**Техническая спецификация**

**на Услуги по внедрению стратегий по информационной безопасности**

**(Оперативный центр информационной безопасности)**

**Глоссарий:**

|  |  |  |
| --- | --- | --- |
| **Термин** |  | **Определение** |
| **ИБ** |  | Информационная безопасность |
| **Инфраструктура Заказчика** |  | означает совокупность СЗИ, а также аппаратных и программных средств Заказчика, которые находятся в границах корпоративной сети Заказчика |
| **ОЦИБ – оперативный центр информационной безопасности** |  | Юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации |
| **Центр мониторинга и реагирования на киберугрозы**  **(далее – SOC)** |  | это подразделение Поставщика услуг, отвечающее за получение и обработку событий ИБ, которое обеспечивает круглосуточный мониторинг инцидентов ИБ силами аналитиков 1-ой линии, анализ инцидентов ИБ силами аналитиков 2-ой линии, расследование инцидентов ИБ, в том числе проведение ретроспективной аналитики и актуализация информации об угрозах и атаках, способах их детектирования и противодействия силами 3-ей экспертной линии. В состав Центра также входят средства защиты информации, с помощью которых происходит сбор событий ИБ, их последующая корреляция и детектирование инцидентов ИБ. |
| **Инцидент ИБ** |  | событие ИБ, создавшее предпосылки к нарушению или реализовавшее нарушение свойств / характеристик информационных ресурсов, одно или серия нежелательных, или неожиданных событий ИБ, которые со значительной степенью вероятности указывают на свершившуюся ранее или предпринимаемую в настоящее время реализацию угрозы ИБ. |
| **Событие ИБ** |  | любое событие, связанное с информационными ресурсами, которое является непредвиденным, не предопределённым (не документированным политиками, регламентами, инструкциями, техническими настройками) или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности |
| **Угроза ИБ** |  | совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. |
| **Площадка** |  | Инфраструктура Заказчика на которой размещаются компоненты Подсистемы по управлению событиями ИБ |
| **SLA (Service Level Agreement**  **(Соглашение об уровне обслуживания))** |  | документированные параметры предоставляемой услуги. Параметры услуги — описание количественных и / или качественных действий (гарантированного состояния услуг(и)) с учетом фактора времени. |
|  |  |  |
| **Комплекс услуг** |  | Комплекс услуг, состоящий из: услуги «Мониторинг и анализ событий ИБ»;  услуги «Управление ИБ»; |
| **Web-интерфейс SOC** |  | программное обеспечение (далее — ПО), предназначенное для автоматизированного сбора информации о выявляемых в рамках оказания Услуги инцидентах и предоставления доступа к ней уполномоченным специалистам Заказчика через личный кабинет в WEB-Интерфейсе ПО. |
| **Корреляция** |  | определение взаимосвязи между данными, содержащимися в двух и более событиях ИБ. |
| **Агрегирование** |  | объединение событий ИБ, содержащих одинаковую информацию. |
| **Сценарий выявления атаки (далее — use – case; сценарий)** |  | это возможный сценарий реализации угрозы ИБ в отношении важных для Заказчика областей̆, таких как критичные системы, сегменты сети, группы сотрудников с учетом негативного влияния на целостность, конфиденциальность и доступность информации. Сценарий представляет собой описание ситуации, которую требуется наблюдать, отслеживать и предпринимать определенные действия в случае обнаружения. |
| **Типовой источник** |  | источник событий ИБ Заказчика, при подключении которых Поставщик может руководствоваться собственной базой знаний. |
| **Нетиповой источник** |  | источник событий ИБ, который относится к системам собственной разработки Заказчика и/или требуется дополнительный анализ журналов событий и разработка парсера (обработчика) со стороны Поставщика |
| **Запрос на изменение** |  | Обращение, связанное с запросами на изменение конфигурации и (или) настроек ПО |
| **Дашборд**  **(англ. – dashboard)** |  | Утилиты, позволяющие визуализировать различные тренды и показатели в виде консоли или панели управления с различными диаграммами, графиками, обновляемыми таблицами или виджетами |
| **Личный кабинет Заказчика** |  | Система, предназначенная для предоставления актуально й информации по статусу инцидентов ИБ, предоставления отчётности и иной информации Заказчику |
| **Национальный координационный центр информационной безопасности (НКЦИБ)** |  | Структурное подразделение республиканского государственного предприятия на праве хозяйственного ведения "Государственная техническая служба" Комитета национальной безопасности Республики Казахстан |
| **Security information and event management (SIEM) СИЕМ** |  | Объединение двух [терминов](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD), обозначающих область применения программного обеспечения: SIM ([Security information management](https://ru.wikipedia.org/wiki/Security_information_management" \o "Security information management)) — управление информацией о безопасности, и SEM ([Security event management](https://ru.wikipedia.org/w/index.php?title=Security_event_management&action=edit&redlink=1" \o "Security event management (страница отсутствует))) — управление событиями безопасности.  Технология SIEM обеспечивает анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений, и позволяет реагировать на них до наступления существенного ущерба |
| **ЕШДИ** |  | Единый шлюз доступа к Интернету – аппаратно-программный комплекс, предназначенный для защиты сетей телекоммуникаций при доступе к Интернету и (или) сетям связи, имеющим выход в Интернет. |

1. Цель:

Повышение уровня защищённости ИТ-инфраструктуры в ТОО «Управляющая компания «Қазмедиа Орталығы» и создания условий для своевременного реагирования на инциденты информационной безопасности (далее – ИБ).

1. **Задачи оказания Услуги:**

Настоящая техническая спецификация, содержит общие и частные требования к реализации оказания комплекса услуг, состоящий из: услуги «Мониторинг и анализ событий ИБ»;

услуги «Управление ИБ» в ИТ-инфраструктуре и помощь в реагировании на инциденты ИБ (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 компонентов Подсистемы (далее – Зона мониторинга);
* круглосуточный мониторинг событий ИБ, зафиксированных системами мониторинга и управления событиями информационной безопасности в Зоне мониторинга и системами защиты внешнего периметра;
* круглосуточный мониторинг событий ИБ, зафиксированных на серверном оборудовании и сетевых устройствах Заказчика;
* направление Клиенту 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 ОЦИБ:

В границы оказания Услуги в целом входит следующая площадка Заказчика, на которых размещены ИС:

|  |  |  |
| --- | --- | --- |
| **Тип**  **ЦОД/Филиал/Представительство** | **Объекты** | **Местонахождение** |
| Здание ТОО «Управляющая компания  «Қазмедиа орталығы» | ИТ-Инфраструктура Товарищества | г. Астана  ул. Кунаева 4 |

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 заключение договора с обязательным подписанием **«Соглашения о неразглашений конфиденциальной информации»**.

Потенциальный поставщик должен находиться и должен быть представлен в городе местонахождения Заказчика, в г. Астана, для осуществления более быстрого и эффективного взаимодействия по устранению инцидентов ИБ критического уровня.

Требования к составу работ по подключению, можно разделить на 4 этапа, в рамках каждого этапа определена цель и поставлены задачи для ее достижения.

**Этап 1. Обследование:**

Цель этапа – определить целевую архитектуру 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 приоритизации подключаемых источников событий ИБ (далее – источников);
* определение потребностей Заказчика в части подключения уже существующих и разработки новых сценариев выявления атак. Для этого Заказчику направляется аналитический опросный лист для заполнения. Также при реализации сценариев будут учитываться результаты комплексного анализа защищенности;
* выработка организационно-технических решений по целевой архитектуре 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;
* выбор одного из способов интеграции с системой управления инцидентами Заказчика:
* 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;
    - Fully Qualified Domain Name;
    - IP-адрес.

**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 Товарищества.

* 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 инсталляционные работы по внедрению компонентов Услуги в ИТ-инфраструктуре 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, этапа №1 перечню источников, Поставщик предоставляет инструкции по их подключению;
* Поставщик 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 Дашборде 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 ИТ-инфраструктуру Заказчика, настроить отправку уведомлений об инцидентах ИБ в соответствии с SLA:

Задачи, которые должны быть решены для достижения цели:

В рамках оказания Услуги на базе Центра мониторинга и реагирования на киберугрозы Поставщик должен выполнять:

* анализ событий ИБ в режиме 24х7 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 ведется аналитиками 2 и 3 линии. Аналитики проводят углубленный 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 сводной информации о текущем количестве потребляемых EPS и детальная информация по распределению EPS по источникам событий;
* просмотр информации по каждому инциденту ИБ, который снабжен описанием выявленных техник атак;
* предоставление в унифицированном шаблоне карточки инцидента по каждому выявленному инциденту ИБ;
* предоставление доступа через Дашборд для просмотра информации по подключенным источникам событий, значению EPS на каждом источнике, а также дате подключения источника, что позволяет учитывать ИТ-активы, подключенные в SIEM-систему;
* просмотр сводной информации о подозрительных действиях ТОП-5 выделенных групп пользователей;
* выгрузка унифицированных отчетов из Личного кабинета.

**4. Требования к оказанию услуг Поставщика и Заказчика:**

Настоящие требования устанавливают порядок обеспечения комплекса услуг междуПоставщиком и Заказчиком и описывает 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 высокий, критичный.

В случае обнаружения Заказчиком инцидента, Заказчик информирует Поставщика по контактным данным технической службы Поставщика согласно таблице №4.

Поставщик регистрирует инцидент и сообщает Заказчику:

**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 ежеквартально руководителями организации с обеих сторон.
* Согласно отчётам оплата за услуги будут производиться ежеквартально.

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

* **Unauthorized Access/Compromised**. Инциденты, связанные с неавторизованным получением физического/логического доступ 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 proxy, 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.

**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 Услуг, 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.

**Целевые показатели уровня предоставления услуги:**

Инциденты ИБ должны подразделяться на приоритеты по степени срочности их решения, указанными в таблице №1.

Таблица №1 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 №2.

Таблица №2 Показатели уровня оказания услуги

| № | Показатель | Приоритет | Время выполнения показателя | Табель | Время реакции Заказчика на запросы Поставщика |
| --- | --- | --- | --- | --- | --- |
|  | 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 |
|  | 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 |
|  | 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 | 8х5 | Не применимо |
| 4 — Низкий | Не применимо | 8х5 | Не применимо |

**Поставщик услуг должен обрабатывать запросы Заказчика согласно показателям, указанным в таблице №3.**

Таблица №3 Целевые показатели проведения изменений в месяц

| **№** | **Показатель** | | **Кол-во обращений** |
| --- | --- | --- | --- |
|  | Запрос на изменение | Заявки, связанные с изменением конфигурации Услуги (добавление/удаление источника событий ИБ, адаптация сценария) | не более 8 |
|  | Информационный запрос | Заявки, связанные с консультационными вопросами, по Услуге (вопросы по Договору и т.п.) | не более 5 |
|  | 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 №2. | Не ограничено |

Таблица 4. Целевые показатели уровня предоставления Услуги для стандартных источников

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Показатель** | **Приоритет** | **Время реакции Поставщика** | **Время реакции Заказчика на запросы Поставщика** |
| 1 | Решение Запросов на изменение | 1 – Критический | Не более 8 часов | Не более 1 час. |
| 2 – Высокий | Не более 16 раб. часов | Не более 8 раб. часов |
| 3 – Средний | Не более 32 раб. часов |
| 4– Низкий | Согласовывается дополнительно | Согласовывается дополнительно |
| 2 | Решение Информационных запросов | 2 – Высокий | Не более 8 раб. часов | Не более 1 раб. дня |
| 4– Низкий | Не более 16 раб. часов |

**5. Состав технических средств SOC:**

Поставщик Услуг должен быть обеспечен технической поддержкой от производителей решений

на срок действия Договора, что должно быть подтверждено официальным письмом от производителя со ссылками на веб-ресурсы или технической документацией и предоставлены Заказчику. Обязательные технические и программные средства Услуги должны включать элементы, указанные в таблице №5.

Таблица №5. Состав технических средств

|  |  |  |
| --- | --- | --- |
| **№** | **Название компонента** | **Описание** |
| 1 | Личный кабинет Заказчика | Система Поставщика, Заказчику в рамках оказания Услуги предоставляется доступ к интерфейсу системы.  Функционал личного кабинета:   * предоставление актуальной информации по статусу инцидентов ИБ, * самостоятельная регистрация инцидентов Заказчиком. * предоставлять возможность просмотра статистики о произошедших инцидентах (DashBoard); * предоставлять отчётность по каждому выявленному инциденту ИБ; * получать доступные отчёты и уведомления от Поставщика; |
| 2 | Платформа по управлению событиями информационной безопасности | Подсистема сбора, обработки и корреляции событий информационной безопасности, развёрнутая у Заказчика. |
| 3 | Коллекторы событий Платформы по управлению событиями информационной безопасности | Размещаются на стороне Заказчика. |
| 4 | VPN-шлюз | Используется оборудование Заказчика |

**6. 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, указанных в настоящем Регламенте.

1. **Аварийные ремонтные работы:**

Аварийные ремонтные работы подсистем, на базе которых оказывается Услуга, проводятся, когда отмечаются периодически возникающие прерывания в оказании Услуги или существенные ухудшения параметров качества, которые могут в дальнейшем привести к состоянию аварии.

Поставщик должен уведомить Заказчика о проведении аварийных ремонтных работ не менее чем за 4 (четыре) часа до начала работ.

Заказчик должен уведомить Поставщика о проведении любых аварийных ремонтных работ на своем оборудовании, которые могут привести к временной недоступности защищаемых ресурсов Заказчика и, как следствие, к перерыву в оказании Услуги, минимум за 2 (два) часа до начала работ.

В уведомлении должны быть указаны:

* время, дата и продолжительность аварийных ремонтных работ;
* контактные данные лица ответственного за предоставление информации о проводимых работах;
* информация о необходимости участия сотрудников Заказчика в аварийных ремонтных работах (только при проведении работ Поставщика).

1. **Зоны ответственности на период оказания ОЦИБ:**

Таблица №6 Зоны ответственности всех 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 | Мониторинг и анализ событий ИБ, зарегистрированных или касающихся элементов инфраструктуры Клиентов, не входящих в Зону мониторинга. | + |  |
| 1.3 | Мониторинг состояния компонентов подсистемы управления событиями ИБ, установленных как на площадке Заказчика, так и на площадке Поставщика |  | + |
| 1.4 | Обеспечение корректного функционирования подсистемы управления событиями ИБ |  | + |
| 1.5 | Установка агентов на источниках для отправки логов | + |  |
| 1.6. | 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 | + |  |
| 1.7 | Направление сетевых потоков с источников в коллекторы | + |  |
| 1.8 | Реагирование на инциденты ИБ, их локализация, устранение последствий и восстановление штатного режима работы, согласно рекомендациям, предоставленным Поставщиком | + | + |
| 1.9 | Выполнение рекомендаций ОЦИБ и своевременное реагирование на инциденты ИБ | + |  |
| 1.10 | Предоставление актуального перечня серверного, коммуникационного и компьютерного оборудования, а также информационных систем, входящих в Зону мониторинга | + |  |
| 1.11 | Обеспечение работоспособности защищённых каналов передачи информации между площадками Заказчика и Поставщика. |  | + |
| 1.12 | Применение рекомендаций Поставщика с целью исключения вероятности возникновения повторного инцидента | + |  |
| 1.13 | 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. | + |  |
| 1.14 | Хранение получаемых данных (события, сетевые потоки) от Заказчика в период действия Договора | + |  |
| 1.15 | Выдача рекомендации по началу проведения полноценного расследования с использованием Услуги «Расширенная экспертиза по расследованию ИБ |  | + |

**Разграничение зон ответственности на период оказания Комплекса услуг приведены в таблице №7.**

Таблица №7. Разграничение зон ответственности

| **Параметр** | | **Компоненты Услуги, размещённые в ИТ-Инфраструктуре Заказчика** |
| --- | --- | --- |
| Уровень приложения | Мониторинг работоспособности | Поставщик |
| Обеспечение работоспособности | Поставщик |
| Восстановление работоспособности | Поставщик |
| Уровень ОС | Мониторинг работоспособности | Поставщик |
| Обеспечение работоспособности | Поставщик |
| Восстановление работоспособности | Поставщик |
| Уровень оборудования | Мониторинг работоспособности | Заказчик |
| Обеспечение работоспособности | Заказчик |
| Восстановление работоспособности | Заказчик |

1. **Требования по стандартизации и унификации:**

Услуги должны оказываться в соответствии с Законом Республики Казахстан от 24 ноября 2015 года «Об информатизации» и Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, а также международным стандартом по информационной безопасности ISO/IEC 27001 «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью». Также услуги должны оказываться в соответствии с требованиями к использованию ЕШДИ и в соответствии с внутренними нормативными документами Заказчика (Политики и Правила по информационной безопасности Заказчика).

Хранение данных Заказчика осуществляется в базах, которые располагаются на территории РК (требования ст.12 Закона РК «О персональных данных и их защите», Постановление Правительства РК № 832 от 20.12.2016 года «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»).