и ИБ-системах (для стандартных систем-источников);
* подключает события ИБ с систем-источников, которые передаются на заранее подготовленные Заказчиком коллекторы, к Системе SOC. Технические требования приведены в пункте 6.4 Технического задания;
* совместно с Заказчиком адаптирует правила обнаружения инцидентов ИБ, включающие в себя:
* правила корреляции;
* логику определения событий ИБ, относящихся к одному/разным инцидентам ИБ, в рамках одного правила;
* определение степени критичности инцидента ИБ;
* проводит совместно с сотрудниками ИБ/ИТ Заказчика профилирование сетевой и хостовой активности для минимизации ложных срабатываний правил корреляции.
  1. В рамках подключения к Услуге Заказчик:
* осуществляет создание и первоначальную настройку (в том числе установку операционной системы) коллекторов с техническими характеристиками, указанными в пункте 6.4 Технического задания, в сетевой зоне DMZ (рекомендованный параметр). Лицензии на операционные системы и другое прикладное программное обеспечение для оборудования из пункта 6.4 Технического задания Заказчик предоставляет самостоятельно;
* ознакамливается с правилами корреляции, перечень которых доступен в ЛК SOC либо предоставляется по запросу;
* организовывает и предоставляет ответственному сотруднику Исполнителя, удалённый доступ–туннель на коллекторы с целью настройки передачи событий ИБ с коллекторов в Систему SOC. В случае отказа Заказчика предоставить данный доступ, Заказчик самостоятельно проводит работы по установке и настройке передачи событий ИБ в Систему SOC. Ответственность за корректность работы в таком случае лежит на Заказчике;
* организовывает сетевой доступ и передачу данных между системами-источниками и коллекторами;
* осуществляет настройку сбора событий ИБ на системах-источниках с передачей событий ИБ на коллекторы. Эксплуатацию и настройку систем-источников Заказчик осуществляет самостоятельно. Заказчик может обратиться к Исполнителю за консультацией по настройке сбора событий ИБ на системах-источниках.

Факт завершения этапа подключения Заказчика к Услуге подтверждается путем подписания Протокола об успешном подключении Услуги.

* 1. Минимальные требования к серверному оборудованию (коллекторам) на стороне Заказчика:

|  |  |  |  |
| --- | --- | --- | --- |
| Параметры сервера | Сервер 1 | Сервер 2 | Сервер 3 |
| Тип сервера | виртуальный или физический | виртуальный или физический | виртуальный или физический |
| Центральный процессор | 6 CPU | 6 CPU | 8 CPU |
| Оперативная память | 12 Гб | 16 Гб | 16 Гб |
| Дисковое пространство | 80 Гб (RAID 10) | 80 Гб (RAID 10) | 500 Гб доступного места на диске, смонтированного в разделе /opt |
| Операционная система | РЕД ОС 7.3.4 и выше | Windows 2016 и выше | РЕД ОС 7.3.4 и выше |
| Примечание | Диски SSD  / - по умолчанию.  /var – 8 Гб  /queue – 20 Гб  /opt – 10 Гб  /home (или /tmp) – 5 Гб для обмена файлами | Диски SSD.  При установке обязательно английская локализация. Должен быть в домене тех компьютеров, с которых нужно будет собирать события ИБ |  |

* 1. Требования к каналу передачи данных от коллекторов к Системе SOC.

Требования к скорости и объёму передачи данных исходят из следующей информации:

* 1,5 Мбит/с пропускной способности на каждые 100 событий ИБ в секунду;
* 0,7 Мбит/c пропускной способности для коррелятора Системы SOC;
* 0,7 Мбит/c пропускной способности для хранилища Системы SOC.

**7. ПОРЯДОК ОКАЗАНИЯ УСЛУГИ**

* 1. Мониторинг и реагирование на инциденты ИБ.

Исполнитель осуществляет мониторинг всех инцидентов ИБ с систем-источников, фиксируемых в Системе SOC.

В рамках взаимодействия Заказчика с ГосСОПКА:

* передачу в автоматическом режиме в НКЦКИ вносимых Заказчиком в ЛК SOC сведений от систем-источников – ОИИ и (или) ОКИИ, об ИИ, КИИ, о КА и КИ в ИИ и КИИ;
* передачу в автоматическом режиме Заказчику через ЛК SOC сведений от НКЦКИ, об индикаторах компрометации и методических рекомендациях для Заказчика по обнаружению, предупреждению и ликвидации последствий типовых КА на ОИИ и ОКИИ Заказчика.

При возникновении инцидента ИБ Исполнитель проводит первичный анализ данных с целью выявления ложных срабатываний правил корреляции. В случае, если Исполнителем принято решение о ложном срабатывании, соответствующий инцидент ИБ закрывается с обоснованием причин, информация о нем и причинах его закрытия предоставляется в рамках регулярной отчетности Системы SOC, а также доступна в ЛК SOC.

По итогам проведенной обработки Исполнитель информирует Заказчика о факте возникновения инцидента ИБ.

На основании предоставленной информации Заказчик вправе повысить или понизить критичность инцидента ИБ для изменения процесса его обработки в дальнейшем.

После информирования Заказчика о факте инцидента ИБ Исполнитель продолжает установление причин и источника инцидента ИБ, если это возможно. По итогам анализа данная информация передается Заказчику.

Исполнитель вправе запросить у Заказчика дополнительную информацию об ИИ, системах-источниках или событиях ИБ в случае, если она требуется для анализа инцидента ИБ.

Сотрудники Заказчика вправе запросить дополнительную информацию о причинах и источнике инцидента ИБ, если данная информация может быть получена средствами Системы SOC, из информации об ИИ, переданной Исполнителем, или общедоступных источников информации.

По результатам анализа предоставленной информации Заказчик подтверждает факт возникновения инцидента ИБ (с указанием принятых мер реагирования), сообщает о ложном срабатывании правила корреляции, необходимости внесения исключений или о легитимности инцидента ИБ, либо запрашивает дополнительную информацию.

При отсутствии обратной связи от Заказчика в течение 8-ми календарных дней, инцидент ИБ закрывается в ЛК SOC с соответствующим статусом и может быть повторно открыт при обращении Заказчика.

Связанные инциденты ИБ закрываются в Системе SOC с соответствующей пометкой с указанием основного инцидента ИБ без оповещения Заказчика, информация о нем и причинах его закрытия предоставляется в рамках регулярной отчетности Системы SOC, а также доступна в ЛК SOC.

Ограничения работ:

* Исполнитель обрабатывает только инциденты ИБ, зафиксированные в системах-источниках;
* время реакции Исполнителя на инцидент ИБ отсчитывается от момента фиксации инцидента ИБ в Системе SOC;
* время анализа Исполнителем инцидента ИБ может быть увеличено в случае, если Заказчик запросил обработку большого количества данных в Системе SOC или системах-источниках;
* время реакции Исполнителя не включает в себя работы Заказчика по верификации и оценке полноты предоставленных Исполнителем данных.
  1. Превышение допустимого Заказом количества EPS.

В случае превышения количества EPS, указанных в Заказе, Заказчик дополнительно оплачивает каждый использованный пакет по 100 EPS.

Стороны согласовали, что предельно допустимая нагрузка на Систему SOC не должна превышать среднего значения EPS, указанного в Заказе.

* 1. Расширенный экспертный анализ по инцидентам ИБ.

При необходимости проведения дополнительного экспертного анализа по инцидентам ИБ, зафиксированным в системах-источниках, Заказчик инициирует через ЛК SOC (при отсутствии доступа к ЛК SOC, через электронную почту) запрос Исполнителю. При обработке запроса сотрудник Исполнителя проводит сбор следующей информации у Заказчика, который предоставляет следующие данные:

* местонахождение структурного подразделения Заказчика, в котором зафиксирован инцидент ИБ;
* дата и время возникновения инцидента ИБ;
* ИС, IP-адреса, MAC-адреса, FQDN-имена хостов, относящихся к инциденту ИБ;
* контактные данные сотрудника (ФИО, тел., адрес эл. почты), ответственного за эксплуатацию систем-источников, которые относятся к инциденту ИБ;
* критичность инцидента ИБ.

После сбора первичной информации по инциденту ИБ лицо, ответственное за расследование инцидента ИБ со стороны Исполнителя, приступает к сбору расширенной информации по инциденту ИБ, которая включает в себя:

* сбор дополнительных данных о фигурантах инцидента ИБ (события ИБ с фигурантами в других информационных, инфраструктурных системах-источниках, СЗИ за предшествующий период глубиной от 1 месяца; имеющиеся доступы/роли/привилегии; наличие ранее зафиксированных инцидентов ИБ);
* сбор дополнительных данных об информационных системах участниках инцидента ИБ (зафиксированные события и инциденты ИБ, результаты автоматизированных сканирований, проверок и аудитов);
* другая дополнительная информация.

Данная работа ведётся совместно с Заказчиком. Качество зависит от данных, предоставляемых Заказчиком.

По результатам собранной информации проводится анализ инцидента ИБ.

В процессе сотрудник Исполнителя, устанавливает:

* хронологию событий, повлекших за собой возникновение инцидента ИБ;
* причины, из-за которых возник инцидент ИБ;
* ложность или истинность инцидента ИБ;
* последствия инцидента ИБ.

По итогам формируется отчёт о проделанной работе. Исполнитель, помимо анализа инцидента ИБ, установления системы-источника и причин, формирует набор технических рекомендаций, позволяющих предотвратить или снизить вероятность возникновения аналогичных инцидентов ИБ в дальнейшем.

Заказчик анализирует предоставленную ему информацию, принимает решение о применимости выданных рекомендаций в своей ИИ и реализует при необходимости предложенные технические мероприятия.

Предложенный механизм предотвращения анализируется Исполнителем и Заказчиком на возможность повторного применения при возникновении инцидента ИБ и фиксируется в Системе SOC, описывающей профиль Услуги.

Ограничения работ:

* количество запросов на расширенный экспертный анализ по инцидентам ИБ не должно превышать установленное Заказом;
* работы проводятся удалённо. Расследование инцидентов ИБ на площадке Заказчика оценивается и оплачивается отдельно. В стоимость включаются командировочные расходы. Детали командировки оговариваются отдельно;
* время выработки рекомендаций может быть увеличено по согласованию Сторон в случае, если выданные Исполнителем рекомендации оказались неприменимыми на ИИ Заказчика в силу особенностей архитектуры, ресурсных либо бюджетных ограничений;
* выдаваемые Исполнителем рекомендации основываются на общих архитектурных и инфраструктурных положениях обеспечения ИБ и не включают в себя детализированных настроек специфического оборудования либо приложений Заказчика. Анализ применимости рекомендаций и разработка инструкций для специфических приложений является ответственностью уполномоченных специалистов Заказчика.
  1. Подключение новых систем-источников к Системе SOC.

Заказчик инициирует через ЛК SOC (при отсутствии доступа к ЛК SOC, через электронную почту) запрос на подключение дополнительной системы-источника к Системе SOC, предоставляя следующую информацию:

* + - * + тип новой системы-источника;
        + информация по получению данных с новой системы-источника (ip-адрес, данные доступа);
        + список правил обнаружения инцидентов ИБ, которые необходимо контролировать в рамках данной системы-источника;
        + дополнительная информация, необходимая для определения системы-источника в правилах обнаружения инцидентов ИБ.

Исполнитель, совместно с Заказчиком, оценивает техническую возможность сбора требуемых событий ИБ с новой системы-источника и согласовывает механизм и способ подключения.

Исполнитель оценивает достаточность предоставленной информации для выполнения работ и вносит изменения в правила обнаружения инцидентов с учетом подключения новой системы-источника.

Заказчик организовывает сетевой доступ и передачу данных между новой системой-источником и коллекторами, осуществляет настройку сбора событий ИБ на новой системе-источнике с передачей событий ИБ на коллекторы.

Исполнитель и Заказчик выполняют требуемые настройки в Системе SOC и коллекторах для подключения новой системы-источника.

По завершению подключения и проверки работоспособности Исполнителем проводится изменение Системы SOC, описывающей профиль Услуги.

Ограничения работ:

* + - * + подключение новой системы-источника производится только в том случае, если количество EPS за текущий период не превышает количество EPS, указанных в Заказе;
        + подключение системы-источника производится только при наличии технической возможности получения событий ИБ, необходимых для реализации правил обнаружения инцидентов ИБ. Наличие технической возможности определяется Исполнителем с использованием консультаций администраторов новой системы-источника;
        + время работ по подключению зависит от своевременного выполнения работ на стороне Заказчика по настройкам передачи необходимых данных для анализа в Систему SOC. Исполнитель начинает выполнять работы только после организации Заказчиком передачи необходимых событий ИБ в Систему SOC;
        + Исполнитель определяет и согласовывает с Заказчиком необходимый уровень журналирования системы-источника и типы событий ИБ, для реализации требуемых правил корреляции. При отсутствии технической возможности использовать рекомендованный уровень журналирования Исполнитель совместно с Заказчиком определяет необходимость и порядок решения инцидентов ИБ.
  1. Отключение системы-источника от Системы SOC.

Заказчик инициирует через ЛК SOC (при отсутствии доступа к ЛК SOC, через электронную почту) запрос на отключение системы-источника, предоставляя следующую информацию:

* тип системы-источника;
* идентификатор системы-источника (IP-адрес, приложение).

Исполнитель проводит анализ существующих правил обнаружения инцидентов ИБ и информирует Заказчика в случае, если отключение системы-источника приводит к их модификации либо исключению из списка контролируемых инцидентов ИБ.

В случае необходимости Исполнитель и Заказчик выполняют работы по изменению состава инцидентов ИБ в Системе SOC, коллекторах и системы-источнике для его отключения.

Ограничения работ:

* время, необходимое Заказчику для согласования изменений в списке контролируемых правил обнаружения инцидентов ИБ и проведение требуемых работ на системе-источнике для ее отключения не учитывается в метриках отключения системы-источника.
  1. Реализация новых правил обнаружения инцидентов ИБ по запросу Заказчика.

Заказчик инициирует через ЛК SOC (при отсутствии доступа к ЛК SOC, через электронную почту) запрос на реализацию нового правила обнаружения инцидентов ИБ, предоставляя следующую информацию:

* + - * + общее описание и критерии возникновения инцидента ИБ;
        + тип систем-источников для обнаружения инцидента ИБ;
        + плановую критичность инцидента ИБ.

Исполнитель анализирует техническую возможность реализации правила корреляции в рамках ИИ Заказчика в Системе SOC, привлекая Заказчик для более детальной проработки правила корреляции.

Исполнитель и Заказчик согласовывают итоговое правило обнаружения инцидента ИБ, определяют его критичность и процесс взаимодействия по инциденту ИБ.

Исполнитель выполняет работы по реализации нового правила, производя настройки Системы SOC.

По завершению подключения и проверки работоспособности Исполнителем проводится изменение Системы SOC, описывающей профиль Услуги.

Ограничения работ:

* в случае, если реализация нового правила требует подключения дополнительных систем-источников, то для реализации данного правила требуется Заказчику сначала подключить эти системы-источники к Системе SOC;
* при подключении нового правила обнаружения инцидентов ИБ Заказчику выделяется тестовый период отладки инцидента ИБ (2 недели), в течение которого выявляемые по новому правилу инциденты ИБ обрабатываются согласно метриками инцидента ИБ низкой критичности и происходит дополнительная доработка правила. По результатам успешного завершения тестового периода критичность сценария устанавливается в соответствии с согласованным уровнем. Период отладки может быть изменен по согласованию Сторон.
  1. Реализация новых правил обнаружения инцидентов ИБ по инициативе Исполнителя.

Исполнитель информирует Заказчика о расширении списка правил обнаружения инцидентов ИБ в Системе SOC, указывая следующую информацию:

* общее описание и критерии возникновения инцидента ИБ;
* тип систем-источников для обнаружения инцидента ИБ;
* плановую критичность инцидента ИБ.

Заказчик анализирует предоставленную информацию и принимает решение о включении новых правил в список контролируемых. В случае, если адаптация сценариев под требования Заказчика требует дополнительной информации, Заказчик предоставляет ее Исполнителю.

Исполнитель включает контроль инцидентов ИБ по новым правилам обнаружения инцидентов ИБ для ИИ Заказчика, производя необходимые настройки Системы SOC.

По завершению активации и проверки работоспособности Исполнителем проводится изменение Системы SOC, описывающей профиль Услуги.

Ограничения работ:

* в случае, если реализация правила требует подключения дополнительных систем-источников, то для реализации данного правила требуется Заказчику сначала подключить эти системы-источники к Системе SOC;
* при подключении нового правила обнаружения инцидентов ИБ Заказчику выделяется тестовый период отладки инцидента ИБ (2 недели), в течение которого выявляемые по новому правилу инциденты ИБ обрабатываются согласно метриками инцидента ИБ низкой критичности и происходит дополнительная доработка правила. По результатам успешного завершения тестового периода критичность сценария устанавливается в соответствии с согласованным уровнем. Период отладки может быть изменен по согласованию Сторон.
  1. Управление критичностью правил обнаружения инцидентов ИБ или процесса взаимодействия.

Заказчик инициирует через ЛК SOC (при отсутствии доступа к ЛК SOC, через электронную почту) запрос на изменение уровня критичности или процесса взаимодействия при обработке инцидента ИБ, предоставляя следующую информацию:

* + - * + название правила обнаружения;
        + новую плановую критичность (при необходимости);
        + новый алгоритм взаимодействия (при необходимости).

Исполнитель проводит анализ предоставленной Заказчиком информации на достаточность и возможность реализации в Системе SOC.

Исполнитель проводит необходимые работы и вносятся изменения в Систему SOC, описывающей профиль Услуги.

Ограничения работ:

* количество правил обнаружения инцидентов ИБ с высокой степенью критичности не может превышать 35 (тридцати пяти) процентов от общего числа правил обнаружения инцидентов ИБ.

**7.9** Регламент взаимодействия Корпоративного центра ГосСОПКА Исполнителя и Заказчика при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак с ЦЗИиСС описывается в Приложении № 1.

Приложение № 1

**Регламент взаимодействия Корпоративного центра ГосСОПКА Исполнителя и Заказчика при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак с ЦЗИиСС**

**ОБЩИЕ ПОЛОЖЕНИЯ**

**Назначение и область действия**

КЦ ГосСОПКА взаимодействует с ЦЗИиСС посредством направления сведений и обращений через каналы НКЦКИ.

В ходе организованного в рамках Услуги для Заказчика его информационного взаимодействия с НКЦКИ ГосСОПКА, через КЦ ГосСОПКА, осуществляется обмен сведениями с ГосСОПКА об ИИ, КИИ Заказчика, о КА и КИ в ИИ и КИИ Заказчика, индикаторах компрометации и методических рекомендациях НКЦКИ ГосСОПКА для Заказчика по обнаружению, предупреждению и ликвидации последствий типовых КА на ОИИ и ОКИИ Заказчика.

Исполнителем организовывается подключение систем-источников ОИИ и (или) ОКИИ Заказчика к Системе SOC, в соответствии с Техническим заданием, для организации информационного взаимодействия Заказчика через КЦ ГосСОПКА с НКЦКИ.

Заказчику в КЦ ГосСОПКА предоставляется доступ в ЛК SOC для взаимодействия Заказчика с НКЦКИ. Передача информации Заказчика в ГосСОПКА и Заказчику из ГосСОПКА организовывается через ЛК SOC.

Регламент разработан для осуществления взаимодействия между КЦ ГосСОПКА и Заказчиком при осуществлении информационного обмена Заказчика в области обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, находящиеся в зоне ответственности Заказчика, с ЦЗИиСС. Обмен информацией происходит через предоставленный Заказчику ЛК SOC, развёрнутый на стороне Исполнителя. Регламент устанавливает основные положения по процессу данного взаимодействия между Заказчиком и Исполнителем.

Исполнитель обеспечивает для Заказчика предоставление ЛК SOC для взаимодействия Заказчика с НКЦКИ и функционирование канала между ЛК SOC и НКЦКИ.

Заказчик самостоятельно осуществляет размещение информации для передачи в ГосСОПКА в предоставленном Исполнителем Заказчику ЛК SOC для взаимодействия Заказчика с НКЦКИ, самостоятельно принимает решение о необходимости информирования НКЦКИ о КА и КИ в ИИ и КИИ Заказчика, о чем должен уведомлять КЦ ГосСОПКА посредством направления сообщения по каналам взаимодействия, указанным в разделе 4 Регламента.

Все работники Сторон, участвующие в процессах взаимодействия по Регламенту, должны быть ознакомлены с Регламентом.

**Нормативные ссылки**

Регламент разработан в соответствии с требованиями следующих нормативно-правовых актов:

* Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
* Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»;
* Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
* Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам»;
* Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
* Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;
* Приказ ФСБ России от 19 июня 2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;
* Приказ ФСБ России от 6 мая 2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».

**1. Передача информации о КА и КИ в ЦЗИиСС**

* 1. Передача информации Заказчика о КА и КИ в ИИ и КИИ Заказчика и принятых им мерах по ликвидации последствий КА в НКЦКИ происходит путём регистрации и заполнения Заказчиком необходимых сведений о КА на предоставленном Исполнителем ЛК SOC для взаимодействия Заказчика с НКЦКИ.
  2. Уведомления о получении информации о КА и КИ от НКЦКИ поступают в КЦ ГосСОПКА и в автоматическом режиме в течение 2 дней с даты поступления в КЦ ГосСОПКА передаётся Заказчику путём размещения в предоставленном Исполнителем ЛК SOC для взаимодействия Заказчика с НКЦКИ.

**2. Функции участников**

* 1. В Функции Исполнителя входит:
     1. Прием КЦ ГосСОПКА от ЦЗИиСС информации об актуальных угрозах безопасности и необходимых мерах по противодействию им, о средствах и способах проведения КА и методах их обнаружения, предупреждения и противодействия им, а также о признаках КИ.
     2. Информирование Заказчика о рекомендациях, полученных КЦ ГосСОПКА от ЦЗИиСС, в рамках п. 2.1.1 Регламента, в следующем порядке: путём направления Заказчику указанных рекомендаций с использованием каналов взаимодействия, указанных в разделе 4 Регламента.
     3. Предоставление Заказчикудоступа к ЛК SOC для взаимодействия Заказчика с НКЦКИ.
  2. В функции Заказчикавходит:
     1. Предоставление в ЦЗИиСС через ЛК SOC и в КЦ ГосСОПКА с использованием каналов взаимодействия, указанных в разделе 4 Регламента, следующих сведений: о составе и характеристиках ИР Заказчика, находящихся в его зоне ответственности, а также своевременная актуализация таких сведений (в течение 10 рабочих дней с даты любых изменений в преданных ранее Заказчиком сведениях).
     2. Предоставление сведений о выявляемых КА и КИ в ИР, находящихся в зоне ответственности Заказчика, а также информации о предпринятых мерах и результатах реагирования на такие КА и КИ через ЛК SOC в ЦЗИиСС и в КЦ ГосСОПКА с использованием каналов взаимодействия, указанных в разделе 4 Регламента.
     3. Своевременное предоставление в ЦЗИиСС через ЛК SOC и в КЦ ГосСОПКА с использованием каналов взаимодействия, указанных в разделе 4 Регламента, а также поддержание в актуальном состоянии сведений об ответственных лицах, на которых возложены обязанности по взаимодействию с НКЦКИ.
     4. Предоставление в ЦЗИиСС через ЛК SOC, а также в КЦ ГосСОПКА с использованием каналов взаимодействия, указанных в разделе 4 Регламента, сведений об изменении внешних сетевых реквизитов ИР Заказчика, в срок не более 2 рабочих дней с момента их изменения.
     5. Предоставление в ЦЗИиСС, через ЛК SOC, а также в КЦ ГосСОПКА с использованием каналов взаимодействия, указанных в разделе 4 Регламента, сведений об ИР (наименование ИР, используемое телекоммуникационное оборудование и программное обеспечение, а также общее и специальное программное обеспечение).

2.3. Сроки предоставления Заказчиком информации, указанной в настоящем разделе Регламента, приведены в разделе 6 Регламента.

1. **Перечень передаваемой информации**

В рамках взаимодействия между участниками информационного обмена: Заказчиком и ЦЗИиСС через ГосСОПКА, может передаваться информация:

* о КИ в ИР в соответствии с определенными НКЦКИ форматами, в том числе требующих содействия в реагировании со стороны ЦЗИиСС;
* о признаках КИ в соответствии с форматами, определенными НКЦКИ;
* о мерах, предпринятых для локализации КИ в ИР, а также о результатах этих мер;
* о выявленных угрозах безопасности информации, реализация которых может повлиять на штатное функционирование ИР и о необходимых мерах по противодействию им;
* о средствах и способах проведения КА и о методах их обнаружения, предупреждения и противодействия им;
* содержащая запросы на получение дополнительных сведений об угрозах безопасности информации и вредоносной активности;
* содержащая сведения об ИР.

Информационные сообщения и запросы, передаваемые по каналам взаимодействия, не должны содержать информацию, составляющую охраняемую законом Российской Федерации тайну.

1. **Каналы взаимодействия**

При передаче информации, указанной в разделах 2 и 3 Регламента, в качестве основных каналов передачи информации в адрес ЦЗИиСС и ГосСОПКА Исполнителем используются:

* средства автоматизированного обмена информацией между Заказчиком и ГосСОПКА – ЛК SOC, на основе программного интерфейсаКЦ ГосСОПКА;
* электронная почта Заказчика и Исполнителя, предоставленные Сторонами.

В качестве дополнительных каналов передачи информации используются:

* телефонная связь, номерателефонов Заказчика и Исполнителя, предоставленные Сторонами.*.*

1. **Порядок взаимодействия участников информационного обмена**

Информации о КИ в информационных ресурсах, находящихся в зоне ответственности Заказчика, передаваемой Заказчиком в ЦЗИиСС, в ТИ НКЦКИ присваивается уникальный идентификатор КИ.

**6. Сроки предоставления информации**

Информация о КИ, связанном с функционированием значимых объектов КИИ, в соответствии с пунктом 4 Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденного приказом ФСБ России от 19 июня 2019 г. № 282, направляется Заказчиком в НКЦКИ и в КЦ ГосСОПКА в срок не позднее **3-х часов** с момента обнаружения КИ.

Информация о КИ, связанном с функционированием иных ИР, не указанных выше, т.е. об ОИИ передаётся Заказчиком в НКЦКИ и в КЦ ГосСОПКА в срок не позднее **24-х часов** с момента его обнаружения.

Сведения об изменении внешних сетевых реквизитов ИР передаются Заказчиком в ЦЗИиСС и КЦ ГосСОПКА в срок не более **2-х рабочих дней** с момента указанных изменений.

Передача Заказчиком сведений в ЦЗИиСС и КЦ ГосСОПКА об ИР (наименование ИР, используемое телекоммуникационное оборудование и программное обеспечение, а также общее и специальное программное обеспечение) осуществляется в течение **10-ти рабочих дней** с момента включения (изменения) ИР.

**3. Порядок проведения запроса предложений Инструкции по подготовке Предложений**

1. **Общий порядок проведения открытого запроса предложений**

3.1.1. С учетом положений пункта 1.1.5 открытый запрос предложений проводится в следующем порядке:

* 1. Извещение к участию в открытом запросе предложений, осуществляется однократно в течение всей процедуры Запроса предложений;
  2. Предоставление Документации по запросу предложений исполнителям (подраздел 3.3), может повторяться на каждом из этапов Запроса предложений;
  3. Подготовка Участниками своих Предложений и разъяснение Заказчиком Документации по запросу предложений, если необходимо (подраздел 3.4), повторяется на каждом из этапов Запроса предложений;
  4. Подача Предложений и их прием (подраздел 3.6), повторяется на каждом из этапов Запроса предложений;
  5. Оценка Предложений (подраздел 3.8), повторяется на каждом из этапов Запроса предложений;
  6. Принятие решения о проведении следующих этапов Запроса предложений или определение Победителя (подраздел 3.9), повторяется на каждом из этапов Запроса предложений;
  7. Подписание Договора (подраздел 3.10), осуществляется однократно в течение всей процедуры Запроса предложений;

1. **Извещение к участию в открытом запросе предложений**

3.2.1 Извещение к участию в открытом запросе предложений было опубликовано в порядке, указанном в пункте [1.1.1.](#bookmark3)

1. **Предоставление Документации по запросу предложений Исполнителям**
2. Исполнители могут получить Документацию по открытому запросу предложений в открытом доступе, в порядке, указанном в извещении к участию в открытом запросе предложений, расположенной на сайте [www.staves.ru](http://www.staves.ru) в разделе закупки/текущие закупки/2025/проведение процедур закупок в 2025г.
3. Порядок предоставления Документации по открытому запросу предложений на последующие этапы (пункт 1.1.5), в случае их проведения, будет доведен до сведения Участников дополнительно.

**3.4 Подготовка Предложений**

3.4.1 **Общие требования к Предложению**

1. Участник должен подготовить Предложение, включающее:
2. Письмо о подаче оферты (согласно разделу 5 Документации).
   1. Коммерческое предложение в виде расчета стоимости услуг согласно техническому заданию (Раздел 2 Документации).
   2. документы, подтверждающие соответствие Участника требованиям настоящей Документации по запросу предложений (подраздел 3.5 Документации).
3. На последующих этапах данной процедуры Запроса предложений (пункт 1.1.5) в случае их проведения состав документов, включаемых в Предложение, а требования к ним, могут измениться.
4. Участник имеет право подать только одно Предложение. В случае нарушения этого требования все Предложения такого Участника отклоняются без рассмотрения по существу.
5. Никакие исправления в тексте Предложения не имеют силу, за исключением тех случаев, когда эти исправления заверены рукописной надписью «исправленному верить» и собственноручной подписью уполномоченного лица, расположенной рядом с каждым исправлением.

**3.4.2** **Требования к сроку действия Предложения**

3.4.2.1 Предложение должно быть действительно не менее чем 60 календарных дней со дня, следующего за днем окончания приема Предложений.

3.4.2.2 Указание меньшего срока действия может являться основанием для отклонения предложения Участника.

1. **Требования к языку Предложения**
2. Все документы, входящие в Предложение, должны быть подготовлены на русском языке за исключением нижеследующего.
3. Документы, оригиналы которых выданы Участнику третьими лицами на ином языке, могут быть представлены на языке оригинала при условии, что к ним приложен перевод этих документов на русский язык (в специально оговоренных случаях — апостилированный). При выявлении расхождений между русским переводом и оригиналом документа на ином языке Заказчик будет принимать решение на основании перевода.
4. Заказчик вправе не рассматривать документы, не переведенные на русский язык.
5. **Требования к валюте Предложения**

3.4.4.1 Все суммы денежных средств в документах, входящих в Предложение, должны быть выражены в российских рублях.

1. **Разъяснение Документации по запросу предложений**
2. Участники вправе обратиться к Заказчику за разъяснениями настоящей Документации по запросу предложений. Запросы на разъяснение Документации по запросу предложений должны подаваться в письменной форме за подписью руководителя организации или иного ответственного лица Участника.
3. Заказчик ответит на любой вопрос, который он получит не позднее, чем за 1 день до истечения срока приема Предложений.
4. **Продление срока окончания приема Предложений**
5. При необходимости Заказчик имеет право продлевать срок окончания приема Предложений с уведомлением на официальном сайте.
6. **Начальная (предельная) цена**
7. Начальная (предельная) цена – 3 835 000 (Три миллиона восемьсот тридцать пять тысяч) рублей без НДС.
8. Комиссия оставляет за собой право отклонить Предложения с ценами, существенно превышающими цены, сложившиеся на рынке аналогичных услуг.

3.4.7.3 Комиссия оставляет за собой право отклонить Предложения с ценами, завышенными за счет предложения условий, существенно превышающих требования настоящей Документации.

**3.5** **Требования к Участникам. Подтверждение соответствия предъявляемым требованиям**

3.5.1 **Требования к Участникам**

1. Участвовать в процедуре запроса предложений может любое юридическое или физическое лицо (индивидуальный предприниматель). Участие коллективных участников не допускается.
2. На последующих этапах Запроса предложений (пункт 1.1.5), в случае их проведения, требования к Участникам и к документам, подтверждающих их соответствие указанным требованиям, могут быть изменены с уведомлением всех участников.
3. Чтобы претендовать на победу в данной процедуре Запроса предложений и на право заключения Договора, Участник самостоятельно в целом должен отвечать следующим требованиям:
   1. Участник должен обладать необходимыми профессиональными знаниями и опытом, иметь ресурсные возможности (финансовыми, материально-техническими, производственными, трудовыми), управленческой компетентностью, опытом и репутацией;
   2. Участник должен обладать гражданской правоспособностью в полном объеме для заключения и исполнения Договора (должен быть зарегистрирован в установленном порядке и иметь соответствующие действующие лицензии на выполнение видов деятельности в рамках Договора);
   3. Участник не должен являться неплатежеспособным или банкротом, находится в процессе ликвидации, на имущество Участника в части, существенной для исполнения договора, не должен быть наложен арест, экономическая деятельность Участника не должна быть приостановлена.
   4. У Участника должна отсутствовать задолженность по начисленным налогам, сборам и иным обязательным платежам в бюджеты любого уровня или государственные внебюджетные фонды за прошедший календарный год.

**3.5.2** Требования к документам, подтверждающим соответствие Участника установленным требованиям

3.5.2.1 В связи с вышеизложенным Участник должен включить в состав Предложения следующие документы, подтверждающие его соответствие вышеуказанным требованиям:

а) фирменное наименование (наименование), сведения об организационно-правовой форме, о месте нахождения, почтовый адрес (для юридического лица), фамилия, имя, отчество, паспортные данные (копию паспорта для Физических лиц)., сведения о месте жительства (для физического лица), номер контактного телефона (по форме, раздел № 6) ;

б) полученную не ранее чем за шесть месяцев до дня размещения на официальном сайте закупок извещения о проведения процедуры закупки выписку из единого государственного реестра юридических лиц или заверенную копию такой выписки (нотариально или печатью организации и штампом «Копия верна» с подписью руководителя) (для юридических лиц), полученную не ранее чем за шесть месяцев до дня размещения на официальном сайте закупок извещения о проведения процедуры закупки выписку из единого государственного реестра индивидуальных предпринимателей или заверенную копию такой выписки (нотариально или штампом «Копия верна» с подписью руководителя) (для индивидуальных предпринимателей), копии документов, удостоверяющих личность (для иных физических лиц), надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица или физического лица в качестве индивидуального предпринимателя в соответствии с законодательством соответствующего государства (для иностранных лиц), полученные не ранее чем за шесть месяцев до дня размещения на официальном сайте закупок извещения о проведения процедуры закупки;

в) документ, подтверждающий полномочия лица на осуществление действий от имени юридического лица (копия решения о назначении или об избрании либо приказа о назначении физического лица на должность, в соответствии с которым такое физическое лицо обладает правом действовать от имени участника закупки и лица, выступающего на стороне участника закупки без доверенности (далее для целей настоящего раздела - руководитель). В случае, если от имени юридического лица действует иное лицо, заявка на участие должна содержать также соответствующую доверенность, заверенную печатью и подписанную руководителем юридического лица или уполномоченным этим руководителем лицом, либо нотариально заверенную копию такой доверенности. В случае, если указанная доверенность подписана лицом, уполномоченным руководителем, заявка на участие должна содержать также документ, подтверждающий полномочия такого лица;

г) копии учредительных документов (Устав для юридических лиц);

д) заверенную контрагентом копию свидетельства о внесении записи в единый государственный реестр юридических лиц – для юридических лиц, в единый государственный реестр индивидуальных предпринимателей – для индивидуальных предпринимателей;

е) заверенную контрагентом копию свидетельства о постановке на налоговой учет;

з) коммерческое предложение - расчеты согласно техническому заданию (раздел 2).

и) реестр договоров подобных работ

l) иные документы, которые, по мнению Участника, подтверждают его соответствие установленным требованиям (**иметь соответствующие лицензии и допуск к данным видам услуг согласно техническому заданию)**, с соответствующими комментариями, разъясняющими цель предоставления этих документов.

**3.6 Подача Предложений и их прием**

1. Участники должны обеспечить доставку своих Предложений в запечатанных конвертах в бумажной форме по адресу: 357633, Ставропольский край, г. Ессентуки, ул. Большевистская, 59 а, каб. 303, тел. (87934) 4-26-84.
2. Заказчик заканчивает принимать Предложения в 10 часов 00 минут (время московское) 14.05.2025 года. Предложения, полученные позже установленного выше срока, будут отклонены Заказчиком без рассмотрения по существу, независимо от причин опоздания.
3. При необходимости Заказчик имеет право продлевать срок окончания приема Предложений, установленный в п. 3.6.2, с уведомлением об этом всех Участников.
4. Заказчик ведет запись в журнале приема заявок на участие поступивших предложений.
5. Сведения о сроке и месте окончания приема Предложений на последующие этапы, в случае их проведения, будут доведены до сведения Участников дополнительно.
6. **Рассмотрение поступивших предложений.**

3.7.1 Процедура публичного вскрытия конвертов на бумажном носителе состоится в 12:00 часов (время московское) 14.05.2025 года. Место проведения процедуры вскрытия конвертов с заявками: Ставропольский край, г. Ессентуки, улица Большевистская, 59 а, конференц-зал управления ПАО «Ставропольэнергосбыт». Участник до момента окончания приема Предложений имеет право отозвать своё Предложение, направив в адрес Организатора соответствующее официальное заявление.

1. **Оценка Предложений и проведение переговоров**

**3.8.1** Общие положения

3.8.1.1 Оценка Предложений осуществляется Комиссией по запросу предложений и иными лицами (экспертами и специалистами), привлеченными Комиссией по запросу предложений.

1. Оценка Предложений включает отборочную стадию (пункт 3.8.2), проведение при необходимости переговоров (пункт 3.8.3) и оценочную стадию (пункт 3.8.4).
2. Порядок, критерии и методики оценки Предложений на последующие этапы (пункт 1.1.5), в случае их проведения, могут быть изменены. Это будет отражено в Документации по запросу предложений на последующие этапы с уведомлением участников, прошедших на этот этап.

**3.8.2** **Отборочная стадия**

1. В рамках отборочной стадии закупочная комиссия (далее - Комиссия по запросу предложений) проверяет:
   1. правильность оформления Предложений и их соответствие требованиям настоящей Документации по запросу предложений по существу;
   2. соответствие Участников требованиям настоящей Документации по запросу предложений;
2. В рамках отборочной стадии Комиссия по запросу предложений может запросить Участников разъяснения или дополнения их Предложений, в том числе представления отсутствующих документов. При этом Комиссия по запросу предложений не вправе запрашивать разъяснения или требовать документы, меняющие суть Предложения.
3. При проверке правильности оформления Предложения Комиссия по запросу предложений вправе не обращать внимания на мелкие недочеты и погрешности, которые не влияют на существо Предложения. Комиссия по запросу предложений с письменного согласия Участника также может исправлять очевидные арифметические и грамматические ошибки.
4. По результатам проведения отборочной стадии Комиссия по запросу предложений имеет право отклонить Предложения, которые:
   1. в существенной мере не отвечают требованиям к оформлению настоящей Документации по запросу предложений;
   2. поданы Участниками, которые не отвечают требованиям настоящей Документации по запросу предложений;
   3. содержат очевидные арифметические или грамматические ошибки, с исправлением которых не согласился Участник.
5. Проведение переговоров
6. После рассмотрения и оценки Предложений Заказчик вправе провести переговоры с любым из Участников по любому положению его Предложения.
7. Переговоры могут проводиться в один или несколько туров. Очередность переговоров устанавливает Заказчик. При проведении переговоров Заказчик будет избегать раскрытия другим Участникам содержания полученных Предложений, а также хода и содержания переговоров, т.е.:
   1. любые переговоры между Заказчиком и Участником носят конфиденциальный характер;
   2. ни одна из сторон переговоров не раскрывает никакому другому лицу никакой технической, ценовой или иной рыночной информации, относящейся к этим переговорам, без согласия другой стороны.
8. **Оценочная стадия**

3.8.4.1 В рамках оценочной стадии Комиссия по запросу предложений оценивает и сопоставляет Предложения с учетом результатов переговоров (пункт 3.8.3) и проводит их ранжирование по степени предпочтительности для Заказчика, исходя из следующих критериев:

а) Цена договора – цена оказания услуг, предложенная участником, при условии, что она не должна превышать предельную сумму - (значимость критерия 50%)

б) Квалификация участника: наличие опыта (приложить ряд соответствующих лицензий и допусков к данным видам услуг) - (значимость критерия 25%);

в) Надежность и деловая репутация Участника (приложить реестр договоров подобных услуг) - (значимость критерия 25%);

**3.9** **Принятие решения о проведении следующих этапов Запроса предложений или определение Победителя**

3.9.1 Комиссия по запросу предложений на своем заседании принимает решение либо по определению Победителя и заключению Договора (пункт 1.1.5), либо по проведению дополнительных этапов Запроса предложений, либо по завершению данной процедуры Запроса предложений без определения Победителя:

* + 1. в случае если Предложение какого-либо из Участников окажется существенно лучше Предложений остальных Участников, и это Предложение полностью удовлетворит Заказчика, Заказчик определит данного Участника Победителем и подпишет с ним Договор (подраздел 3.10); процедура Запроса предложений на этом будет завершена;
    2. в случае если самое лучше Предложение не удовлетворит Заказчика полностью, Комиссия по запросу предложений вправе принять решение о проведении дополнительных этапов Запроса предложений и внесении изменений в условия Запроса предложений;
    3. если, по мнению Комиссии по запросу предложений возможностей для улучшения Предложений Участников не предвидится и проведение дальнейших этапов бессмысленно, Комиссия вправе принять решение о прекращении процедуры Запроса предложений.

3.9.2 Решение Комиссии по открытому запросу предложений оформляется протоколом заседания Закупочной комиссии.

1. **Подписание Договора**
2. Договор между Заказчиком и Победителем подписывается в течение 10 (десяти) дней с момента определения Победителя открытого запроса предложений.
3. Условия Договора определяются в соответствии с требованиями Заказчика и пунктом [1.2.5.](#bookmark6)
4. **Уведомление Участников о результатах запроса предложений**
5. Организатор открытого запроса предложений опубликует информацию о результатах открытого запроса предложений на официальном сайте ПАО «Ставропольэнергосбыт»
6. Если между моментом подписания Протокола и Договора изменился Победитель (например, вследствие отказа), то Победителем запроса предложения признаётся участник, занявший второе место в итоговой ранжировке заявок.

**4. Проект договора**

**Договор на оказание услуг № \_\_\_\_\_\_\_**

г. Ессентуки \_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ г.

**Публичное акционерное общество «Ставропольэнергосбыт»**, именуемое в дальнейшем «Заказчик», в лице исполнительного директора Салпагарова Игоря Борисовича, действующего на основании доверенности от 23 сентября 2024 г. (зарегистрирована в реестре за № 26/118-н/26-2024-1-1710, удостоверенной врио нотариуса Ессентукского городского нотариального округа Ставропольского края РФ Созоновой Е.М.), с одной стороны, и **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, именуемое в дальнейшем «Исполнитель», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, именуемые в дальнейшем «Стороны», подписали Договор на оказание услуг № \_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_ (далее – Договор) о нижеследующем:

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ
   1. **Информационная безопасность (ИБ)** – сохранение конфиденциальности, целостности и доступности информации.
   2. **Событие ИБ** – выявленное состояние системы, услуги или сети Заказчика, указывающее на возможное нарушение политики обеспечения ИБ или сбой мер обеспечения ИБ, или ранее неизвестная ситуация, которая может иметь отношение к вопросам ИБ.
   3. **ИИС** – информационные инфраструктурные сервисы
   4. **Security operation center (SOC)** –центр оперативного мониторинга событий ИБ Исполнителя, реализующий Услугу.
   5. **Инцидент ИБ** – срабатывание одного или нескольких правил корреляции, не сопровождаемых наличием связных событий ИБ, достоверно указывающих на ложное срабатывание, или подозрительная активность, замеченная сотрудниками SOC в процессе работы.
   6. **Система SOC** –программное обеспечение и/или аппаратно-программный комплекс SOC, предназначенные для автоматизированного сбора событий ИБ, обнаружения и регистрации инцидентов ИБ и последующего реагирования на них.
   7. **Правило корреляции** – соотнесение между собой в Системе SOC событий ИБ, удовлетворяющих определенным условиям с целью обнаружения инцидентов ИБ. Правила корреляции являются коммерческой тайной Исполнителя.
   8. **Услуга** – услуга по мониторингу и реагированию на инциденты ИБ, представляющая собой обеспечение круглосуточного мониторинга событий ИБ, проведения их анализа, своевременного обнаружения и разрешение инцидентов ИБ, а также организацию информационного взаимодействия Заказчика с ГосСОПКА через КЦ ГосСОПКА.
   9. **ГосСОПКА** – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
   10. **КЦ ГосСОПКА** – корпоративный центр ГосСОПКА Исполнителя, являющийся частью Системы SOC.
   11. **НКЦКИ** –Национальный координационный центр по компьютерным инцидентам.
   12. **Реагирование на инцидент ИБ** – структурированная совокупность действий Исполнителя, направленная на установление деталей инцидента ИБ и информирование о нем Заказчика.
   13. **СЗИ** – средства защиты информации Заказчика.
   14. **БД** – база данных.
   15. **ИР** – информационные ресурсы.
   16. **Хост источника** – оконечные устройства Заказчика, на которых настроена отправка событий ИБ в Систему SOC (например, конкретный сервер или приложение).
   17. **Системы-источники** – совокупность хостов-источников (серверов, приложений), объединённых по функциональному назначению, например, Система антивирусной защиты (может состоять из нескольких серверов БД), Система документооборота (может состоять из нескольких серверов-приложений).
   18. **Коллектор** – централизованный сервер, аккумулирующий события ИБ с различных систем-источников, расположенный в инфраструктуре Заказчика и сопровождаемый силами Заказчика.
   19. **Личный кабинет SOC (ЛК SOC)** – информационный портал Исполнителя, предназначенный для взаимодействия Заказчика и SOC, предоставления аналитической и отчетной информации, а также взаимодействия Заказчика с ГосСОПКА, являющийся частью Системы SOC.
   20. **Event per second (EPS)** – события ИБ в секунду, передаваемые в Систему SOC.
   21. **Технологическое окно** – запланированный период времени для проведения технических работ, в течение которого ЛК SOC будет недоступен.
   22. **Простой** – недоступность ЛК SOC для Заказчика.
   23. **Заказ** – выбираемый Заказчиком набор параметров и опций Услуги, содержащий информацию об оказываемой Услуге, включающий её стоимость и срок действия (период оказания). Заказ является неотъемлемой частью Договора.
   24. **Отчётный период** – период с первого по последнее число соответствующего календарного месяца, в котором были оказаны Услуги.
   25. **Информационная инфраструктура (ИИ)** – информационная инфраструктура Заказчика.
   26. **ОИИ** – объект информационной инфраструктуры Заказчика.
   27. **Критическая информационная инфраструктура (КИИ)** – объекты критической информационной инфраструктуры Заказчика, а также сети электросвязи, используемые для организации взаимодействия таких объектов.
   28. **Объект критической информационной инфраструктуры (ОКИИ)** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления КИИ Заказчика.
   29. **Компьютерная атака (КА)** – целенаправленное воздействие программных и (или) программно-аппаратных средств на ОКИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.
   30. **Компьютерный инцидент (КИ)** – факт нарушения и (или) прекращения функционирования ОКИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате КА.
   31. **ЦЗИиСС** – Центр защиты информации и специальной связи Федеральной службы безопасности Российской Федерации.
   32. **Virtual private network (VPN)** – технология, позволяющая обеспечить одно или несколько сетевых соединений поверх другой сети, с повышенным уровнем защиты благодаря использованию средств криптографии.
   33. **Demilitarized Zone (DMZ)** – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных.
2. ПРЕДМЕТ ДОГОВОРА
   1. По поручению Заказчика в период действия настоящего договора Исполнитель обязуется оказывать услуги по мониторингу и реагированию на инциденты ИБ, представляющих собой обеспечение круглосуточного мониторинга событий ИБ, проведения их анализа, своевременного обнаружения и разрешения инцидентов ИБ, а также организацию информационного взаимодействия Заказчика с ГосСОПКА через КЦ ГосСОПКА, в соответствии с условиями Договора и соответствующего Заказа к Договору, подписанного Заказчиком и Исполнителем.
   2. Услуга, включая отдельные опции и параметры, заказывается Заказчиком путем формирования Заказа, подписываемого Заказчиком и Исполнителем, и являющегося неотъемлемой частью Договора.
   3. Заказчик обязуется уведомлять Исполнителя о планируемых и проводимых работах, затрагивающих взаимодействие систем-источников с Системой SOC, КЦ ГосСОПКА, и влияющих на полноту передаваемых данных от систем-источников и в ГосСОПКА.
   4. Исполнитель не несёт ответственность перед Заказчиком:

* за любые неисправности, возникшие на оборудовании Заказчика и повлекшие за собой сбой в передаче событий ИБ в Систему SOC, КЦ ГосСОПКА;
* за несоблюдение Заказчиком пункта 2.3 Договора и его последствия.

Размер возможной ответственности Исполнителя по Договору в любых случаях ограничивается реальным, действительным, документально подтверждённым Заказчиком ущербом, наступившим в результате доказанных судебными актами виновных действий Исполнителя.

* 1. Услуги оказываются c даты подписания Сторонами Протокола об успешном подключении Услуги, составляемого по форме, приведённой в Приложении № 2 к Договору.

1. ОПИСАНИЕ УСЛУГИ
   1. Порядок оказания Услуг описан в Приложениях № 1 и № 4 к Договору.
   2. При необходимости Заказчик может заказать дополнительные опции и параметры Услуг, перечень которых указывается в Заказе.
2. ТАРИФИКАЦИЯ УСЛУГИ
   1. Схема тарификации предусматривает разовый инсталляционный платеж за организацию подключения к Системе SOC и фиксированный ежемесячный платеж в размере, определяемом в соответствии с заказанными параметрами и опциями Услуг, указанными в Заказе. Оплата разового инсталляционного платежа производится Заказчиком на основании счета выставленного Исполнителем, который должен быть оплачен в срок, указанный в счете, выставляемом в течение 10 (десяти) рабочих дней с даты окончания первого Отчетного периода оказания Услуг.
   2. Общая стоимость услуг по договору составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ руб., из которых инсталляционный платеж в размере \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ руб., фиксированный ежемесячный платеж в размере \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ руб.
   3. Договор предусматривает постоплатную систему расчетов.

Заказчик производит оплату за фактически оказанные Услуги в Отчетном периоде после подписания Акта сдачи-приемки оказанных услуг в течение 20 (двадцати) рабочих дней с момента выставления счета Исполнителем Оплата производится в соответствии с перечнем, объемом потребленных Заказчиком Услуг и тарифами, установленными соответствующими Заказами. Оплата стоимости Услуг осуществляется Заказчиком на расчетный счет Исполнителя, указанный в п.13 Договора.

* 1. В случае, если Услуга была оказана за неполный Отчётный период и, если это произошло не вследствие неисполнения/ненадлежащего исполнения Заказчиком его обязательств, стоимость Услуг за соответствующий Отчётный период рассчитывается пропорционально количеству дней, в течение которых была оказана Услуга в таком Отчётном периоде.
  2. При не поступлении в срок на счет Исполнителя денежных средств, достаточных для оплаты оказанных Услуг, Исполнитель вправе ограничить Объем предоставляемых Услуг или полностью прекратить предоставление Услуг. Исполнитель вправе устанавливать лимиты (пределы) кредитования для Заказчика в рамках Договора, при достижении которых Исполнитель имеет право ограничить или прекратить оказание Услуг, соответственно, и/или выставить внеочередной счет за фактически оказанные Услуги, который должен быть оплачен в срок, указанный Исполнителем. Размер лимита (предела) кредитования может определяться Исполнителем в зависимости от перечня, объема и стоимости используемых Услуг и иных данных. В случае поступления на счет Исполнителя излишних сумм, уплаченных Заказчиком по выставленному счету, указанные излишние суммы используются для расчетов за Услуги, оказанные Исполнителем за иной Отчетный период.
  3. Обязательство Заказчика по оплате Услуг считается исполненным с момента поступления денежных средств на расчетный счет Исполнителя. Положения данного пункта применяются ко всем случаям платежей Заказчика по Договору.

1. ОТВЕТСТВЕННОСТЬ СТОРОН
   1. За невыполнение положений Договора Стороны несут ответственность в соответствии с законодательством России и Договором.
   2. Сторона Договора, право которого нарушено, может требовать возмещения причиненного ей документально подтвержденного реального ущерба.
   3. В случае нарушения Заказчиком срока оплаты Услуг Исполнитель вправе требовать уплаты пени в размере 0,1 % (ноль целых одна десятая процента) от неуплаченной суммы за каждый день просрочки.
   4. В случае нарушения Исполнителем условий договора Заказчик вправе требовать уплаты пени в размере 0,1 % (ноль целых одна десятая процента) от стоимости не оказанных услуг за каждый день просрочки.
   5. Ни одна мера ответственности не считается начисленной и не подлежит оплате, если Сторона, имеющая право требовать ее уплаты, не направляет другой Стороне письменное требование о её уплате.
2. ПОРЯДОК СДАЧИ-ПРИЕМКИ УСЛУГ
   1. Не позднее 10 (десяти) рабочих дней с момента окончания Отчетного периода Исполнитель предоставляет Заказчику Акт сдачи-приемки оказанных услуг, выполненных на основании соответствующих Заказов, за Отчетный период в 2 (двух) экземплярах, счет-фактуру и счет. Вместо Акта сдачи-приемки оказанных услуг и счета-фактуры Исполнителем может быть предоставлен Универсальный передаточный документ (далее – УПД). Вышеуказанные документы могут быть направлены посредством системы электронного документооборота (ЭДО).
   2. Заказчик в течение 5 (пяти) рабочих дней обязан подписать указанный Акт / УПД или направить мотивированный отказ от подписания Акта / УПД, в письменной форме, с указанием списка претензий и их подробного обоснования, неточностей или ошибок, допущенных Исполнителем, в противном случае Услуги считаются принятыми Заказчиком в полном объеме без замечаний и подлежат оплате.
3. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ (ФОРС-МАЖОР)
   1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств в случае, если такое неисполнение явилось следствием обстоятельств непреодолимой силы, то есть событий, которые нельзя было предвидеть или предотвратить. К таким событиям относятся: стихийные бедствия, военные действия, принятие государственными органами или органами местного самоуправления нормативных или правоприменительных актов и иные действия, находящиеся вне разумного предвидения и контроля Сторон.
   2. При наступлении обстоятельств непреодолимой силы каждая Сторона должна не позднее 5 (пяти) рабочих дней с момента наступления таких обстоятельств известить о них в письменном виде другую Сторону. Извещение должно содержать данные о характере обстоятельств, оценку их влияния на возможность исполнения Стороной своих обязательств, а также предполагаемые сроки их действия.
   3. В случае наступления обстоятельств непреодолимой силы срок выполнения Стороной обязательств отодвигается соразмерно времени, в течение которого действуют эти обстоятельства и их последствия.
   4. Если действие обстоятельств непреодолимой силы продолжается свыше одного месяца, Стороны проводят дополнительные переговоры для выявления приемлемых альтернативных способов исполнения Договора либо Договор подлежит расторжению в установленном порядке.
4. ЗАВЕРЕНИЯ ОБ ОБСТОЯТЕЛЬСТВАХ
   1. Стороны заверяют и гарантируют друг другу, что:
      1. Сторона является надлежащим образом, учрежденным и зарегистрированным юридическим лицом и имеет законное право осуществлять вид экономической деятельности, предусмотренный Договором (имеет надлежащий ОКВЭД).
      2. Исполнительный орган Стороны находится и осуществляет функции управления по месту нахождения (регистрации) юридического лица.
      3. Для заключения и исполнения Договора Стороны получили все необходимые согласия, одобрения и разрешения, получение которых необходимо в соответствии с действующим законодательством Российской Федерации, учредительными и локальными документами, а также не существует законодательных, подзаконных нормативных и индивидуальных актов, локальных документов, а также решений органов управления, запрещающих Сторонам или ограничивающих их право заключать и исполнять Договор.
      4. Лицо, подписывающее (заключающее) Договор от имени и по поручению Стороны на день подписания (заключения) имеет все необходимые для такого подписания полномочия и занимает должность, указанную в преамбуле Договора.
      5. Стороны уплачивают все налоги и сборы в соответствии с действующим законодательством Российской Федерации, а также ими ведется и своевременно подается в налоговые и иные государственные органы налоговая, статистическая и иная государственная отчетность в соответствии с действующим законодательством Российской Федерации.
      6. Все операции Сторон полностью отражены в первичной документации, в бухгалтерской, налоговой, статистической и любой иной отчетности, обязанность по ведению которой возлагается на Стороны.
      7. В случае недостоверности каких-либо из заверений об обстоятельствах, предусмотренных в настоящем разделе Договора, Сторона обязуется по письменному требованию другой Стороны выплатить штрафную неустойку в двойном размере общей стоимости по соответствующему приложению, а также возместить все убытки, причиненные такой недостоверностью, в части, не покрытой неустойкой.
5. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ
   1. Настоящий раздел регламентирует порядок обмена претензиями между Сторонами. Стороны имеют право направлять друг другу претензии посредством почтовой связи, нарочным, либо по электронной почте. Претензии, отправленные любым из указанных способов, влекут за собой предусмотренные законом и Договором правовые последствия для отправителя и адресата.
   2. Претензии, направляемые посредством электронной почты:
   3. Принимая во внимание содержание п. 2 ст. 160 ГК РФ, 165.1, ч. 4 ст. 11 ФЗ от 27.07.2006 N149-ФЗ «Об информации, информационных технологиях и о защите информации», Стороны установили, что признают претензии, направленные с адресов электронной почты, указанных в настоящем разделе, равнозначными документам на бумажных носителях, подписанным собственноручной подписью уполномоченного лица. Послание по электронной почте (далее – электронное письмо) должно содержать файл с подписанной претензией.
   4. Информация об адресе электронной почты отправителя в соответствующей строке браузера (программы) электронной почты является подтверждением того, что претензия исходит непосредственно от Стороны по Договору и подписана уполномоченным лицом. Считается, что полномочия лица, направившего послание с претензией, явствуют из обстановки и не нуждаются в дополнительном подтверждении.
   5. Стороны гарантируют, что доступ к указанным в п.п. 9.6, 9.7 настоящего раздела адресам электронной почты имеют только сами Стороны и надлежащим образом уполномоченные ими лица. Стороны гарантируют соблюдение конфиденциальности паролей (ключей), используемых для доступа в электронную почту.
   6. Адрес электронной почты Заказчика: \_\_\_\_\_\_\_\_.
   7. Адрес электронной почты Исполнителя: \_\_\_\_\_\_\_\_.
   8. Моментом получения Адресатом претензии, отправленной на адрес электронной почты в соответствии с настоящим регламентом, считается рабочий день, следующий за датой отправки электронного письма с претензией. Дата отправки электронного письма определяется по соответствующей записи в строке браузера (программы) электронной почты отправителя.
   9. Стороны признают юридическую и доказательную силу претензий, отправленных по электронной почте в соответствии с настоящим регламентом, в том числе целях доказывания в арбитражном, гражданском, административном и уголовном процессах, в том числе для подтверждения соблюдения обязательного претензионного порядка разрешения споров.
   10. Подтверждением отправки претензии по электронной почте являются соответствующие записи в строках браузера (программы) электронной почты отправителя.
   11. Стороны несут обязанность своевременного ознакомления с корреспонденцией, поступившей на адреса электронной почты, указанные в настоящем разделе. Сторона, не обеспечившая такую возможность, самостоятельно несет риск неполучения такой корреспонденции. В целях применения действующего материального и процессуального законодательства все претензии, направленные по адресам, указанным в настоящем разделе, в соответствии с настоящим регламентом считаются полученными адресатом.
   12. Стороны несут обязанность обеспечить техническую возможность отправки с адресов, указанных в настоящем разделе, и получения на такие адреса электронных писем размером до 20 Mb (двадцати мегабайт) включительно каждое письмо. В случае необходимости отправки электронного письма, размер которого превышает 20 Mb (двадцать мегабайт), отправитель несет обязанность разделить отправляемый пакет документов на несколько электронных писем, размер каждого из которых не превышает 20 Mb (двадцати мегабайт).

В целях настоящего пункта размер электронного письма в каждом случае включает в себя вложенные файлы.

* 1. Соотношение положений регламента обмена претензиями, закрепленного в Договоре.

Положения настоящего регламента имеют преимущественную силу перед любыми положениями иных соглашений, прямо или косвенно регулирующими порядок обмена претензиями, за исключением случаев заключения между Сторонами дополнительного соглашения в целях изменения непосредственно настоящего регламента со ссылкой на изменяемые пункты настоящего раздела, а также заключения дополнительного соглашения, изменяющего реквизиты Сторон, установленные в Договоре в части адресов электронной почты для направления и получения претензий.

* 1. Любые споры и разногласия, возникающие из Договора, в том числе касающиеся его исполнения, изменения, нарушения, прекращения, незаключенности или недействительности, могут быть переданы на разрешение арбитражного суда после принятия Сторонами мер по досудебному урегулированию по истечении 10 (десяти) календарных дней со дня направления претензии (требования).
  2. В соответствии со ст. 37 Арбитражного процессуального кодекса РФ Стороны пришли к соглашению об изменении подсудности, установленной статьями 35 и 36 Арбитражного процессуального кодекса РФ, следующим образом.
  3. Если иное не установлено подпунктом 9.17 Договора, то иск (заявление), вытекающий из Договора, в том числе касающийся его исполнения, изменения, нарушения, прекращения, незаключенности или недействительности, предъявляется в арбитражный суд по месту нахождения истца. Выбор между арбитражными судами, которым согласно настоящему подпункту подсудно дело, принадлежит истцу.

1. АНТИКОРРУПЦИОННАЯ ОГОВОРКА
   1. Сторонам известно о том, что они реализуют требования статьи 13.3 Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции», принимают меры по предупреждению коррупции, ведут Антикоррупционную политику и развивают не допускающую коррупционных проявлений культуру, поддерживают деловые отношения с контрагентами, которые гарантируют добросовестность своих партнеров и поддерживают антикоррупционные стандарты ведения бизнеса.
   2. При исполнении своих обязательств по настоящему Договору Стороны, их аффилированные лица, работники или посредники не выплачивают, не предлагают выплатить и не разрешают выплату каких-либо денежных средств или ценностей (прямо или косвенно) любым лицам для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества или достичь иных неправомерных целей.

Стороны отказываются от стимулирования каким-либо образом работников друг друга, в том числе путем предоставления денежных сумм, подарков, безвозмездного выполнения для них работ (оказания услуг) и другими, не поименованными здесь способами, ставящими работника в определенную зависимость и направленными на обеспечение выполнения этим работником каких-либо действий в пользу стимулирующей его стороны.

* 1. В случае возникновения у одной из Сторон подозрений, что произошло или может произойти нарушение каких-либо положений пунктов 10.1, 10.2 настоящего Договора, указанная Сторона обязуется уведомить об этом другую Сторону в письменной форме. После письменного уведомления Сторона имеет право приостановить исполнение настоящего Договора до получения подтверждения, что нарушения не произошло или не произойдет. Это подтверждение должно быть направлено в течение 10 (десяти) рабочих дней с даты направления письменного уведомления.

В письменном уведомлении Сторона обязана сослаться на факты и/или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений пунктов 10.1, 10.2 настоящего Договора любой из Сторон, аффилированными лицами, работниками или посредниками.

* 1. В случае нарушения одной из Сторон обязательств по соблюдению требований, предусмотренных пунктами 10.1, 10.2 настоящего Договора, Исполнитель или Заказчик имеет право расторгнуть настоящий Договор в одностороннем порядке полностью или в части, направив письменное уведомление о расторжении. Сторона, по чьей инициативе был расторгнут настоящий Договор, в соответствии с положениями настоящего пункта вправе требовать возмещения реального ущерба, возникшего в результате такого расторжения.

1. ДЕЙСТВИЕ ДОГОВОРА, ПОРЯДОК ЕГО ИЗМЕНЕНИЯ И РАСТОРЖЕНИЯ
   1. Договор вступает в силу с даты его подписания Сторонами и действует в течение 1 года. Договор может быть досрочно расторгнут по соглашению Сторон либо по инициативе любой из Сторон, с предварительным письменным уведомлением другой стороны не менее чем за 10 (десять) календарных дней до даты расторжения.
   2. В случае неисполнения/ненадлежащего исполнения Заказчиком обязательств, предусмотренных Договором, Исполнитель имеет право в одностороннем внесудебном порядке отказаться от исполнения Договора, направив Заказчику соответствующее уведомление.
2. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ
   1. Если иное не определено Договором, обмен информацией (материалами) между Сторонами по Договору совершается исключительно в письменной форме. Письменные сообщения Сторон (в том числе претензии, уведомления и др.) отправляются по почте, электронной почте, курьером, выдаются Стороне (её уполномоченному представителю) на руки или доставляются другими способами, позволяющими зафиксировать факт (дату, время) его передачи и отправителя.
   2. В случае изменения адресов и/или расчётных реквизитов Сторон, Сторона, чьи реквизиты изменились, обязана уведомить об этом другую Сторону в течение 5 (пять) рабочих дней с момента вступления в силу таких изменений. При этом заключения между Сторонами какого-либо дополнительного соглашения не требуется.
   3. Стороны соглашаются, что лица, отправляющие и (или) принимающие Заказы, уведомления и прочие документы, связанные с исполнением Договора, с использованием адресов электронной почты, указанными в Договоре, являются уполномоченными представителями Сторон по вопросам взаимодействия в рамках Договора, а полномочия таких лиц явствуют из обстановки и не нуждаются в дополнительном подтверждении.
   4. Любое сообщение по Договору считается надлежащим образом переданным:

* если вручается лично или заказным почтовым отправлением, то с момента вручения; или
* если отправлено по адресу электронной почты – в более ранний из следующих сроков:

(1) в момент создания почтовым сервером получателя автоматического сообщения о доставке;

(2) в момент подтверждения получения получателем;

(3) через 24 часа после отправки сообщения, если отправителем не будет получено уведомление об ошибке доставки электронного письма.

При этом если предполагаемое получение состоится до 09:00 часов Рабочего дня, оно считается произошедшим в 09:00 такого дня, и, если предполагаемое получение состоится после 17:00 часов Рабочего дня или в день, не являющийся Рабочим днем, оно считается произошедшим в 09:00 следующего Рабочего дня.

* 1. Сообщения, переданные по электронной почте, в информационной системе, посредством системы электронного документооборота и (или) факсимильной или иными видами связи, признаются Сторонами юридически значимыми сообщениями в соответствии со ст. 165.1 ГК РФ. Стороны гарантируют, что принятие решений и обмен юридически значимыми сообщениями осуществляются уполномоченными лицами, и действуют из презумпции наличия у лица, вступившего в такое взаимодействие от имени одной из Сторон, необходимых полномочий.
  2. Все изменения и дополнения к Договору имеют силу, только если они совершены в письменной форме и подписаны надлежаще уполномоченными представителями Сторон. В актах, приложениях, дополнительных соглашениях и прочих документах, составленных Сторонами, должна быть ссылка на Договор и указана дата подписания документа.
  3. Все исправления по тексту Договора, в том числе исправления текста, сделанные от руки или путем внесения данных с использованием любого печатающего устройства, имеют юридическую силу только в том случае, если они удостоверены подписями Сторон и печатями в каждом отдельном случае.
  4. Все изменения и дополнения к Договору оформляются дополнительным соглашением.
  5. Все приложения, изменения и дополнения к Договору являются его неотъемлемой частью и действительны лишь в случае, если они совершенны в письменной форме и подписаны представителями обеих сторон.
  6. Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из сторон.
  7. Приложения к Договору, являющиеся его неотъемлемыми частями на дату заключения Договора, и обязательные для исполнения Сторонами:

Приложение № 1 – Условия и порядок оказания Услуги.

Приложение № 2 – Форма Протокола об успешном подключении Услуги.

Приложение № 3 – Соглашение о порядке обработки и защиты персональных данных.

Приложение № 4 – Регламент взаимодействия Корпоративного центра ГосСОПКА Исполнителя и Заказчика при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак с ЦЗИиСС.

**13. АДРЕСА И ПЛАТЕЖНЫЕ РЕКВИЗИТЫ СТОРОН**

**Исполнитель Заказчик**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | |  | |
|  |  | ПАО "Ставропольэнергосбыт"  357633, Ставропольский край,  г. Ессентуки, ул. Большевистская, 59-а  тел.: (879-34) 4-21-80  ОГРН 1052600222927  ИНН/КПП 2626033550/785150001  р/с 40702810560090101705  Ставропольское отделение №5230  ПАО Сбербанк г. Ставрополь  БИК 040702615  к/с 30101810907020000615 | |
| **От имени Исполнителя** |  | **От имени Заказчика** | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_/  МП |  | Исполнительный директор  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Салпагаров И.Б./  МП | |

Приложение 1

к Договору на оказание услуг

№\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_/\_\_\_/\_\_\_.

**Условия и порядок оказания Услуги**

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
   1. Услуга по мониторингу и реагированию на инциденты ИБ представляет собой обеспечение круглосуточного мониторинга событий ИБ, проведения их анализа, своевременного обнаружения и разрешение инцидентов ИБ, а также организацию информационного взаимодействия Заказчика с ГосСОПКА через КЦ ГосСОПКА.
   2. В рамках оказываемой Услуги Исполнитель осуществляет:
   3. совместно с Заказчиком подключение систем-источников событий ИБ к Системе SOC и профилирование их активности;
   4. мониторинг и реагирование на инциденты ИБ, зарегистрированные в подключенных системах-источниках. Данная услуга предполагает подключение в качестве источников событий ИБ следующих элементов ИИС Заказчика:

* межсетевые экраны, маршрутизаторы;
* прокси-серверы;
* DHCP-серверы;
* система обнаружения/предупреждения вторжений;
* контроллеры домена;
* почтовые серверы;
* прикладные, файловые, терминальные серверы, серверы баз данных;
* АРМ критичных пользователей;
* антивирусное ПО;
* системы и серверы виртуализации;
* элементы объектов критической информационной инфраструктуры (по согласованию Исполнителя и Заказчика);
* другие источники по запросу Заказчика.

Системы-источники определяются в соответствии с Приложением № 1.1 к Приложению 1 к Договору;

* 1. организацию совместно с Заказчиком и в соответствии с Заказом, Договором, Приложением 4 к Договору, информационного взаимодействия Заказчика с ГосСОПКА через КЦ ГосСОПКА.

**2. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ**

* 1. Взаимодействие Сторон в рамках оказываемой Услуги осуществляется через ЛК SOC (преимущественно) и/или способом из Матрицы контактов, указанной в пункте 2.4.
  2. Внесение изменений в Матрицу контактов, указанную пункте 2.4, а также запрос на предоставление нового доступа в ЛК SOC осуществляется путем обращения через ЛК SOC или по электронной почте.
  3. Контактное лицо Заказчика оповещается при выявлении инцидента ИБ в нерабочее время посредством телефона при указании данного параметра в Матрице контактов из пункта 2.4.
  4. Матрица контактов Сторон:

Контакты Исполнителя

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Уровень обращения** | **Контактное лицо** | **Адрес электронной почты** | **Телефон** |
| 1 | Взаимодействие по инцидентам ИБ | Дежурная смена SOC |  |  |

Контакты Заказчика

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **ФИО/наименование группы рассылки** | **Направление (зона ответствен-ности)** | **Адрес электронной почты** | **Телефон** | **Оповещение в нерабочее время по телефону**  **(да/нет)** | **Доступ к ЛК SOC**  **(да/нет)** |
| 1 | Отдел ИБ | ИБ |  |  | нет | да |

Уровень критичности инцидентов ИБ для оповещения по контактному телефону в нерабочее время: *(****высокая****/*средняя/*низкая/не оповещать)*

**2.5.** Обеспечение работоспособности ЛК SOC:

|  |  |  |
| --- | --- | --- |
| Период работы и обслуживания | Период работы | 24\*7 |
| Количество технологических окон за месяц | не более 1 |
| Уведомление о технологическом окне | за 3 рабочих дня |
| Максимальная длительность технологического окна | не более 6 часов |
| Уведомление о простоях | в течение 60 минут |

1. **ПАРАМЕТРЫ ОКАЗАНИЯ УСЛУГИ**
   1. При подготовке к запуску Услуги Заказчик заполняет Перечень систем-источников, подключаемых к Системе SOC в соответствии с Приложением № 1.1 к данному Приложению.
   2. Исполнитель обязуется осуществлять мониторинг и реагирование на инциденты ИБ, зафиксированные в подключенных системах-источниках. Параметры и опции Услуги мониторинга и реагирования на инциденты ИБ представлены в Заказе.
   3. Услуга не включает в себя оказание консультаций и обучения по работе с СЗИ и системами-источниками.
   4. Услуга не включает в себя проведение аудита инфраструктуры Заказчика.
2. **ПОДКЛЮЧЕНИЕ ЗАКАЗЧИКА К СИСТЕМЕ SOC**
   1. Процесс оказания Услуги включает в себя процедуру подключения инфраструктуры Заказчика к Системе SOC, предоставление Заказчику доступа в ЛК SOC для взаимодействия Заказчика с НКЦКИ и осуществления мониторинга и реагирования на зафиксированные инциденты ИБ в Системе SOC с поэтапным отчетным периодом.

Подключение систем-источников, настройка отчетности, профилирование активности, настройка автоматических уведомлений о возникающих инцидентах осуществляются в течение 20 (двадцати) рабочих дней с момента подписания Договора, при своевременном выполнении работ со стороны Заказчика, а также при наличии у Заказчика необходимых технических возможностей (оборудование для организации и организация туннеля доступа к системам-источникам (равнозначно также, «VPN», «VPN–канал», организуемого Заказчиком, серверного оборудования и т.д.).

* 1. В рамках подключения к Услуге Исполнитель:
* согласовывает итоговый перечень подключаемых систем-источников. Для систем-источников должно быть готовое правило корреляции (перечень правил доступен в ЛК SOC либо предоставляется по запросу);
* совместно с Заказчиком подключается по организованному и предоставленному Заказчиком туннелю доступа к коллекторам, настраивает защищённое соединение между коллекторами и Системой SOC с целью передачи событий ИБ с систем-источников на коллекторы и с них в Систему SOC в режиме реального времени. При настройке соединения за основу берётся схема, представленная на рисунке 1:

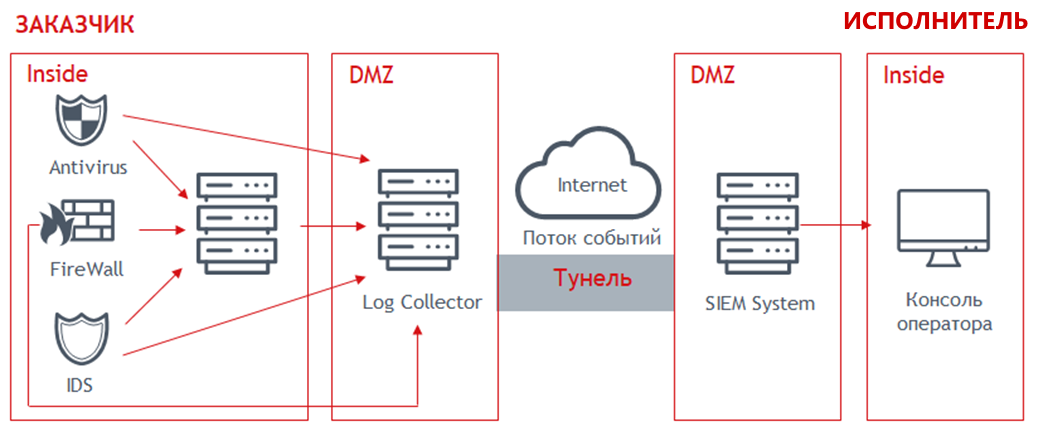


Рисунок 1. Схема взаимодействия

* направляет в адрес сотрудников Заказчика, указанных в Матрице контактов из пункта 2.4, инструкции по настройке сбора событий ИБ на соответствующих ИТ и ИБ-системах (для стандартных систем-источников);
* подключает события ИБ с систем-источников, которые передаются на заранее подготовленные Заказчиком коллекторы, к Системе SOC. Технические требования приведены в пункте 4.4 Приложения;
* совместно с Заказчиком адаптирует правила обнаружения инцидентов ИБ, включающие в себя:
* правила корреляции;
* логику определения событий ИБ, относящихся к одному/разным инцидентам ИБ, в рамках одного правила;
* определение степени критичности инцидента ИБ;
* проводит совместно с сотрудниками ИБ/ИТ Заказчика профилирование сетевой и хостовой активности для минимизации ложных срабатываний правил корреляции.
  1. В рамках подключения к Услуге Заказчик:
* осуществляет создание и первоначальную настройку (в том числе установку операционной системы) коллекторов с техническими характеристиками, указанными в пункте 4.4 Приложения, в сетевой зоне DMZ (рекомендованный параметр). Лицензии на операционные системы и другое прикладное программное обеспечение для оборудования из пункта 4.4 Приложения Заказчик предоставляет самостоятельно;
* ознакамливается с правилами корреляции, перечень которых доступен в ЛК SOC либо предоставляется по запросу;
* организовывает и предоставляет ответственному сотруднику Исполнителя, удалённый доступ–туннель на коллекторы с целью настройки передачи событий ИБ с коллекторов в Систему SOC. В случае отказа Заказчика предоставить данный доступ, Заказчик самостоятельно проводит работы по установке и настройке передачи событий ИБ в Систему SOC. Ответственность за корректность работы в таком случае лежит на Заказчике;
* организовывает сетевой доступ и передачу данных между системами-источниками и коллекторами;
* осуществляет настройку сбора событий ИБ на системах-источниках с передачей событий ИБ на коллекторы. Эксплуатацию и настройку систем-источников Заказчик осуществляет самостоятельно. Заказчик может обратиться к Исполнителю за консультацией по настройке сбора событий ИБ на системах-источниках.

Факт завершения этапа подключения Заказчика к Услуге подтверждается путем подписания Протокола об успешном подключении Услуги.

* 1. Минимальные требования к серверному оборудованию (коллекторам) на стороне Заказчика:

|  |  |  |  |
| --- | --- | --- | --- |
| Параметры сервера | Сервер 1 | Сервер 2 | Сервер 3 |
| Тип сервера | виртуальный или физический | виртуальный или физический | виртуальный или физический |
| Центральный процессор | 6 CPU | 6 CPU | 8 CPU |
| Оперативная память | 12 Гб | 16 Гб | 16 Гб |
| Дисковое пространство | 80 Гб (RAID 10) | 80 Гб (RAID 10) | 500 Гб доступного места на диске, смонтированного в разделе /opt |
| Операционная система | РЕД ОС 7.3.4 и выше | Windows 2016 и выше | РЕД ОС 7.3.4 и выше |
| Примечание | Диски SSD  / - по умолчанию.  /var – 8 Гб  /queue – 20 Гб  /opt – 10 Гб  /home (или /tmp) – 5 Гб для обмена файлами | Диски SSD.  При установке обязательно английская локализация. Должен быть в домене тех компьютеров, с которых нужно будет собирать события ИБ |  |

* 1. Требования к каналу передачи данных от коллекторов к Системе SOC.

Требования к скорости и объёму передачи данных исходят из следующей информации:

* 1,5 Мбит/с пропускной способности на каждые 100 событий ИБ в секунду;
* 0,7 Мбит/c пропускной способности для коррелятора Системы SOC;
* 0,7 Мбит/c пропускной способности для хранилища Системы SOC.

**5. ПОРЯДОК ОКАЗАНИЯ УСЛУГИ**

* 1. Мониторинг и реагирование на инциденты ИБ.

Исполнитель осуществляет мониторинг всех инцидентов ИБ с систем-источников, фиксируемых в Системе SOC.

В рамках взаимодействия Заказчика с ГосСОПКА:

* передачу в автоматическом режиме в НКЦКИ вносимых Заказчиком в ЛК SOC сведений от систем-источников – ОИИ и (или) ОКИИ, об ИИ, КИИ, о КА и КИ в ИИ и КИИ;
* передачу в автоматическом режиме Заказчику через ЛК SOC сведений от НКЦКИ, об индикаторах компрометации и методических рекомендациях для Заказчика по обнаружению, предупреждению и ликвидации последствий типовых КА на ОИИ и ОКИИ Заказчика.

При возникновении инцидента ИБ Исполнитель проводит первичный анализ данных с целью выявления ложных срабатываний правил корреляции. В случае, если Исполнителем принято решение о ложном срабатывании, соответствующий инцидент ИБ закрывается с обоснованием причин, информация о нем и причинах его закрытия предоставляется в рамках регулярной отчетности Системы SOC, а также доступна в ЛК SOC.

По итогам проведенной обработки Исполнитель информирует Заказчика о факте возникновения инцидента ИБ.

На основании предоставленной информации Заказчик вправе повысить или понизить критичность инцидента ИБ для изменения процесса его обработки в дальнейшем.

После информирования Заказчика о факте инцидента ИБ Исполнитель продолжает установление причин и источника инцидента ИБ, если это возможно. По итогам анализа данная информация передается Заказчику.

Исполнитель вправе запросить у Заказчика дополнительную информацию об ИИ, системах-источниках или событиях ИБ в случае, если она требуется для анализа инцидента ИБ.

Сотрудники Заказчика вправе запросить дополнительную информацию о причинах и источнике инцидента ИБ, если данная информация может быть получена средствами Системы SOC, из информации об ИИ, переданной Исполнителем, или общедоступных источников информации.

По результатам анализа предоставленной информации Заказчик подтверждает факт возникновения инцидента ИБ (с указанием принятых мер реагирования), сообщает о ложном срабатывании правила корреляции, необходимости внесения исключений или о легитимности инцидента ИБ, либо запрашивает дополнительную информацию.

При отсутствии обратной связи от Заказчика в течение 8-ми календарных дней, инцидент ИБ закрывается в ЛК SOC с соответствующим статусом и может быть повторно открыт при обращении Заказчика.

Связанные инциденты ИБ закрываются в Системе SOC с соответствующей пометкой с указанием основного инцидента ИБ без оповещения Заказчика, информация о нем и причинах его закрытия предоставляется в рамках регулярной отчетности Системы SOC, а также доступна в ЛК SOC.

Ограничения работ:

* Исполнитель обрабатывает только инциденты ИБ, зафиксированные в системах-источниках;
* время реакции Исполнителя на инцидент ИБ отсчитывается от момента фиксации инцидента ИБ в Системе SOC;
* время анализа Исполнителем инцидента ИБ может быть увеличено в случае, если Заказчик запросил обработку большого количества данных в Системе SOC или системах-источниках;
* время реакции Исполнителя не включает в себя работы Заказчика по верификации и оценке полноты предоставленных Исполнителем данных.
  1. Превышение допустимого Заказом количества EPS.

В случае превышения количества EPS, указанных в Заказе, Заказчик дополнительно оплачивает каждый использованный пакет по 100 EPS.

Стороны согласовали, что предельно допустимая нагрузка на Систему SOC не должна превышать среднего значения EPS, указанного в Заказе.

* 1. Расширенный экспертный анализ по инцидентам ИБ.

При необходимости проведения дополнительного экспертного анализа по инцидентам ИБ, зафиксированным в системах-источниках, Заказчик инициирует через ЛК SOC (при отсутствии доступа к ЛК SOC, через электронную почту) запрос Исполнителю. При обработке запроса сотрудник Исполнителя проводит сбор следующей информации у Заказчика, который предоставляет следующие данные:

* местонахождение структурного подразделения Заказчика, в котором зафиксирован инцидент ИБ;
* дата и время возникновения инцидента ИБ;
* ИС, IP-адреса, MAC-адреса, FQDN-имена хостов, относящихся к инциденту ИБ;
* контактные данные сотрудника (ФИО, тел., адрес эл. почты), ответственного за эксплуатацию систем-источников, которые относятся к инциденту ИБ;
* критичность инцидента ИБ.

После сбора первичной информации по инциденту ИБ лицо, ответственное за расследование инцидента ИБ со стороны Исполнителя, приступает к сбору расширенной информации по инциденту ИБ, которая включает в себя:

* сбор дополнительных данных о фигурантах инцидента ИБ (события ИБ с фигурантами в других информационных, инфраструктурных системах-источниках, СЗИ за предшествующий период глубиной от 1 месяца; имеющиеся доступы/роли/привилегии; наличие ранее зафиксированных инцидентов ИБ);
* сбор дополнительных данных об информационных системах участниках инцидента ИБ (зафиксированные события и инциденты ИБ, результаты автоматизированных сканирований, проверок и аудитов);
* другая дополнительная информация.

Данная работа ведётся совместно с Заказчиком. Качество зависит от данных, предоставляемых Заказчиком.

По результатам собранной информации проводится анализ инцидента ИБ.

В процессе сотрудник Исполнителя, устанавливает:

* хронологию событий, повлекших за собой возникновение инцидента ИБ;
* причины, из-за которых возник инцидент ИБ;
* ложность или истинность инцидента ИБ;
* последствия инцидента ИБ.

По итогам формируется отчёт о проделанной работе. Исполнитель, помимо анализа инцидента ИБ, установления системы-источника и причин, формирует набор технических рекомендаций, позволяющих предотвратить или снизить вероятность возникновения аналогичных инцидентов ИБ в дальнейшем.

Заказчик анализирует предоставленную ему информацию, принимает решение о применимости выданных рекомендаций в своей ИИ и реализует при необходимости предложенные технические мероприятия.

Предложенный механизм предотвращения анализируется Исполнителем и Заказчиком на возможность повторного применения при возникновении инцидента ИБ и фиксируется в Системе SOC, описывающей профиль Услуги.

Ограничения работ:

* количество запросов на расширенный экспертный анализ по инцидентам ИБ не должно превышать установленное Заказом;
* работы проводятся удалённо. Расследование инцидентов ИБ на площадке Заказчика оценивается и оплачивается отдельно. В стоимость включаются командировочные расходы. Детали командировки оговариваются отдельно;
* время выработки рекомендаций может быть увеличено по согласованию Сторон в случае, если выданные Исполнителем рекомендации оказались неприменимыми на ИИ Заказчика в силу особенностей архитектуры, ресурсных либо бюджетных ограничений;
* выдаваемые Исполнителем рекомендации основываются на общих архитектурных и инфраструктурных положениях обеспечения ИБ и не включают в себя детализированных настроек специфического оборудования либо приложений Заказчика. Анализ применимости рекомендаций и разработка инструкций для специфических приложений является ответственностью уполномоченных специалистов Заказчика.
  1. Подключение новых систем-источников к Системе SOC.

Заказчик инициирует через ЛК SOC (при отсутствии доступа к ЛК SOC, через электронную почту) запрос на подключение дополнительной системы-источника к Системе SOC, предоставляя следующую информацию:

* + - * + тип новой системы-источника;
        + информация по получению данных с новой системы-источника (ip-адрес, данные доступа);
        + список правил обнаружения инцидентов ИБ, которые необходимо контролировать в рамках данной системы-источника;
        + дополнительная информация, необходимая для определения системы-источника в правилах обнаружения инцидентов ИБ.

Исполнитель, совместно с Заказчиком, оценивает техническую возможность сбора требуемых событий ИБ с новой системы-источника и согласовывает механизм и способ подключения.

Исполнитель оценивает достаточность предоставленной информации для выполнения работ и вносит изменения в правила обнаружения инцидентов с учетом подключения новой системы-источника.

Заказчик организовывает сетевой доступ и передачу данных между новой системой-источником и коллекторами, осуществляет настройку сбора событий ИБ на новой системе-источнике с передачей событий ИБ на коллекторы.

Исполнитель и Заказчик выполняют требуемые настройки в Системе SOC и коллекторах для подключения новой системы-источника.

По завершению подключения и проверки работоспособности Исполнителем проводится изменение Системы SOC, описывающей профиль Услуги.

Ограничения работ:

* + - * + подключение новой системы-источника производится только в том случае, если количество EPS за текущий период не превышает количество EPS, указанных в Заказе;
        + подключение системы-источника производится только при наличии технической возможности получения событий ИБ, необходимых для реализации правил обнаружения инцидентов ИБ. Наличие технической возможности определяется Исполнителем с использованием консультаций администраторов новой системы-источника;
        + время работ по подключению зависит от своевременного выполнения работ на стороне Заказчика по настройкам передачи необходимых данных для анализа в Систему SOC. Исполнитель начинает выполнять работы только после организации Заказчиком передачи необходимых событий ИБ в Систему SOC;
        + Исполнитель определяет и согласовывает с Заказчиком необходимый уровень журналирования системы-источника и типы событий ИБ, для реализации требуемых правил корреляции. При отсутствии технической возможности использовать рекомендованный уровень журналирования Исполнитель совместно с Заказчиком определяет необходимость и порядок решения инцидентов ИБ.
  1. Отключение системы-источника от Системы SOC.

Заказчик инициирует через ЛК SOC (при отсутствии доступа к ЛК SOC, через электронную почту) запрос на отключение системы-источника, предоставляя следующую информацию:

* тип системы-источника;
* идентификатор системы-источника (IP-адрес, приложение).

Исполнитель проводит анализ существующих правил обнаружения инцидентов ИБ и информирует Заказчика в случае, если отключение системы-источника приводит к их модификации либо исключению из списка контролируемых инцидентов ИБ.

В случае необходимости Исполнитель и Заказчик выполняют работы по изменению состава инцидентов ИБ в Системе SOC, коллекторах и системы-источнике для его отключения.

Ограничения работ:

* время, необходимое Заказчику для согласования изменений в списке контролируемых правил обнаружения инцидентов ИБ и проведение требуемых работ на системе-источнике для ее отключения не учитывается в метриках отключения системы-источника.
  1. Реализация новых правил обнаружения инцидентов ИБ по запросу Заказчика.

Заказчик инициирует через ЛК SOC (при отсутствии доступа к ЛК SOC, через электронную почту) запрос на реализацию нового правила обнаружения инцидентов ИБ, предоставляя следующую информацию:

* + - * + общее описание и критерии возникновения инцидента ИБ;
        + тип систем-источников для обнаружения инцидента ИБ;
        + плановую критичность инцидента ИБ.

Исполнитель анализирует техническую возможность реализации правила корреляции в рамках ИИ Заказчика в Системе SOC, привлекая Заказчик для более детальной проработки правила корреляции.

Исполнитель и Заказчик согласовывают итоговое правило обнаружения инцидента ИБ, определяют его критичность и процесс взаимодействия по инциденту ИБ.

Исполнитель выполняет работы по реализации нового правила, производя настройки Системы SOC.

По завершению подключения и проверки работоспособности Исполнителем проводится изменение Системы SOC, описывающей профиль Услуги.

Ограничения работ:

* в случае, если реализация нового правила требует подключения дополнительных систем-источников, то для реализации данного правила требуется Заказчику сначала подключить эти системы-источники к Системе SOC;
* при подключении нового правила обнаружения инцидентов ИБ Заказчику выделяется тестовый период отладки инцидента ИБ (2 недели), в течение которого выявляемые по новому правилу инциденты ИБ обрабатываются согласно метриками инцидента ИБ низкой критичности и происходит дополнительная доработка правила. По результатам успешного завершения тестового периода критичность сценария устанавливается в соответствии с согласованным уровнем. Период отладки может быть изменен по согласованию Сторон.
  1. Реализация новых правил обнаружения инцидентов ИБ по инициативе Исполнителя.

Исполнитель информирует Заказчика о расширении списка правил обнаружения инцидентов ИБ в Системе SOC, указывая следующую информацию:

* общее описание и критерии возникновения инцидента ИБ;
* тип систем-источников для обнаружения инцидента ИБ;
* плановую критичность инцидента ИБ.

Заказчик анализирует предоставленную информацию и принимает решение о включении новых правил в список контролируемых. В случае, если адаптация сценариев под требования Заказчика требует дополнительной информации, Заказчик предоставляет ее Исполнителю.

Исполнитель включает контроль инцидентов ИБ по новым правилам обнаружения инцидентов ИБ для ИИ Заказчика, производя необходимые настройки Системы SOC.

По завершению активации и проверки работоспособности Исполнителем проводится изменение Системы SOC, описывающей профиль Услуги.

Ограничения работ:

* в случае, если реализация правила требует подключения дополнительных систем-источников, то для реализации данного правила требуется Заказчику сначала подключить эти системы-источники к Системе SOC;
* при подключении нового правила обнаружения инцидентов ИБ Заказчику выделяется тестовый период отладки инцидента ИБ (2 недели), в течение которого выявляемые по новому правилу инциденты ИБ обрабатываются согласно метриками инцидента ИБ низкой критичности и происходит дополнительная доработка правила. По результатам успешного завершения тестового периода критичность сценария устанавливается в соответствии с согласованным уровнем. Период отладки может быть изменен по согласованию Сторон.
  1. Управление критичностью правил обнаружения инцидентов ИБ или процесса взаимодействия.

Заказчик инициирует через ЛК SOC (при отсутствии доступа к ЛК SOC, через электронную почту) запрос на изменение уровня критичности или процесса взаимодействия при обработке инцидента ИБ, предоставляя следующую информацию:

* + - * + название правила обнаружения;
        + новую плановую критичность (при необходимости);
        + новый алгоритм взаимодействия (при необходимости).

Исполнитель проводит анализ предоставленной Заказчиком информации на достаточность и возможность реализации в Системе SOC.

Исполнитель проводит необходимые работы и вносятся изменения в Систему SOC, описывающей профиль Услуги.

Ограничения работ:

* количество правил обнаружения инцидентов ИБ с высокой степенью критичности не может превышать 35 (тридцати пяти) процентов от общего числа правил обнаружения инцидентов ИБ.

|  |  |  |
| --- | --- | --- |
| **От имени Исполнителя** |  | **От имени Заказчика** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_/  МП |  | Исполнительный директор  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Салпагаров И.Б./  МП |

**Приложение № 1.1**

**к Приложению № 1 от\_\_\_**

**к Договору на оказание услуг**

**№\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_/\_\_\_/\_\_\_.**

**Перечень систем-источников, подключаемых к Системе SOC**

Для оказания Услуги по мониторингу и реагированию на инциденты ИБ, подключены следующие источники системы-источники:

Таблица 1 – Перечень систем-источников

|  |  |
| --- | --- |
| **Наименование/тип системы-источника** | **Количество хостов** |
| Система-источник 1 |  |
| Система-источник 2 |  |
| Система-источник 3 |  |
| Система-источник 4 |  |
| Система-источник 5 |  |
| Система-источник 6 |  |
| Система-источник 7 |  |
| Система-источник 8 |  |
| Система-источник 9 |  |
| Система-источник 10 |  |

Подключение дополнительных систем-источников осуществляется в соответствии с порядком, указанным в разделе 5 Приложения № 1 к Договору.

|  |  |  |
| --- | --- | --- |
| **От имени Исполнителя** |  | **От имени Заказчика** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_/  МП |  | Исполнительный директор  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Салпагаров И.Б./  МП |

**Заказ**

**к Договору на оказание услуг №\_\_\_\_\_\_\_ от\_\_\_\_\_\_\_\_\_**

**Заказ №\_\_\_\_**

г. Ессентуки «*\_\_*» \_\_\_\_\_\_\_\_\_\_\_20*\_\_* г.

**1.** Услуга: «Интеграционный бизнес. Инфраструктурные решения и сети связи. Услуги. Работы» (услуга по мониторингу и реагированию на инциденты ИБ)

**2. Состав и параметры заказываемой Услуги:**

**2.1.** **Состав Услуги**

|  |  |  |
| --- | --- | --- |
| п/п | Наименование | Стоимость, руб. без учета НДС |
| 1 | Мониторинг и реагирование на инциденты ИБ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ руб/мес |
| 2 | Инсталляционный платеж за организацию подключения к Системе SOC | (руб/единоразово) |
| Дополнительные опции Услуги | | |
| 1 | Выбираются и указываются параметры из п. 2.2 формы Заказа | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ руб/мес |
| Итого платёж за Отчётный период: | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ руб/мес |

**2.1.1.** Услуга включает в себя работы по подключению систем-источников Заказчика к Системе SOC на стороне Исполнителя и подлежит оплате в указанном размере в случае, если среднее значение за месяц Максимального количества EPS данного Заказа не превышает установленное количество ХХХ EPS. Дополнительно оплачивается каждый следующий пакет в размере 100 EPS, если среднее значение за месяц превышает XXX EPS в размере XXXX рублей в месяц без учета НДС.

Среднее значение за месяц Максимального количества EPS определяется Исполнителем на основании данных из Системы SOC.

**2.2. Перечень и стоимость дополнительных опций** *(выбрать и указать в пункте 2.1 Заказа актуальное для соответствующего Заказа)***:**

| **Наименование опции** | **Цена за ед., руб. без учета НДС** |
| --- | --- |
| Стоимость дополнительных EPS (пакетами по 100 EPS), в месяц |  |
| Расширенный экспертный анализ по инцидентам ИБ, за один инцидент ИБ |  |
| Увеличенная длительность хранения собранных событий ИБ с момента их фиксации в Системе SOC, за месяц |  |
| Разработка дополнительных правил обнаружения инцидентов ИБ (за правило), за ед. |  |
| Расширенный анализ событий с использованием EDR-решения, за услугу |  |
| Анализ защищенности инфраструктуры с использованием автоматизированных средств, за услугу |  |
| Подключение нестандартных источников событий ИБ, за ед. |  |
| Передача инцидентов в ГосСОПКУ |  |
| Выявление целевых кибератак с использованием решения Distributed Deception Platform |  |

**3. Параметры Услуги:**

| **Наименование параметра** | **Значение параметра** | |
| --- | --- | --- |
| Обработка и анализ поступающих событий ИБ | Анализ событий ИБ в реальном времени в соответствие с правилами корреляции | |
| Длительность хранения собранных событий ИБ с момента их фиксации в Системе SOC | 3 месяца | |
| Максимальное количество EPS (среднее значение за месяц). Превышение данного лимита оплачиваются отдельно. | 400 EPS | |
| SIEM-платформа | Kaspersky KUMA | |
| **Дежурная смена**  *Обеспечение мониторинга и реагирования на регистрируемые в Системе SOC инциденты ИБ силами Исполнителя* | | |
| Период предоставления Услуги | 24\*7 | |
| Предоставление первичных рекомендаций по инциденту с момента его фиксации в Системе SOC | 20 минут | |
| Время реагирования на инцидент ИБ с момента его фиксации в Системе SOC | Высокая критичность | 60 минут |
| Средняя критичность | 90 минут |
| Низкая критичность | 120 минут |
| **Изменение профиля Услуги** | | |
| Время выполнения работ по подключению новых систем-источников | | 20 рабочих дней/1 источник |
| Кол-во подключаемых новых систем-источников по запросу Заказчика | | не более 1-го в месяц |
| Время выполнения запроса на разработку правил обнаружения инцидентов ИБ | | 10 рабочих дней/1 правило |
| Кол-во разрабатываемых правил обнаружения инцидентов ИБ по запросу Заказчика | | не более 3-х в год |
| Расширенный экспертный анализ по инцидентам ИБ | | не более 3-х в год |

4. Начало оказания Услуги: с даты подписания Сторонами Протокола об успешном подключении Услуги.

5. Услуга оказывается с даты начала оказания Услуги и до даты прекращения действия Заказа.

6. Заказ действует до \_\_\_\_\_\_\_\_\_\_.

7. В случае необходимости отключения Услуги Заказчик направляет Исполнителю на электронную почту: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ соответствующее Заявление по форме, установленной Приложением № 1 к данному Заказу за 15 (пятнадцать) календарных дней до планируемой даты отключения.

8. Заказ составлен в 2 (двух) экземплярах, имеющих равную юридическую силу, по 1 (одному) для каждой из Сторон.

9. С даты вступления в силу Заказа прекращают действие следующие Заказы: *указать номер и дату Заказа, номер и дату Приложения, номер и дату Договора.*

|  |  |  |
| --- | --- | --- |
| **От имени Исполнителя** |  | **От имени Заказчика** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_/  МП |  | Исполнительный директор  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Салпагаров И.Б./  МП |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  | От | **Приложение № 1 к Заказу** |
|  |  | Наименование организации |
|  | № Договора |  |
|  |  |  |
|  |  |
|  |  |
|  |  |

***ФОРМА***

**Заявление  
на отключение услуг**

1. **Прошу с «\_\_\_» \_\_\_\_20\_\_ г. отключить следующие услуги, оказываемые в рамках Договора** **на оказание услуг № \_\_\_\_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_ 20\_\_ г.**

|  |  |
| --- | --- |
| Номер п/п | Наименование услуг |
|  |  |
|  |  |
|  |  |
|  |  |

1. Оплату услуг, оказанных до момента отключения, гарантируем.

Подпись уполномоченного

представителя Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

Дата «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**Приложение № 2**

**к Договору на оказание услуг**

**№\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_/\_\_\_/\_\_\_.**

***ФОРМА***

**Протокол об успешном подключении Услуги**

г. Ессентуки «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

В данном Протоколе об успешном подключении Услуги по мониторингу и реагированию на инциденты ИБ между \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Исполнитель», и ПАО «Ставропольэнергосбыт», именуемое в дальнейшем «Заказчик», подтверждается следующее:

1. Исполнитель выполнил следующие действия по подключению и настройке Услуги по мониторингу и реагированию на инциденты ИБ (далее – Услуга) для Заказчика:
2. На выделенных серверах Заказчика сконфигурированы коллекторы сбора событий ИБ с систем-источников.
3. Между Системой SOC на стороне Исполнителя и коллекторами на стороне Заказчика организовано сетевое взаимодействие.
4. Согласован перечень систем-источников, который будет подключён к Системе SOC.
5. Согласован и настроен перечень правил обнаружения инцидентов ИБ и степень критичности по ним. Перечень правил доступен в ЛК SOC либо предоставляется по запросу.
6. Организован сбор событий ИБ с систем-источников, приведённых в Договоре на оказание Услуги.
7. Организована работа SOC по реагированию на инциденты ИБ в режиме 24/7.
8. Организовано подключение систем-источников - ОИИ и (или) ОКИИ Заказчика к Системе SOC для организации информационного взаимодействия через КЦ ГосСОПКА с НКЦКИ.
9. Заказчику в КЦ ГосСОПКА предоставлен ЛК SOC для взаимодействия с НКЦКИ.
10. Организована передача информации Заказчика в ГосСОПКА и Заказчику из ГосСОПКА через ЛК SOC.
11. По факту завершения вышеуказанных работ, Заказчик подтверждает, что подключение к Услуге прошло успешно и работоспособность обеспечена. Услуга начинает предоставляться с \_\_\_.\_\_\_.20\_\_ г.

В случае получения информации от Исполнителя о превышении лимита количества событий ИБ (EPS), установленного в Заказе, Заказчик ограничивает передачу событий ИБ в сторону Системы SOC или докупает необходимое количество EPS.

1. Подключение дополнительных систем-источников и правил реагирования на инциденты ИБ осуществляется в соответствии с порядком, указанным в Договоре на оказание Услуги.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **От имени Исполнителя** | |  | **От имени Заказчика** | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_/  МП | |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_/  МП | |
|  |  | |  |
|  |  | |  |

**Приложение № 3**

**к Договору на оказание услуг**

**№\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_/\_\_\_/\_\_\_.**

**Регламент взаимодействия Корпоративного центра ГосСОПКА Исполнителя и Заказчика при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак с ЦЗИиСС**

**ОБЩИЕ ПОЛОЖЕНИЯ**

**Назначение и область действия**

КЦ ГосСОПКА взаимодействует с ЦЗИиСС посредством направления сведений и обращений через каналы НКЦКИ.

В ходе организованного в рамках Услуги для Заказчика его информационного взаимодействия с НКЦКИ ГосСОПКА, через КЦ ГосСОПКА, осуществляется обмен сведениями с ГосСОПКА об ИИ, КИИ Заказчика, о КА и КИ в ИИ и КИИ Заказчика, индикаторах компрометации и методических рекомендациях НКЦКИ ГосСОПКА для Заказчика по обнаружению, предупреждению и ликвидации последствий типовых КА на ОИИ и ОКИИ Заказчика.

Исполнителем организовывается подключение систем-источников ОИИ и (или) ОКИИ Заказчика к Системе SOC, в соответствии с Приложением 1 к Договору, для организации информационного взаимодействия Заказчика через КЦ ГосСОПКА с НКЦКИ.

Заказчику в КЦ ГосСОПКА предоставляется доступ в ЛК SOC для взаимодействия Заказчика с НКЦКИ.

Передача информации Заказчика в ГосСОПКА и Заказчику из ГосСОПКА организовывается через ЛК SOC.

Регламент разработан для осуществления взаимодействия между КЦ ГосСОПКА и Заказчиком при осуществлении информационного обмена Заказчика в области обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, находящиеся в зоне ответственности Заказчика, с ЦЗИиСС. Обмен информацией происходит через предоставленный Заказчику ЛК SOC, развёрнутый на стороне Исполнителя. Регламент устанавливает основные положения по процессу данного взаимодействия между Заказчиком и Исполнителем.

Исполнитель обеспечивает для Заказчика предоставление ЛК SOC для взаимодействия Заказчика с НКЦКИ и функционирование канала между ЛК SOC и НКЦКИ.

Заказчик самостоятельно осуществляет размещение информации для передачи в ГосСОПКА в предоставленном Исполнителем Заказчику ЛК SOC для взаимодействия Заказчика с НКЦКИ, самостоятельно принимает решение о необходимости информирования НКЦКИ о КА и КИ в ИИ и КИИ Заказчика, о чем должен уведомлять КЦ ГосСОПКА посредством направления сообщения по каналам взаимодействия, указанным в разделе 4 Регламента.

Все работники Сторон, участвующие в процессах взаимодействия по Регламенту, должны быть ознакомлены с Регламентом.

**Нормативные ссылки**

Регламент разработан в соответствии с требованиями следующих нормативно-правовых актов:

* Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
* Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»;
* Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
* Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам»;
* Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
* Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;
* Приказ ФСБ России от 19 июня 2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;
* Приказ ФСБ России от 6 мая 2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».

**1. Передача информации о КА и КИ в ЦЗИиСС**

* 1. Передача информации Заказчика о КА и КИ в ИИ и КИИ Заказчика и принятых им мерах по ликвидации последствий КА в НКЦКИ происходит путём регистрации и заполнения Заказчиком необходимых сведений о КА на предоставленном Исполнителем ЛК SOC для взаимодействия Заказчика с НКЦКИ.
  2. Уведомления о получении информации о КА и КИ от НКЦКИ поступают в КЦ ГосСОПКА и в автоматическом режиме в течение 2 дней с даты поступления в КЦ ГосСОПКА передаётся Заказчику путём размещения в предоставленном Исполнителем ЛК SOC для взаимодействия Заказчика с НКЦКИ.

**2. Функции участников**

* 1. В Функции Исполнителя входит:
  2. Прием КЦ ГосСОПКА от ЦЗИиСС информации об актуальных угрозах безопасности и необходимых мерах по противодействию им, о средствах и способах проведения КА и методах их обнаружения, предупреждения и противодействия им, а также о признаках КИ.
  3. Информирование Заказчика о рекомендациях, полученных КЦ ГосСОПКА от ЦЗИиСС, в рамках п. 2.1.1 Регламента, в следующем порядке: путём направления Заказчику указанных рекомендаций с использованием каналов взаимодействия, указанных в разделе 4 Регламента.
  4. Предоставление Заказчикудоступа к ЛК SOC для взаимодействия Заказчика с НКЦКИ, в порядке и сроки, указанные в Приложении 1 к Договору.
  5. В функции Заказчикавходит:
  6. Предоставление в ЦЗИиСС через ЛК SOC и в КЦ ГосСОПКА с использованием каналов взаимодействия, указанных в разделе 4 Регламента, следующих сведений: о составе и характеристиках ИР Заказчика, находящихся в его зоне ответственности, а также своевременная актуализация таких сведений (в течение 10 рабочих дней с даты любых изменений в преданных ранее Заказчиком сведениях).
  7. Предоставление сведений о выявляемых КА и КИ в ИР, находящихся в зоне ответственности Заказчика, а также информации о предпринятых мерах и результатах реагирования на такие КА и КИ через ЛК SOC в ЦЗИиСС и в КЦ ГосСОПКА с использованием каналов взаимодействия, указанных в разделе 4 Регламента.
  8. Своевременное предоставление в ЦЗИиСС через ЛК SOC и в КЦ ГосСОПКА с использованием каналов взаимодействия, указанных в разделе 4 Регламента, а также поддержание в актуальном состоянии сведений об ответственных лицах, на которых возложены обязанности по взаимодействию с НКЦКИ.
  9. Предоставление в ЦЗИиСС через ЛК SOC, а также в КЦ ГосСОПКА с использованием каналов взаимодействия, указанных в разделе 4 Регламента, сведений об изменении внешних сетевых реквизитов ИР Заказчика, в срок не более 2 рабочих дней с момента их изменения.
  10. Предоставление в ЦЗИиСС, через ЛК SOC, а также в КЦ ГосСОПКА с использованием каналов взаимодействия, указанных в разделе 4 Регламента, сведений об ИР (наименование ИР, используемое телекоммуникационное оборудование и программное обеспечение, а также общее и специальное программное обеспечение).

2.11 Сроки предоставления Заказчиком информации, указанной в настоящем разделе Регламента, приведены в разделе 6 Регламента.

1. **Перечень передаваемой информации**

В рамках взаимодействия между участниками информационного обмена: Заказчиком и ЦЗИиСС через ГосСОПКА, может передаваться информация:

* о КИ в ИР в соответствии с определенными НКЦКИ форматами, в том числе требующих содействия в реагировании со стороны ЦЗИиСС;
* о признаках КИ в соответствии с форматами, определенными НКЦКИ;
* о мерах, предпринятых для локализации КИ в ИР, а также о результатах этих мер;
* о выявленных угрозах безопасности информации, реализация которых может повлиять на штатное функционирование ИР и о необходимых мерах по противодействию им;
* о средствах и способах проведения КА и о методах их обнаружения, предупреждения и противодействия им;
* содержащая запросы на получение дополнительных сведений об угрозах безопасности информации и вредоносной активности;
* содержащая сведения об ИР.

Информационные сообщения и запросы, передаваемые по каналам взаимодействия, не должны содержать информацию, составляющую охраняемую законом Российской Федерации тайну.

1. **Каналы взаимодействия**

При передаче информации, указанной в разделах 2 и 3 Регламента, в качестве основных каналов передачи информации в адрес ЦЗИиСС и ГосСОПКА Исполнителем используются:

* средства автоматизированного обмена информацией между Заказчиком и ГосСОПКА – ЛК SOC, на основе программного интерфейсаКЦ ГосСОПКА;
* электронная почта Заказчика и Исполнителя, указанная в Приложении 1 к Договору и (или) Заказе на Услугу.

В качестве дополнительных каналов передачи информации используются:

* телефонная связь, номерателефонов Заказчика и Исполнителя, указанные в Приложении 1 к Договору и (или) Заказе на Услугу*.*

1. **Порядок взаимодействия участников информационного обмена**

Информации о КИ в информационных ресурсах, находящихся в зоне ответственности Заказчика, передаваемой Заказчиком в ЦЗИиСС, в ТИ НКЦКИ присваивается уникальный идентификатор КИ.

**6. Сроки предоставления информации**

Информация о КИ, связанном с функционированием значимых объектов КИИ, в соответствии с пунктом 4 Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденного приказом ФСБ России от 19 июня 2019 г. № 282, направляется Заказчиком в НКЦКИ и в КЦ ГосСОПКА в срок не позднее **3-х часов** с момента обнаружения КИ.

Информация о КИ, связанном с функционированием иных ИР, не указанных выше, т.е. об ОИИ передаётся Заказчиком в НКЦКИ и в КЦ ГосСОПКА в срок не позднее **24-х часов** с момента его обнаружения.

Сведения об изменении внешних сетевых реквизитов ИР передаются Заказчиком в ЦЗИиСС и КЦ ГосСОПКА в срок не более **2-х рабочих дней** с момента указанных изменений.

Передача Заказчиком сведений в ЦЗИиСС и КЦ ГосСОПКА об ИР (наименование ИР, используемое телекоммуникационное оборудование и программное обеспечение, а также общее и специальное программное обеспечение) осуществляется в течение **10-ти рабочих дней** с момента включения (изменения) ИР.

**Приложение № 4**

**к Договору на оказание услуг**

**№\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_/\_\_\_/\_\_\_.**

**СОГЛАШЕНИЕ О ПОРЯДКЕ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**(далее – Соглашение)**

1. **Общие положения**
   1. Стороны при обработке персональных данных (далее – **ПДн**) обязуются руководствоваться условиями Соглашения, требованиями Федерального закона от 27.07.2006   
      № 152-ФЗ «О персональных данных» (далее – **Закон № 152-ФЗ**), а также положениями иных нормативно-правовых актов Российской Федерации в сфере персональных данных и защиты информации.
   2. Поскольку исполнение условий Договора на оказание услуг № \_\_\_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г. (далее по тексту – «Договор»), предполагает обработку персональных данных, такие правоотношения, в соответствии с требованиями части 3 статьи 6 Закона № 152-ФЗ, следует рассматривать как поручение Заказчика обработки ПДн Исполнителю.
   3. Заказчик выступает оператором ПДн, а Исполнитель выступает в качестве лица, осуществляющего обработку ПДн по поручению Заказчика.
2. **Цели обработки ПДн и перечень ПДн**
   1. Заказчик поручает Исполнителю обработку ПДн в целях реализации Исполнителем принятых на себя обязательств по предоставлению Заказчику Услуг «Security Operation Center» (SOC) в рамках заключенного Договора на оказание услуг № \_\_\_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.
   2. Исполнитель не вправе выходить за пределы установленных данным пунктом целей. При нарушении данного обязательства Исполнитель будет являться оператором ПДн и обязуется самостоятельно обеспечивать правомерность обработки ПДн.
   3. Заказчик поручает Исполнителю обработку следующих категорий ПДн - фамилия, имя, отчество; должность; наименование организации; номер телефона; адрес электронной почты, а также иных персональных данных, перечень которых дополнительно определяется Заказчиком по тексту Договора/Заказа/Дополнительного соглашения.
3. **Перечень действий (операций) по обработке ПДн**
   1. Заказчик поручает Исполнителю обработку ПДн как с использованием средств автоматизации, так и без использования таковых средств, путем совершения следующих действий (операций) - запись, систематизация, накопление, хранение, извлечение, использование, передача (предоставление, доступ), удаление, уничтожение ПДн.
4. **Обязанности Исполнителя**
   1. Исполнитель обязуется:
      1. соблюдать принципы и правила обработки ПДн, предусмотренные Законом № 152-ФЗ;
      2. соблюдать конфиденциальность ПДн и принимать необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.
      3. обеспечивать безопасность ПДн при их обработке в информационных системах персональных данных Исполнителя (далее – ИСПДн), что в том числе должно достигаться:
      * определением угроз безопасности ПДн;
      * применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн;
      * применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
      * проведением оценки эффективности принимаемых Исполнителем мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
      * обнаружением фактов несанкционированного доступа к ПДн и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них;
      * восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
      * установлением правил доступа к ПДн, обрабатываемым в ИСПДн, обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
      * обеспечением контроля за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.
      1. принимать меры, установленные статьей 18.1. Закона № 152-ФЗ;
      2. по запросу Заказчика предоставить документы и иную информацию, подтверждающую принятие Исполнителем мер и соблюдение обязанности по обеспечению безопасности ПДн, а также документов, подтверждающих принятие Исполнителем мер, предусмотренных статьей 18.1. Закона № 152-ФЗ;
      3. осуществлять обработку ПДн только с использованием баз данных, находящихся на территории Российской Федерации, если иное не предусмотрено Договором;
      4. в случае установления Исполнителем факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, уведомить Заказчика:

* о произошедшем инциденте;
* предполагаемых причинах, повлекших нарушение прав субъектов ПДн;
* предполагаемом вреде, нанесенном правам субъектов ПДн;
* о принятых мерах по устранению последствий соответствующего инцидента в разумные сроки, но не позднее 24 (двадцати четырех) часов с момента его выявления.

Дополнительно необходимо уведомить Заказчика о результатах проведенного Исполнителем внутреннего расследования выявленного инцидента и предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии такой информации) в разумные сроки, но не позднее 72 (семидесяти двух) часов с момента его выявления.

1. **Порядок взаимодействия с субъектами ПДн и   
   уполномоченным органом по защите прав субъектов ПДн (Роскомнадзором)**
   1. Исполнитель при получении от уполномоченного органа по защите прав субъектов ПДн, иного органа государственной власти или суда запроса информации об обработке ПДн конкретного субъекта ПДн или при получении от субъекта ПДн (его представителя) запроса информации об обработке ПДн, отзыва согласия на обработку ПДн, требования о прекращении обработки ПДн, или иного запроса, обязуется направить копию полученного запроса (отзыва, требования) в адрес Заказчика в течение 2 (двух) рабочих с даты получения запроса (отзыва, требования).
2. **Гарантии Заказчика**
   1. Заказчик гарантирует Исполнителю наличие соответствующих правовых оснований на передачу ПДн/поручение обработки ПДн. Заказчик обязуется за собственный счет обеспечить для Исполнителя отсутствие любых претензий (требований), связанных с неправомерной обработкой ПДн. В случае нарушения указанной гарантии, Заказчик возмещает Исполнителю убытки.
3. **Порядок привлечения третьих лиц к обработке ПДн**
   1. Исполнитель вправе привлекать к обработке ПДн третьих лиц только после получения согласия (поручения на привлечение третьего лица) от Заказчика.
   2. Если Исполнитель получил согласие Заказчика на привлечение третьих лиц, Исполнитель обязуется заключить с третьим лицом соглашение, которое должно включать в себя аналогичные требования, ограничения и условия обработки ПДн, которые содержатся в настоящем Соглашении.
4. **Сроки обработки ПДн**
   1. Исполнитель обязуется прекратить обработку ПДн и/или обеспечить ее прекращение (в случае привлечения к обработке ПДн третьего лица) и уничтожить ПДн или обеспечить их уничтожение (в случае привлечения к обработке ПДн третьего лица) в срок, не превышающий 30-ти календарных дней или в сроки, установленные в уведомлении Заказчика, при наступлении одного из следующих событий:
   * прекращение действия Соглашения или Договора;
   * получение Исполнителем от Заказчика уведомления о необходимости прекращения обработки ПДн;
   * достижение Исполнителем заявленных Заказчиком целей обработки ПДн или утраты необходимости в достижении такой цели.
5. **Ответственность**
   1. В случае нарушения Исполнителем, т.е. неисполнения или ненадлежащего исполнения Исполнителем какого-либо из предусмотренных Соглашением обязательств, Заказчик вправе требовать от Исполнителя возместить Заказчику убытки.
6. **Срок действия Соглашения**
   1. Соглашение является неотъемлемой частью Договора на оказание услуг № \_\_\_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г. Соглашение вступает в силу с даты его подписания Сторонами и действует в течении всего срока действия Договора.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **От имени Исполнителя** | |  | | **От имени Заказчика** | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_/  МП | |  | | Исполнительный директор  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Салпагаров И.Б./  МП | |
|  |  | |  | |
|  |  | |  | |

**5.** **Информационная карта открытого запроса предложений**

Настоящее Информационная карта об открытом запросе предложений содержит информацию и данные для конкретного открытого запроса предложений, уточняющие, дополняющие, а в некоторых случаях изменяющие отдельные положения разделов 1 – 4 Документации о проведении открытого запроса предложений.

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Название пункта** | **Текст пояснений** |
| **1** | **Наименование, место нахождения, почтовый адрес и адрес электронной почты, номер контактного телефона и факса Заказчика/ Организатора размещения заказа, адрес официального сайта, на котором размещены Извещение и Документация о проведении открытого запроса предложений** | Заказчик (Организатор): Публичноое акционерное общество «Ставропольэнергосбыт» (ПАО «Ставропольэнергосбыт»).  Место нахождения 357633, Ставропольский край, г. Ессентуки, ул. Большевистская, 59а  E-mail: s.vetlitskiy@staves.ru  Телефон/Факс: (87934) 4-26-84  Контактное лицо: Ветлицкий Станислав Юрьевич  Официальный сайт ПАО «Ставропольэнергосбыт» в сети Интернет, на котором размещены Извещение и Документация о проведении открытого запроса предложений: [www.staves.ru](http://www.staves.ru), в разделе закупки/текущие закупки/2025/проведение процедур закупок в 2025г. |
| **2** | **Способ закупки** | Открытый запрос предложений |
| **3** | **Предмет открытого запроса предложений** | Оказание услуг по мониторингу и реагированию на инциденты информационной безопасности и организацию информационного взаимодействия с ГосСОПКА для нужд ПАО «Ставропольэнергосбыт». |
| **4** | **Перечень работ по предмету открытого запроса предложений** | Перечень и объемы выполняемых работ указаны в техническом задании настоящего запроса предложений (раздел 2 документации). |
| **5** | **Сведения о начальной (максимальной) цене договора (цене лота)** | Начальная (максимальная) цена Договора составляет 3 835 000 руб. 00 коп. без НДС |
| **6** | **Порядок формирования цены договора** | Начальная (максимальная) цена контракта обоснована и сформирована в текущем уровне цен |
| **7** | **Сведения о валюте, используемой для формирования цены договора и расчетов по договору** | Российский рубль |
| **8** | **Порядок применения официального курса иностранной валюты к рублю РФ, установленного ЦБ РФ и используемого при оплате заключенного договора** | Не используется. |
| **9** | **Сведения о возможности Заказчика изменить предусмотренные договором количество товаров, объем работ, услуг и процент такого изменения** | Возможно в проценте согласованном сторонами |
| **10** | **Форма, сроки и порядок оплаты товара, работы, услуги** | Безналичный расчет. Оплата производится в соответствии с проектом договора к настоящей Документации. |
| **11** | **Срок, место подачи Заявок на участие в открытом запросе предложений** | Начало подачи Заявок на участие в открытом запросе предложений: 30.04.2025 г.  Окончание подачи Заявок на участие в открытом запросе предложений: 10:00 (по московскому времени) 14.05.2025г.  Предложения на участие в открытом запросе предложений подаются ежедневно по рабочим дням с 09:00 до 18:00 (понедельник – пятница), по адресу: г. Ессентуки, ул. Большевистская, 59 а, кабинет №303 в ОМТС. |
| **12** | **Место и дата рассмотрения предложений участников закупки и подведения итогов закупки** | г. Ессентуки, ул. Большевистская, 59 а, конференц- зал ПАО «Ставропольэнергосбыт», 14.05.2025 г. в 12:00 по московскому времени. |
| **13** | **Срок отказа от проведения открытого запроса предложений** | За один день до момента окончания приема предложений для участия в открытом запросе предложений |
| **14** | **Критерии оценки Предложений участников, значимость таких критериев и порядок оценки** | В соответствии с Положением о закупках товаров, работ, услуг ПАО «Ставропольэнергосбыт» и документации открытого запроса предложений |

**6. Форма письма о подаче предложения (оферты).**

|  |  |
| --- | --- |
| Реквизиты организации, или ИП на фирменном бланке | **Исполнительному директору**  **ПАО «Ставропольэнергосбыт»,**  **Председателю закупочной комиссии**  **И. Б. Салпагарову** |

Изучив извещение о проведении открытого запроса предложений, опубликованное на официальном на сайте ПАО «Ставропольэнергосбыт» www.staves.ru в разделе закупки/текущие закупки/2025/проведение процедур закупок в 2025г., и Документацию по открытому запросу на право заключения договора на оказание услуг по мониторингу и реагированию на инциденты информационной безопасности и организацию информационного взаимодействия с ГосСОПКА для нужд ПАО «Ставропольэнергосбыт» в 2025г., от 30.04.2025г. и, принимая установленные в них требования и условия открытого запроса предложений, --------------------------- (Наименование организации), зарегистрированное по адресу-------------------------, предлагает заключить Договор на оказание услуг по мониторингу и реагированию на инциденты информационной безопасности и организацию информационного взаимодействия с ГосСОПКА для нужд ПАО «Ставропольэнергосбыт» в 2025г., на условиях и в соответствии с коммерческим предложением, и другими документами, являющимися неотъемлемыми приложениями к настоящему письму и составляющими вместе с настоящим письмом Предложение, на общую сумму---------------- **(указать сумму).**

**Наличие лицензий-------------------------**

**К письму прилагаются:**

1

2

3

Настоящая заявка действует до (указать дату), ***но не менее 60дней****.*

**Участник размещения заказа: (Подпись, печать)**

**7. Критерии оценок и сопоставления заявок**

**КРИТЕРИИ И ПОРЯДОК ОЦЕНКИ ЗАЯВОК НА УЧАСТИЕ В ЗАКУПКЕ**

1. Настоящий порядок применяется для проведения оценки заявок на участие в конкурсе и оценки заявок на участие в запросе предложений.
2. Для применения настоящего порядка Заказчику необходимо включить в конкурсную документацию, документацию о запросе предложений конкретные критерии из числа нижеперечисленных, конкретизировать предмет оценки по каждому критерию, установить требования о предоставлении документов и сведений соответственно предмету оценки по каждому критерию, установить значимость критериев.
3. Совокупная значимость всех критериев должна быть равна 100%.
4. Оценка и сопоставление заявок в целях определения победителя (победителей) процедуры осуществляется ЗК с привлечением при необходимости экспертов в соответствующей области предмета закупки.
5. Для оценки заявок могут использоваться следующие критерии с соответствующими предельным значимостями:

| **Номер  критерия** | **Критерии оценки  заявок** | **Для проведения оценки в документации необходимо установить:** | **Значимость критериев в процентах.**  **Точная значимость критерия должна быть установлена заказчиком в документации** |
| --- | --- | --- | --- |
| 1 | Цена договора | Итоговая сумма не должна превышать максимальную | 50% |
| 2 | Квалификация участника | Конкретный предмет оценки по критерию (приложить ряд соответствующих лицензий и допусков к данным видам услуг) | 25% |
| 3 | Надежность и деловая репутация участника | Требования о предоставлении документов и сведений по соответствующему предмету оценки (приложить реестр договоров подобных услуг) | 25% |

1. Оценка заявок осуществляется в следующем порядке.
   1. Для оценки заявки осуществляется расчет итогового рейтинга по каждой заявке. Итоговый рейтинг заявки рассчитывается путем сложения рейтингов по каждому критерию оценки заявки, умноженных на их значимость.
   2. Присуждение каждой заявке порядкового номера по мере уменьшения степени привлекательности предложения участника производится по результатам расчета итогового рейтинга по каждой заявке. Заявке, набравшей наибольший итоговый рейтинг, присваивается первый номер. Первый номер может быть присвоен нескольким заявкам, набравшим наибольший итоговый рейтинг. Дальнейшее распределение порядковых номеров заявок осуществляется в порядке убывания итогового рейтинга.
   3. Для получения рейтинга заявок по критериям «Квалификация участника», «Надежность, деловая репутация» каждой заявке по каждому из критериев ЗК выставляется значение от 0 до 100 баллов.

Рейтинг, присуждаемый заявке по критерию «Цена договора», определяется по формуле:

,

где:

Rai - рейтинг, присуждаемый i-й заявке по указанному критерию;

Amax - начальная цена договора;

Ai - цена договора, предложенная i-м участником.

Для расчета итогового рейтинга по заявке рейтинг, присуждаемый этой заявке по критерию «Цена договора», умножается на соответствующую указанному критерию значимость.

Для получения рейтинга заявок по критериям «Квалификация участника», «Качество товара», «Наличие производственных мощностей» каждой заявке по каждому из критериев ЗК выставляется значение от 0 до 100 баллов.