

Утверждаю  
Исполнительный директор  
Лахов С.В.  
2026г.

Техническая спецификация закупаемой Услуги оперативного центра  
информационной безопасности

Настоящая техническая спецификация, содержит общие и частные требования к реализации оказания комплекса услуг по обеспечению информационной безопасности (далее — «Услуга»).

В рамках Услуги должны быть решены следующие задачи:

- организация и осуществление мониторинга событий и обработки инцидентов ИБ (далее – Организация мониторинга инцидентов ИБ), включая развёртывание в инфраструктуре Заказчика необходимых компонентов;
- круглосуточный мониторинг событий ИБ, зафиксированных на серверном оборудовании, сетевых устройствах и информационных системах Заказчика, подключенных к SIEM-системе Поставщика (далее – Зона мониторинга);
- выявление инцидентов ИБ, произошедших в Зоне мониторинга;
- направление Заказчику информации о выявленных инцидентах и методах реагирования на них и предоставления рекомендаций по их устранению;
- предоставление экспертной поддержки в процессе реагирования на инциденты ИБ;
- оказание помощи в проведении расследования инцидентов ИБ, однако в случае если в Зоне мониторинга будет выявлено подозрительное событие, касающееся систем, не входящих в Зону мониторинга, – о данном событии уведомляется Заказчик. Дальнейшее расследование Заказчик осуществляет самостоятельно, Поставщик при необходимости оказывает консультации для определения степени критичности и дополнительного анализа, с целью выявления источника проблемы и помощи в устранении инцидента специалистами Заказчика;

1. Границы оказания Услуги и подключение к ситуационному центру ИБ:

В границы оказания Услуги в целом входит следующие площадки Заказчика, на которых размещены ИС

Услуги оказываются удаленно с места нахождения Поставщика. В случае необходимости работники Поставщика могут оказывать Услуги с выездом на территорию Заказчика (монтаж оборудования, настройка оборудования и др.). Заказчик должен обеспечить необходимый доступ работникам Поставщика, который обговаривается после заключения договора.

В рамках предоставления Услуги Поставщик предоставляет специализированные системы и услуги, приведенные в Таблице 2 для выполнения целей и задач Услуги с учетом необходимого аппаратного и программного обеспечения:

Таблица №2. Состав Услуги

| № | Название компонента            | Описание                                                                                                                                                       |
|---|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Услуга ситуационного центра ИБ | Включает услуги по мониторингу и анализу событий ИБ, помощь в реагировании на инциденты ИБ, а также управление технологическим стеком ситуационного центра ИБ. |

|   |                                                      |                                                                                                                                                                                                                                                  |
|---|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2 | Платформа ситуационного центра ИБ                    | Платформа на основе которой осуществляется услуга ситуационного центра ИБ, включающая в себя функционал системы сбора, мониторинга и анализа событий информационной безопасности, системы управления и автоматизации инцидентов и анализа угроз. |
| 3 | Коллекторы событий Платформы ситуационного центра ИБ | Размещаются на стороне Заказчика (при необходимости).                                                                                                                                                                                            |
| 4 | VPN-шлюз                                             | Используется оборудование Заказчика                                                                                                                                                                                                              |

2. Срок оказания услуги и порядок оплаты

Срок оказания услуг с момента заключения договора по 31 декабря 2027.  
Сумма договора заложена на 12 месяцев. В случае заключения договора позже 01.01.2027 года сумма подлежит корректировке пропорционально оставшемуся периоду.

3. Функциональные требования к оказываемым услугам

В рамках оказания услуг по обеспечению информационной безопасности предоставляются следующие сервисы и системы с соответствующими функциональными характеристиками.

5.1. Услуга ситуационного центра ИБ

Состав услуги ситуационного центра ИБ

Требования к составу Услуги ситуационного центра ИБ, состоят из 4 этапов, в рамках каждого этапа определена цель и поставлены задачи для ее достижения.

Этап 1. Обследование:

Цель этапа – определить зону мониторинга оказания услуги и определить список источников.

Задачи, которые должны быть решены для достижения цели:

На основании опросного листа, заполненного со стороны Заказчика, и интервьюирования представителей Заказчика, Поставщик проводит анализ ИТ-Инфраструктуры Заказчика, на основании которого производится:

- выдача рекомендаций по составу и приоритезации подключаемых источников событий ИБ (далее – источников);
- определение потребностей Заказчика в части подключения существующих и разработки новых сценариев выявления атак. Для этого Заказчику направляется аналитический опросный лист для заполнения.
- выработка организационно-технических решений по зоне мониторинга предоставления услуги и порядку развертывания компонентов Услуги на площадке Заказчика;
- техническим характеристикам и требованиям к вычислительным ресурсам, выделяемых Заказчиком, включая расчет емкости файловых хранилищ, для возможного хранения событий в течение 3 (трех) месяцев в ИТ-инфраструктуре Заказчика.
- порядку и организации межсетевого взаимодействия компонентов Услуги на площадке Заказчика и Центра мониторинга и реагирования на киберугрозы;
- в рамках данного этапа должны быть

собраны, как минимум следующие сведения:

- название источника;
- описание функционала источника (принадлежность к ИС);
- площадка размещения;
- производитель/марка/модель;
- тип/версия операционной системы;
- тип/версия программного обеспечения;

Количество подключаемых объектов инфраструктуры (источников событий) – 11 физических серверов, 24 виртуальных, 30 конечных устройств, 2 межсетевых экранов Palo Alto

## **Этап 2. Внедрение:**

Цель этапа – развернуть компоненты услуги на площадке Заказчика и построить VPN-туннель между площадкой Заказчика и Поставщика:

Задачи, которые должны быть решены для достижения цели:

В случае отсутствия L3 связности между распределенными площадками, Поставщик и Заказчик выполняют организацию VPN-туннеля между площадкой Заказчика и Поставщика, где Заказчик обеспечивает соединение до границы ИТ-инфраструктуры Заказчика.

- При взаимодействии не должна осуществляться фильтрация трафика путём блокирования используемого транспортного протокола;
- Организация сетевых доступов между компонентами услуги и источниками событий, согласно запросу Поставщика;
- Поставщик выполняет при необходимости инсталляционные работы по внедрению компонентов Услуги в ИТ-инфраструктуру Заказчика;
- в случае необходимости предоставить Заказчику требования к вычислительным ресурсам, подсистеме(ам) хранения и рекомендации по конфигурированию для установки дополнительных компонентов Услуги.
- Поставщик ставит на мониторинг работоспособности компоненты услуги, а также обеспечивает бесперебойную работу активного сетевого оборудования, на котором организовано VPN соединение с Заказчиком;

## **Этап 3. Подключение:**

Цель данного этапа – подключить источники событий и убедиться, что события в SIEM-систему поступают корректно, а также разработать новые сценарии выявления нарушений и инцидентов ИБ на основании запроса Поставщика (при необходимости):

Задачи, которые должны быть решены для достижения цели:

- Согласно, перечню источников, определенного в Этапе 1, Поставщик предоставляет инструкции по их подключению;
- Поставщик, при необходимости, разрабатывает индивидуальные адаптеры для нетиповых источников;
- после подключения источников Поставщик проверяет полноту поступаемых событий и, при необходимости, оптимизирует их;
- Поставщик выполняет конфигурирование и профилирование SIEM-системы под ИТ Инфраструктуру Заказчика на основании заполненного Заказчиком аналитического опросного листа. Данные работы гарантируют работоспособность сценариев выявления нарушений и инцидентов ИБ;
- Поставщик разрабатывает новые сценарии, а именно расширение категорий инцидентов и правил корреляции на основании специфичных запросов Заказчика и/или основываясь на результатах анализа уязвимостей;
- Поставщик предоставляет доступ уполномоченным представителям Заказчика в SOAR для мониторинга услуги;
- Заказчик предоставляет Поставщику список сотрудников, которым необходимо направлять информацию по инцидентам ИБ, после чего Поставщик настраивает соответствующие группы уведомлений.

## **Этап 4. Операционная работа:**

Цель этапа – адаптировать SIEM-систему под зону мониторинга заказчика Заказчика, настроить отправку уведомлений об инцидентах ИБ в соответствии с SLA:

Задачи, которые должны быть решены для достижения цели:

В рамках оказания Услуги ситуационного центра ИБ Поставщик должен выполнять:

- анализ событий ИБ в режиме 24x7 силами аналитиков 1-ой линии Поставщика, которая является единой «точкой входа», поступающих от различных источников

событий. Аналитики 1-ой линии должны обеспечивать обработку инцидентов ИБ, проверку ложного срабатывания, проведение первичной аналитики и выделение инцидентов ИБ на основе категорий инцидентов и правил, регистрацию и последующее сопровождение инцидента ИБ в соответствии со стандартами ITIL (категорирование, приоритизация, SLA и т.д.). Режим оповещения по инцидентам ИБ:

- обработку инцидентов ИБ силами аналитиков 2-ой линии Поставщика в режиме 8x5, проведение углублённой аналитики при решении инцидентов ИБ с использованием различных специализированных инструментов; адаптацию правил корреляции в соответствии с изменениями в ИТ-инфраструктуре Заказчика; добавление исключений в правила корреляции как по требованию Заказчика, так и на основании самостоятельного анализа профиля Заказчика;
- при подтверждении Заказчиком, что данное событие является инцидентом ИБ, инцидент переводится в статус и дальнейшая работа по инциденту ведётся аналитиками 2 и 3 линии. Аналитики проводят углублённый анализ, ретроспективных событий, которые привели к инциденту ИБ.
- Проведение первичного расследования инцидента ИБ происходит, путем выдачи рекомендаций, подготовки инструкций по реагированию на инцидент ИБ, которые могут включать в себя также конфигурационные файлы для сбора событий непосредственно с источника.

В рамках услуг должна быть реализована возможность визуализации аналитической информации по инцидентам ИБ с помощью виджетов и/или Дашбордов (Личный кабинет), в котором Заказчику доступны следующие функции:

- просмотр карточки инцидента по каждому инциденту ИБ, с возможностью самостоятельного управления статусом инцидента;
- просмотр статистики о произошедших инцидентах ИБ;
- регистрация обращений/инцидентов ИБ и отслеживание их статуса в режиме реального времени;
- получение визуально представленной информации о параметрах оказания услуги, таких как выполнение SLA;
- просмотр информации по каждому инциденту ИБ, который снабжен описанием выявленных техник атак;
- предоставление в унифицированном шаблоне карточки инцидента по каждому выявленному инциденту ИБ;
- выгрузка унифицированных отчетов в Личном кабинете.

### **Требования к оказанию услуги ситуационного центра ИБ**

Настоящие требования устанавливают порядок обеспечения услуги ситуационного центра ИБ и описывают процедуры взаимодействия, связанные с выявлением и реагированием на инциденты ИБ.

Должно быть реализовано заведение Инцидента ИБ в учётной системе Поставщика путём заполнения карточки инцидента и отправка её Заказчику, оповещение об инциденте осуществляется путём отображения карточки инцидента в Личном кабинете и/или отправленным электронным письмом и/или подтверждённым звонком ответственному специалисту Заказчика для инцидентов с уровнем критичный, высокий, средний и низкий.

В случае обнаружения Заказчиком инцидента, Заказчик информирует Поставщика по контактными данным технической службы Поставщика.

**Карточка инцидента должна содержать в себе следующую обязательную информацию:**

Общая информация:

- номер зарегистрированного инцидента (в учётной системе Поставщика);
- приоритет инцидента;

- время регистрации;
- тема (кратное описание);
- информация об инциденте (текущий статус, комментарий к данному статусу);

**Ключевая информация (при наличии возможности обнаружения):**

- список затронутых хостов и активных учётных записей на них в момент инцидента;
- источник/и событий ИБ, на базе которых выявлен инцидент;
- список выявленных индикаторов компрометации;
- описание инцидента в хронологическом порядке;
- ссылки на дополнительные файлы, прикладываемые к инциденту;

**Рекомендации:**

- какие первичные действия должны быть предприняты для предотвращения инцидента ИБ или минимизации последствий от него, либо же какая дополнительная информация требуется от Поставщика для проведения Поставщиком дальнейшего анализа инцидента ИБ
- После подписания договора на оказание услуги, между Поставщиком и Заказчиком совместно должна быть разработана форма отчёта, где будут учтены все инциденты ИБ, обновления и рекомендации в рамках оказываемых услуг, который будет утверждаться ежемесячно руководством организации с обеих сторон.

**В рамках исполнения требований услуги Поставщик должен уметь выявлять основные категории инцидентов ИБ:**

- **Unauthorized Access/Compromised.** Инциденты, связанные с неавторизованным получением физического/логического доступа к защищаемой сети/системе/приложению/данным.
- **Scans/Probes/Attempted Access.** Инциденты, связанные с активностью, направленной на получение сведений о доступных хостах, открытых портах, уязвимостях, установленном ПО или иных сведений о целевом объекте, которые могут быть использованы нарушителем для дальнейшего планирования и развития атаки.
- **Brute Force.** Инциденты, связанные с успешными и неуспешными попытками подбора паролей в защищаемые системы.
- **Vulnerability.** Инциденты, связанные с успешной эксплуатацией уязвимостей, а также выявлением (с использованием сканеров) критичных уязвимостей (уязвимостей реализации), эксплуатация которых может привести к реализации угроз информационной безопасности.
- **Malware.** Инциденты, связанные с активностью вредоносного программного обеспечения (например, запуск шифровальщика, прописывание в автозагрузку трояна и т.п.).
- **Malware C&C Communication.** Инциденты, связанные с выявлением взаимодействия хостов защищаемой инфраструктуры с известными командными центрами.
- **Malicious Host.** Инциденты, связанные с доступом к ресурсам, выполняющим распространение вредоносного ПО (исключая известные командные центры ботнет сетей), либо связанные непосредственно с размещением в сети Интернет таковых ресурсов.
- **Spam.** Инциденты, связанные с распространением незапрашиваемой электронной почты, носящей информативный/рекламный характер.
- **Fraud.** Инциденты, связанные с мошенническими действиями пользователей защищаемой информационной системы.
- **Social Engineering.** Инциденты, связанные с побуждением пользователей защищаемой информационной системы к совершению действий (путём обмана или злоупотребления доверием), направленных на достижение целей нарушителя

(осуществление операций по переводу денежных средств, переход по вредоносной ссылке, разглашение парольной информации и т.п.).

- **Improper Usage.** Инциденты, связанные с нарушениями требований политик/регламентов/инструкций ИБ (например, доступ в Интернет в обход прокси, подключение к публичным Wi-Fi сетям, использование учётных записей доменного администратора на запрещённом хосте и т.п.).
- **Suspicious Process Activity.** Инциденты, связанные с аномальным поведением легитимных процессов.

#### Целевые показатели уровня предоставления услуги ситуационного центра ИБ:

Инциденты ИБ должны подразделяться на приоритеты по степени срочности их решения, указанными в таблице №3.

Таблица №3. Показатели приоритетов

| Приоритет   | Описание приоритета                                                                                                                                                                                                                                                                                                                  | Пример                                                                                                                                                                              |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Критический | Инцидент, приводящий либо к полной недоступности всех защищаемых ресурсов Заказчика продолжительностью более 15 минут, либо к фактам компрометации большого количества защищаемых ресурсов Заказчика, которые могут нанести существенный ущерб Заказчику. Либо же инцидент носит таргетированный характер.                           | Таргетированная атака, в рамках которой была скомпрометирована учётная запись администратора домена                                                                                 |
| Высокий     | Инцидент, приводящий к частичной недоступности защищаемых ресурсов Заказчика, продолжительностью не более 15 минут, возникающие с периодичностью не более 1 раза в 1 час, либо к возможности или созданию условий для компрометации защищаемых ресурсов Заказчика: злонамеренная активность не была заблокирована превентивными СЗИ. | Активность вредоносного программного обеспечения не детектируемого используемыми средствами антивирусной защиты                                                                     |
| Средний     | Инцидент, не приводящий в данный момент к недоступности защищаемых ресурсов Заказчика, но имеющий высокую вероятность привести в будущем к инциденту с более высоким приоритетом. Злонамеренная активность была локализована и заблокирована превентивными СЗИ.                                                                      | Успешная эксплуатация уязвимости браузера с последующей попыткой заражения хоста вредоносным программным обеспечением, заблокированной используемыми средствами антивирусной защиты |
| Низкий      | Инцидент, в рамках которого не было нанесено какого-либо ущерба Заказчику, осуществлялся сбор информации о системе в рамках имеющихся прав доступа.                                                                                                                                                                                  | Сбор информации о защищаемом периметре                                                                                                                                              |

#### Требование к целевым показателям услуги:

Оказание Услуги должно осуществляться в соответствии с целевыми показателями, приведёнными в таблице №4.

Таблица №4. Показатели уровня оказания услуги

| №  | Показатель                                                                                                                                            | Приоритет       | Время выполнения показателя   | Табель | Время реакции Заказчика на запросы Поставщика |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------------------|--------|-----------------------------------------------|
| 1. | Обнаружение инцидента ИБ, Регистрация инцидента ИБ                                                                                                    | 1 — Критический | до 30 минут                   | 24x7   | Не применимо                                  |
|    |                                                                                                                                                       | 2 — Высокий     | до 30 минут                   | 24x7   | Не применимо                                  |
|    |                                                                                                                                                       | 3 — Средний     | до 30 минут                   | 24x7   | Не применимо                                  |
|    |                                                                                                                                                       | 4 — Низкий      | до 60 минут                   | 24x7   | Не применимо                                  |
| 2. | С момента регистрации инцидента ИБ Поставщик проводит проверку ложного срабатывания и категорирование инцидента, уведомляет Заказчика об инциденте ИБ | 1 — Критический | до 60 минут                   | 24x7   | До 30 минут                                   |
|    |                                                                                                                                                       | 2 — Высокий     | до 90 минут                   | 24x7   | До 45 минут                                   |
|    |                                                                                                                                                       | 3 — Средний     | до 120 минут                  | 24x7   | До 60 минут                                   |
|    |                                                                                                                                                       | 4 — Низкий      | до 240 минут                  | 24x7   | До 120 минут                                  |
| 3. | В случае, если Заказчик подтвердил инцидент ИБ, то Поставщик выдаёт рекомендации по противодействию                                                   | 1 — Критический | 2 часов с момента регистрации | 24x7   | Не применимо                                  |
|    |                                                                                                                                                       | 2 — Высокий     | 4 часов с момента регистрации | 24x7   | Не применимо                                  |
|    |                                                                                                                                                       | 3 — Средний     | 6 часов с момента регистрации | 24x7   | Не применимо                                  |
|    |                                                                                                                                                       | 4 — Низкий      | 24 часа с момента регистрации | 24x7   | Не применимо                                  |
| 4. | Время на расследование инцидента ИБ и анализа журналов событий, предоставленных Заказчиком Поставщику                                                 | 1 — Критический | Не применимо                  | 24x7   | Не применимо                                  |
|    |                                                                                                                                                       | 2 — Высокий     | Не применимо                  | 24x7   | Не применимо                                  |
|    |                                                                                                                                                       | 3 — Средний     | Не применимо                  | 8x5    | Не применимо                                  |
|    |                                                                                                                                                       | 4 — Низкий      | Не применимо                  | 8x5    | Не применимо                                  |

**Поставщик услуг должен обрабатывать запросы Заказчика согласно показателям, указанным в таблице №5.**

Таблица №5. Целевые показатели проведения изменений в месяц

| №  | Показатель                |                                                                                                                                                                                                                                                    | Кол-во обращений |
|----|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| 1. | Запрос на изменение       | Заявки, связанные с изменением конфигурации Услуги (добавление/удаление источника событий ИБ, адаптация сценария)                                                                                                                                  | не более 8       |
| 2. | Информационный запрос     | Заявки, связанные с консультационными вопросами, по Услуге (вопросы по Договору и т.п.)                                                                                                                                                            | не более 5       |
| 3. | Подозрение на Инцидент ИБ | Заявка, связанная с подозрением Заказчика на Инцидент ИБ. Изначально данному обращению присваивается «низкий» приоритет. При необходимости Заказчик может повысить приоритет. Работа по данному типу запроса ведется в соответствии с таблицей №4. | Не ограничено    |

#### **5.2. Технические требования для обеспечения информационной безопасности.**

Услуга должна оказываться на базе технологического решения, предоставляемого Поставщиком.

В целях повышения эффективности, надежности предоставляемых услуг решение должно быть представлено в виде единой платформы ситуационного центра ИБ (далее – Платформа).

Платформа должна включать в себя функционал системы сбора, мониторинга и анализа событий информационной безопасности, системы управления и автоматизации инцидентов и анализа угроз.

Функциональные требования к Платформе:

- Платформа должна являться единой интегрированной системой, включающей в себя функционал SIEM, SOAR и Threat Intelligence в едином интерфейсе и с общей базой данных, без необходимости установки или интеграции сторонних компонентов.
- Платформа должна обеспечивать единое хранилище событий, инцидентов и индикаторов угроз, обеспечивая кросс-корреляцию данных между SIEM, SOAR и TI без коннекторов.
- Платформа должна поддерживать единую систему лицензирования, без необходимости приобретения отдельных лицензий на SIEM, SOAR или TI.
- Платформа должна обеспечивать бесшовную интеграцию между аналитикой TI и корреляционными правилами SIEM, что позволяет автоматически использовать новые индикаторы угроз в детектирующих правилах.
- Платформа должна поддерживать двунаправленную синхронизацию между инцидентами SOAR и событиями SIEM в режиме реального времени.
- Платформа должна поддерживать централизованное обновление и управление всеми компонентами через единый интерфейс.
- Платформа должна работать в полностью контейнеризованной архитектуре (Docker/Kubernetes) с возможностью горизонтального масштабирования.
- Платформа должна поддерживать установку в изолированных (air-gapped) сетях без доступа в интернет.
- Платформа должна иметь встроенные средства контроля целостности и аудита всех действий администраторов.

- Платформа должна обеспечивать централизованное управление всеми своими компонентами и функционалом через единый веб-интерфейс, без необходимости использования сторонних приложений, дополнительных окон, интерфейсов или скриптов.
- Платформа должна автоматически определять основные типы источников событий без использования сторонних средств.
- Платформа должна поддерживать создание настраиваемых дашбордов (dashboards).
- Платформа должна предоставлять функционал управления учетными записями пользователей и их ролями.
- Платформа должна обладать автоматическим механизмом резервного копирования конфигурации.
- Платформа должна иметь встроенные средства самодиагностики и уведомлять пользователя о возникновении неполадок.
- Платформа должна включать модуль координации и автоматизации процессов реагирования и расследования инцидентов, разработанный производителем платформы.
- Платформа должна быть масштабируемой и обеспечивать расширение функционала при добавлении новых устройств, офисов и приложений в инфраструктуре Заказчика.
- Платформа должна поддерживать использование распределенных баз данных для хранения событий при обеспечении доступа к ним через единый пользовательский интерфейс.
- Платформа должна работать с запасом производительности и выдерживать кратковременные пики нагрузки, превышающие расчетные значения.
- Платформа должна обеспечивать целостность собираемых и обрабатываемых данных.
- Платформа должна поддерживать расширенную таксономию событий и полей, предоставляя пользователю возможность присваивать им собственные наименования.
- Платформа должна предоставлять возможность настройки автоматической классификации событий по степени важности в соответствии с политикой пользователя.
- Платформа должна обеспечивать прозрачное получение, агрегацию, фильтрацию, сортировку и анализ данных.
- Платформа должна иметь встроенный модуль сбора и архивации журналов событий, поддерживающий как кратковременное (online), так и долгосрочное (offline) хранение данных.
- Платформа должна поддерживать стандартные протоколы сбора событий и обеспечивать безагентный сбор данных там, где это технически возможно.
- Платформа должна предоставлять доступ к историческим данным о событиях за длительный период времени для проведения расследований и аналитики.
- Платформа должна автоматически нормализовать поля событий, поступающих с различных устройств, без необходимости дополнительных настроек.
- Платформа должна обеспечивать стандартную категоризацию событий без предварительной конфигурации.
- Платформа должна сохранять события как в исходном, так и в нормализованном виде для последующего анализа.
- Платформа должна иметь возможность обрабатывать и нормализовать нестандартные поля, отсутствующие в исходных настройках.
- Платформа должна обеспечивать анализ событий как в режиме реального времени, так и за выбранные пользователем временные периоды.

- Платформа должна предоставлять возможность сбора и анализа событий на основе пользовательских фильтров, а также обеспечивать получение дополнительной информации по запросу.
- Платформа должна отображать события в режиме реального времени с возможностью мгновенного применения фильтров через веб-интерфейс.
- Платформа должна обеспечивать формирование отчетности по событиям, доступной пользователям через веб-интерфейс.
- Платформа должна предоставлять пользователям возможность самостоятельной настройки параметров отчетности и создания собственных отчетов.
- Платформа должна обеспечивать преобразование поисковых параметров по нормализованному и исходным данным в SQL-подобный язык запросов с использованием графического интерфейса.
- Платформа должна поддерживать расширение количества корреляционных правил.
- Платформа должна обеспечивать мультиарендность (multitenancy) с разграничением прав доступа между пользователями и арендаторами.
- Платформа должна поддерживать увеличение количества нормализуемых полей при необходимости.
- Платформа должна обеспечивать отчеты и визуализацию по методологиям MITRE ATT&CK, NIST, и ISO/IEC 27035.
- Платформа должна поддерживать интеграцию с системой Service Desk заказчика (например, Jira) через API.
- Платформа должна обеспечивать визуализацию типовых угроз в соответствии с MITRE ATT&CK Framework, а также предоставлять оценку уровня покрытия правил обнаружения угроз по тактикам и техникам MITRE.
- Платформа должна обеспечивать возможность установки неограниченного количества компонентов для сбора событий с удаленных сетей с использованием защищенных протоколов передачи данных, без дополнительных затрат на лицензирование.
- Платформа должна включать модуль поведенческого анализа (UBA), использующий методы машинного обучения и не требующий отдельного лицензирования.
- Платформа должна не иметь ограничений по количеству анализируемых учетных записей и пользователей, а модуль поведенческого анализа должен поддерживать не менее 10 категорий активности.
- Платформа должна обеспечивать централизованное управление всеми вышеуказанными модулями и компонентами через единый веб-интерфейс.
- Платформа должна обеспечивать развертывание всех компонентов из единого программного образа, при этом требуемый функционал активируется лицензией без необходимости установки или лицензирования дополнительного программного обеспечения сторонних производителей.
- Платформа должна обеспечивать актуальность и синхронную корреляцию данных в единой базе, с задержкой не более 1 секунды с момента получения событий от источника.
- Платформа должна использовать единую базу данных для хранения и обработки информации всеми своими модулями.
- Платформа должна обеспечивать возможность установки агентов на серверы и рабочие станции для сбора событий при наличии технической возможности.
- Платформа должна обеспечивать безагентный приём, обработку и нормализацию событий (журналов регистрации) от источников информационной инфраструктуры Заказчика по протоколу Syslog с поддержкой передачи данных по UDP и TCP, включая возможность защищённой передачи с использованием TLS. Функциональность проверяется при настройке услуги путём тестовой передачи события от источника и его отображения в интерфейсе платформы. Платформа

должна обеспечивать передачу Заказчику архивной базы данных событий и базы данных оперативного доступа по окончании срока действия договора, с последующим полным удалением данных на стороне Поставщика.

- Платформа должна включать встроенный SOAR-модуль, использующий единый движок корреляции событий и оркестрации реакций.
- Платформа должна поддерживать создание сценариев реагирования (playbooks) через визуальный конструктор без необходимости написания кода.
- Платформа должна обеспечивать автоматическую генерацию задач для ситуационного центра на основе выявленных инцидентов и их маршрутизацию по ролям.
- Платформа должна поддерживать интеграцию с мессенджерами и почтовыми системами для уведомления работников Поставщика и Заказчика в режиме реального времени.
- Платформа должна обеспечивать поддержку “human-in-the-loop” сценариев — когда аналитик утверждает или отменяет автоматические действия.
- Платформа должна предоставлять актуальную информацию о статусе зарегистрированных инцидентов информационной безопасности (ИБ) в режиме, близком к реальному времени.
- Платформа должна обеспечивать возможность самостоятельной регистрации инцидентов информационной безопасности Заказчиком посредством встроенных интерфейсов.
- Платформа должна предоставлять функционал визуализации статистических данных об обработанных и текущих инцидентах в виде интерактивных панелей мониторинга (Dashboard).
- Платформа должна обеспечивать получение пользователями доступных отчетов и уведомлений, формируемых Поставщиком в соответствии с утвержденным регламентом взаимодействия.
- Платформа должна обеспечивать автоматизацию процессов управления и реагирования на инциденты информационной безопасности, включая регистрацию, классификацию, эскалацию, расследование и закрытие инцидентов.
- Платформа должна обеспечивать возможность отслеживания задач, связанных с обработкой инцидентов, включая контроль текущего статуса, сроков исполнения и результатов выполнения.
- Платформа должна обеспечивать мониторинг индикаторов компрометации (IoC) и иных объектов, связанных с инцидентом, с возможностью их корреляции между различными кейсами и инцидентами.
- Платформа должна обеспечивать формирование отчетов по установленным показателям, включая технические, временные и организационные метрики реагирования.
- Платформа должна обеспечивать сбор технических индикаторов угроз, включая IP-адреса, домены, сигнатуры вредоносных файлов и сценарии атак.
- Платформа должна обеспечивать интеграцию данных от внутренних сенсоров (XDR, EDR, SIEM), песочниц, даркнет-источников, инфраструктуры и внешних фидов.
- Платформа должна обеспечивать очистку, атрибуцию и обогащение сырых данных для формирования структурированных Threat Intelligence Feeds (TI Feeds), которые автоматически обновляются и передаются в системы защиты.
- Платформа должна обеспечивать формирование аналитики, включая установление взаимосвязей между индикаторами, тактиками злоумышленников, группами и целями атак.
- Платформа должна обеспечивать автоматизацию обнаружения, реагирования и блокировки угроз посредством интеграции с системами SIEM, SOAR и другими средствами защиты.

- Платформа должна обеспечивать реализацию реальных сценариев реагирования, включая изоляцию конечной точки, уведомление аналитиков и создание задач для расследования и анализа инцидентов.
- Платформа должна иметь документацию, интерфейс и обучение на казахском, русском и английском языках.
- Платформа должна иметь локальную техническую поддержку от производителя.
- Платформа должна поддерживать государственный язык и являться отечественной разработкой.

Потенциальный поставщик должен предоставить авторизационное письмо от производителя или его представительства в Республике Казахстан, подтверждающее наличие доступа к Платформе в рамках предоставления тендерной документации. Письмо должно быть выдано в адрес Заказчика с указанием наименования закупки и наименования Заказчика. Наименования должны быть указаны полностью. Текст письма предоставляется на государственном или русском языках.

Для проверки качества и функциональности платформы поставщик в составе заявки должен предоставить официальное письмо с указанием ссылок для доступа на платформу.

Для проверки качества и функциональности платформы Потенциальный Поставщик в составе тендерной заявки должен предоставить ссылку на платформу.

В течении 3-х календарных дней с даты подписания договора потенциальный Поставщик должен подтвердить соответствие предлагаемых решений требованиям настоящей ТС, а также предоставить наличие разрешительных документов на поставку и сопровождение указанных системы (письмо от производителя или его локального представителя).

### **5.3. Требования к услуге предоставления системы обеспечения сетевой безопасности.**

#### **Характеристика системы:**

В рамках оказания услуги Поставщик предоставляет Заказчику право временного использования программного решения исключительно для целей оказания услуги информационной безопасности.

Система должна состоять в реестре доверенного программного обеспечения и продукции электронной промышленности в соответствии с пунктом 3-1 статьи 54 Закона Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации» и пунктом 29 Параграфа 2 Постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

ПО должно иметь сертификат соответствия согласно требованиям СТ РК ISO/IEC 15408-3-2017F и оценочный уровень доверия 4.

В составе конкурсной заявки поставщик должен предоставить разрешительное письмо от производителя, разрешающее предоставлять услугу предоставления права пользования программного обеспечения Заказчику с указанием наименования закупки и наименования Заказчика.

Для проверки качества, функциональности и подтверждения соответствия Системы требованиям настоящей спецификации Потенциальный поставщик в составе тендерной заявки должен предоставить ссылку и учетные данные к системе письмом на бланке.

Межсетевой экран предназначен для обеспечения задачи безопасного межсетевого взаимодействия, учета и контроля использования ресурсов глобальной сети Интернет.

Право использования (лицензия) программы должно включать в себя подписку с правами на:

- получение обновлений программы для возможность получать новые версии продукта, обновление сигнатур);
- получение технической поддержки программы;

- использование модуля предотвращения вторжений (возможность использовать модуль и получать его обновления);
- использование модуля по контролю приложений (возможность использовать модуль и получать его обновления);
- использование модуля по фильтрации контента (возможность использовать модуль и получать его обновления).

**Функциональные, технические, качественные и эксплуатационные характеристики межсетевого экрана:**

- Наличие модуля постоянного слежения за системой, предотвращающий возможность нарушения работы служб при выходе параметров их работы за определенные установленные рамки
- Возможность работы сервера в режиме кластера отказоустойчивости
- Проверка системой при загрузке всех параметров оборудования, состояния файловой системы и баз данных, а также контрольной суммы всех неизменяемых файлов
- Система автоматического обновления, позволяющая своевременно переходить на новые версии программного обеспечения
- Проверка всех загружаемых файлов электронной цифровой подписью
- Авторизация для доступа в Интернет для каждого пользователя по логину и паролю через WEB, через VPN PPTP, IKEv2/IPSec, L2TP/IPSec, SSTP, идентификация по IP адресу, MAC адресу и по IP + MAC
- Аутентификация VPN-пользователей через RADIUS-сервер
- Возможность авторизации пользователей терминального сервера при помощи прокси-сервера
- Обеспечение защиты от прослушивания трафика и подстановки IP-адреса при авторизации через VPN
- SSL VPN портал с возможностью публикации HTTPS, HTTP, SSH, RDP-ресурсов
- Возможность синхронизации пользователей Active Directory, Samba DC
- Прозрачная (Single Sign-On) авторизация по протоколу Kerberos
- Идентификация через журнал безопасности Active Directory
- Возможность интеграции с несколькими независимыми доменами Active Directory
- Хранение всей информации о пользователях в базе данных SQLite
- Хранение детализированной статистики каждого пользователя и каждой группы
- Netflow-сенсор для передачи информации Netflow коллектору
- Поддержка Netflow версий
- Возможность в любой момент времени посмотреть в форме отчета, какие ресурсы Интернет посещал пользователь или вся группа
- Ведение статистики посещения ресурсов Интернет в Мегабайтах
- Возможность просмотра в журнале событий работы модуля контентной фильтрации
- Возможность просмотра в едином журнале событий работы модулей предотвращения вторжений, контроль приложений и фаервол
- Система автоматического резервного копирования базы данных, конфигурационных файлов в локальное хранилище и их отправка на FTP-сервер или общую папку SMB
- Возможность восстановления политик конфигурации без перезагрузки сервера
- Встроенная возможность управления из локальной консоли с полным доступом к файловой системе и системным командам (в том числе удаленный доступ из доверенной сети по протоколу SSH)

- Возможность подключения и удаленного управления из Интернет по VPN (IKEv2/IPsec, L2TP/IPsec, SSTP, PPTP)
- Возможность исключения адресов из маршрутов передаваемых VPN-пользователям
- Возможность использования нескольких учетных записей администратора для администрирования через WEB интерфейс с возможностью назначения различных ролей администраторов
- Возможность импортировать группы администраторов из Microsoft AD, RADIUS – сервера.
- Возможность выдавать IP-адреса из разных подсетей разным группам VPN-пользователей
- Аудит действий администраторов
- Функции маршрутизатора с поддержкой неограниченного числа интерфейсов (как локальных, так и внешних)
- Возможность поддерживать виртуальные 802.1q VLAN интерфейсы, PPTP, PPPoE интерфейсы
- Поддержка Loopback интерфейсов
- Возможность создавать SPAN интерфейсы для зеркалирования трафика
- Поддержка WCCP протокола на L2 и L3 уровнях
- Возможность указания маршрутов по источнику (в том числе использовать пользователей или сети в качестве источника)
- Динамическая маршрутизация по протоколам OSPF, BGP
- Обеспечение поддержки нескольких каналов провайдеров и нескольких внешних сетей с возможностью полного разделения пользователей для выхода в Интернет через разных провайдеров или балансировки трафика между каналами
- Возможность агрегирования каналов для повышения пропускной способности и увеличения надежности
- Автоматическая проверка связи с провайдером и переключение на альтернативного провайдера при необходимости
- Возможность создания подключения к провайдеру по протоколам PPTP VPN, PPPoE и L2TP
- Возможность включения функции контент-фильтра, позволяющего управлять доступом к сайтам определенных категорий
- Количество категорий в контент-фильтре
- Количество URL адресов в контент-фильтре
- Возможность фильтрации скачиваемых файлов по расширению
- Возможность фильтрации по HTTP-методам (get, post, put, delete, head, options, patch, trace)
- Возможность фильтрации трафика по MIME-типам
- Возможность перенаправлять запросы к выбранным категориям на указанный URL
- Возможность формирования веб-отчетности по трафику пользователей в соответствии с категориями сайтов
- Возможность Контент-фильтра фильтровать как HTTP, так и HTTPS-трафик, как с его расшифровкой, так и без расшифровки (с помощью анализа SNI и данных сертификата)
- Возможность морфологического анализа сайтов
- Возможность автоматического обновления Базы данных контент-фильтра
- Защита компьютеров от атак из Интернет с использованием технологии NAT и межсетевого экрана с контролем состояния соединений
- Возможность блокировки IP-адресов и протоколов по заданным условиям
- Возможность блокировки IP адресов по его местоположению (Geo IP)

- Защита от DoS-атак и блокирование чрезмерной активности
- Публикация ресурсов при помощи технологии DNAT (portmapper)
- Возможность прозрачной переадресации адресов и портов на другой адрес
- Возможность создания правил межсетевого экрана с использованием зон, включающих в себя один или несколько интерфейсов (Zone Based Firewall)
- Возможность указания порта источника в межсетевом экране
- Возможность проверки работы правил таблицы FORWARD и INPUT
- Возможность заблокировать весь трафик, попадающий под условия специальной таблицы, до просмотра таблиц файрвола (предварительная фильтрация)
- Возможность использования пула IP-адресов для SNAT
- Возможность аппаратной фильтрации трафика по MAC-адресам
- Возможность создания правил с определенным временем действия
- Возможность доступа сотрудников к внутренней локально-вычислительной сети посредством удаленного подключения по защищенному каналу через сеть Интернет
- Возможность объединения всех удаленных подразделений в общую сеть на единой платформе по шифрованному протоколу IKEv2/IPsec
- Возможность создания GRE туннеля для объединения удаленных подразделений в общую сеть. Возможность создать подключение как без шифрования, так и зашифрованного канала связи между устройствами с использованием IPsec.
- Возможность ограничения полосы пропускания до Интернет-ресурсов (шейпера трафика) для пользователей и групп
- Обеспечение возможности интеграции с SIEM-системами по протоколу SYSLOG, формата CEF и выбор протокола передачи TCP/UDP
- Обеспечение возможности интеграции с системами мониторинга по протоколу SNMP.
- Обеспечение возможности интеграции с DLP-системами по протоколу ICAP
- Встроенный Zabbix агент работающий в двух режимах, активном и пассивном
- VPN сервер с возможностью подключений пользователей по протоколам IKEv2/IPSec, PPTP, L2TP/IPSec, SSTP; возможность использования двухфакторной аутентификации пользователей подключающихся к VPN серверу
- Возможность интеграции с сервисом Мультифактор для двухфакторной аутентификации
- Возможность использования службы предотвращения вторжений, анализирующую и блокирующую опасный трафик и атаки на сервер, сохраняющую информацию о заблокированном трафике и предупреждения в логах на срок не менее трех месяцев; базы сигнатур службы обновляются автоматически, без участия администратора
- Возможность добавлять собственные сигнатуры для модуля предотвращения вторжений
- Возможность использования службы контроля приложений с возможностью ограничения трафика приложений
- Количество протоколов и приложений в службе контроля приложений
- Возможность определения протоколов АСУ ТП (EtherSIO, FINS, HART-IP, Modbus, OPC-UA, UMAS)
- Обратный прокси-сервер для публикации HTTP и HTTPS-сайтов
- Балансировка трафика на несколько серверов обратным прокси-сервером
- Возможность использования встроенного межсетевого экрана уровня веб-приложений с возможностью блокировки SQL Injection, XSS и других атак на опубликованные веб-сайты

- Возможность создания и применения различных профилей для служб: предотвращение вторжений, контроль приложений и межсетевого экрана уровня веб-приложений
- Возможность включения защиты от DoS атак для ресурсов, публикуемых обратным прокси сервером
- Поддержка IGMP Proxy
- Полнофункциональный DNS-сервер с возможностями поддержки forward DNS-зон и кэширования DNS-запросов из локальной сети; перехвата запросов на внешние DNS-сервера и принудительного разрешения доменных имен через встроенный сервер
- Реализация поддержки динамических доменных имен (DDNS)
- DHCP-сервер для автоматического распределения IP адресов в локальной сети
- Возможность выдавать произвольный шлюз по DHCP и любые опции
- Возможность фиксированной привязки IP к MAC адресу компьютера
- Возможность выдачи DNS, DNS суффикса и WINS для DHCP клиентов
- Возможность выдачи маршрутов для DHCP клиентов; мониторингом аренды выданных адресов
- Возможность мониторинга аренды выданных адресов
- Возможность указания разных диапазонов на разных интерфейсах и VLAN
- Возможность работы в режиме DHCP-Relay
- Возможность создания виртуальных контекстов. VCE / VDOM / VSX
- Почтовый релей с возможностью фильтрации почтового трафика
- Возможность настройки почтового сервера с поддержкой протокола IMAP и POP3
- Возможность настройки веб-интерфейса для работы с личной почтой, позволяющий работать с почтой из любой точки мира по зашифрованному каналу через обычный браузер
- Возможность централизованного управления группой серверов с помощью центральной консоли управления
- Возможность использования экономичного режима работы процессора
- NTP-сервер точного времени, для синхронизации времени с серверов устройствами локальной сети
- Возможность включения перехвата NTP-запросов к внешним серверам
- Выбор языка веб интерфейса (русский, английский, казахский)

Потенциальный поставщик должен предоставить авторизационное письмо от производителя или его представительства в Республике Казахстан, подтверждающее наличие доступа к Платформе в рамках предоставления тендерной документации. Письмо должно быть выдано в адрес Заказчика с указанием наименования закупки и наименования Заказчика. Наименования должны быть указаны полностью. Текст письма предоставляется на государственном или русском языках.

Для проверки качества и функциональности платформы поставщик в составе заявки должен предоставить официальное письмо с указанием ссылок для доступа на платформу.

В течении 3-х календарных дней с даты подписания договора потенциальный Поставщик должен подтвердить соответствие предлагаемых решений требованиям настоящей ТС, а также предоставить наличие разрешительных документов на поставку и сопровождение указанных системы (письмо от производителя или его локального представителя).

#### **5.4.Дополнительные услуги**

Услуги компьютерной криминалистики (форензики) критических инцидентов.

Оказание услуги по расследованию критических инцидентов, связанных с несанкционированным доступом, удалением, модификацией данных, выявлению фактов

проникновения и заражения специализированным вредоносным программным обеспечением. В рамках оказания услуг проводятся работы по анализу сетевой активности, логов, изменений настроек, восстановлению удаленной информации, поиску и локализации вектора атаки.

## **6. Прочие положения**

### **6.1. Условия надлежащего оказания Услуги:**

Поставщик не несет ответственности за Инциденты и другие обстоятельства, повлекшие за собой перерывы в предоставлении Услуги, вызванные любой из перечисленных ниже причин:

- проведение плановых и аварийных ремонтных работ на оборудовании, участвующем в оказании Услуги, с уведомлением Заказчика;
- отказ или неспособность Заказчика обеспечить содействие Поставщику в установлении и устранении инцидентов в срок, определенный уровнем предоставления Услуги;
- отказ или неспособность Заказчика предоставить необходимые данные для настройки программного обеспечения или оборудования в рамках предоставления Услуги в соответствии с требованиями настоящего Регламента в срок до 5 рабочих дней;
- в случае обстоятельств непреодолимой силы, как они определены по Договору.

Поставщик вправе запрашивать у Заказчика информацию (об ИТ-инфраструктуре, информационных активах) необходимую для реализации сценария выявления атаки, а также оперировать данной информацией для минимизации ложных срабатываний. Поставщик формирует запрос по электронной почте уполномоченному лицу со стороны Заказчика, в запросе должна быть указана аргументированная причина данного обращения. Заказчик в течение 5 рабочих дней предоставляет обратную связь по данному запросу, при необходимости данные сроки могут быть скорректированы. Запрос информации может быть следующего вида:

- список DNS-серверов;
- IP-адреса сканнеров безопасности;
- список ресурсов доступных из сети интернет;
- список белых IP-адресов, принадлежавших Заказчику;
- владельцев информационных систем и ресурсов;
- информация о принадлежности IP-адреса пользователю или системе.

В течение 15 (пятнадцати) рабочих дней после заключения Договора Поставщик предоставляет, а Заказчик согласовывает регламент взаимодействия.

Ежемесячные отчеты предоставляются Поставщиком не позднее 5 (пятого) числа месяца, следующего за отчетным. В случае если указанная дата приходится на выходной или праздничный день, отчет предоставляется не позднее рабочего дня, предшествующего этой дате. Подписанные сторонами отчеты являются основанием для оформления и подписания акта оказанных услуг.

Активирование оказанных услуг производится ежемесячно.

### **6.2. Плановое техническое обслуживание:**

Поставщик может проводить плановое техническое обслуживание, обновление или усовершенствование подсистем, на базе которых оказывается Услуга. Эти работы определяются как плановые ремонтные работы и могут вызвать перерывы в оказании Услуги. Плановые ремонтные работы проводятся по согласованному с Заказчиком периоду времени прерывания предоставления Услуги.

Поставщик обязуется уведомить Заказчика о проведении любых плановых ремонтных работ, которые могут вызвать перерывы в работе Услуги, минимум за 1 (один) день до начала работ. Исключением являются случаи, когда работы выполняются по запросу Заказчика, а также в случаях, когда Поставщик не может соблюсти указанный срок в связи

с тем, что плановые ремонтные работы на сети Поставщика проводятся по требованию государственных органов или компетентных органов отрасли телекоммуникаций Казахстана.

Заказчик при необходимости направляет предложения по корректировке сроков проведения работ, которые учитываются по технической возможности Поставщика. В уведомлении, направленном Поставщику, указываются:

- время проведения плановых ремонтных работ;
- дата проведения плановых ремонтных работ;
- продолжительность проведения плановых ремонтных работ;
- контактные данные лица, ответственного за предоставление информации о проводимых работах;
- информация о необходимости участия сотрудников Заказчика в плановых ремонтных работах, например, для проведения проверок работоспособности информационной системы Заказчика.

Заказчик обязуется выделить ответственных сотрудников для участия в работах. В случае невозможности привлечения сотрудника к работам на указанную дату, Заказчик направляет предложения по корректировке сроков проведения работ.

При отмене плановых работ Поставщик оповещает Заказчика в кратчайшие сроки после принятия решения.

Заказчик также должен уведомить Поставщика о проведении любых плановых работ на своем оборудовании, которые могут привести к временной недоступности защищаемых ресурсов Заказчика и, как следствие, к перерыву в оказании Услуги, минимум за 1 (одни) сутки до начала работ.

В уведомлении должно быть указано: время, дата, продолжительность проведения плановых работ, контактные данные лица, ответственного за предоставление информации о проводимых работах.

При изменении сроков проведения плановых работ Заказчик оповещает Поставщика в кратчайшие сроки после принятия решения, но не менее, чем за 1 (одни сутки) до начала проведения работ.

Все уведомления Заказчика или Поставщика должны направляться на электронный адрес уполномоченных представителей.

### **6.3. Аварийные ремонтные работы:**

Аварийные и восстановительные работы проводятся при возникновении отказов, периодических прерываний в оказании Услуги либо существенного ухудшения параметров её качества, которые могут привести к полной или частичной недоступности Услуги.

В рамках стоимости Услуги Поставщик своими силами и за свой счёт выполняет диагностику неисправностей и оперативные восстановительные работы, не требующие приобретения или замены основного оборудования, его функциональных модулей, запасных частей и дополнительных лицензий, в том числе:

- восстановление, переустановку, обновление и настройку программного обеспечения, агентов, коллекторов и иных компонентов Услуги;
- восстановление конфигураций и настроек;
- перезапуск и переконфигурирование компонентов Услуги;
- восстановление сетевого взаимодействия и передачи событий;
- устранение неисправностей соединений, замену соединительных кабелей и разъёмов, если их стоимость включена в цену Услуги;
- иные восстановительные действия, не требующие модернизации или замены оборудования Заказчика.

Ремонт и замена оборудования, программного обеспечения и компонентов, принадлежащих Поставщику либо предоставленных Поставщиком для оказания Услуги, независимо от объема необходимых работ осуществляются Поставщиком своими силами и за свой счёт и входят в стоимость Услуги.

При выявлении неисправности оборудования Заказчика, устранение которой требует замены основного оборудования или его функциональных модулей, приобретения запасных частей, дополнительных лицензий, проведения модернизации либо привлечения специализированной сервисной организации, Поставщик не позднее одного рабочего дня с момента выявления неисправности направляет Заказчику техническое заключение или акт дефектации. Документ должен содержать описание неисправности, предполагаемую причину, перечень необходимых работ и материалов, возможный срок простоя, а также рекомендуемые временные меры по обеспечению работоспособности Услуги.

Решение о ремонте или замене принадлежащего Заказчику оборудования принимается Заказчиком. Работы и приобретения, не предусмотренные настоящей технической спецификацией и стоимостью Договора, осуществляются Заказчиком посредством отдельной закупки либо на ином законном основании в соответствии с законодательством Республики Казахстан о государственных закупках. Дополнительная оплата таких работ в рамках действующего Договора без предусмотренного законодательством основания не допускается.

До устранения неисправности Поставщик при наличии технической возможности обязан предложить и реализовать временное решение, позволяющее минимизировать перерыв в оказании Услуги.

Поставщик уведомляет Заказчика о необходимости проведения аварийных работ незамедлительно после выявления соответствующих обстоятельств. Если отсрочка проведения работ может привести к увеличению продолжительности перерыва, утрате данных или ухудшению состояния компонентов Услуги, Поставщик вправе приступить к работам одновременно с направлением уведомления Заказчику.

Заказчик уведомляет Поставщика о проведении аварийных работ на принадлежащем ему оборудовании, способных повлиять на оказание Услуги, незамедлительно после принятия решения об их проведении.

В уведомлении указываются:

- дата и время начала работ;
- предполагаемая продолжительность работ;
- описание причины и характера работ;
- перечень затрагиваемого оборудования и компонентов Услуги;
- контактные данные ответственного лица;
- информация о необходимости участия представителей Заказчика и Поставщика.

Устранение неисправностей компонентов Услуги, не требующее приобретения или замены основного оборудования, его функциональных модулей, запасных частей и дополнительных лицензий, выполняется Поставщиком своими силами и за свой счёт в рамках стоимости Услуги.

В случае выявления неисправности оборудования Заказчика, устранение которой требует замены оборудования или его функциональных модулей, приобретения запасных частей, дополнительных лицензий либо проведения модернизации, Поставщик не позднее одного рабочего дня предоставляет Заказчику акт дефектации или техническое заключение с описанием неисправности, перечнем необходимых работ и материалов, а также рекомендуемыми временными мерами.

Решение о ремонте или замене оборудования Заказчика принимается Заказчиком. Работы и приобретения, не предусмотренные технической спецификацией и стоимостью Договора, осуществляются посредством отдельной закупки либо на ином законном

основании в соответствии с законодательством Республики Казахстан о государственных закупках.

Ремонт и замена оборудования, программного обеспечения и иных компонентов, принадлежащих Поставщику либо предоставленных им для оказания Услуги, независимо от объёма работ выполняются Поставщиком за свой счёт и входят в стоимость Услуги.

#### 6.4. Зоны ответственности на период оказания ОЦИБ:

Таблица №7 Зоны ответственности участников комплекса услуг.

| №                                              | Параметр                                                                                                                                                                                                                                                                                      | Заказчик | Поставщик |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-----------|
| Оказание услуги Мониторинг и анализ событий ИБ |                                                                                                                                                                                                                                                                                               |          |           |
| 1.1                                            | Мониторинг и анализ событий ИБ (включая предоставление рекомендаций по реагированию на инциденты), зарегистрированных и касающихся элементов инфраструктуры Клиентов, входящих в Зону мониторинга.                                                                                            |          | +         |
| 1.2                                            | Обеспечение, восстановление и мониторинг работоспособности оборудования Заказчика.                                                                                                                                                                                                            | +        |           |
| 1.3                                            | Мониторинг и анализ событий ИБ, зарегистрированных или касающихся элементов инфраструктуры Клиентов, не входящих в Зону мониторинга.                                                                                                                                                          | +        |           |
| 1.4                                            | Мониторинг состояния компонентов подсистемы управления событиями ИБ, установленных как на площадке Заказчика, так и на площадке Поставщика                                                                                                                                                    |          | +         |
| 1.5                                            | Обеспечение корректного функционирования подсистемы управления событиями ИБ                                                                                                                                                                                                                   |          | +         |
| 1.6                                            | Установка агентов на источниках для отправки логов                                                                                                                                                                                                                                            | +        |           |
| 1.7                                            | Предоставление необходимых технологических мощностей для развёртывания коллекторов событий/потоков и иных инфраструктурных элементов подсистемы управления событиями ИБ в соответствии с рекомендациями Поставщика. Поддержка отказоустойчивости и доступности соответствующей инфраструктуры | +        |           |
| 1.8                                            | Направление сетевых потоков с источников в коллекторы                                                                                                                                                                                                                                         | +        |           |
| 1.9                                            | Реагирование на инциденты ИБ, их локализация, устранение последствий и восстановление штатного режима работы, согласно рекомендациям, предоставленным Поставщиком                                                                                                                             | +        | +         |
| 1.10                                           | Выполнение рекомендаций ОЦИБ и своевременное реагирование на инциденты ИБ                                                                                                                                                                                                                     | +        |           |
| 1.11                                           | Предоставление актуального перечня серверного, коммуникационного и компьютерного оборудования, а также информационных систем, входящих в Зону мониторинга                                                                                                                                     | +        |           |
| 1.12                                           | Обеспечение работоспособности защищённых каналов передачи информации между площадками Заказчика и Поставщика.                                                                                                                                                                                 |          | +         |
| 1.13                                           | Применение рекомендаций Поставщика с целью исключения вероятности возникновения повторного инцидента                                                                                                                                                                                          | +        |           |
| 1.14                                           | Оперативное предоставление информации обо всех изменениях в Зоне мониторинга, включая, но не ограничиваясь, информацией о новых сетевых устройствах, IP адресации, внешних авторизованных подключениях и др.                                                                                  | +        |           |
| 1.15                                           | Хранение получаемых данных (события, сетевые потоки) от Заказчика в период действия Договора                                                                                                                                                                                                  | +        |           |

| №    | Параметр                                                                                                                                             | Заказчик | Поставщик |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-----------|
| 1.16 | Выдача рекомендации по началу проведения полноценного расследования с использованием Услуги «Расширенная экспертиза по расследованию инцидентов ИБ». |          | +         |

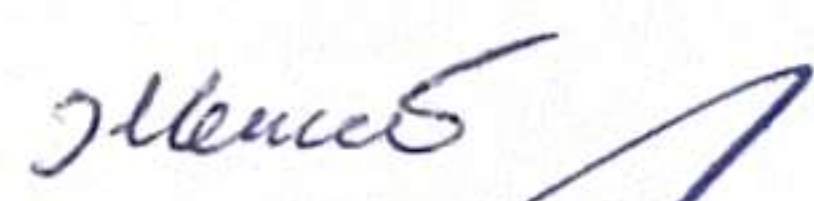
## 7. Требования, регулируемые законами и стандартами

Услуги должны оказываться в соответствии с Законом Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 11.02.2024 г.) и Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (с изменениями и дополнениями по состоянию на 25.02.2023 г.), а также согласно рекомендациям стандарта по информационной безопасности ISO/IEC 27001 «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью».

Хранение данных Заказчика осуществляется в базах, которые располагаются на территории РК (требования статьи 12 Закона Республики Казахстан от 21 мая 2013 года N 94-V «О персональных данных и их защите», Постановление Правительства Республики Казахстан № 832 от 20 декабря 2016 года «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»).

В соответствии с пунктом 2 статьи 7-2 Закона об информатизации Республики Казахстан от 24 ноября 2015 года потенциальный поставщик должен предоставить и осуществлять деятельность на основании лицензии «Оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий», выдаваемой Комитетом национальной безопасности Республики Казахстан.

Руководитель управления внутреннего контроля



Жексембаев Е.К.

Руководитель департамента цифровизации



Альчимбаев А.Б.

Руководитель департамента закупок и мониторинга



Бейсенова С.А.

И.о. руководителя  
управления претензионно-исковой работы



Мадихан М.М.

Руководитель  
управления мониторинга



Кенесбеков Н.Н.