|  |
| --- |
| **«УТВЕРЖДАЮ»** |
| **Председатель закупочной комиссии по направлению «энергосбытовая деятельность»**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.Г. Салтыков |
| «Согласовано»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Т.В. Абрамова  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.В. Пушкарев  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.Д. Ураева  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.В. Ковалев  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.К. Абрамов  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Д.В. Момотов  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.М. Челноков  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Г.А. Жмыхов |
| 27.11.2024 г. |

**ДОКУМЕНТАЦИЯ**

**Аукцион в электронной форме**

Мониторинг ИБ на базе системы RUSIEM в течение 12 мес.

**Калуга**

**2024 год**

СОДЕРЖАНИЕ:

1. [ОБЩИЕ ПОЛОЖЕНИЯ………………………………………………………………….….3](#_Toc116632198)
2. **ТЕХНИЧЕСКОЕ ЗАДАНИЕ…………..……………………………….…………………....6**
3. **ОБЩИЙ ПОРЯДОК ПРОВЕДЕНИЯ АУКЦИОНА………………………………….....23**
4. [ОБРАЗЦЫ ОСНОВНЫХ ФОРМ ДОКУМЕНТОВ, ВКЛЮЧАЕМЫХ В](#_Toc116632210) заявку……………………………………………………………………………………... 30
5. ПРИЛОЖЕНИЕ 1 (Проект договора)…………………………………………..….35

**6. ПРИЛОЖЕНИЕ 2 (ОБОСНОВАНИЕ НМЦД)………………………………………….56**

# ОБЩИЕ ПОЛОЖЕНИЯ

## Общие сведения об аукционе

Заказчик (Организатор) – ПАО «Калужская сбытовая компания», юр. адрес: 248001, г. Калуга, пер. Суворова, д.8, Извещением о проведении аукциона в электронной форме, опубликованным 27.11.2024 г. в Единой информационной системе в сфере закупок https://zakupki.gov.ru, на официальном сайте Заказчика https://kskkaluga.ru и на электронной торговой площадке Газпромбанка (ЭТП ГПБ) https://etpgpb.ru, приглашает юридических лиц и индивидуальных предпринимателей к участию в аукционе в электронной форме.

### Настоящий аукцион проводится в соответствии с правилами и с использованием функционала ЭТП ГПБ.

### Предмет аукциона – оказание услуг по мониторингу и анализу инцидентов информационной безопасности информационных ресурсов и разработке организационно-распорядительной документации.

### Количество лотов — 1 (один).

### Объемы закупаемой продукции и подробные требования изложены в Техническом задании (здесь и далее ссылки относятся к настоящей Документации). Проект договора, который будет заключен по результатам Аукциона, приведен в Приложении № 1 к Документации. Порядок проведения аукциона и участия в нем, а также инструкции по подготовке заявок, приведены в Разделе 3. Формы документов, которые необходимо подготовить и подать в составе заявки, приведены в Разделе 4.

1.1.5. Начальная (максимальная) цена договора рассчитана как минимальное значение предложенных цен, от четырех исполнителей аналогичных видов услуг в размере:  
**- 1 600 000 (Один миллион шестьсот тысяч) рублей 00 копеек**, в том числе НДС 20% - 266 666 руб. 67 коп.

### Обеспечение заявки на участие в закупке: не требуется.

Обеспечение исполнения договора: не требуется.

### Для справок обращаться: Момотов Дмитрий Владимирович – начальник службы АСУ и телекоммуникаций, тел.: (4842)701-869, [momotov@ksk.kaluga.ru](mailto:momotov@ksk.kaluga.ru); Жмыхов Георгий Андреевич – начальник отдела информационной безопасности, тел.: (4842)701-847, zhmykhov.ga@ksk.kaluga.ru.

### В условия аукциона, прежде всего (но не ограничиваясь) в Техническое задание, в проект Договора, в требования к Участникам, могут быть внесены изменения, в том числе существенные.

### Для участия в аукционе юридическое лицо или индивидуальный предприниматель должны быть зарегистрированы в системе ЭТП ГПБ в качестве участников данной системы, т.е., должны заключить соответствующий договор с оператором системы в соответствии с правилами, условиями и порядком регистрации системы ЭТП ГПБ, а также должны быть зарегистрированы системой ЭТП ГПБ в качестве Участника данного аукциона в установленном порядке.

### Участники аукциона должны подать заявки в электронном виде через систему ЭТП ГПБ.

## Правовой статус документов

### Аукцион проводится в соответствии с «Положением о порядке проведения регламентированных закупок товаров, работ, услуг для нужд ПАО «Калужская сбытовая компания», утвержденным решением Совета Директоров ПАО «Калужская сбытовая компания».

### Опубликованное Извещение о проведении Аукциона вместе с настоящей Документацией, являющейся его неотъемлемым приложением, не являются офертой Заказчика (Организатора) закупки и должны рассматриваться Участниками аукциона в соответствии с этим в течение срока, определенного для проведения Аукциона.

### Заключенный по результатам Аукциона и преддоговорных переговоров Договор фиксирует все достигнутые сторонами договоренности.

### При определении условий договора с Победителем используются следующие документы с соблюдением указанной иерархии (в случае их противоречия):

* Протокол преддоговорных переговоров между Заказчиком и Победителем (по условиям, не оговоренным ни в настоящей Документации, ни в Предложении Победителя аукциона);

- Извещение о проведении Аукциона и настоящая Документация со всеми дополнениями и разъяснениями;

- Предложение Победителя со всеми дополнениями и разъяснениями, соответствующими требованиям заказчика.

- Иные документы Заказчика и Участников Аукциона не определяют права и обязанности сторон в связи с данным Аукционом.

### Во всем, что не урегулировано Извещением о проведении Аукциона и настоящей Закупочной документацией, стороны руководствуются законодательством Российской Федерации.

### Если в отношении сторон договора, заключаемого по результатам Аукциона, действуют также иные специальные нормативно-правовые акты, изданные и зарегистрированные в установленном порядке, настоящая Закупочная документация (и проект договора как ее часть) и Предложение Победителя Аукциона будут считаться приоритетными по отношению к диспозитивным нормам указанных документов.

## Обжалование

### Настоящий аукцион не является офертой или публичной офертой Заказчика.

### Любой участник, который заявляет о нарушении своих прав Заказчиком (Организатором) или отдельными членами закупочной комиссии по направлению «энергосбытовая деятельность» (далее – закупочная комиссия), имеет право подать заявление о рассмотрении разногласий, связанных с проведением аукциона (далее — разногласий).

### Все споры и разногласия, возникающие в связи с проведением аукциона, в том числе касающиеся исполнения Заказчиком и Участниками аукциона своих обязательств, в связи с проведением аукциона и участия в нём, должны решаться в претензионном порядке. Для реализации этого порядка заинтересованная сторона в случае нарушения её прав должна обратиться с претензией к другой стороне. Сторона, получившая претензию, должна направить другой стороне мотивированный ответ на претензию в течение 20 рабочих дней с момента её получения.

### Все споры и разногласия, возникающие в связи с проведением аукциона, в том числе, касающиеся исполнения Заказчиком и Участниками аукциона своих обязательств, не урегулированные в порядке, предусмотренном п.1.3.3, могут быть решены в Арбитражном суде Калужской области в соответствии с документами, определяющими его правовой статус и порядок разрешения споров, действующими на дату подачи искового заявления.

## Прочие положения

### Участник самостоятельно несет все расходы, связанные с подготовкой и подачей заявки, а Заказчик по этим расходам не отвечает и не имеет обязательств, независимо от хода и результатов процедуры, за исключением случаев, прямо предусмотренных действующим законодательством Российской Федерации.

### Предполагается, что Участник изучит все инструкции, формы, условия, технические условия и другую информацию, содержащуюся в Закупочной документации. Никакие претензии Заказчику не будут приниматься на том основании, что Участник не понимал какие-либо вопросы. Неполное представление информации, запрашиваемой в Закупочной документации, или же подача Предложения, не отвечающего требованиям Закупочной документации, представляют собой риск для Участника и может привести к отклонению его Предложения.

### Заказчик обеспечивает разумную конфиденциальность относительно всех полученных от Участников Аукциона сведений, в том числе содержащихся в заявках. Предоставление этой информации другим Участникам или третьим лицам возможно только в случаях, прямо предусмотренных действующим законодательством Российской Федерации или настоящей Закупочной документацией.

### Заказчик, по решению закупочной комиссии, вправе отклонить заявку, если он установит, что Участник прямо или косвенно дал, согласился дать или предложил сотруднику Заказчика вознаграждение в любой форме: работу, услугу, какую-либо ценность, в качестве стимула, который может повлиять на принятие закупочной комиссией решения по определению Победителя аукциона.

### Заказчик, по решению закупочной комиссии, вправе отклонить заявки Участников, заключивших между собой какое-либо соглашение с целью повлиять на определение Победителя.

# ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на оказание услуг по мониторингу и анализу инцидентов информационной безопасности информационных ресурсов и разработке организационно-распорядительной документации

г. Калуга, 2024

1. **Определения и сокращения**
   1. В настоящем документе применяются следующие термины с соответствующими определениями:

**Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)** –единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

**Заказчик** – Публичное акционерное общество "КАЛУЖСКАЯ СБЫТОВАЯ КОМПАНИЯ".

**Зона ответственности –** совокупность информационных ресурсов, в отношении которых субъектом ГосСОПКА обеспечиваются обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты.

**Информационная безопасность (ИБ)** – комплекс организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность дает гарантию обеспечения следующих целей: конфиденциальность информации (свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц); целостность информации и связанных с ней процессов (неизменность информации в процессе ее передачи или хранения); доступность информации, когда она нужна (свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц); учет всех процессов, связанных с информацией.

**Информационный ресурс** – информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления.

**Исполнитель** – организация (юридическое лицо) либо индивидуальный предприниматель, выбранная/выбранный Заказчиком по результатам проведения открытого аукциона в электронной форме.

**Компьютерная атака** – целенаправленное воздействие программных и (или) программно-аппаратных средств на информационный ресурс в целях нарушения и (или) прекращения его функционирования и (или) создания угрозы безопасности, обрабатываемой таким ресурсом информации.

**Компьютерный инцидент** – факт нарушения и (или) прекращения функционирования информационного ресурса, сети электросвязи, используемой для организации взаимодействия информационных ресурсов, и (или) нарушения безопасности, обрабатываемой в информационном ресурсе информации, в том числе произошедший в результате компьютерной атаки.

**Критическая информационная инфраструктура (КИИ)** – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

**Национальный координационный центр по компьютерным инцидентам (НКЦКИ) –** наивысшая структура в иерархии ГосСОПКА, осуществляющая нормативное и методическое сопровождение.

**Объекты критической информационной инфраструктуры** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

**Субъекты ГосСОПКА** – государственные органы Российской Федерации, российские юридические лица и индивидуальные предприниматели в силу закона или на основании заключенных с ФСБ России соглашений, осуществляющие обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

**Субъекты критической информационной инфраструктуры** – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

**ТЗ** –техническое задание на оказание услуг по Договору.

**ФСБ России -** Федеральная служба безопасности Российской Федерации.

**ФСТЭК России** - Федеральная служба по техническому и экспортному контролю.

**SIEM-система (Security Information and Event Manager)** - Система сбора и обработки событий информационной безопасности.

**2. Общие сведения**

**2.1.** В соответствии с настоящим Техническим заданием Исполнитель должен оказать услуги по мониторингу и анализу инцидентов информационной безопасности информационных ресурсов Заказчика, взаимодействию с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак и разработке организационно-распорядительной документации (далее – услуги).

Результатом оказания услуг по настоящему Техническому заданию является представление Сводных отчетов по мониторинг и анализ инцидентов информационной безопасности информационных ресурсов Заказчика, взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак и разработанная организационно-распорядительной документации.

* 1. **Заказчик -** Публичное акционерное общество "Калужская сбытовая компания"

ИНН/КПП: 4029030252 / 402801001.

Юридический адрес: 248001, г. Калуга, пер. Суворова, д. 8.

* 1. **Исполнитель -**  определяется по результатам проведения открытого аукциона в электронной форме.
  2. **Основание для оказания услуг**
* Договор на оказание услуг по мониторингу и анализу инцидентов информационной безопасности информационных ресурсов и разработке организационно-распорядительной документации (далее – Договор).
  1. **Место оказания услуг**

Оказание услуг осуществляется применительно к информационным ресурсам Заказчика, развернутым на объекте информатизации, расположенном по адресу: 248001, г. Калуга, пер. Суворова, д. 8.

* 1. **Объект оказания услуг**

Объектом оказания услуг является программные и программно-технические средства, включенные в состав информационных ресурсов Заказчика и являющиеся источниками событий ИБ, приведенные в Таблице 1.

Таблица № 1

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Тип источника событий ИБ** | **Наименование** | **Количество** |
|  | Межсетевой экран | UserGate 500 | 1 |
|  | Контроллеры домена | Active Directory | 2 |
|  | Рабочие станции под управлением ОС Windows |  | 2 |
|  | Сервера под управлением ОС Windows |  | 1 |
|  | Сервера под управлением ОС Linux |  | 3 |
|  | Сервер электронной почты | Kaspersky Secure Mail Gateway (KSMG) | 1 |
|  | Прокси-сервер |  | 1 |
|  | Антивирус с централизованным управлением, расположенный на отдельном сервере | Kaspersky Security Center (KSC) | 1 |
|  | Наличие VPN (координатор защищенной сети), с учетом филиалов | АПКШ «Континент 3.9» (Сервер доступа) | 1 |

* 1. **Цели и задачи оказания услуг**

Целями оказания услуг является:

* обеспечение непрерывности процесса защиты информации;
* повышение уровня защиты информации, содержащейся в информационных ресурсах Заказчика
* выполнение требований нормативных правовых актов и методических документов Российской Федерации в сфере защиты информации.

Задачи, которые должны быть решены в ходе оказания услуг:

* подключение инфраструктуры Заказчика к Центру мониторинга Исполнителя;
* инвентаризация информационных ресурсов (узлов);
* проведение оптимизации предоставляемой услуги под инфраструктурные особенности и технические требования Заказчика;
* обеспечение постоянного мониторинга компьютерных инцидентов ИБ Заказчика;
* регистрация компьютерных атак и компьютерных инцидентов;
* информационное обеспечение для своевременного реагирования на компьютерные инциденты ИБ;
* информационное обеспечение для своевременной ликвидации последствий компьютерных инцидентов;
* анализ угроз информационной безопасности и консолидация компьютерных событий и инцидентов ИБ;
* предоставление аналитической отчетности;
* обеспечение взаимодействие с НКЦКИ.
  1. **Состав и сроки оказания услуг**
* Начало оказания услуг – после подписания Договора Сторонами со дня развертывания Исполнителем инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика

Срок оказания услуг – 12 месяцев ( 1 год).

В состав услуг входит:

* развертывание инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика;
* мониторинг, выявление и реагирование на события информационной безопасности;
* разработка организационно-распорядительной документации.

Очередность и сроки оказания отдельных составляющих услуг указаны в разделе 4 настоящего ТЗ.

* 1. **Нормативно-технические документы, методические материалы, регламентирующие оказание услуг**
* Указ Президента Российской Федерации от 22.12.2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
* Федеральный закон №187 от 26.07.2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации»;
* Приказ ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам (НКЦКИ)»;
* Приказ ФСБ России от 24.07.2018 г. № 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 г. № 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 06 мая 2019 г. №196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»;
* Приказ ФСБ России от 19 июня 2019 г. №281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»;
* Приказ ФСБ России от 19 июня 2019 г. №282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятие мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;
* Методические рекомендации ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
* Методические рекомендации ФСБ России по обнаружению компьютерных атак на информационные ресурсы Российской Федерации;
* Методические рекомендации ФСБ России по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации;
* Методические рекомендации НКЦКИ по проведению мероприятий по оценке степени защищенности от компьютерных атак.
  1. **Требования к Исполнителю**

Исполнитель должен соответствовать требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим оказание услуг, являющихся объектом закупки, а именно:

* наличие собственной действующей лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), при условии наличия в данной действующей лицензии работ (услуг), предусмотренных пунктами «12», «20» Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств, утверждённого постановлением Правительства Российской Федерации от 16.04.2012 № 313;
* наличие собственной действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, при условии наличия в данной действующей лицензии работ (услуг), предусмотренных подпунктами «б», «в», «е», пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого постановлением Правительства Российской Федерации от 03.02.2012 № 79.

1. **Требования к оказанию услуг**
   1. В соответствии с настоящим Техническим заданием Исполнитель должен оказать услуги в следующем порядке после завершения развертывания инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика:

- мониторинг, выявление и реагирование на события информационной безопасности;

- разработка организационно-распорядительной документации**;**

- взаимодействие с органами ГосСОПКА.

* 1. **Требования к развертыванию инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика**

Развертывание инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика включает:

* обследование действующей инфраструктуры Заказчика;
* подключение инфраструктуры Заказчика к Центру мониторинга Исполнителя.
  1. **Требования к обследованию действующей инфраструктуры Заказчика**

В рамках проведения обследования действующей инфраструктуры Заказчика Исполнитель должен обеспечить:

* сбор исходных данных об основных источниках событий ИБ инфраструктуры Заказчика;
* модернизацию структурно-функциональной схемы основных источников событий ИБ;
* документальную фиксацию количественных и качественных характеристик основных источников событий ИБ инфраструктуры Заказчика.
  1. **Требования к сбору исходных данных об инфраструктуре Заказчика**

Для достижения требуемого результата Исполнитель должен реализовать сбор исходных данных инфраструктуры Заказчика на предмет идентификации и учета источников ИБ, подлежащих мониторингу, посредством:

* проведения интервьюирования ответственного персонала Заказчика;
* фактической оценки наличия программных и технических средств в инфраструктуре Заказчика;
* инструментальной инвентаризации источников событий ИБ.

Для достижения требуемого результата Заказчик должен обеспечить:

* назначение ответственных со стороны Заказчика (Ф.И.О., должности и контактные данные лиц, ответственных за функционирование информационного ресурса);
* предоставление сведений об информационных ресурсах (назначении, архитектуре объекта, применяемых программных средствах (системном, прикладном программном обеспечении и т.п.), информационных средствах (базах данных, файлах данных и т.п.), программно-аппаратных средствах (компьютерах, серверах, коммутационном оборудовании, носителях данных и т.п.; сведения о взаимодействии информационных ресурсов с другими информационными ресурсами и (или) о зависимости функционирования информационных ресурсов от других таких объектов;
* предоставление доступа к источникам событий информационной безопасности в инфраструктуре Заказчика.

По результату сбора исходных данных Исполнитель должен разработать документ Предварительный перечень источников событий ИБ для осуществления мониторинга.

* 1. **Требования к модернизации структурно-функциональной схемы основных источников событий ИБ**

Структурно-функциональная схема основных источников событий ИБ предоставляется Заказчиком и при необходимости дорабатывается Исполнителем.

После доработки Исполнителем, структурно-функциональная схема основных источников событий ИБ должна содержать:

состав и взаимосвязи между основными источниками событий ИБ.

* 1. **Требования к документальной фиксации количественных и качественных характеристик инфраструктуры Заказчика**

Для достижения требуемого результата Исполнитель должен обеспечить документальную фиксацию исходных характеристик инфраструктуры Заказчика в режиме штатного функционирования на момент начала оказания Услуг.

Полученные исходные характеристики должны быть согласованы с Заказчиком и использоваться Исполнителем в рамках оказания Услуг в части обнаружения изменений и\или отклонений в их значениях, в случаях, когда такие изменения влияют или могут повлиять на штатное функционирование инфраструктуры Заказчика.

Документальной фиксации подлежат:

* итоговый состав источников событий ИБ;
* сведения о каждом из источников событий ИБ;
* технологический статус источников событий ИБ (подключен/не подключен к SIEM-системе);
* особенности инфраструктуры Заказчика, которые влияют или могут повлиять на качество оказываемых Услуг;
* планируемый к реализации способ получения доступа Исполнителя к ресурсам SIEM-системы.

Результаты документальной фиксации должны быть оформлены в форме Отчета по результатам обследования действующей инфраструктуры Заказчика.

* 1. **Требования к подключению инфраструктуры Заказчика к Центру мониторинга Исполнителя**

В рамках подключения инфраструктуры Заказчика к Центру мониторинга Исполнитель обеспечивает:

* настройку защищенного канала связи между инфраструктурой Заказчика и центром мониторинга Исполнителя;
* настройку SIEM-системы;
* методическое и консультационное сопровождение Заказчика по подключению источников событий ИБ к SIEM-системе;
* организацию взаимодействия с НКЦКИ для обмена информацией о компьютерных инцидентах ИБ;
* разработку регламента взаимодействия сторон в рамках оказания услуг по мониторингу событий ИБ;
* приемочные испытания системы сбора событий ИБ Заказчика.
  1. **Требования к настройке защищенного канала связи между инфраструктурой Заказчика и центром мониторинга Исполнителя**

Для достижения требуемого результата Исполнитель должен обеспечить защиту канала связи между технологической площадкой Заказчика и центром мониторинга Исполнителя.

Защита канала связи должна обеспечиваться с использованием средств криптографической защиты информации, имеющих действующий сертификат ФСБ России.

Защищенный канал связи должен обеспечивать технологический информационный обмен в рамках сбора информации о событиях ИБ в объеме достаточном для оказания Услуг.

* 1. **Требования к настройке SIEM-системы**

Для достижения требуемого результата Исполнитель должен осуществить настройку SIEM-системы, имеющийся у Заказчика, в объеме, предусмотренном эксплуатационной документацией производителя системы.

* 1. **Требования к методическому и консультационному сопровождению Заказчика по подключению источников событий ИБ к SIEM-системе**

Для достижения требуемого результата Исполнитель должен осуществить подключение источников событий ИБ, выявленных в рамках обследования действующей инфраструктуры Заказчика и имеющих статус «не подключен к SIEM-системе», по решению Заказчика и в объеме достаточном для подключения к SIEM-системе.

* 1. **Требования к организация взаимодействия с НКЦКИ для обмена информацией о компьютерных инцидентах ИБ**

В рамках организации взаимодействия с НКЦКИ для обмена информацией о компьютерных инцидентах ИБ Исполнитель в течение 5 (Пяти) рабочих дней, с момента заключения Договора, должен обеспечить:

- отправку уведомления в адрес НКЦКИ о включении ресурсов Заказчика в зону ответственности Центра мониторинга Исполнителя;

- разработку проекта уведомления о принятом решении информировать НКЦКИ через Центр ГосСОПКА.

Для достижения требуемого результата Заказчик в течение 5 (Пяти) рабочих дней, с момента получения от Исполнителя проекта уведомления, должен обеспечить:

оформление и отправку уведомления о принятом решении информировать НКЦКИ через Центр ГосСОПКА.

* 1. **Требования к разработке регламента взаимодействия сторон в рамках оказания услуг по мониторингу событий ИБ**

Регламент разрабатывается Исполнителем с учетом специфики эксплуатации инфраструктуры Заказчика, подлежит согласованию с Заказчиком и должен включать следующие разделы:

* мониторинг и первичная обработка инцидентов ИБ;
* анализ инцидента ИБ;
* обработка запросов по заявкам от уполномоченных сотрудников Заказчика;
* регламент обработки высокочастотных срабатываний подозрений на инциденты ИБ;
* регламент обработки повторных подозрений на инцидент ИБ;
* разработка технических мер по блокированию инцидента;
* участие в процессе нейтрализации последствий инцидента;
* подключение новых типовых источников к Центру мониторинга;
* подключение новых нетиповых источников к Центру мониторинга;
* отключение источников от Центра мониторинга;
* реализация новых сценариев обнаружения подозрений на инциденты ИБ по инициативе Исполнителя;
* реализация новых сценариев обнаружения подозрений на инциденты ИБ по запросу уполномоченных сотрудников Заказчика;
* управление критичностью сценариев обнаружения подозрений на инциденты ИБ.
  1. **Приемочные испытания системы сбора событий ИБ**

Испытания проводятся в соответствии с Программой и методикой испытаний, разрабатываемой Исполнителем в соответствии с ГОСТ 59792-2021.

В рамках приемочных испытаний Исполнитель совместно с Заказчиком проводит оценку:

* работоспособности функционала инфраструктуры;
* достаточности подключенных к SIEM-системе источников событий ИБ;
* соответствия документации, разработанной Исполнителем, требованиям настоящего ТЗ;
* возможности приемки системы сбора событий ИБ в эксплуатацию и возможности начала Исполнителем оказания услуг по Мониторингу, выявлению и реагированию на события ИБ.

Результаты приемочных испытаний оформляются в форме:

* протокола приемочных испытаний;
* заключения по результатам приемочных испытаний.
  1. **Требования к мониторингу, выявлению и реагированию на события информационной безопасности**

Мониторинг, выявление и реагирование на события информационной безопасности включают в себя:

* обнаружение и регистрация компьютерных инцидентов;
* реагирование на компьютерные инциденты;
* выявление и анализ уязвимостей в защищаемом информационном ресурсе Заказчика;
* анализ деятельности по управлению компьютерными инцидентами;
* актуализация перечня источников событий информационной безопасности;
* формирование отчетности по мониторингу событий информационной безопасности.
  1. **Требования к обнаружению и регистрации компьютерных инцидентов**

В рамках проведения обнаружения и регистрации компьютерных инцидентов, Исполнитель осуществляет:

* сбор и анализ информации о событиях безопасности и иных данных мониторинга, необходимых для поиска признаков возможного возникновения компьютерных инцидентов;
* наблюдение за событиями ИБ в SIEM-системе, просмотр логов на предмет нахождения аномальных событий ИБ, не распознанных SIEM-системой
* регистрация признаков возможного возникновения компьютерных инцидентов;
* подтверждение факта возникновения компьютерного инцидента, определение характера влияния на информационные ресурсы с целью принятия решения о регистрации компьютерного инцидента;
* регистрация компьютерного инцидента (в случае подтверждения факта прекращения или нарушения критического процесса, или нарушения безопасности информации);

Проведение обнаружения и регистрации компьютерных инцидентов осуществляются 24 часа 7 дней в неделю.

Реагирование и оповещение о компьютерных инцидентах осуществляется в рабочие дни с 8:30 – 18:00 по московскому времени.

Реагирование и оповещение о критичных компьютерных инцидентах осуществляется 24 часа 7 дней в неделю.

* 1. **Требования к информационному обеспечению для своевременного реагирования на компьютерные инциденты**

В рамках реагирования на компьютерные инциденты Исполнитель обеспечивает:

* информирование Заказчика о компьютерном инциденте. При необходимости, по согласованию с Заказчиком, информация о компьютерном инциденте направляется Исполнителем в НКЦКИ в течение 2-х часов после согласования на отправку;
* совместно с заказчиком определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;
* обработку инцидентов, полученных из ГосСОПКА и НКЦКИ;
* оказание методической помощи Заказчику по локализации компьютерного инцидента;
* оказание методической помощи Заказчику по выявлению последствий компьютерного инцидента;
* оказание методической помощи Заказчику по ликвидации последствий компьютерного инцидента;
* закрытие компьютерного инцидента. В случае информирования НКЦКИ ранее о компьютерном инциденте, необходимо проинформировать о закрытии данного инцидента.

В случае обнаружения события, Исполнитель регистрирует и оповещает ответственного сотрудника Заказчика по средствам уведомления через мессенджер «Телеграм» в специальную группу и сотовой связи на номер ответственного со стороны заказчика для классификации события как инцидент в сроки, указанные в Таблице № 2. Оповещение ответственного сотрудника Заказчика осуществляется 24х7 в случае регистрации критического события и в рабочие дни с 08:00 до 17:00 местного времени Заказчика в остальных случаях.

Таблица № 2

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Критичность** | **Описание** | **Время оповещения** |
|  | Высокая | Сбой или отказ в работе, вызвавший полную или частичную недоступность/неработоспособность информационных ресурсов Заказчика | 1 час |
|  | Средняя | Сбой или отказ в работе, оказывающий значительное воздействие на функциональность информационных ресурсов Заказчика, производительность значительно снижена по сравнению с нормальной работой. | 3 часа |
|  | Низкая | Сбой или отказ в работе, не оказывающий или оказывающий незначительное воздействие на общую функциональность и производительность информационных ресурсов Заказчика. | 5 часов |

После подтверждения ответственным сотрудником Заказчика инцидента ИБ, Исполнитель регистрирует компьютерный инцидент и выдает рекомендации, предоставляет консультации по инциденту ИБ, путем анализа логов с источников событий ИБ и SIEM-системы. При необходимости, Исполнитель разрабатывает новые и корректирует существующие правила анализа событий информационной безопасности и данных мониторинга, а также оказывает содействие Заказчику при локализации и устранении компьютерного инцидента. Заказчик подтверждает закрытие компьютерного инцидента.

* 1. **Требования к анализу деятельности по управлению компьютерными инцидентами**

В целях проведения анализа деятельности по управлению компьютерными инцидентами, Исполнитель 1 раз в квартал на протяжении оказания услуг, осуществляет:

- идентификацию методов и способов обнаружения и реагирования на компьютерные инциденты, которые показали свою эффективность;

- разработку рекомендаций по внедрению более эффективных методов обнаружения компьютерных инцидентов и необходимым мерам по недопущению повторного возникновения компьютерных инцидентов вследствие недостаточно эффективного управления;

- разработку новых, и корректировка существующих правил анализа событий безопасности и данных мониторинга.

Заказчик проводит оценку рекомендаций и возможности их реализации. Исполнитель обеспечивает методическую помощь по внедрению данных рекомендаций.

* 1. **Требования к актуализации перечня источников событий информационной безопасности**

Исполнитель, совместно с Заказчиком 1 раз в квартал с момента подключения инфраструктуры Заказчика к Центру мониторинга осуществляет актуализацию перечня основных источников событий ИБ.

Актуализация перечня основных источников событий ИБ осуществляется с использованием защищенного канала связи.

Соответствующие изменения должны быть внесены в последующие сводные отчеты.

* 1. **Требования к формированию отчетности по мониторингу событий информационной безопасности**

Исполнитель должен предоставлять Заказчику сводные отчеты об оказании услуг, включающие информацию о подключенных источниках, типах зарегистрированных инцидентов, статистике по собранным событиям ИБ, запущенным в процессе мониторинга сценариям выявления инцидентов, доступности и работоспособности центра мониторинга Исполнителя.

Сводные отчеты предоставляются Исполнителем ежемесячно не позднее 10-го числа месяца, следующего за месяцем оказания услуг.

* 1. **Требования к разработке организационно-распорядительной документации**

Исполнитель в рамках оказания Услуг должен обеспечить Заказчику возможность разработки организационно-распорядительной документации, регламентирующей порядок обработки ПДн, в объеме достаточном для реализации организационных мер по обеспечению безопасности ПДн при их обработке в ИСПДн, предусмотренных действующим законодательством в области защиты информации.

* 1. **Общие требования к разработке ОРД**

Разработка ОРД должна быть обеспечена посредством предоставления Исполнителем доступа к веб-сервису, реализующему функции автоматизированного создания ОРД в соответствии с параметрами, заданными пользователем, (далее – Веб-сервис).

Доступ к Веб-сервису должен предоставляться Исполнителем посредством регистрации Исполнителем в базе данных нового Пользователя, уполномоченного для работы с Веб-сервисом со стороны Заказчика, (далее – Пользователь) с произвольными логином и паролем.

Данные учетной записи Пользователя предоставляются в адрес Заказчика в течение 3 (трех) рабочих дней с даты подписания Договора. Одновременно с предоставлением данных учетной записи Пользователя Исполнитель должен передать Заказчику неисключительные имущественные права (лицензию) на право использования Веб-сервиса.

Срок действия неисключительных имущественных прав (лицензии) на право использования Веб-сервиса должен соответствовать сроку гарантийных обязательств на результат оказанных Услуг, но не менее 13 месяцев с даты передачи имущественных прав.

Доступ к Веб-сервису должен предоставляться бесперебойно в режиме «24/7», за исключением нештатных ситуаций (длительное отключение электропитания, сбой работы программных или аппаратных средств и т.п.).

Веб-сервис должен иметь клиент-серверную архитектуру, где серверная часть развернута на мощностях Исполнителя.

В течение всего срока действия имущественных прав (лицензии) на использование Веб-сервиса Исполнитель должен обеспечивать:

- сопровождение Пользователей по вопросам, связанным с использованием функционала Веб-сервиса, включая вопросы, связанные с содержанием ОРД;

- актуализацию состава и содержания шаблонов ОРД, доступных для разработки с использованием Веб-сервиса, (далее – Шаблоны) посредством их добавления и\или изменении в соответствии с изменениями в требованиях законодательства в области защиты ПДн к реализации организационных мер по обеспечению безопасности ПДн.

Сопровождение Пользователей должно осуществляться по электронной почте на основании заявки Пользователя, сформированной посредством функционала интерфейса Веб-сервиса.

Веб-сервис должен быть зарегистрирован в Едином реестре российских программ для электронных вычислительных машин и баз данных в соответствии с действующим законодательством.

**3.22** **Требования** **к обеспечению безопасности персональных данных при разработке организационно-распорядительной документации**

Функционал Веб-сервиса должен соответствовать требованиям законодательства Российской Федерации к обеспечению безопасности ПДн, в том числе при их передаче по открытым каналам связи (наличие аттестата соответствия требованиям по безопасности информации или иного документального подтверждения).

Пользователю должна предоставляться возможность подключения к Веб-сервису посредством совместного использования: программного обеспечения на основе браузеров, поддерживающих защищенные протоколы TLS, на базе российских криптографических алгоритмов ГОСТ (Яндекс Браузер или аналоги) и криптопровайдера, поддерживающего российские криптографические алгоритмы ГОСТ («КриптоПро CSP» версии 4.0 и выше или аналог).

**3.23 Требования к разработке организационно-распорядительной документации в части автоматизированных функций**

Функционал Веб-сервиса в части заполнения Шаблонов должен быть максимально автоматизирован и включать возможность обработки следующих типов сведений:

* общедоступные сведения;
* фиксированные сведения;
* кастомизированные сведения.

**3.24 Требования к общедоступным сведениям**

Под общедоступными сведениями подразумеваются данные реквизитов организации Заказчика, доступные с использованием ресурса Единый государственный реестр юридических лиц (далее - ЕГРЮЛ).

Заполнение общедоступных сведений должно производиться автоматически по номеру ОГРН на основе данных ЕГРЮЛ.

**3.25 Требования к фиксированным сведениям**

Под фиксированными сведениями подразумеваются сведения, перечень и содержание которых ограничены функционалом Веб-сервиса посредством предоставления Пользователю возможности выбора единственного значения из выпадающего списка.

**3.26 Требования к кастомизированным сведениям**

Под кастомизированными сведениями подразумеваются сведения, которые вносятся Пользователем в Веб-сервис вручную.

Для полей кастомизированных сведений «Фамилия», «Имя», «Отчество», при их заполнении в именительном падеже, должна производиться автоматическая генерация падежных форм «родительный падеж», «дательный падеж», «творительный падеж», «предложный падеж». Выбор и сопоставление сгенерированной падежной формы с содержанием Шаблонов должно осуществляться автоматически в соответствии с контекстом содержания Шаблонов, дополняемых указанными кастомизированными сведениями.

Заполненные шаблоны должны быть доступны Пользователю для просмотра, редактирования и выгрузки в форматах \*.docx или \*.rtf в виде единого архива в формате \*.zip

Результатом разработки организационно-распорядительной документации является:

полученный Заказчиком комплект организационно-распорядительной документации, разработанный с помощью Веб-сервиса.

**3.27 Общие требования к документированию**

Язык оформления документации – русский, за исключением общепринятых названий и оригинальных наименований программно-аппаратных средств импортного производства.

Вся отчетная документация должна быть оформлена и передана Заказчику в электронном виде, в формате Word и PDF с использованием защищенного канала связи.

**3.28 Общие требования к безопасности оказываемых услуг**

Все сведения о составе и характеристиках объектов информатизации Заказчика являются конфиденциальной информацией.

Исполнитель обязуется:

* не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся на объектах информатизации Заказчика;
* не осуществлять несанкционированный доступ к информационным ресурсам объектов информатизации Заказчика;
* не проводить незаконное копирование информации, циркулирующей или хранящейся на объектах информатизации Заказчика;
* не предпринимать манипулирование информацией, циркулирующей или хранящейся на объектах информатизации (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);
* не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;
* не внедрять на объектах информатизации программы-вирусы (загрузочные, файловые и др.);
* не устанавливать программные и аппаратные закладные устройства в технические средства объектов информатизации Заказчика;
* не устанавливать в технические средства объектов информатизации программное обеспечение, зараженное вирусами.

Нарушение настоящих требований влечёт за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законом Российской Федерации.

1. **Состав и содержание услуг**
   1. Требования к порядку сдачи услуг и составу отчетной документации приведены в Таблице № 3.

Исполнитель вправе досрочно оказать услуги.

Результаты оказания услуг на 1 этапе представляются Заказчику по мере их выполнения, в рабочее время (понедельник – четверг: с 8-30 до 16-30 часов 00 минут (время московское), пятница – с 8-30 до 16 -00.

Результаты оказания услуг на 2 этапе (сводные отчеты) представляются Заказчику в рабочее время ежемесячно, не позднее 10-го числа месяца, следующего за месяцем оказания услуг.

Таблица №3

| **№ этапа** | **Наименование услуг** | **Сроки выполнения** | **Результаты оказания услуг** |
| --- | --- | --- | --- |
|  | **Развертывание инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика** | В течение 50 (пятидесяти) рабочих дней с даты заключения Договора при условии выполнения Заказчиком своих обязательств | Отчетные документы:   * Предварительный перечень источников событий ИБ для осуществления мониторинга; * Структурно-функциональная схема основных источников событий ИБ; * Отчет по результатам обследования действующей инфраструктуры Заказчика; * Регламент взаимодействия сторон в рамках оказания услуг по мониторингу событий ИБ; * Документ о приемке, подписанный Заказчиком. |
|  | Обследование действующей инфраструктуры Заказчика |
|  | Подключение инфраструктуры Заказчика к Центру мониторинга Исполнителя |
|  | **Мониторинг, выявление и реагирование на события информационной безопасности** | В течение 12 (месяцев) с момента завершения Этапа № 1  В течение 5 (пяти) календарных дней с даты заключения Договора | Отчетные документы:   * сводные отчеты (предоставляются ежемесячно); * Акт приемки оказанных услуг подписанный Сторонами.   1. Отчетные документы:  - комплект организационно-распорядительной документации;  2. Документ о приемке, подписанный Заказчиком. |
|  | Обнаружение и регистрация компьютерных инцидентов |
|  | Реагирование на компьютерные инциденты |
|  | Анализ деятельности по управлению компьютерными инцидентами |
|  | Актуализация перечня источников событий информационной безопасности |
|  | Формирование отчетности по мониторингу событий информационной безопасности |
| **3.** | **Разработка организационно-распорядительной документации** |

# ОБЩИЙ ПОРЯДОК ПРОВЕДЕНИЯ АУКЦИОНА

## Общий порядок проведения аукциона

### Аукцион проводится в следующем порядке:

- Публикация Извещения о проведении аукциона;

- Предоставление Документации Участникам процедуры;

- Разъяснение Закупочной документации;

- Внесение поправок в Документацию;

- Требования к Участникам аукциона. Требования к Заявкам Участников;

- Подача Заявок на участие в Аукционе и их прием, отзыв Заявок;

- Рассмотрение заявок;

- Проведение торгов;

- Сопоставление ценовых предложений Участников;

- Подведение итогов;

- Заключение договора;

- Извещение Участников о результатах аукциона (осуществляется однократно в течение всей процедуры Аукциона).

## Публикация Извещения о проведении аукциона

### Извещение о проведении аукциона опубликовано в порядке, указанном в п. 1.1.

### Иные публикации не являются официальными и не влекут для Заказчика никаких последствий.

## Предоставление Документации Участникам процедуры

### Участники аукциона должны получить Документацию в порядке, указанном в Извещении.

### Заказчик отвечает за выполнение условий Извещения о проведении аукциона и Документации только перед теми Участниками аукциона, которые получили Документацию в порядке, указанном в пункте 3.3.1.

## Разъяснение Закупочной документации

### В процессе подготовки к участию в Аукционе Участники вправе обратиться к Заказчику за разъяснениями положений настоящей Документации. Запросы на разъяснение Документации должны размещаться на ЭТП ГПБ.

### Заказчик обязуется в разумный срок ответить на любой вопрос, который он получит не позднее, чем за 3 дня до истечения срока приема Заявок. Заказчик оставляет за собой право (но не обязанность) ответа на вопрос, полученный в более поздний срок, если обстоятельства позволят Заказчику ответить на него в разумное время до установленного срока подачи Заявок. При этом ответ будет размещен Заказчиком на ЭТП ГПБ. Такой ответ Заказчика имеет силу неотъемлемых дополнений к документации, если в тексте ответа не будет указано иное.

## Внесение поправок в Документацию

### Заказчик, по решению закупочной комиссии, в любой момент до истечения срока приема Заявок вправе внести поправки в настоящую Документацию.

### Все Участники, оформившие свое участие в Аукционе через систему ЭТП ГПБ, получат соответствующие уведомления в порядке, установленными правилами данной системы.

## Требования к Участникам аукциона. Требования к Заявкам Участников.

### Участвовать в Аукционе могут юридические лица и индивидуальные предприниматели, зарегистрированные в системе ЭТП ГПБ в качестве участников данной системы.

### Участник вправе подать только одну заявку на участие в данном Аукционе.

### Требования к заявке Участника

Участник должен включить в состав заявки следующие документы:

1) анкету по установленной форме (Форма 3);

2) копию документа, подтверждающего полномочия лица действовать от имени участника, за исключением случаев подписания заявки:

а) индивидуальным предпринимателем, если Участником закупки является индивидуальный предприниматель;

б) лицом, указанным в едином государственном реестре юридических лиц в качестве лица, имеющего право без доверенности действовать от имени юридического лица, если Участником является юридическое лицо;

3) копию решения о согласии на совершение крупной сделки или о последующем одобрении этой сделки, если требование о наличии указанного решения установлено законодательством Российской Федерации и для Участника закупки заключение по результатам такой закупки договора является крупной сделкой;

4) декларацию, подтверждающую на дату подачи заявки на участие в закупке\*:

а) непроведение ликвидации Участника - юридического лица и отсутствие решения арбитражного суда о признании Участника - юридического лица или индивидуального предпринимателя несостоятельным (банкротом);

б) неприостановление деятельности Участника в порядке, установленном Кодексом Российской Федерации об административных правонарушениях;

в) отсутствие у Участника недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах) за прошедший календарный год, размер которых превышает двадцать пять процентов балансовой стоимости активов Участника закупки, по данным бухгалтерской (финансовой) отчетности за последний отчетный период. Участник считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по данному заявлению на дату рассмотрения заявки на участие в закупке не принято;

г) отсутствие у Участника закупки - физического лица, зарегистрированного в качестве индивидуального предпринимателя, либо у руководителя, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа, или главного бухгалтера юридического лица - Участника закупки непогашенной или неснятой судимости за преступления в сфере экономики и (или) преступления, предусмотренные статьями 289, 290, 291, 291.1 Уголовного кодекса Российской Федерации, а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся предметом осуществляемой закупки, и административного наказания в виде дисквалификации;

д) отсутствие фактов привлечения в течение двух лет до момента подачи заявки на участие в закупке Участника такой закупки - юридического лица к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях;

е) отсутствие сведений об участнике в реестре недобросовестных поставщиков, предусмотренном Федеральными законами от 18.07.2011г. №223-ФЗ и от 05.04.2013 №44-ФЗ.

*\*Декларация представляется в составе заявки участником с использованием программно-аппаратных средств электронной площадки. Оператор электронной площадки обеспечивает участнику возможность включения в состав заявки и направления заказчику информации и документов, посредством программно-аппаратных средств электронной площадки в случае их представления оператору при аккредитации на ЭТП ГПБ.*

5) Техническое предложение по форме и в соответствии с инструкциями, приведенными в настоящей Документации (Форма 1);

1. Протокол разногласий к проекту Договора по форме и в соответствии с инструкциями, приведенными в настоящей Документации (Форма 2).

### Участник должен подготовить Заявку в электронной форме с использованием функционала системы ЭТП ГПБ. Электронные версии документов должны иметь одни из распространенных форматов документов: Microsoft Word Document (\*.doc), Rich Text Format (\*.rtf), Microsoft Excel Sheet (\*.xls), Portable Document Format (\*.pdf) и т.п. Все файлы не должны иметь защиты от их открытия, изменения, копирования их содержимого или их печати. Файлы должны быть именованы так, чтобы из их названия было бы понятно, какой документ в каком файле располагается.

### Участники при оформлении Заявки должны использовать формы и инструкции по их заполнению, предусмотренные настоящей документацией.

### Все файлы Заявки, размещенные Участником на ЭТП ГПБ, должны иметь наименование либо комментарий, позволяющие идентифицировать содержание данного файла.

### Прочие правила оформления Заявок через систему ЭТП ГПБ определяются правилами данной системы.

### Заявка действительна в течение срока, указанного Участником в Коммерческом предложении. В любом случае этот срок не должен быть менее чем 60 календарных дней со дня, следующего за днем проведения процедуры вскрытия поступивших Заявок. Указание меньшего срока действия может служить основанием для отклонения Предложения.

### Все документы, входящие в состав Заявки, должны быть подготовлены на русском языке.

### Все суммы денежных средств в документах, входящих в Заявку, должны быть выражены в российских рублях.

## Подача Заявок на участие в Аукционе и их прием, отзыв Заявок

### Заявки Участников должны быть поданы до истечения сроков, указанных в Извещении о проведении аукциона.

### Порядок подачи Заявок на ЭТП ГПБ определяется правилами и инструкциями данной системы.

### Участник вправе отозвать поданную Заявку не позднее даты окончания приема заявок Участников.

### В случае отзыва Заявки Участник должен подготовить соответствующие документы в соответствии с правилами системы ЭТП ГПБ.

## Порядок рассмотрения Заявок Участников

### В рамках процедуры рассмотрения заявок Участников закупочная комиссия проверяет:

### - Правильность оформления, подачи Заявок, их соответствие требованиям настоящей Документации по существу;

### - Соответствие технического предложения Участников требованиям Документации

### - Правоспособность, квалификацию участников.

### Участники не вправе каким-либо способом влиять, участвовать или присутствовать при рассмотрении Заявок.

### Закупочная комиссия может запросить у Участников Аукциона разъяснения или дополнения их Заявок, в том числе представления отсутствующих документов. При этом закупочная комиссия не вправе запрашивать разъяснения или требовать документы, меняющие суть Заявок.

### В случае если Участник закупки, которому был направлен запрос о разъяснении сведений, содержащихся в заявке, не предоставит соответствующие разъяснения заявки в порядке и срок, установленный в запросе, заявка такого Участника закупки может быть отклонена.

### Заказчик, по решению закупочной комиссии, вправе отклонить Заявки Участников, аффилированных между собой (понятие аффилированного лица согласно ст. 4 закона РФ от 22.03.1991 № 948-1).

### Заказчик вправе проверять соответствие предоставленных Участником заявлений, документов и информации действительности, в том числе путем направления запросов в государственные органы, лицам, указанным в заявке, а также проводить выездные проверки. При предоставлении заведомо ложных сведений или намеренном искажении информации или документов, приведенных в составе Заявки, Заказчик имеет право отклонить Заявку Участника от дальнейшего рассмотрения.

### По результатам рассмотрения Заявок закупочная комиссия отклоняет заявки Участников, которые:

### - не отвечают требованиям настоящей Документации к оформлению и подаче Заявок;

### - содержат предложения, не отвечающие техническим, коммерческим или договорным требованиям настоящей Документации

### - поданы Участниками, не предоставившими документы, требуемые настоящей Документацией, либо в представленных документах имеются недостоверные сведения об Участнике или о предлагаемых им услугах;

### - поданы Участниками, не предоставившими сведения об исполнении аналогичных договоров (Форма 5), либо не имеющими опыта выполнения аналогичных работ (услуг).

### В случае если по результатам рассмотрения заявок только одна заявка на участие в аукционе (в том числе единственная заявка) была признана соответствующей условиям аукциона, или ни одна заявка не была признаны соответствующей условиям аукциона, аукцион признается несостоявшимся.

### В случае если после окончания срока подачи заявок на участие в аукционе не поступило ни одной заявки, аукцион признается несостоявшимся.

### По результатам рассмотрения Заявок Участников, Заказчик направляет оператору ЭТП ГПБ протокол рассмотрения Заявок Участников.

## Проведение торгов

### Порядок проведения Аукциона определяется «Регламентом работы электронной торговой площадки ЭТП ГПБ», расположенным по адресу https://etpgpb.ru/help/faq\_docs/ (Раздел 10. ПОРЯДОК ПРОВЕДЕНИЯ ЭТАПА (СТАДИИ) ТОРГОВ)

### «Шаг аукциона» составляет от 0,5 процента до 5 процентов начальной (максимальной) цены.

### Снижение текущего минимального предложения о цене договора осуществляется на величину в пределах «шага аукциона».

### Время приема ценовых предложений участников аукциона составляет пятнадцать минут от начала проведения аукциона до истечения срока подачи предложений о цене Договор, а также пятнадцать минут после поступления последнего предложения. Если в течение указанного времени ни одного предложения о более низкой цене Договора не поступило, аукцион автоматически, при помощи программных и технических средств, обеспечивающих его проведение, завершается.

## Сопоставление ценовых предложений участников

### В качестве единого базиса сравнения ценовых предложений, обеспечения равной и объективной оценки, **сравнение предложений проводится по цене без НДС.**

### Сопоставление ценовых предложений, а также заключение договора с Победителем осуществляются с соблюдением требований Постановления Правительства РФ от 16.09.2016 №925 «О приоритете товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами».

### В течение одного часа после окончания подачи предложений о цене договора оператор ЭТП ГПБ составляет и размещает на электронной площадке и в единой информационной системе протокол подачи предложений о цене договора, содержащий минимальные предложения о цене договора каждого Участника с указанием времени их поступления.

## Подведение итогов

### Подведение итогов состоится не позднее 18.12.2024 г.

### Закупочная комиссия на своем заседании принимает решение либо по определению Победителя, либо по завершению данной процедуры Аукциона без определения Победителя и заключения Договора.

### Закупочная комиссия на своем заседании определяет Победителя Аукциона как Участника, Заявка которого соответствует требованиям Аукциона и который предложил самую низкую цену Договора.

### Решение закупочной комиссии по подведению итогов Аукциона оформляется протоколом заседания закупочной комиссии. Участники Аукциона незамедлительно уведомляются об итогах аукциона системой ЭТП ГПБ согласно правилам данной системы.

### Участник незамедлительно уведомляется о признании его Победителем Аукциона и о месте и порядке подписания Договора с Заказчиком.

### Если в период между подписанием Протокола и Договора изменился Победитель (например, вследствие отказа), то Победителем Аукциона может быть признан Участник, занявший второе место по предпочтительности ценового предложения, Участники извещаются о новом Победителе в том же порядке.

## Подписание Договора

### Договор между Заказчиком и Победителем подписывается не ранее 10 и не позднее 20 дней с момента публикации в Единой информационной системе итогового протокола.

### По всем вопросам, не нашедшим отражение в Извещении о проведении Аукциона, настоящей Закупочной документации и Предложении Победителя аукциона, стороны имеют право вступить в преддоговорные переговоры, по результатам преддоговорных переговоров стороны подписывают протокол преддоговорных переговоров. При проведении преддоговорных переговоров не допускается изменение существенных условий Закупочной документации.

### В случае если в соответствии с действующим законодательством РФ и учредительными документами Заказчика потребуется предварительное согласование (одобрение, утверждение) заключаемого на предложенных Победителем условиях договора компетентными органами управления Заказчика (Общим собранием акционеров, Советом директоров и т.п.), договор с Победителем заключается только после такого согласования (одобрения, утверждения), а указанный в п. 2.12.1 срок отсчитывается после получения такого согласования (одобрения, утверждения).

### В случае если Победитель Аукциона не подпишет Договор в установленные Протоколом о результатах Аукциона он утрачивает статус Победителя, а Заказчик имеет право выбрать иного Победителя из числа остальных действующих заявок.

### Заказчик заключит договор с Участником закупки, который предложил такие же, как и Победитель закупки, условия исполнения договора или предложение которого содержит лучшие условия исполнения договора, следующие после условий, предложенных Победителем закупки, который признан уклонившимся от заключения договора.

# ОБРАЗЦЫ ОСНОВНЫХ ФОРМ ДОКУМЕНТОВ, ВКЛЮЧАЕМЫХ В ЗАЯВКУ

## Техническое предложение (форма )

### Форма технического предложения

**начало формы**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Техническое предложение**  (Здесь Участник в свободной форме приводит свое техническое предложение, опираясь на проект Технического задания).  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (фамилия, имя, отчество подписавшего, должность)  **М.П.**  **конец формы** Инструкции по заполнениюУчастник указывает наименование страны происхождения поставляемых товаров (в соответствии с Общероссийским классификатором стран мира).Техническое предложение будет служить основой для подготовки приложения к Договору. В этой связи в целях снижения общих затрат сил и времени Заказчика и Участника на подготовку Договора данное предложение следует подготовить так, чтобы его можно было с минимальными изменениями включить в Договор. Протокол разногласий по проекту Договора (форма 2)Форма Протокола разногласий к проекту Договора **начало формы**  **Протокол разногласий к проекту Договора**  **«Обязательные» условия Договора**   |  |  |  |  |  | | --- | --- | --- | --- | --- | | № п/п | № пункта проекта Договора | Исходные формулировки | Предложения Участника | Примечания, обоснование | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | | … |  |  |  |  |   **«Желательные» условия Договора**   |  |  |  |  |  | | --- | --- | --- | --- | --- | | № п/п | № пункта проекта Договора | Исходные формулировки | Предложения Участника | Примечания, обоснование | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | | … |  |  |  |  |   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (фамилия, имя, отчество подписавшего, должность)  **М.П.**  **конец формы** Инструкции по заполнениюДанная форма заполняется как в случае наличия у Участника требований или предложений по изменению проекта Договора, так и в случае отсутствия таких требований или предложений; в последнем случае в таблицах приводятся слова «Согласны с предложенным проектом Договора».В случае наличия у Участника предложений по внесению изменений в проект Договора, Участник должен представить в составе своей Заявки данный протокол разногласий. В подготовленном протоколе разногласий Участник должен четко разделить обязательные и желательные для него условия Договора. «Обязательными» здесь считаются предложения и условия, в случае непринятия которых он откажется подписать Договор. «Желательными» здесь считаются предложения по условиям Договора, которые он предлагает на рассмотрение Заказчика, но отклонение которых Заказчиком не повлечет отказа Участника от подписания Договора в случае признания его Победителем.Заказчик оставляет за собой право рассмотреть и принять перед подписанием Договора предложения и дополнительные (не носящие принципиального характера) изменения к Договору. В случае если стороны не придут к соглашению об этих изменениях, стороны будут обязаны подписать Договор на условиях, изложенных в настоящей Документации по Аукциону и Заявке Победителя.В любом случае Участник должен иметь в виду что: - если какое-либо из обязательных Договорных предложений и условий, выдвинутых Участником, будет неприемлемо для Заказчика, такая Заявка будет отклонена независимо от содержания технико-коммерческих предложений;  - в любом случае, предоставление Участником протокола разногласий по подготовленному Заказчиком исходному проекту Договора не лишает Участника и Заказчика права обсуждать эти условия и изменять их в процессе преддоговорных переговоров для достижения соглашения в отношении изменения этих условий. Анкета Участника (форма 3)Форма Анкеты Участника **начало формы**  **Анкета Участника**  Наименование и адрес Участника: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   | № п/п | Наименование | Сведения об Участнике | | --- | --- | --- | |  | Организационно-правовая форма и фирменное наименование Участника |  | |  | Учредители (перечислить наименования и организационно-правовую форму или Ф.И.О. всех учредителей, чья доля в уставном капитале превышает 10%) |  | |  | Свидетельство о внесении в Единый государственный реестр юридических лиц (дата и номер, кем выдано) |  | |  | ИНН, КПП, ОГРН |  | |  | ОКОПФ, ОКПО, ОКТМО |  | |  | Юридический адрес |  | |  | Почтовый адрес |  | |  | Фактический адрес |  | |  | Филиалы: перечислить наименования и почтовые адреса |  | |  | Банковские реквизиты (наименование и адрес банка, номер расчетного счета Участника в банке, телефоны банка, прочие банковские реквизиты) |  | |  | Телефоны Участника (с указанием кода города) |  | |  | Факс Участника (с указанием кода города) |  | |  | Адрес электронной почты Участника |  | |  | Фамилия, Имя и Отчество руководителя Участника, имеющего право подписи согласно учредительным документам Участника, с указанием должности и контактного телефона |  | |  | Фамилия, Имя и Отчество главного бухгалтера Участника |  | |  | Фамилия, Имя и Отчество ответственного лица Участника с указанием должности и контактного телефона |  |   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (фамилия, имя, отчество подписавшего, должность)  **М.П.**  **конец формы**   * + 1. Инструкции по заполнению        1. Участник указывает свое фирменное наименование (в т.ч. организационно-правовую форму) и свой адрес.        2. Участники должны заполнить приведенную выше таблицу по всем позициям. В случае отсутствия каких-либо данных указать слово «нет».        3. В графе 9 «Банковские реквизиты…» указываются реквизиты, которые будут использованы при заключении Договора. |

**Приложение 1 к Документации**

**ДОГОВОР ОКАЗАНИЯ УСЛУГ №** \_\_\_\_\_\_\_\_\_\_\_

г. Калуга «\_\_\_\_»\_\_\_\_\_\_\_\_\_2024 г.

ПАО «Калужская сбытовая компания», именуемое в дальнейшем «**Заказчик**», в лице Генерального директора Новиковой Г.В. действующего на основании Устава, с одной стороны и

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «**Исполнитель**», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, в дальнейшем совместно именуемые Стороны, заключили настоящий Договор о нижеследующем:

**1. Предмет Договора**

1.1. В целях обеспечения безопасности информационных ресурсов Заказчика Исполнитель обязуется оказывать Заказчику услуги по мониторингу и анализу инцидентов информационной безопасности, разработке организационно-распорядительной документации по вопросам безопасности информационных ресурсов и взаимодействию с органами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), а Заказчик обязуется оплачивать услуги Исполнителя в порядке, установленном настоящим Договором.

1.2. Перечень услуг по настоящему Договору, условия и порядок их представления установлены Техническим заданием (Приложение № 1 к настоящему Договору).

**2. ПОРЯДОК ОКАЗАНИЯ УСЛУГ И ВЗАИМОДЕЙСТВИЯ СТОРОН**

2.1. Услуги по мониторингу и анализу инцидентов информационной безопасности оказываются Исполнителем по настоящему Договору непрерывно, в течение 12 месяцев.

2.1. Исполнитель обязан оказывать услуги по настоящему Договору своими силами. Привлечение Исполнителем третьих лиц к оказанию услуг по настоящему Договору, в т.ч. предоставление третьим лицам доступа к сведениям об информационных ресурсах Заказчика, а также к информации и документам, полученным Исполнителем при исполнении настоящего Договора, без письменного согласия Заказчика не допускается.

2.2. Заказчик представляет Исполнителю сведения об информационных ресурсах (назначении, архитектуре объекта, применяемых программных средствах и т.д.) согласно

п. 3.1. «Требования к сбору исходных данных об инфраструктуре Заказчика» Раздела № 3 Приложения № 1 к настоящему Договор и обеспечивает доступ Исполнителя к источникам событий информационной безопасности в инфраструктуре Заказчика для обследования и подключения к Центру мониторинга Исполнителя.

2.3. Порядок оказания Исполнителем услуг определен Разделом № 3 «Требования к оказанию услуг» Приложения № 1 к настоящему Договору.

2.4. Требования к порядку сдачи Исполнителем оказываемых услуг Заказчику, и составу представляемой отчетной документации, определены Разделом № 4 «Состав и содержание услуг» Приложения № 1 к настоящему Договору.

2.5. Уполномоченным представителем Заказчика по вопросам взаимодействия с Исполнителем по настоящему Договору, является: Начальник службы АСУ и телекоммуникаций ПАО «Калужская сбытовая компания» Момотов Дмитрий Владимирович (к. тел\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; E-mail\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Уполномоченным представителем Исполнителя по вопросам взаимодействия с Заказчиком по настоящему Договору, является: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(к.тел\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_; E-mail\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

2.6. Уполномоченные представители Сторон в т.ч.:

- разрабатывают и согласовывают планы мероприятий, подлежащие применению Сторонами в период взаимодействия по настоящему Договору, и осуществляют контроль их выполнения;

- согласовывают Регламент взаимодействия Сторон, разрабатываемый Исполнителем в соответствии с Техническим заданием (Приложение № 1);

- оформляют отчетные документы, предусмотренные Техническим заданием (Приложение № 1);

- подписывают Акты сдачи-приемки оказанных услуг за расчетный период.

2.7. Подготовленный Исполнителем проект Акта сдачи-приемки оказанных услуг за расчетный период, представляется Заказчику совместно с ежемесячным Сводным отчетом, не позднее 10-го числа месяца, следующего за отчетным месяцем.

Заказчик обязан подписать и вернуть Акт сдачи-приемки оказанных услуг Исполнителю не позднее чем в течение 3-х рабочих дней со дня его получения, либо представить Исполнителю мотивированный отказ от подписания Акта.

Выявленные недостатки подлежат устранению Исполнителем безвозмездно, в согласованный Сторонами срок.

В случае, если Заказчик в указанный срок не направит Исполнителю мотивированный отказ в принятии Акта сдачи-приемки оказанных услуг, Акт считается принятым Заказчиком без возражений.

2.8. Уполномоченный представитель Исполнителя обязан незамедлительно информировать уполномоченного представителя Заказчика обо всех случаях возникновения угроз безопасности в отношении информационных ресурсов Заказчика и оказывать Заказчику возможное содействие в их устранении.

**3. СТОИМОСТЬ УСЛУГ И ПОРЯДОК РАСЧЕТОВ**

3.1. Общая стоимость услуг Исполнителя по настоящему Договору (включая развертывание инфраструктуры для сбора событий с источников информационной безопасности Заказчика и выполнение в течение 12 месяцев мониторинга, выявления и реагирования на события информационной безопасности), составляет:

\_\_\_\_\_\_\_\_\_\_\_\_руб. (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) рублей, в т.ч. НДС \_\_\_\_\_\_\_\_\_руб.

3.2. Расчетным периодом по настоящему Договору является календарный месяц.

3.3. Оплата производиться Заказчиком за оказанные Исполнителем услуги, путем перечисления денежных средств на расчетный счет Исполнителя равными платежами в размере1/12 от общей стоимости услуг, в течение 7-и рабочих дней со дня получения счета и счета-фактуры (УСПД**)** выставленных Исполнителем не позднее чем на следующий рабочий день, после подписания уполномоченными представителями Сторон Акта сдачи-приемки оказанных услуг (за расчетный период) (Приложение № 2).

3.4. Датой оплаты считается дата списания денежных средств с р/счета Заказчика.

Обязательства Заказчика по оплате считаются исполненными полностью, со дня списания обслуживающим банком с его расчетного счета денежных средств за 12-й расчетный период.

3.5. По заявлению одной из Сторон, Стороны обязаны проводить сверку расчетов не реже 1 раза в квартал.

**4. СРОК ДЕЙСТВИЯ ДОГОВОРА**

4.1. Настоящий Договор вступает в силу с момента его подписания Сторонами и действует в течение 12 месяцев со дня начала оказания Исполнителем услуг по мониторингу ИБ на базе системы RUSIEM (Таблица № 3 Приложения № 1).

4.2. Договор может быть досрочно расторгнут по соглашению Сторон, или по требованию одной из сторон (в одностороннем порядке) в случаях, предусмотренных действующим законодательством РФ.

О предстоящем расторжении договора в одностороннем порядке, заинтересованная сторона обязана уведомить другую сторону не менее чем за 15 дней.

**5. КОНФИДЕНЦИАЛЬНОСТЬ**

5.1. Условия настоящего Договора конфиденциальны и не подлежат разглашению.

Стороны в течение срока действия настоящего Договора, а также в течение 3 (трёх) лет по окончании его действия, обязуются обеспечить конфиденциальность условий Договора, а также любой иной информации и данных, получаемых друг от друга в связи с исполнением настоящего Договора (в том числе персональных данных), за исключением информации и данных, являющихся общедоступными (далее – конфиденциальная информация). Каждая из Сторон обязуется не разглашать конфиденциальную информацию третьим лицам без получения предварительного письменного согласия Стороны, являющейся владельцем конфиденциальной информации.

Стороны обязуются принимать все разумные меры для защиты конфиденциальной информации друг друга от несанкционированного доступа третьих лиц, в том числе:

- хранить конфиденциальную информацию исключительно в предназначенных для этого местах, исключающих доступ к ней третьих лиц;

- ограничивать доступ к конфиденциальной информации, в том числе для сотрудников, не имеющих служебной необходимости в ознакомлении с данной информацией.

Стороны гарантируют полное соблюдение всех условий обработки, хранения и использования полученных персональных данных, согласно ФЗ «О персональных данных» № 152 ФЗ от 27.07.2006.

Стороны обязаны незамедлительно сообщить друг другу о допущенных ими либо ставших им известным фактах разглашения или угрозы разглашения, незаконном получении или незаконном использовании конфиденциальной информации третьими лицами.

Под разглашением конфиденциальной информации в рамках настоящего Договора понимается действие или бездействие одной из Сторон Договора, в результате которого конфиденциальная информация становится известной третьим лицам в отсутствие согласия на это другой Стороны. При этом форма разглашения конфиденциальной информации третьим лицам (устная, письменная, с использованием технических средств и др.) не имеет значения.

В случаях неисполнения обязательств, предусмотренных настоящим Разделом Договора, Сторона, допустившее такое нарушение, обязуется возместить причиненный этим реальный ущерб в течение 5 (пяти) рабочих дней после получения соответствующего письменного требования пострадавшей Стороны.

5.2. Не является нарушением конфиденциальности предоставление конфиденциальной информации по законному требованию правоохранительных и иных уполномоченных государственных органов и должностных лиц в случаях и в порядке, предусмотренных применимым законодательством.

В случае раскрытия конфиденциальной информации указанным органам и/или лицам Сторона, раскрывшая конфиденциальную информацию, письменно уведомляет владельца конфиденциальной информации о факте предоставления такой информации, ее содержании и органе, которому предоставлена конфиденциальная информация, не позднее двух рабочих дней с момента раскрытия конфиденциальной информации.

**6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

6.1. В случае неисполнения или ненадлежащего исполнения обязательств по Договору Стороны несут ответственность согласно действующего законодательства РФ.

6.2. Обмен документами и юридически значимыми сообщениями (ст. 165.1 ГК РФ) уполномоченные представители Стороны осуществляют электронной почтой (по электронным адресам, указанным в Договоре), с последующим направлением оригиналов необходимых документов.

6.3. Изменения условий настоящего Договора могут производиться исключительно путем заключения письменных Дополнительных соглашений, подписанных обеими Сторонами, в течение срока действия Договора.

6.4. Споры по настоящему Договору, разрешаются Сторонами путем переговоров. В случаях не достижения соглашения по имеющимся разногласиям, заинтересованная Сторона вправе передать спор на рассмотрение Арбитражного суда Калужской области.

Споры о взыскании денежных средств по требованиям, возникшим из настоящего Договора, могут быть переданы заинтересованной Стороной на разрешение Арбитражного суда по истечении 30 календарных дней со дня предъявления другой Стороне письменной претензии.

**ПРИЛОЖЕНИЯ:**

-Приложение № 1 – Техническое задание;

- Приложение № 2 – Форма Акта сдачи-приемки оказанных услуг (за расчетный период).

|  |  |
| --- | --- |
| **ЗАКАЗЧИК** | **ИСПОЛНИТЕЛЬ:** |
| ПАО «Калужская сбытовая компания» |  |
| 248001 г. Калуга, переулок Суворова, д.8.  ИНН 4029030252 КПП 77505001  р/с: 40702810802180060156  в Тульском филиале АО «АБ «Россия» г. Тула.  к/с банка: 30101810600000000764  БИК: 047003764  к. тел. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Г.В. Новикова  М.П. | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **М.П.** |

**ПРИЛОЖЕНИЕ № 1**

к Договору оказания услуг от \_\_\_\_\_\_\_\_\_\_\_2024 г. №\_\_\_\_\_\_\_\_\_\_\_\_

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

на оказание услуг по мониторингу и анализу инцидентов информационной безопасности информационных ресурсов и разработке организационно-распорядительной документации

1. **Определения и сокращения**
   1. В настоящем документе применяются следующие термины с соответствующими определениями:

**Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)** –единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

**Заказчик** – Публичное акционерное общество "КАЛУЖСКАЯ СБЫТОВАЯ КОМПАНИЯ".

**Зона ответственности –** совокупность информационных ресурсов, в отношении которых субъектом ГосСОПКА обеспечиваются обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты.

**Информационная безопасность (ИБ)** – комплекс организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность дает гарантию обеспечения следующих целей: конфиденциальность информации (свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц); целостность информации и связанных с ней процессов (неизменность информации в процессе ее передачи или хранения); доступность информации, когда она нужна (свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц); учет всех процессов, связанных с информацией.

**Информационный ресурс** – информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления.

**Исполнитель** – организация (юридическое лицо) либо индивидуальный предприниматель, выбранная/выбранный Заказчиком по результатам проведения открытого аукциона в электронной форме.

**Компьютерная атака** – целенаправленное воздействие программных и (или) программно-аппаратных средств на информационный ресурс в целях нарушения и (или) прекращения его функционирования и (или) создания угрозы безопасности, обрабатываемой таким ресурсом информации.

**Компьютерный инцидент** – факт нарушения и (или) прекращения функционирования информационного ресурса, сети электросвязи, используемой для организации взаимодействия информационных ресурсов, и (или) нарушения безопасности, обрабатываемой в информационном ресурсе информации, в том числе произошедший в результате компьютерной атаки.

**Критическая информационная инфраструктура (КИИ)** – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

**Национальный координационный центр по компьютерным инцидентам (НКЦКИ) –** наивысшая структура в иерархии ГосСОПКА, осуществляющая нормативное и методическое сопровождение.

**Объекты критической информационной инфраструктуры** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

**Субъекты ГосСОПКА** – государственные органы Российской Федерации, российские юридические лица и индивидуальные предприниматели в силу закона или на основании заключенных с ФСБ России соглашений, осуществляющие обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

**Субъекты критической информационной инфраструктуры** – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

**ТЗ** –техническое задание на оказание услуг по Договору.

**ФСБ России -** Федеральная служба безопасности Российской Федерации.

**ФСТЭК России** - Федеральная служба по техническому и экспортному контролю.

**SIEM-система (Security Information and Event Manager)** - Система сбора и обработки событий информационной безопасности.

**2. Общие сведения**

**2.1.** В соответствии с настоящим Техническим заданием Исполнитель должен оказать услуги по мониторингу и анализу инцидентов информационной безопасности информационных ресурсов Заказчика, взаимодействию с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак и разработке организационно-распорядительной документации (далее – услуги).

Результатом оказания услуг по настоящему Техническому заданию является представление Сводных отчетов по мониторинг и анализ инцидентов информационной безопасности информационных ресурсов Заказчика, взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак и разработанная организационно-распорядительной документации.

* 1. **Заказчик -** Публичное акционерное общество "Калужская сбытовая компания"

ИНН/КПП: 4029030252 / 402801001.

Юридический адрес: 248001, г. Калуга, пер. Суворова, д. 8.

* 1. **Исполнитель -**  определяется по результатам проведения открытого аукциона в электронной форме.
  2. **Основание для оказания услуг**
* Договор на оказание услуг по мониторингу и анализу инцидентов информационной безопасности информационных ресурсов и разработке организационно-распорядительной документации (далее – Договор).
  1. **Место оказания услуг**

Оказание услуг осуществляется применительно к информационным ресурсам Заказчика, развернутым на объекте информатизации, расположенном по адресу: 248001, г. Калуга, пер. Суворова, д. 8.

* 1. **Объект оказания услуг**

Объектом оказания услуг является программные и программно-технические средства, включенные в состав информационных ресурсов Заказчика и являющиеся источниками событий ИБ, приведенные в Таблице 1.

Таблица № 1

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Тип источника событий ИБ** | **Наименование** | **Количество** |
|  | Межсетевой экран | UserGate 500 | 1 |
|  | Контроллеры домена | Active Directory | 2 |
|  | Рабочие станции под управлением ОС Windows |  | 2 |
|  | Сервера под управлением ОС Windows |  | 1 |
|  | Сервера под управлением ОС Linux |  | 3 |
|  | Сервер электронной почты | Kaspersky Secure Mail Gateway (KSMG) | 1 |
|  | Прокси-сервер |  | 1 |
|  | Антивирус с централизованным управлением, расположенный на отдельном сервере | Kaspersky Security Center (KSC) | 1 |
|  | Наличие VPN (координатор защищенной сети), с учетом филиалов | АПКШ «Континент 3.9» (Сервер доступа) | 1 |

* 1. **Цели и задачи оказания услуг**

Целями оказания услуг является:

* обеспечение непрерывности процесса защиты информации;
* повышение уровня защиты информации, содержащейся в информационных ресурсах Заказчика
* выполнение требований нормативных правовых актов и методических документов Российской Федерации в сфере защиты информации.

Задачи, которые должны быть решены в ходе оказания услуг:

* подключение инфраструктуры Заказчика к Центру мониторинга Исполнителя;
* инвентаризация информационных ресурсов (узлов);
* проведение оптимизации предоставляемой услуги под инфраструктурные особенности и технические требования Заказчика;
* обеспечение постоянного мониторинга компьютерных инцидентов ИБ Заказчика;
* регистрация компьютерных атак и компьютерных инцидентов;
* информационное обеспечение для своевременного реагирования на компьютерные инциденты ИБ;
* информационное обеспечение для своевременной ликвидации последствий компьютерных инцидентов;
* анализ угроз информационной безопасности и консолидация компьютерных событий и инцидентов ИБ;
* предоставление аналитической отчетности;
* обеспечение взаимодействие с НКЦКИ.
  1. **Состав и сроки оказания услуг**
* Начало оказания услуг – после подписания Договора Сторонами со дня развертывания Исполнителем инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика

Срок оказания услуг – 12 месяцев ( 1 год).

В состав услуг входит:

* развертывание инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика;
* мониторинг, выявление и реагирование на события информационной безопасности;
* разработка организационно-распорядительной документации.

Очередность и сроки оказания отдельных составляющих услуг указаны в разделе 4 настоящего ТЗ.

* 1. **Нормативно-технические документы, методические материалы, регламентирующие оказание услуг**
* Указ Президента Российской Федерации от 22.12.2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
* Федеральный закон №187 от 26.07.2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации»;
* Приказ ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам (НКЦКИ)»;
* Приказ ФСБ России от 24.07.2018 г. № 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 г. № 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 06 мая 2019 г. №196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»;
* Приказ ФСБ России от 19 июня 2019 г. №281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»;
* Приказ ФСБ России от 19 июня 2019 г. №282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятие мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;
* Методические рекомендации ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
* Методические рекомендации ФСБ России по обнаружению компьютерных атак на информационные ресурсы Российской Федерации;
* Методические рекомендации ФСБ России по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации;
* Методические рекомендации НКЦКИ по проведению мероприятий по оценке степени защищенности от компьютерных атак.
  1. **Требования к Исполнителю**

Исполнитель должен соответствовать требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим оказание услуг, являющихся объектом закупки, а именно:

* наличие собственной действующей лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), при условии наличия в данной действующей лицензии работ (услуг), предусмотренных пунктами «12», «20» Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств, утверждённого постановлением Правительства Российской Федерации от 16.04.2012 № 313;
* наличие собственной действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, при условии наличия в данной действующей лицензии работ (услуг), предусмотренных подпунктами «б», «в», «е», пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого постановлением Правительства Российской Федерации от 03.02.2012 № 79.

1. **Требования к оказанию услуг**
   1. В соответствии с настоящим Техническим заданием Исполнитель должен оказать услуги в следующем порядке после завершения развертывания инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика:

- мониторинг, выявление и реагирование на события информационной безопасности;

- разработка организационно-распорядительной документации**;**

- взаимодействие с органами ГосСОПКА.

* 1. **Требования к развертыванию инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика**

Развертывание инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика включает:

* обследование действующей инфраструктуры Заказчика;
* подключение инфраструктуры Заказчика к Центру мониторинга Исполнителя.
  1. **Требования к обследованию действующей инфраструктуры Заказчика**

В рамках проведения обследования действующей инфраструктуры Заказчика Исполнитель должен обеспечить:

* сбор исходных данных об основных источниках событий ИБ инфраструктуры Заказчика;
* модернизацию структурно-функциональной схемы основных источников событий ИБ;
* документальную фиксацию количественных и качественных характеристик основных источников событий ИБ инфраструктуры Заказчика.
  1. **Требования к сбору исходных данных об инфраструктуре Заказчика**

Для достижения требуемого результата Исполнитель должен реализовать сбор исходных данных инфраструктуры Заказчика на предмет идентификации и учета источников ИБ, подлежащих мониторингу, посредством:

* проведения интервьюирования ответственного персонала Заказчика;
* фактической оценки наличия программных и технических средств в инфраструктуре Заказчика;
* инструментальной инвентаризации источников событий ИБ.

Для достижения требуемого результата Заказчик должен обеспечить:

* назначение ответственных со стороны Заказчика (Ф.И.О., должности и контактные данные лиц, ответственных за функционирование информационного ресурса);
* предоставление сведений об информационных ресурсах (назначении, архитектуре объекта, применяемых программных средствах (системном, прикладном программном обеспечении и т.п.), информационных средствах (базах данных, файлах данных и т.п.), программно-аппаратных средствах (компьютерах, серверах, коммутационном оборудовании, носителях данных и т.п.; сведения о взаимодействии информационных ресурсов с другими информационными ресурсами и (или) о зависимости функционирования информационных ресурсов от других таких объектов;
* предоставление доступа к источникам событий информационной безопасности в инфраструктуре Заказчика.

По результату сбора исходных данных Исполнитель должен разработать документ Предварительный перечень источников событий ИБ для осуществления мониторинга.

* 1. **Требования к модернизации структурно-функциональной схемы основных источников событий ИБ**

Структурно-функциональная схема основных источников событий ИБ предоставляется Заказчиком и при необходимости дорабатывается Исполнителем.

После доработки Исполнителем, структурно-функциональная схема основных источников событий ИБ должна содержать:

состав и взаимосвязи между основными источниками событий ИБ.

* 1. **Требования к документальной фиксации количественных и качественных характеристик инфраструктуры Заказчика**

Для достижения требуемого результата Исполнитель должен обеспечить документальную фиксацию исходных характеристик инфраструктуры Заказчика в режиме штатного функционирования на момент начала оказания Услуг.

Полученные исходные характеристики должны быть согласованы с Заказчиком и использоваться Исполнителем в рамках оказания Услуг в части обнаружения изменений и\или отклонений в их значениях, в случаях, когда такие изменения влияют или могут повлиять на штатное функционирование инфраструктуры Заказчика.

Документальной фиксации подлежат:

* итоговый состав источников событий ИБ;
* сведения о каждом из источников событий ИБ;
* технологический статус источников событий ИБ (подключен/не подключен к SIEM-системе);
* особенности инфраструктуры Заказчика, которые влияют или могут повлиять на качество оказываемых Услуг;
* планируемый к реализации способ получения доступа Исполнителя к ресурсам SIEM-системы.

Результаты документальной фиксации должны быть оформлены в форме Отчета по результатам обследования действующей инфраструктуры Заказчика.

* 1. **Требования к подключению инфраструктуры Заказчика к Центру мониторинга Исполнителя**

В рамках подключения инфраструктуры Заказчика к Центру мониторинга Исполнитель обеспечивает:

* настройку защищенного канала связи между инфраструктурой Заказчика и центром мониторинга Исполнителя;
* настройку SIEM-системы;
* методическое и консультационное сопровождение Заказчика по подключению источников событий ИБ к SIEM-системе;
* организацию взаимодействия с НКЦКИ для обмена информацией о компьютерных инцидентах ИБ;
* разработку регламента взаимодействия сторон в рамках оказания услуг по мониторингу событий ИБ;
* приемочные испытания системы сбора событий ИБ Заказчика.
  1. **Требования к настройке защищенного канала связи между инфраструктурой Заказчика и центром мониторинга Исполнителя**

Для достижения требуемого результата Исполнитель должен обеспечить защиту канала связи между технологической площадкой Заказчика и центром мониторинга Исполнителя.

Защита канала связи должна обеспечиваться с использованием средств криптографической защиты информации, имеющих действующий сертификат ФСБ России.

Защищенный канал связи должен обеспечивать технологический информационный обмен в рамках сбора информации о событиях ИБ в объеме достаточном для оказания Услуг.

* 1. **Требования к настройке SIEM-системы**

Для достижения требуемого результата Исполнитель должен осуществить настройку SIEM-системы, имеющийся у Заказчика, в объеме, предусмотренном эксплуатационной документацией производителя системы.

* 1. **Требования к методическому и консультационному сопровождению Заказчика по подключению источников событий ИБ к SIEM-системе**

Для достижения требуемого результата Исполнитель должен осуществить подключение источников событий ИБ, выявленных в рамках обследования действующей инфраструктуры Заказчика и имеющих статус «не подключен к SIEM-системе», по решению Заказчика и в объеме достаточном для подключения к SIEM-системе.

* 1. **Требования к организация взаимодействия с НКЦКИ для обмена информацией о компьютерных инцидентах ИБ**

В рамках организации взаимодействия с НКЦКИ для обмена информацией о компьютерных инцидентах ИБ Исполнитель в течение 5 (Пяти) рабочих дней, с момента заключения Договора, должен обеспечить:

- отправку уведомления в адрес НКЦКИ о включении ресурсов Заказчика в зону ответственности Центра мониторинга Исполнителя;

- разработку проекта уведомления о принятом решении информировать НКЦКИ через Центр ГосСОПКА.

Для достижения требуемого результата Заказчик в течение 5 (Пяти) рабочих дней, с момента получения от Исполнителя проекта уведомления, должен обеспечить:

оформление и отправку уведомления о принятом решении информировать НКЦКИ через Центр ГосСОПКА.

* 1. **Требования к разработке регламента взаимодействия сторон в рамках оказания услуг по мониторингу событий ИБ**

Регламент разрабатывается Исполнителем с учетом специфики эксплуатации инфраструктуры Заказчика, подлежит согласованию с Заказчиком и должен включать следующие разделы:

* мониторинг и первичная обработка инцидентов ИБ;
* анализ инцидента ИБ;
* обработка запросов по заявкам от уполномоченных сотрудников Заказчика;
* регламент обработки высокочастотных срабатываний подозрений на инциденты ИБ;
* регламент обработки повторных подозрений на инцидент ИБ;
* разработка технических мер по блокированию инцидента;
* участие в процессе нейтрализации последствий инцидента;
* подключение новых типовых источников к Центру мониторинга;
* подключение новых нетиповых источников к Центру мониторинга;
* отключение источников от Центра мониторинга;
* реализация новых сценариев обнаружения подозрений на инциденты ИБ по инициативе Исполнителя;
* реализация новых сценариев обнаружения подозрений на инциденты ИБ по запросу уполномоченных сотрудников Заказчика;
* управление критичностью сценариев обнаружения подозрений на инциденты ИБ.
  1. **Приемочные испытания системы сбора событий ИБ**

Испытания проводятся в соответствии с Программой и методикой испытаний, разрабатываемой Исполнителем в соответствии с ГОСТ 59792-2021.

В рамках приемочных испытаний Исполнитель совместно с Заказчиком проводит оценку:

* работоспособности функционала инфраструктуры;
* достаточности подключенных к SIEM-системе источников событий ИБ;
* соответствия документации, разработанной Исполнителем, требованиям настоящего ТЗ;
* возможности приемки системы сбора событий ИБ в эксплуатацию и возможности начала Исполнителем оказания услуг по Мониторингу, выявлению и реагированию на события ИБ.

Результаты приемочных испытаний оформляются в форме:

* протокола приемочных испытаний;
* заключения по результатам приемочных испытаний.
  1. **Требования к мониторингу, выявлению и реагированию на события информационной безопасности**

Мониторинг, выявление и реагирование на события информационной безопасности включают в себя:

* обнаружение и регистрация компьютерных инцидентов;
* реагирование на компьютерные инциденты;
* выявление и анализ уязвимостей в защищаемом информационном ресурсе Заказчика;
* анализ деятельности по управлению компьютерными инцидентами;
* актуализация перечня источников событий информационной безопасности;
* формирование отчетности по мониторингу событий информационной безопасности.
  1. **Требования к обнаружению и регистрации компьютерных инцидентов**

В рамках проведения обнаружения и регистрации компьютерных инцидентов, Исполнитель осуществляет:

* сбор и анализ информации о событиях безопасности и иных данных мониторинга, необходимых для поиска признаков возможного возникновения компьютерных инцидентов;
* наблюдение за событиями ИБ в SIEM-системе, просмотр логов на предмет нахождения аномальных событий ИБ, не распознанных SIEM-системой
* регистрация признаков возможного возникновения компьютерных инцидентов;
* подтверждение факта возникновения компьютерного инцидента, определение характера влияния на информационные ресурсы с целью принятия решения о регистрации компьютерного инцидента;
* регистрация компьютерного инцидента (в случае подтверждения факта прекращения или нарушения критического процесса, или нарушения безопасности информации);

Проведение обнаружения и регистрации компьютерных инцидентов осуществляются 24 часа 7 дней в неделю.

Реагирование и оповещение о компьютерных инцидентах осуществляется в рабочие дни с 8:30 – 18:00 по московскому времени.

Реагирование и оповещение о критичных компьютерных инцидентах осуществляется 24 часа 7 дней в неделю.

* 1. **Требования к информационному обеспечению для своевременного реагирования на компьютерные инциденты**

В рамках реагирования на компьютерные инциденты Исполнитель обеспечивает:

* информирование Заказчика о компьютерном инциденте. При необходимости, по согласованию с Заказчиком, информация о компьютерном инциденте направляется Исполнителем в НКЦКИ в течение 2-х часов после согласования на отправку;
* совместно с заказчиком определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;
* обработку инцидентов, полученных из ГосСОПКА и НКЦКИ;
* оказание методической помощи Заказчику по локализации компьютерного инцидента;
* оказание методической помощи Заказчику по выявлению последствий компьютерного инцидента;
* оказание методической помощи Заказчику по ликвидации последствий компьютерного инцидента;
* закрытие компьютерного инцидента. В случае информирования НКЦКИ ранее о компьютерном инциденте, необходимо проинформировать о закрытии данного инцидента.

В случае обнаружения события, Исполнитель регистрирует и оповещает ответственного сотрудника Заказчика по средствам уведомления через мессенджер «Телеграм» в специальную группу и сотовой связи на номер ответственного со стороны заказчика для классификации события как инцидент в сроки, указанные в Таблице № 2. Оповещение ответственного сотрудника Заказчика осуществляется 24х7 в случае регистрации критического события и в рабочие дни с 08:00 до 17:00 местного времени Заказчика в остальных случаях.

Таблица № 2

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Критичность** | **Описание** | **Время оповещения** |
|  | Высокая | Сбой или отказ в работе, вызвавший полную или частичную недоступность/неработоспособность информационных ресурсов Заказчика | 1 час |
|  | Средняя | Сбой или отказ в работе, оказывающий значительное воздействие на функциональность информационных ресурсов Заказчика, производительность значительно снижена по сравнению с нормальной работой. | 3 часа |
|  | Низкая | Сбой или отказ в работе, не оказывающий или оказывающий незначительное воздействие на общую функциональность и производительность информационных ресурсов Заказчика. | 5 часов |

После подтверждения ответственным сотрудником Заказчика инцидента ИБ, Исполнитель регистрирует компьютерный инцидент и выдает рекомендации, предоставляет консультации по инциденту ИБ, путем анализа логов с источников событий ИБ и SIEM-системы. При необходимости, Исполнитель разрабатывает новые и корректирует существующие правила анализа событий информационной безопасности и данных мониторинга, а также оказывает содействие Заказчику при локализации и устранении компьютерного инцидента. Заказчик подтверждает закрытие компьютерного инцидента.

* 1. **Требования к анализу деятельности по управлению компьютерными инцидентами**

В целях проведения анализа деятельности по управлению компьютерными инцидентами, Исполнитель 1 раз в квартал на протяжении оказания услуг, осуществляет:

- идентификацию методов и способов обнаружения и реагирования на компьютерные инциденты, которые показали свою эффективность;

- разработку рекомендаций по внедрению более эффективных методов обнаружения компьютерных инцидентов и необходимым мерам по недопущению повторного возникновения компьютерных инцидентов вследствие недостаточно эффективного управления;

- разработку новых, и корректировка существующих правил анализа событий безопасности и данных мониторинга.

Заказчик проводит оценку рекомендаций и возможности их реализации. Исполнитель обеспечивает методическую помощь по внедрению данных рекомендаций.

* 1. **Требования к актуализации перечня источников событий информационной безопасности**

Исполнитель, совместно с Заказчиком 1 раз в квартал с момента подключения инфраструктуры Заказчика к Центру мониторинга осуществляет актуализацию перечня основных источников событий ИБ.

Актуализация перечня основных источников событий ИБ осуществляется с использованием защищенного канала связи.

Соответствующие изменения должны быть внесены в последующие сводные отчеты.

* 1. **Требования к формированию отчетности по мониторингу событий информационной безопасности**

Исполнитель должен предоставлять Заказчику сводные отчеты об оказании услуг, включающие информацию о подключенных источниках, типах зарегистрированных инцидентов, статистике по собранным событиям ИБ, запущенным в процессе мониторинга сценариям выявления инцидентов, доступности и работоспособности центра мониторинга Исполнителя.

Сводные отчеты предоставляются Исполнителем ежемесячно не позднее 10-го числа месяца, следующего за месяцем оказания услуг.

* 1. **Требования к разработке организационно-распорядительной документации**

Исполнитель в рамках оказания Услуг должен обеспечить Заказчику возможность разработки организационно-распорядительной документации, регламентирующей порядок обработки ПДн, в объеме достаточном для реализации организационных мер по обеспечению безопасности ПДн при их обработке в ИСПДн, предусмотренных действующим законодательством в области защиты информации.

* 1. **Общие требования к разработке ОРД**

Разработка ОРД должна быть обеспечена посредством предоставления Исполнителем доступа к веб-сервису, реализующему функции автоматизированного создания ОРД в соответствии с параметрами, заданными пользователем, (далее – Веб-сервис).

Доступ к Веб-сервису должен предоставляться Исполнителем посредством регистрации Исполнителем в базе данных нового Пользователя, уполномоченного для работы с Веб-сервисом со стороны Заказчика, (далее – Пользователь) с произвольными логином и паролем.

Данные учетной записи Пользователя предоставляются в адрес Заказчика в течение 3 (трех) рабочих дней с даты подписания Договора. Одновременно с предоставлением данных учетной записи Пользователя Исполнитель должен передать Заказчику неисключительные имущественные права (лицензию) на право использования Веб-сервиса.

Срок действия неисключительных имущественных прав (лицензии) на право использования Веб-сервиса должен соответствовать сроку гарантийных обязательств на результат оказанных Услуг, но не менее 13 месяцев с даты передачи имущественных прав.

Доступ к Веб-сервису должен предоставляться бесперебойно в режиме «24/7», за исключением нештатных ситуаций (длительное отключение электропитания, сбой работы программных или аппаратных средств и т.п.).

Веб-сервис должен иметь клиент-серверную архитектуру, где серверная часть развернута на мощностях Исполнителя.

В течение всего срока действия имущественных прав (лицензии) на использование Веб-сервиса Исполнитель должен обеспечивать:

- сопровождение Пользователей по вопросам, связанным с использованием функционала Веб-сервиса, включая вопросы, связанные с содержанием ОРД;

- актуализацию состава и содержания шаблонов ОРД, доступных для разработки с использованием Веб-сервиса, (далее – Шаблоны) посредством их добавления и\или изменении в соответствии с изменениями в требованиях законодательства в области защиты ПДн к реализации организационных мер по обеспечению безопасности ПДн.

Сопровождение Пользователей должно осуществляться по электронной почте на основании заявки Пользователя, сформированной посредством функционала интерфейса Веб-сервиса.

Веб-сервис должен быть зарегистрирован в Едином реестре российских программ для электронных вычислительных машин и баз данных в соответствии с действующим законодательством.

**3.22** **Требования** **к обеспечению безопасности персональных данных при разработке организационно-распорядительной документации**

Функционал Веб-сервиса должен соответствовать требованиям законодательства Российской Федерации к обеспечению безопасности ПДн, в том числе при их передаче по открытым каналам связи (наличие аттестата соответствия требованиям по безопасности информации или иного документального подтверждения).

Пользователю должна предоставляться возможность подключения к Веб-сервису посредством совместного использования: программного обеспечения на основе браузеров, поддерживающих защищенные протоколы TLS, на базе российских криптографических алгоритмов ГОСТ (Яндекс Браузер или аналоги) и криптопровайдера, поддерживающего российские криптографические алгоритмы ГОСТ («КриптоПро CSP» версии 4.0 и выше или аналог).

**3.23 Требования к разработке организационно-распорядительной документации в части автоматизированных функций**

Функционал Веб-сервиса в части заполнения Шаблонов должен быть максимально автоматизирован и включать возможность обработки следующих типов сведений:

* общедоступные сведения;
* фиксированные сведения;
* кастомизированные сведения.

**3.24 Требования к общедоступным сведениям**

Под общедоступными сведениями подразумеваются данные реквизитов организации Заказчика, доступные с использованием ресурса Единый государственный реестр юридических лиц (далее - ЕГРЮЛ).

Заполнение общедоступных сведений должно производиться автоматически по номеру ОГРН на основе данных ЕГРЮЛ.

**3.25 Требования к фиксированным сведениям**

Под фиксированными сведениями подразумеваются сведения, перечень и содержание которых ограничены функционалом Веб-сервиса посредством предоставления Пользователю возможности выбора единственного значения из выпадающего списка.

**3.26 Требования к кастомизированным сведениям**

Под кастомизированными сведениями подразумеваются сведения, которые вносятся Пользователем в Веб-сервис вручную.

Для полей кастомизированных сведений «Фамилия», «Имя», «Отчество», при их заполнении в именительном падеже, должна производиться автоматическая генерация падежных форм «родительный падеж», «дательный падеж», «творительный падеж», «предложный падеж». Выбор и сопоставление сгенерированной падежной формы с содержанием Шаблонов должно осуществляться автоматически в соответствии с контекстом содержания Шаблонов, дополняемых указанными кастомизированными сведениями.

Заполненные шаблоны должны быть доступны Пользователю для просмотра, редактирования и выгрузки в форматах \*.docx или \*.rtf в виде единого архива в формате \*.zip

Результатом разработки организационно-распорядительной документации является:

полученный Заказчиком комплект организационно-распорядительной документации, разработанный с помощью Веб-сервиса.

**3.27 Общие требования к документированию**

Язык оформления документации – русский, за исключением общепринятых названий и оригинальных наименований программно-аппаратных средств импортного производства.

Вся отчетная документация должна быть оформлена и передана Заказчику в электронном виде, в формате Word и PDF с использованием защищенного канала связи.

**3.28 Общие требования к безопасности оказываемых услуг**

Все сведения о составе и характеристиках объектов информатизации Заказчика являются конфиденциальной информацией.

Исполнитель обязуется:

* не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся на объектах информатизации Заказчика;
* не осуществлять несанкционированный доступ к информационным ресурсам объектов информатизации Заказчика;
* не проводить незаконное копирование информации, циркулирующей или хранящейся на объектах информатизации Заказчика;
* не предпринимать манипулирование информацией, циркулирующей или хранящейся на объектах информатизации (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);
* не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;
* не внедрять на объектах информатизации программы-вирусы (загрузочные, файловые и др.);
* не устанавливать программные и аппаратные закладные устройства в технические средства объектов информатизации Заказчика;
* не устанавливать в технические средства объектов информатизации программное обеспечение, зараженное вирусами.

Нарушение настоящих требований влечёт за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законом Российской Федерации.

1. **Состав и содержание услуг**
   1. Требования к порядку сдачи услуг и составу отчетной документации приведены в Таблице № 3.

Исполнитель вправе досрочно оказать услуги.

Результаты оказания услуг на 1 этапе представляются Заказчику по мере их выполнения, в рабочее время (понедельник – четверг: с 8-30 до 16-30 часов 00 минут (время московское), пятница – с 8-30 до 16 -00.

Результаты оказания услуг на 2 этапе (сводные отчеты) представляются Заказчику в рабочее время ежемесячно, не позднее 10-го числа месяца, следующего за месяцем оказания услуг.

Таблица №3

| **№ этапа** | **Наименование услуг** | **Сроки выполнения** | **Результаты оказания услуг** |
| --- | --- | --- | --- |
| **1** | **Развертывание инфраструктуры для сбора событий с источников событий информационной безопасности Заказчика** | В течение 50 (пятидесяти) рабочих дней с даты заключения Договора при условии выполнения Заказчиком своих обязательств | Отчетные документы:   * Предварительный перечень источников событий ИБ для осуществления мониторинга; * Структурно-функциональная схема основных источников событий ИБ; * Отчет по результатам обследования действующей инфраструктуры Заказчика; * Регламент взаимодействия сторон в рамках оказания услуг по мониторингу событий ИБ; * Документ о приемке, подписанный Заказчиком. |
|  | Обследование действующей инфраструктуры Заказчика |
|  | Подключение инфраструктуры Заказчика к Центру мониторинга Исполнителя |
| **2** | **Мониторинг, выявление и реагирование на события информационной безопасности** | В течение 12 (месяцев) с момента завершения Этапа № 1  В течение 5 (пяти) календарных дней с даты заключения Договора | Отчетные документы:   * сводные отчеты (предоставляются ежемесячно); * Акт приемки оказанных услуг, подписанный Сторонами.   1. Отчетные документы:  - комплект организационно-распорядительной документации;  2. Документ о приемке, подписанный Заказчиком. |
|  | Обнаружение и регистрация компьютерных инцидентов |
|  | Реагирование на компьютерные инциденты |
|  | Анализ деятельности по управлению компьютерными инцидентами |
|  | Актуализация перечня источников событий информационной безопасности |
|  | Формирование отчетности по мониторингу событий информационной безопасности |
| **3** | **Разработка организационно-распорядительной документации** |

**ПРИЛОЖЕНИЕ № 2**

к Договору оказания услуг от \_\_\_\_\_\_\_\_\_\_\_202 г. №\_\_\_\_\_\_\_\_\_\_\_\_

**ФОРМА АКТА СОГЛАСОВАНА**

|  |  |
| --- | --- |
| ЗАКАЗЧИК:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Г.В. Новикова  М.П**.** | ИСПОЛНИТЕЛЬ:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / /  М.П. |

**Акт сдачи-приемки ОКАЗАННЫХ УСЛУГ**

(по договору № от 202 г.)

за расчетный месяц\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г.

|  |  |
| --- | --- |
| г. Калуга | «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г. |

**Заказчик** - ПАО «Калужская сбытовая компания», в лице уполномоченного представителя Заказчика;

**Исполнитель** - подписали настоящий Акт о результатах оказания Исполнителем услуг [по мониторингу и анализу инцидентов информационной безопасности, разработке организационно-распорядительной документации по вопросам безопасности информационных ресурсов Заказчика и взаимодействию с органами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) за расчетный месяц.](https://evrone.ru/services/devops?utm_source=yandex&utm_medium=cpc&utm_campaign=search_devops&utm_content=852infrastructure_optimization&utm_term=---autotargeting&yclid=10748733796902764543" \t "_blank)

1. Заказчик \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ претензии к результатам услуг Исполнителя.

(указать: имеет либо не имеет)

1. Претензии Заказчика к результатам оказанных Исполнителем услуг отражены письменно (исх. №\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г.)

(заполняется Заказчиком при наличии претензий).

**ЗАКАЗЧИК ИСПОЛНИТЕЛЬ**

Уполномоченный представитель Уполномоченный представитель

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ /

**Приложение 2 к Документации**

**Обоснование начальной (максимальной) цены договора**

В целях проведения аукциона и определения начальной (максимальной) цены договора использован метод сопоставимых рыночных цен (анализ рынка).

Расчет начальной (максимальной) цены договора:

|  |  |  |  |
| --- | --- | --- | --- |
| Предмет закупки | Основные характеристики объекта закупки | Источники ценовой информации | Цена, руб.,  в т.ч. НДС 20% |
| Мониторинг на базе системы RUSIEM (в течение 12 мес.) и анализ инцидентов информационной безопасности,  разработка организационно-распорядительной документации и взаимодействие с органами ГосСОПКА | В соответствии с Техническим заданием Документации | Коммерческое предложение 1,  Исх. № 994 от 13.08.2024 г. | 1 700 000,00 |
| Коммерческое предложение 2,  Исх. № 24ЭП/8340/КА от 20.06.2024 г. | 1 704 000,00 |
| Коммерческое предложение 3,  Исх. № 169/08-24 от 13.08.2024 г. | 1 680 000,00 |
| Коммерческое предложение 4,  Исх. № СТ-15485 от 09.08.2024 г. | 1 600 000,00 |

Начальная (максимальная) цена договора рассчитана как минимальное значение предложенных цен, от четырех исполнителей аналогичных видов услуг в размере:  
**- 1 600 000 (Один миллион шестьсот тысяч) рублей 00 копеек, в том числе НДС 20% - 266 666 руб. 67 коп.;**

Дата подготовки обоснования начальной (максимальной) цены договора: 11.09.2024 г.