УТВЕРЖДАЮ
Вице-министр
культуры и информации
Республики Казахстан
_____Е. Токтагулов
«__» _____2026 г.

Приложение 16 к конкурсной документации

Техническая спецификация
услуги оперативного центра информационной безопасности для информационной системы «Единый электронный архив документов»

Наименование заказчика	Государственное учреждение «Министерство культуры и информации Республики Казахстан»
Наименование организатора	Государственное учреждение «Министерство культуры и информации Республики Казахстан»
№ конкурса	-
Наименование конкурса	Услуги оперативного центра информационной безопасности для информационной системы «Единый электронный архив документов»
№ лота	-
Наименование лота	Услуги по обеспечению информационной безопасности.
Наименование кода Единого номенклатурного справочника товаров, работ, услуг	801019.000.000010

Наименование услуги:	Услуги оперативного центра информационной безопасности для информационной системы «Единый электронный архив документов»
Единица измерения	Услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость	-
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость	-
Срок оказания услуги:	Со дня вступления договора в силу по 31 декабря 2027 года, но не менее 15 календарных дней.
Размер авансового платежа	-
Гарантийный срок (в месяцах)	12 месяцев

Описание требуемых характеристик, параметров и иных исходных данных	**1. Общие требования** **1.1.** Наименование закупаемых услуг: Услуги оперативного центра информационной безопасности для информационной системы «Единый электронный архив документов» (далее – ОЦИБ). **1.2.** Предметом закупки являются Услуги оперативного центра информационной безопасности (ОЦИБ), направленные на обеспечение мониторинга, анализа и реагирования на инциденты информационной безопасности. Поставка оборудования, программного обеспечения и лицензий осуществляется исключительно в объёме, необходимом для оказания указанных услуг, и носит вспомогательный характер по отношению к основному предмету закупки — оказанию услуг ОЦИБ.

	1.3. Место оказания услуги: Государственное учреждение "Министерство культуры и информации Республики Казахстан», город Астана, район «Есиль», проспект Мәңгілік Ел 8, подъезд 14 **1.4.** Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых услуг: **1.4.** Основные термины и определения: –**ИБ** – информационная безопасность. –**SIEM** (Security Information and Event Management) – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности. –**ИТ** – информационные технологии. –**ITIL** – методология управления, отладки и непрерывного улучшения бизнес-процессов, связанных с ИТ. –**SLA** – соглашение об уровне обслуживания. –**FQDN** – полное доменное имя. –**Связность** – возможность взаимодействия между компьютерами. –**ИС** – информационная система. –**VPN** – виртуальная частная сеть. –**НКЦИБ** – Национальный координационный центр информационной безопасности АО «Государственная техническая служба». –**Инцидент** – любое событие, которое не является частью стандартных услуг и может вызвать прерывание или снижение качества услуг. ▪ **ТС** – техническая спецификация. Оказание Услуг направлено на повышение уровня защищенности ИТ-инфраструктуры Заказчика от современных угроз ИБ, а также проведение превентивных мер по минимизации рисков возникновения инцидентов ИБ. В рамках оказания Услуг должны быть решены следующие задачи: • Организация и осуществление мониторинга событий и обработки инцидентов ИБ, включая развертывание в инфраструктуре Заказчика компонентов Услуг. Настоящая техническая спецификация (далее – ТС) содержит общие и частные требования к оказанию Услуг, обеспечивающих решение вышеуказанных задач. Услуги по выявлению технических каналов утечки информации и специальных технических средств оперативным центром информационной безопасности, включающие:

- предоставление коллекторов событий и сетевых потоков (LOG/FLOW Collector) с суммарным количеством подключаемых источников событий не более 50 (пятидесяти);

Поставщик осуществляет поставку, установку, подключение и настройку технических средств ОЦИБ в течении 15 календарных дней, но не ранее истечения минимального срока, установленного пунктом 569 Правил осуществления государственных закупок, с учетом фактического объема поставки и внедрения.

Факт установки, подключения и настройки оформляется письменным актом, подписанным Заказчиком и Поставщиком.

1.5. Заказчик предоставляет необходимые ресурсы и обеспечивает подключение источников в срок, установленный пунктом 3.6 настоящей ТС.

2. Требования к услуге

2.1. В рамках оказания Услуг поддерживаются следующие функции и дополнительные сервисы:

1) Мониторинг событий ИБ, зафиксированных на серверном оборудовании и сетевых устройствах Заказчика, подключённых к SIEM-системе Поставщика;
2) Выявление инцидентов ИБ в зоне мониторинга;
3) Информирование Заказчика о выявленных инцидентах, методах реагирования на них, а также предоставление рекомендаций по их устранению;
4) Предоставление экспертной поддержки в процессе реагирования на инциденты;
5) Сканирование ИТ-инфраструктуры Заказчика на уязвимости — не реже 1 (одного) раза в месяц (не менее 512 уникальных IP-адресов);
6) Проведение тестирования на проникновение и анализа защищенности ИТ-инфраструктуры Заказчика — 2 (два) раза в течение срока оказания Услуг по заявке Заказчика (не менее 128 уникальных IP-адресов);
7) Консультирование при расследовании критичных инцидентов ИБ;
8) Оказание помощи и консультаций при прохождении испытаний на соответствие требованиям информационной безопасности;
9) Проведение аудита информационной безопасности (1 (один) раз в течение действия договора) в рамках оказания услуги оперативного центра информационной безопасности для ИС «Единый электронный архив документов» на соответствие Единым требованиям в области информационно-коммуникационных технологий и обеспечения информационной безопасности с представлением письменного отчета и рекомендаций;
10) В случае выявления подозрительных событий, касающихся систем, не входящих в зону мониторинга, дальнейшее расследование Заказчик осуществляет самостоятельно. Поставщик при необходимости консультирует Заказчика для определения степени критичности, проводит дополнительный анализ с целью выявления источника проблемы и содействует специалистам Заказчика в устранении инцидента;

11) Сервис управления и мониторинга привилегированного доступа (на 3 (три) пользователя), обеспечивающий централизованное хранение учетных данных, разграничение прав доступа, управление привилегированными сеансами, запись сеансов и журналирование действий пользователей;

2.2. Расширенная экспертиза

По запросу Заказчика может быть предоставлена дополнительная расширенная экспертиза зоны мониторинга согласно приложению 6 к настоящей ТС.

2.3. Услуги оказываются в соответствии с настоящей технической спецификацией с использованием следующих средств мониторинга и реагирования на инциденты информационной безопасности:

1) система управления событиями информационной безопасности (SIEM);
2) сервис управления и мониторинга привилегированного доступа;
3) сканер уязвимостей (Vulnerability Scanner), обеспечивающий обнаружение узлов, выявление уязвимостей операционных систем и приложений, оценку их критичности и формирование отчетов с рекомендациями по устранению;

2.4. Предлагаемые средства должны сопровождаться технической поддержкой от производителей решений на срок действия договора, что должно быть подтверждено официальным письмом от производителя или его официального представителя (дистрибьютора) со ссылками на веб-ресурсы (при наличии), предоставляемым заказчику.

2.5. Уровень критичности инцидентов, которые могут возникнуть в рамках оказания Услуг.

Для каждого инцидента ИБ устанавливается приоритет в соответствии с приложением № 2 к настоящей ТС. Реагирование на инциденты ИБ осуществляется в сроки, определенные временными характеристиками, приведенными в приложении № 3 к настоящей ТС.

3. Поставщик должен:

3.1. На основании опросного листа, заполненного Заказчиком, проводить анализ (обследование) ИТ-инфраструктуры Заказчика в части подключаемых информационных систем (ИС), включая:

1) выдачу рекомендаций по составу подключаемых источников событий информационной безопасности (далее – источники);
2) типизацию источников на стандартные и нестандартные, в соответствии с базой знаний Поставщика;
3) определение потребностей Заказчика в подключении существующих и разработке новых сценариев выявления атак;
4) определение объема требуемых лицензий.

На данном этапе должны быть собраны следующие сведения:

	1) название источника; 2) описание функционала источника (принадлежность к ИС); 3) площадка размещения; 4) производитель/марка/модель; 5) тип/версия ОС; 6) тип/версия ПО; 7) FQDN; 8) IP-адрес. **3.2.** В соответствии с настоящей технической спецификацией, должны быть определены и выработаны организационно-технические решения по: 1) целевой архитектуре оказания Услуг; 2) техническим характеристикам и требованиям к вычислительным ресурсам, выделяемым Заказчиком, включая расчет емкости файловых хранилищ; 3) порядку развертывания компонентов Услуг, в том числе на площадке Заказчика; 4) порядку и организации межсетевого взаимодействия компонентов Услуг на площадке Заказчика и центра мониторинга и реагирования на киберугрозы. **3.3.** Поставщик должен выполнить подключение источников: 1) организовать защищенное VPN-соединение на оборудовании Поставщика (далее – VPN-соединение) между площадкой Заказчика и Поставщика по согласованным параметрам. В случае отсутствия L3-связности между распределенными площадками необходимо обеспечить установление VPN-соединений с каждой из них; 2) произвести инсталляцию компонентов SIEM-системы. При необходимости предоставить Заказчику требования к вычислительным ресурсам, подсистемам хранения и рекомендации по конфигурированию для установки дополнительных компонентов Услуг; 3) выполнить конфигурирование и профилирование SIEM под ИТ-инфраструктуру Заказчика, что гарантирует работоспособность сценариев выявления нарушений и инцидентов информационной безопасности; 4) направить инструкции по подключению источников к сервису мониторинга и анализа событий информационной безопасности; 5) разработать до 3 (трех) индивидуальных адаптеров для нестандартных источников; 6) разработать новые сценарии выявления атак, включая расширение категорий инцидентов и правил корреляции на основе специфичных запросов Заказчика, согласованных с Поставщиком; 7) провести проверку сетевой связности между компонентами SIEM-системы, источниками и площадкой Поставщика в соответствии с настоящей технической спецификацией.

	3.4. На базе центра мониторинга и реагирования на киберугрозы Поставщик должен: 1) обеспечивать анализ событий информационной безопасности в режиме 24/7 силами аналитиков первой линии дежурной смены, которая является единой «точкой входа» для всех поступающих от различных источников событий. Аналитики первой линии должны обеспечивать обработку инцидентов информационной безопасности, первичную проверку ложных срабатываний, проведение первичной аналитики и выделение инцидентов информационной безопасности на основе категорий инцидентов и правил, регистрацию и последующее сопровождение инцидентов в соответствии со стандартами ITIL (категоризация, приоритизация, SLA); 2) мониторинг состояния компонентов SIEM-системы, установленных как на площадке Заказчика, так и на площадке Поставщика; 3) мониторинг состояния VPN-канала; 4) предоставление рекомендаций по обработке инцидентов силами аналитиков второй линии в режиме 8/5, а также решение типовых инцидентов информационной безопасности. В рамках этого процесса должно быть обеспечено проведение углубленной аналитики с использованием специализированных инструментов, а также адаптация правил корреляции в соответствии с изменениями в инфраструктуре Заказчика. При необходимости, добавление исключений в правила корреляции по запросу Заказчика; 5) проведение расследований инцидентов критического уровня силами третьей экспертной линии, предоставление рекомендаций по устранению подтвержденных инцидентов, а также проведение ретроспективной аналитики и актуализация информации о релевантных угрозах и атаках, способах их обнаружения и противодействия; оценка состояния защищенности и устойчивости объектов информатизации (аудит кибербезопасности); 6) Экспертиза инцидентов и угроз кибербезопасности, техническое расследование; 7) Мониторинг, анализ и прогнозирование угроз кибербезопасности; 8) Локализация и нейтрализация последствий инцидентов кибербезопасности; 9) Реагирование на угрозы и инциденты кибербезопасности; 10) в случае обнаружения инцидента ИБ в инфраструктуре Заказчика обеспечить передачу информации об инциденте в НКЦИБ в порядке и сроки, установленные законодательством Республики Казахстан в сфере информатизации, с одновременным уведомлением Заказчика; 11) предоставление отчетности по каждому выявленному инциденту информационной безопасности по одному из каналов связи: электронная почта, телефонный звонок. **3.5.** Заказчику должно быть обеспечено предоставление доступа к интерфейсу систем реагирования и управления инцидентами информационной безопасности. Функционал личного кабинета должен включать:

1) доступ к актуальной информации по статусу инцидентов;
2) возможность самостоятельной регистрации инцидентов;
3) просмотр статистики по произошедшим инцидентам;
4) отчетность по каждому выявленному инциденту;
5) получение отчетов и уведомлений от Поставщика.

3.6. Заказчик обязан в течение 14 (четырнадцати) рабочих дней со дня вступления договора в силу предоставить и выделить необходимые ресурсы, запрашиваемые Поставщиком для внедрения Услуг, а также обеспечить подключение всех необходимых источников к SIEM-системе в указанный срок.

3.7. Поставщик при содействии Заказчика обязан организовать сетевую связность между компонентами, необходимыми для оказания Услуги, и ИТ-инфраструктурой Заказчика.

3.8. Поставщик должен организовать защищенное VPN-соединение на оборудовании Заказчика между площадкой Заказчика и площадкой Поставщика по параметрам, согласованным с Заказчиком.

3.9. Поставщик обязан ежемесячно, не позднее 3 (третьего) числа месяца, следующего за отчетным и декабрьский отчет не позднее 20 декабря 2027 года предоставлять Заказчику подробные отчеты об оказанных Услугах по каждой площадке, на которой размещено оборудование с сопроводительным письмом с обязательной регистрацией в канцелярии Заказчика.

4. Взаимодействие Поставщика и Заказчика

4.1. Разрабатывается Регламент, который устанавливает порядок взаимодействия между Поставщиком и Заказчиком по вопросам оказания услуг по обеспечению ИБ и описывает процедуры, связанные с выявлением и реагированием на инциденты ИБ.

4.2. Взаимодействие центра мониторинга Поставщика и Заказчика включает:

1) регистрацию заявок на несоответствие оказываемых услуг требуемым параметрам качества;
2) организацию процесса восстановления сервиса;
3) взаимное информирование ответственных руководителей обеих сторон о ходе решения вопросов, связанных с восстановлением требуемого качества услуг.

4.3. Поставщик обязан оказывать услуги 24 часа в сутки, 7 дней в неделю.

4.4. Разграничение зон ответственности между Поставщиком и Заказчиком на период оказания услуги ОЦИБ указано в приложении №5 к настоящей ТС.

4.5. Процедура взаимодействия Сторон при выявлении инцидентов

В случае обнаружения инцидента Заказчиком, он уведомляет Поставщика по контактным данным технической службы Поставщика, указанный в регламенте. Поставщик регистрирует инцидент и сообщает Заказчику следующие данные:

1) номер зарегистрированного инцидента;
2) время регистрации;
3) тема (краткое описание);
4) информация об инциденте;
5) рекомендации по его устранению.

4.6. Уведомление об инциденте от Заказчика направляется Поставщику по электронной почте.

Под реагированием на инцидент ИБ понимается структурированный набор действий, направленный на установление деталей инцидента, минимизацию ущерба и предотвращение повторения инцидента в будущем. Действия по выявлению и реагированию на инциденты ИБ, а также их последовательность, представлены в приложении № 1 к настоящей ТС.

4.7. Процедура взаимодействия Сторон при регистрации обращений Заказчика

Заказчику предоставляется возможность отправлять запросы в соответствии с показателями, указанными в приложении № 4 к настоящей ТС. Для этого уполномоченный представитель Заказчика должен отправить запрос на электронный адрес Поставщика с указанием идентификатора в теме письма в следующем формате:

1) Тема письма: идентификатор (предоставляется сервис-менеджером), краткая суть запроса.
2) Тело письма: подробное описание запроса, указание приоритета запроса.

5. Условия надлежащего оказания Услуг

5.1. Поставщик не несет ответственности за инциденты и другие обстоятельства, повлекшие перерывы в оказании Услуг, если они вызваны одной из следующих причин:

1) проведение плановых или аварийных ремонтных работ на оборудовании, участвующем в оказании Услуг, с предварительным уведомлением Заказчика;
2) работы на оборудовании, участвующем в оказании Услуг, проводимые Заказчиком или Поставщиком по запросу Заказчика;
3) тестовое оказание Услуг по запросу Заказчика, при условии, что не было выявлено никаких инцидентов;
4) отказ или неспособность Заказчика обеспечить содействие Поставщику в установлении и устранении инцидентов в сроки, установленные уровнем оказания Услуг;

5) отказ или неспособность Заказчика предоставить необходимые данные для настройки программного обеспечения или оборудования в рамках оказания Услуг в соответствии с требованиями регламента, в срок не более 5 (пяти) рабочих дней;

6) проведение работ Заказчиком по внесению изменений в состав и конфигурацию защищаемых ресурсов без уведомления Поставщика, что может привести к их временной недоступности и, как следствие, к перерыву в оказании Услуг;

7) неработоспособность или несовместимость программного и/или программно-аппаратного обеспечения Заказчика с оказываемыми Услугами;

8) наступление обстоятельств непреодолимой силы в соответствии с условиями Договора.

6. Права Поставщика

6.1. Поставщик вправе запрашивать у Заказчика информацию, необходимую для реализации сценария выявления атак (в том числе информацию об ИТ-инфраструктуре), а также использовать эту информацию исключительно для выполнения своих обязательств по Договору, с целью минимизации ложных срабатываний.

6.2. Запрос формируется Поставщиком и направляется по электронной почте уполномоченному лицу со стороны Заказчика. В запросе должна быть указана причина обращения. Заказчик обязан предоставить обратную связь по данному запросу в течение 3 (трех) рабочих дней, при необходимости срок может быть скорректирован по согласованию сторон.

Примеры запрашиваемой информации могут включать, но не ограничиваются:

1) список DNS-серверов;
2) IP-адреса сканеров безопасности;
3) список ресурсов, доступных из сети интернет;
4) список глобальных IP-адресов, принадлежащих Заказчику;
5) список учетных записей администраторов информационных систем;
6) информацию о владельцах информационных систем и ресурсов;
7) данные о принадлежности IP-адреса пользователю или системе.

Информация предоставляется путем заполнения Заказчиком соответствующих опросных листов для подключения Услуг и интервьюирования уполномоченных представителей Заказчика.

7. Плановое техническое обслуживание оборудования Поставщика

7.1. Поставщик вправе проводить плановое техническое обслуживание или усовершенствование подсистем, на базе которых оказываются Услуги. Эти работы считаются плановыми ремонтными работами и могут повлечь

	за собой перерывы в оказании Услуг. Плановые ремонтные работы проводятся в интервале с 19:00 до 08:00 (время г. Астана) либо в другое время, согласованное с Заказчиком, с возможным перерывом в оказании Услуг. **7.2.** Поставщик обязуется уведомить Заказчика о проведении плановых ремонтных работ, которые могут вызвать перерывы в оказании Услуг, не позднее, чем за 1 (один) рабочий день до начала работ. Исключение составляют случаи, когда работы выполняются по запросу Заказчика, а также ситуации, когда Поставщик не может уведомить в указанный срок, если плановые ремонтные работы проводятся по требованию государственных органов или компетентных телекоммуникационных органов Республики Казахстан. **7.3.** Заказчик, при необходимости, может направить предложения по корректировке сроков проведения работ, которые будут учтены Поставщиком при наличии технической возможности. В уведомлении, направленном Поставщиком, указывается следующая информация: 1) время проведения плановых ремонтных работ; 2) дата проведения работ; 3) продолжительность работ; 4) контактные данные ответственного лица, предоставляющего информацию о работах; 5) необходимость участия сотрудников Заказчика в работах, например, для проведения проверок работоспособности информационных систем Заказчика. **7.4.** Заказчик обязуется выделить ответственных сотрудников для участия в работах. В случае невозможности привлечения сотрудника в указанный срок, Заказчик направляет предложения по корректировке сроков проведения работ. **7.5.** Если плановые работы отменяются, Поставщик уведомляет Заказчика в кратчайшие сроки после принятия решения. **7.6.** Заказчик также обязан уведомить Поставщика о проведении плановых работ на своем оборудовании, если эти работы могут привести к временной недоступности защищаемых ресурсов и, как следствие, к перерыву в оказании Услуг. Уведомление должно быть направлено не позднее чем за 1 (один) рабочий день до начала работ. В уведомлении от Заказчика должны быть указаны: 1) время и дата проведения плановых работ; 2) продолжительность работ; 3) контактные данные ответственного лица, предоставляющего информацию о работах. **7.7.** В случае изменения сроков проведения плановых работ Заказчик обязан уведомить Поставщика в кратчайшие сроки, но не позднее, чем за 1 (один) рабочий день до начала работ. При отмене плановых работ Заказчик также обязан уведомить Поставщика в кратчайшие сроки.

7.8. Все уведомления от Заказчика или Поставщика должны направляться на электронные адреса уполномоченных представителей, указанных в регламенте.

8. Аварийные ремонтные работы на оборудовании Поставщика

8.1. Аварийные ремонтные работы подсистем, на базе которых оказываются Услуги, проводятся в случаях, когда фиксируются периодические прерывания в оказании Услуг или значительное ухудшение параметров качества, которое может привести к аварийной ситуации в будущем.

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

8.3. Заказчик, в свою очередь, обязан уведомить Поставщика о проведении аварийных ремонтных работ на своем оборудовании, если они могут привести к временной недоступности защищаемых ресурсов и, как следствие, к перерыву в оказании Услуг. Уведомление должно быть направлено не менее чем за 2 (два) часа до начала работ.

8.4. Уведомления направляются на электронные адреса уполномоченных представителей, указанных в настоящем техническом регламенте. В уведомлении должны быть указаны:

1) время, дата и продолжительность аварийных ремонтных работ;
2) контактные данные ответственного лица, предоставляющего информацию о проводимых работах;
3) информация о необходимости участия сотрудников Заказчика в аварийных ремонтных работах (если работы проводятся Поставщиком).

9. Анализ вредоносных или подозрительных объектов, имеющихся у Заказчика:

9.1. Объект исследования: один подозрительный файл. В случае анализа составных файлов (архивов) объектом исследования является каждый отдельный файл, входящий в состав архива, а не архив в целом. Если анализируются составные исполняемые файлы (самораспаковывающиеся архивы, инсталляторы), объектом исследования является функционал (сценарий) этих архивов или инсталляторов. Если необходимо исследовать функционал извлечённых файлов, каждый из них рассматривается как отдельный объект исследования.

9.2. Объём исследований: по требованию Заказчика.

9.3. Основные возможные этапы проведения исследований (этапы проводятся исходя из их целесообразности, применимости, с учётом формата и структуры файла, а также необходимости для решения задач исследования. Это означает, что при анализе конкретного файла могут выполняться не все указанные этапы, но должны быть выполнены те, которые позволят достичь целей исследования):

9.4. Базовое статическое исследование объекта:

	1) Определение формата и размера файла; 2) Подсчёт хэш-сумм (MD5, SHA-256); 3) Определение наличия цифровой подписи; 4) Извлечение и анализ строк, содержащихся в файле; 5) Идентификация средств компиляции файла; 6) Анализ заголовка файла, включая импортированные функции, секции, время компиляции и другие временные метки (если такие данные имеются). **9.5.** Поиск данных по открытым источникам: 1) Поиск хэш-сумм, идентифицирующих объект, с помощью Google.com и Virustotal.com (с загрузкой или без загрузки объекта на ресурс, по согласованию с Заказчиком); 2) Поиск примечательных строк, содержащихся в объекте, с использованием Google.com и других сервисов. Список таких строк выбирается аналитиком в зависимости от особенностей объекта исследования. **9.6.** Углубленный статический и при необходимости динамический анализ: 1) Исследование дизассемблированного, декомпилированного или иного доступного кода объекта анализа (в зависимости от формата файла); 2) При необходимости и наличии технической возможности – проведение отладки объекта в изолированной виртуальной среде, с доступом или без доступа к интернету (по согласованию с Заказчиком). **9.7.** Выделение идентификаторов компрометации (в случае обнаружения вредоносного функционала): 1) Структурирование собранной информации и выделение следующих возможных групп идентификаторов, которые могут быть обнаружены в системе, зараженной исследуемым объектом: имена мьютексов, файлов, ключей реестра, процессов, IP-адреса, доменные имена, учетные данные, имена и пароли пользователей, создаваемых вредоносным ПО. **9.8.** Характеристика функционала исследуемого объекта: 1) Классификация объекта по его возможностям распространения и выполняемым функциям (например: троян, червь, вирус, бэкдор, загрузчик и другие.). В случае выявления вредоносного функционала это описывается, либо указывается на его отсутствие, если исследование не подтвердило его наличие. **9.9.** Подготовка рекомендаций для нейтрализации объекта: 1) Формирование рекомендаций для обнаружения заражения объектом, его нейтрализации и восстановления систем (рабочих станций, серверов или другого оборудования), если объект содержит вредоносный функционал. Если вредоносный функционал не выявлен, это также указывается.

	10. Технические требования к межсетевому экрану Количество устройств – 1 шт. – Функционал Next Generation Firewall (NGFW); – Контроль приложений и фильтрация веб-трафика (Application Control & URL Filtering); – Решение должно обеспечивать функционал Системы предотвращения вторжений (IPS); – Система IPS должна обеспечивать обнаружение угроз на основе следующих механизмов: – Сигнатурный анализ для выявления известных атак и эксплойтов; – Отслеживание и анализ аномалий протоколов для выявления нестандартного или вредоносного трафика; – Управление приложениями для контроля и блокировки нежелательной активности приложений; – Обнаружение на основе анализа поведения для выявления ранее неизвестных атак и аномального поведения. – Антивирусная защита (Antivirus) с возможностью проактивного обнаружения угроз; – Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам, а также обнаруживать и блокировать входящие вредоносные файлы; – Защита от ботов и вредоносных программ (Anti-Bot); – Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи, а также иметь механизмы, применяющие интеллектуальную аналитику для автоматической защиты от атак в протоколе DNS, включая механизмы защиты от DGA; – Защита электронной почты от спама (Anti-Spam) с использованием интеллектуального анализа; – Функционал песочницы (sandbox) для анализа файлов и выявления угроз нулевого дня с возможностью эмуляции выполнения в изолированной среде; – Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа трафика и состояния приложений для отслеживания и управления сетевыми потоками; – Решение должно поддерживать работу DHCP в режимах сервера и ретранслятора (relay); – Решение должно поддерживать возможность работы в режиме Transparent (Bridge); – Решение должно поддерживать политику, основанную на белом списке MAC-адресов для ограничения доступа к локальной сети; – Решение должно поддерживать политику, основанную на механизмах QoS; – Решение должно обеспечивать возможность гарантирования или ограничения пропускной способности, а также управления задержкой для определённого IP-источника, IP-назначения или сервиса; – Решение должно поддерживать настройку правил QoS для VPN-трафика, включая возможность гибкого определения параметров приоритезации, ограничения или гарантирования пропускной способности;

	–Решение должно обеспечивать функционал интегрированной системы предотвращения вторжений (IPS) для защиты веб-приложений от вредоносного кода и атак. Система должна обеспечивать блокировку сетевых червей, атак переполнения буфера, SQL-инъекций, инъекций команд, межсайтового скриптинга (XSS), а также поддерживать настраиваемый модуль блокировки HTTP-червей. Дополнительно система должна обеспечивать защиту от обхода каталогов (Directory Traversal), вредоносных или некорректных HTTP-заголовков (Header Rejection), а также от вредоносного HTTP-кода; –Решение должно поддерживать протокол HTTP/3 over QUIC; –Решение должно обеспечивать функционал Песочницы (Sandboxing) (инспекция в облаке или на выделенном локальном устройстве) при наличии лицензии; –Решение должно обеспечивать функционал Идентификации и контроля пользователей; –Должно обеспечивать возможность получения идентификаторов пользователей путем анализа событий безопасности Microsoft Active Directory; –Должно поддерживать аутентификацию пользователей по идентификатору с использованием браузера, предназначенную для устройств и пользователей, не являющихся частью домена; –Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности; –Встроенная поддержка VPN (Site-to-Site VPN, Remote Access VPN); –Аутентификация пользователей через Active Directory, RADIUS, LDAP; –Поддержка аутентификации пользователей по IP/MAC-адресу с гибкими правилами безопасности; –Поддержка современных криптографических алгоритмов шифрования и аутентификации, соответствующих требованиям законодательства Республики Казахстан в области защиты информации; –Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5 (1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20; –Решение должно поддерживать использование как встроенного центра сертификации (CA), так и внешних сторонних центров сертификации; –Решение должно поддерживать как минимум следующие механизмы обеспечения целостности данных с использованием алгоритмов: MD5, SHA-1 SHA-256, SHA-512 и AES-XCBC; –Поддержка ролевого управления доступом (RBAC) для эффективного разграничения полномочий; –Решение должно обеспечивать поддержку двухфакторной аутентификации как через интеграцию с внешними системами двухфакторной аутентификации, так и посредством встроенного механизма двухфакторной аутентификации, предоставляемого производителем;

	–Возможность настройки политик безопасности с разделением по пользователям, группам, IP-адресам, приложениям, категориям приложений и другим параметрам; –Возможность активации политик по расписанию, включая временные ограничения и условия доступа; –Автоматическая генерация отчетов о нарушениях политик безопасности; –База данных управления приложениями должна содержать свыше 10000 известных приложений; –Решение должно обеспечивать детальный контроль безопасности минимум для 250000 Web 2.0 виджетов; –Встроенная система двухфакторной аутентификации без сторонних интеграций; –Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL; –Решение должно обеспечивать функционал «песочницы» Sandboxing (инспекция – в облаке или на выделенном локальном устройстве). Сетевые функции и отказоустойчивость –Поддержка SD-WAN для интеллектуального управления трафиком с учетом приоритизации нагрузки; –Поддержка управления полосой пропускания (Traffic Shaping) для балансировки нагрузки; –Интеграция с внешними системами телеметрии и мониторинга уязвимостей; –Поддержка маршрутизации: OSPFv2, BGPv4, RIP, PIM (SM, DM, SSM), IGMP; –Поддержка IPv6, dual-stack туннелирование IPv4 поверх IPv6; –Кластеризация в режиме Active/Passive с автоматическим переключением в случае отказа; –Централизованное управление через облачный портал; – –Возможность детальной визуализации сетевых соединений и анализ аномального поведения пользователей. Производительность –Пропускная способность NGFW: не менее 1,2 Gbps; –Пропускная способность Threat Prevention (с активированным функционалом Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot и облачный Sandbox): не менее 750 Mbps; –Пропускная способность IPS: не менее 1,7 Gbps; –Пропускная способность Firewall: не менее 2,2 Gbps; –Пропускная способность VPN AES-128: не менее 1,4 Gbps; –Скорость установки новых соединений: не менее 16 000 соединений/сек; –Максимальное количество одновременных соединений: не менее 1 000 000; –Возможность расширенного мониторинга нагрузки на процессор и сетевые интерфейсы; –Поддержка/подписка производителя предоставляется на 12 месяцев и исчисляется с даты активации лицензии/ввода в эксплуатацию, подтверждаемой актом. Гарантийный срок 12 месяцев исчисляется с даты

подписания акта ввода (при
поставленного оборудования/П
гарантийного периода.

Аппаратные характеристики

– WAN-порт: не менее 1x 10/

– LAN-порты: не менее 6x 10

– Консольный порт: не менее

– USB-порт: не менее 2x USE

– Диапазон рабочих температ

Дополнительные требования

– Поддержка управления чер

– Возможность централизова

– Поддержка быстрого развер

– Поддержка отчетности и ве

– Возможность управления н

– Поддержка сертификаций б
WEEE;

– Оборудование, программно
поставляются Поставщиком и
самостоятельным предметом з
отдельно не тарифицируется.

11. Т

Требования к лицензии на
включено в реестр доверенног
соответствии с приказом Замест
развития Республики Казахстан

Общие (системные) требован

11.1.Требования к архитектур

11.1.1Централизованная архи

- Система развернута в едино

- Обработка всех данных и уг

дования/ПО. Гарантийные обязательства/поддержка в части
ются с окончанием срока оказания услуг и действуют в течение

Г RJ-45;
Т RJ-45;

0°C;

риложение;
ия политиками;
Touch Deployment);
ежиме реального времени;
юзами безопасности через единый интерфейс;
B 62368-1, UL 62368-1, FCC IC Class B, CE, VCCI, RoHS, REACH,

и лицензии, указанные в настоящей Технической спецификации,
в целях обеспечения оказания услуг ОЦИБ и не являются
ость указанных элементов включается в стоимость услуг и

рограммному обеспечению класса EDR

ты информации EDR. Программное обеспечение должно быть
го обеспечения и продукции электронной промышленности, в
-Министра – Министра искусственного интеллекта и цифрового
года № 279/НҚ.

ботки данных.
олняется централизованно.

	11.1.2.Отказоустойчивость и резервное копирование: - Поддержка резервного копирования данных и автоматического восстановления. - Настройка узлов для обеспечения высокой доступности. **11.1.3.**Безопасность данных: - Шифрование данных в движении (TLS 1.2/1.3) и в состоянии покоя. - Управление доступом на основе ролей (RBAC). **11.1.4.**Производительность и нагрузка: - Обработка большого объема телеметрии в режиме реального времени. - Минимальные требования к инфраструктуре: процессор от 4 ядер, 16 ГБ ОЗУ, SSD-диски. **11.1.5.**Интеграция и совместимость: - Поддержка стандартных интерфейсов API (REST, JSON). - Интеграция с SIEM, SOAR и другими инструментами кибербезопасности. **11.1.6.**Мониторинг и управление: - Централизованное управление через веб-консоль. - Мониторинг состояния системы в режиме реального времени. - Поддержка журналирования и ведения отчетов. - Поддержка языков аналитических запросов и механизмов поиска, обеспечивающих фильтрацию, корреляцию и анализ событий информационной безопасности в журналах событий. Дополнительные требования - Возможность работы системы в on-premise, публичных облаках и гибридном исполнении. - Масштабируемая поисковая платформа с открытой схемой данных, поддерживающая локальное и мультиоблачное размещение. - Функциональные требования могут быть реализованы как в рамках одного решения, так и посредством интеграции нескольких решений при условии выполнения всех требований настоящей ТС. - Возможность управления модулями интеграции со сторонними решениями и подключения пакетов интеграции через консоль. - Наличие интеллектуальных механизмов автоматизации анализа и приоритизации инцидентов (при наличии у поставщика), не являющихся обязательным условием соответствия ТС. - Назначение политик на группы конечных устройств. - Поддержка ролевого доступа и аудита действий операторов консоли. - Консоль должна поддерживать совместную работу аналитиков над инцидентами, включая делегирование и изменение статусов.

	- Управление конечными точками без VPN для защиты систем за пределами корпоративного периметра. - Наличие предустановленных и настраиваемых дашбордов для анализа событий. - Масштабируемая визуализация связей запущенных процессов. - Поддержка неограниченного числа администраторов. - Обмен данными между консолью управления и модулями через TLS 1.2. - Продукт отечественного производства, либо иного производства, имеющий действующую лицензию правообладателя на использование заказчиком на территории Республики Казахстан и соответствовать требованиям законодательства Республики Казахстан в области информационной безопасности (подпункт 2 пункта 3 статьи 61 ЗРК о Кибербезопасности). - Оборудование, программное обеспечение и лицензии, указанные в настоящей Технической спецификации, поставляются Поставщиком исключительно в целях обеспечения оказания услуг ОЦИБ и не являются самостоятельным предметом закупки. Стоимость указанных элементов включается в стоимость услуг и отдельно не тарифицируется. **Функциональные требования** **11.2.** Поддержка операционных систем **11.2.1.**Рабочие станции: -Windows: Windows 10, Windows 11 (x64). -macOS: Версии от macOS 11 Big Sur и выше. -Linux: Ubuntu 18.04 LTS и выше, Debian 10 и выше. **11.2.2.**Серверы: -Windows Server 2016, 2019, 2022. -Linux: Red Hat Enterprise Linux 8, CentOS 7.9-2009 и выше. **11.2.3.**Мобильные устройства: -Android: Версии от Android 9.0 и выше. - iOS: Версии от iOS 13 и выше. **11.2.4.**Виртуальные среды: -Поддержка виртуализации на VMware, Hyper-V, KVM. **11.3.** Типы сканирований **11.3.1.**Сканирование при доступе (On-access): -Автоматическое сканирование файлов при их создании, открытии, изменении или выполнении. **11.3.2.**Сканирование по требованию (On-demand): -Запуск сканирования вручную через интерфейс агента.

	11.3.3.Сканирование съемных носителей: -Проверка подключенных USB-устройств, внешних жестких дисков и других съемных носителей. **11.3.4.**Плановое сканирование: -Настраиваемые задания сканирования по расписанию (ежедневное, еженедельное, ежемесячное). **11.3.5.**Сканирование оперативной памяти: -Проверка процессов и данных в оперативной памяти на наличие признаков вредоносного ПО. **11.3.6.**Глубокое сканирование системы: - сканирование всей файловой системы с детальным анализом содержимого. **11.4. Сканируемые форматы архивов** **11.4.1.**Поддерживаемые форматы архивов: -7zip, ace, arj, bzip2, cab, gz, gzip, jar, rar, tar, tgz, xz, zip, zipx. **11.4.2.**Особенности сканирования: -Распаковка вложенных архивов. -Поддержка многотомных архивов. -Сканирование на наличие вредоносного содержимого внутри всех поддерживаемых форматов. Сканируемые сетевые протоколы Поддерживаемые протоколы: -HTTP, HTTPS -FTP, FTPS -IMAP, IMAPS -SMTP, SMTPS -POP3, POP3S -DNS Особенности сканирования: -Анализ входящего и исходящего трафика. -Обнаружение вредоносных элементов в протоколах передачи данных. -Инспекция зашифрованного трафика с поддержкой TLS. Сканируемые сетевые ресурсы Поддерживаемые ресурсы: SMB (Windows Shares), NFS (Network File System), WebDAV Особенности сканирования: -Анализ содержимого сетевых ресурсов на наличие угроз. -Проверка доступа и изменений файлов.

	-Обнаружение несанкционированного доступа. Требования к обеспечению целостности и доступности информации Локальное хранение данных: Антивирусный агент должен иметь локальное хранилище отчетов с возможностью просмотра через графический интерфейс. -Должна быть поддержка экспорта отчетов в файл для дальнейшего анализа. Карантин: Возможность перемещения обнаруженных вредоносных файлов в локальное хранилище (карантин) с последующим восстановлением при необходимости. Действия при обнаружении угроз: -Завершение процессов. -Удаление файлов. -Игнорирование ложных срабатываний на основе пользовательских правил. Анализ поведения: -Возможность анализа поведения процессов для выявления вредоносной активности. -Обнаружение попыток эксплуатации уязвимостей. Защита от вмешательства: -Защита от остановки процессов и удаления файлов антивирусного агента. -Возможность установки пароля для защиты настроек от несанкционированного изменения. Обновление антивирусных компонентов: -Обновление через интернет, локальный сервер или сетевой каталог. -Автоматическое обновление сигнатур и базы угроз. **11.5.** Требования к обеспечению целостности и доступности компонента **11.5.1.**Защита от несанкционированного вмешательства: -Защита процессов агента от остановки или удаления. -Блокировка изменений настроек без авторизации. -Настройка прав доступа через административную консоль. **11.5.2.**Механизмы самовосстановления: -Автоматический перезапуск критических служб при сбоях. -Контроль целостности файловых систем и конфигураций компонентов. **11.5.3.**Контроль доступа и аутентификация: -Журналирование всех изменений конфигурации системы. **11.5.4.**Мониторинг работоспособности: -Непрерывный мониторинг состояния системы с оповещениями.

	-Отчеты о статусе компонентов в режиме реального времени. **11.5.5.**Обновления и исправления: -Регулярные обновления и исправления безопасности. -Обновление баз сигнатур и политик безопасности через защищенные каналы связи. **11.6. Источники обновления компонентов антивируса и набора сигнатур** **11.6.1.**Удаленные источники: -Сервер производителя, доступные через интернет (HTTPS). - Облачное хранилище. **11.6.2.**Автоматизация обновлений: -Настраиваемый график автоматических обновлений. -Поддержка ручного запуска обновлений через веб-консоль. **11.6.3.**Защищенная передача данных: -Использование TLS для безопасной передачи обновлений. -Проверка цифровых подписей компонентов перед установкой. Возможности централизованного управления Централизованная установка и обновление: -Установка, обновление и удаление компонентов системы с центральной консоли. -Управление политиками безопасности на всех конечных точках. Мониторинг и контроль: -Централизованный мониторинг работы системы в режиме реального времени. -Просмотр журналов событий и истории обновлений. Управление конфигурацией: -Настройка параметров системы с применением групповых политик. -Управление правами доступа пользователей и ролями. Реагирование на инциденты: -Отправка команд на изоляцию устройств. -Блокировка процессов, файлов и сетевых подключений. -Выполнение удаленных команд на конечных точках. Отчеты и уведомления: -Генерация детализированных отчетов о безопасности. -Настраиваемые уведомления об инцидентах безопасности и обновлениях системы. Интеграция с внешними системами:

	-Интеграция с SIEM, SOAR и другими системами безопасности. -API для взаимодействия с другими ИТ-решениями. **11.7. Реагирование на инциденты** **11.7.1.**Действия по реагированию на инциденты: -Завершить процесс; -Удалить файл; -Загрузить файл с рабочей станции на компьютер аналитика или в хранилище ПК; -Выполнить команду операционной системы с системными привилегиями; -Получить автоматически запускаемые объекты/скрипты; -Блокировка исполняемых файлов (хэш, имя файла); -Функционал создания Playbook для реагирования на инциденты. Интеграция с другими системами **11.7.2.**Интеграция с SIEM-системами: - Поддержка интеграции с промышленными SIEM-системами посредством стандартных протоколов и интерфейсов обмена данными (API, syslog, REST, webhook и иные). -Передача данных об инцидентах и обнаруженных угрозах в реальном времени. **11.7.3.**Интеграция с SOAR: -Поддержка автоматизации процессов реагирования через платформы SOAR (например, IBM Resilient, ServiceNow). **11.7.4.**Интеграция с системами управления уязвимостями: -Обмен данными с системами сканирования уязвимостей (например, Tenable, Qualys). **11.7.5.**Интеграция с системой управления доступом: -Интеграция с LDAP, Active Directory для управления учетными записями. -Поддержка SSO через SAML. **11.7.6.**API и веб-хуки: -REST API для получения данных о событиях, угрозах и инцидентах. -Веб-хуки для передачи данных в системы оповещения. **11.7.7.**Облачные интеграции: -Поддержка облачных сервисов Amazon AWS, Microsoft Azure, Google Cloud. -Встроенные интеграции для управления облачными ресурсами и защиты данных. **11.7.8.**Техническая интеграция: -Интеграция с почтовыми системами для анализа подозрительных писем (SMTP/IMAP).

	-Поддержка форматов отчетов STIX/TAXII для обмена данными о киберугрозах. **11.8. Техническая поддержка** Требования к персональному техническому менеджеру Поставщик выделяет персонального технического менеджера, который: **11.8.1.** Занимается обработкой запросов заказчика. **11.8.2.** Организовывает работы по технической поддержке. **11.8.3.** Информирует заказчика о текущем состоянии решения запросов. **11.8.4.** Доступен в рабочие дни по телефону и электронной почте с понедельника по пятницу с 9.00 часов до 18.00 часов по времени Астаны. Требования ко времени реакции технической поддержки Техническая поддержка должна быть доступна в круглосуточном режиме включая выходные и праздничные дни посредством интернет-портала и (или) телефона и (или) электронной почты. Время реагирования: - Критичный уровень – не более 30 минут - Высокий уровень – не более 4 рабочих часов - Средний уровень – не более 6 рабочих часов - Низкий уровень – не более 8 рабочих часов «Критический уровень»- вся локальная сеть (или критичная часть сети) не работает, что прерывает основные бизнес-процессы. «Высокий уровень»- продукт полностью выведен из строя, но непрерывность основных бизнес процессов не нарушается. «Средний уровень» - продукт частично выведен из строя (работает несоответствующим образом), но другое программное обеспечение пользователя не выведено из строя в результате работы продукта. «Низкий уровень» - означает другие некритичные запросы на обслуживание. Все инциденты, не упомянутые выше, относятся к этому уровню критичности. Типы запросов в техническую поддержку - Консультации по решению инцидентов в процессе установки, конфигурирования и функционирования продукта. -Консультации по лечению файлов, зараженных вредоносными программами; -Осуществление приоритетного выпуска набора антивирусных сигнатур, в том числе: - детектирование отдельных вредоносов из предоставленного набора, по мере готовности сигнатур для каждого из вредоносов такого набора;

	- детектирование набора вредоносов в одно время, после готовности сигнатур для всего этого набора. - Консультации у квалифицированных специалистов производителя антивирусного программного обеспечения (вирусных аналитиков, специалистов по компьютерной криминалистике и реагированию на инциденты), по вопросам исследования вредоносного кода, компьютерной криминалистике и реагированию на компьютерные инциденты, по мере необходимости, но не более 50 часов в течение года; Требования к обновлению программного обеспечения - Периодичность обновления набора антивирусных сигнатур – не реже одного раза в неделю. - Периодичность обновления агентов "ПК антивирусной защиты с централизованным управлением" и "ПК обнаружения и централизованного реагирования на инциденты информационной безопасности с компонентом Sandbox" – не реже одного раза в квартал. - Поставщик должен обеспечить выпуск исправлений (патчей) для программного обеспечения компонентов по запросу заказчика, в котором описывается обнаруженная уязвимость. Требования к обеспечению отказоустойчивости оборудования Поставщик должен иметь запасные части, инструменты, принадлежности и материалы для серверного оборудования компонентов и, в случае выхода из строя оборудования, восстановить их стабильное функционирование в соответствии с уровнем критичности. Требования к хранению и обработке данных: - Полная телеметрия с хранением на срок до 7 дней. - Шифрование всех данных и метаданных по защищенному каналу связи по протоколу TLS. Требования к поставке Поставка оборудования и программного обеспечения осуществляется единовременно, но не ранее истечения минимального срока, установленного пунктом 569 Правил осуществления государственных закупок. Требования к проверке работоспособности: Осуществление поставки для проверки работоспособности и комплектности товара, согласно условиям договора, на территории Заказчика. Проверка работоспособности осуществляется путем активаций и пробного подключения, визуального осмотра на отсутствие повреждений, дефектов, трещин, коррозии. **12. Требования к архитектурным принципам и классификации решений в области информационной безопасности** **1. Принцип соответствия классу решений**

	Каждое функциональное требование к информационной безопасности (ИБ) должно быть реализовано решением, которое соответствует отдельному, четко определенному классу решений, установленному архитектурой и методологией ИБ. **2.** Функциональные требования могут быть реализованы как в рамках одного решения, так и посредством интеграции нескольких решений при условии выполнения всех требований настоящей ТС. **3. Критерий самостоятельности** Каждое внедряемое решение обязано выполнять самостоятельную и независимую функцию обеспечения информационной безопасности.
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (Указываются при необходимости) (Отклонение потенциального поставщика за неуказание и непредставление указанных сведений не допускается)	Потенциальный Поставщик, в случае определения его победителем и заключения договора о государственных закупках, обязан предоставить: Письма (сертификаты) правообладателя (производителя) или его официального представителя, подтверждающие право Поставщика на поставку (предоставление) продуктов, предусмотренных технической спецификацией, представляются в течение 10 (десяти) рабочих дней со дня вступления договора в силу. Дополнительно Поставщик представляет: **1. Таблицу соответствия требований технической спецификации характеристикам предлагаемых продуктов (решений), составленную Поставщиком.** **2.** Подтверждение от вендора о том, что данный продукт сертифицирован и/или поддерживается в актуальной версии для использования соответствующего программного обеспечения.

Приложение 1
к технической спецификации

Базовый процесс реагирования на угрозы и инциденты ИБ

№	Действие	Краткое описание	Ответственный	SLA
1	**Мониторинг и анализ событий информационной безопасности (ИБ)**			
1.1	Мониторинг и анализ событий информационной безопасности предполагает выявление потенциальных инцидентов и оценку их на предмет ложноположительных срабатываний. Это помогает своевременно обнаруживать угрозы и снижать количество ненужных реагирований на ошибочные события, повышая эффективность защиты информационных систем.		Аналитики 1/2 линий SOC	согласно приложению № 3 к ТС
1.2.	Предоставление дополнительной информации об инциденте и подтверждение/опровержение легитимности действий осуществляется в рамках запроса аналитиков 1-й и 2-й линии Поставщика. Этот процесс направлен на более глубокий анализ инцидента, уточнение его деталей и определение, являются ли выявленные действия легитимными или они связаны с угрозой информационной безопасности.		Ответственный работник Заказчика	согласно приложению № 3 к ТС
2	**Анализ угроз и инцидентов ИБ**			
2.1	Анализ потенциальных инцидентов ИБ, оценка их приоритетов и выработка рекомендаций по первичному реагированию		Аналитик 1/2 линий SOC	согласно приложению № 3 к ТС
3	**Уведомление о выявленной угрозе и инциденте ИБ Заказчика**			
3.1	**Заведение инцидента информационной безопасности (ИБ) в учетной системе Поставщика** осуществляется путем заполнения карточки инцидента и её отправки Заказчику. Карточка инцидента может содержать следующую информацию: **Общая информация:** • Заголовок инцидента ИБ; • Номер инцидента ИБ в учетной системе Поставщика; • Время регистрации инцидента ИБ в формате UTC;		Аналитики 1/2/3 линий SOC	согласно приложению № 3 к ТС

	• Приоритет инцидента; **Ключевая информация:** • Список затронутых хостов и активных учетных записей на них в момент инцидента (при наличии данной информации); • Источник(и) событий ИБ, на основании которых был выявлен инцидент ИБ; • Список выявленных индикаторов компрометации (например, хэш-сумма файла, имя файла, адрес C&C сервера, ассоциированные доменные имена и другие.); • Ссылки на дополнительные файлы, прилагаемые к инциденту; **Рекомендации:** • Первичные действия, которые необходимо предпринять для предотвращения инцидента ИБ или минимизации его последствий; • Дополнительная информация, которая может потребоваться от Заказчика для проведения Поставщиком дальнейшего анализа инцидента ИБ.		
4	**Предоставление обратной связи по Инциденту ИБ Заказчиком**		
4.1	После получения карточки инцидента Заказчик обеспечивает соответствующую реакцию на Инцидент ИБ, которая зависит от предоставленных Поставщиком рекомендаций, типа и приоритета Инцидента ИБ.	Ответственный работник Заказчика	согласно приложению № 3 к ТС

Приложение 2
к технической спецификации

Классификация критичности выявленных угроз и инцидентов ИБ

Уровень	Описание уровня критичности	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, возникающей 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

Приложение 3
к технической спецификации

Целевые показатели уровня предоставления услуги Мониторинг событий ИБ

№	Показатель	Приоритет	Время выполнения показателя*	Режим обслуживания	Время реакции Заказчика на запросы Поставщика**
1.	Обнаружение 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.	Регистрация инцидента ИБ 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

№	Показатель	Приоритет	Время выполнения показателя*	Режим обслуживания	Время реакции Заказчика на запросы Поставщика**
3.	В случае, если Заказчик подтвердил инцидент ИБ, то Поставщик выдаёт рекомендации по противодействию	1 — Критический	2 часа с момента регистрации	24x7	Не применимо
		2 — Высокий	4 часа 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

** Срок восстановления и решения Инцидента ИБ приостанавливается на период, когда требуется обращение в техническую поддержку производителя программного обеспечения третьих лиц (третья линия технической поддержки) и (или) получение дополнительной информации от Заказчика. На этот период Инцидент ИБ переводится в статус «Ожидание». ** Время реакции Заказчика исчисляется с момента направления запроса Поставщиком.*

Приложение 4
к технической спецификации

Целевые показатели проведения изменений в месяц

№	Показатель		Количество 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 тому подобное)	не более 4
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 приложением № 3 к ТС.	Не ограничено

Приложение 5
к технической спецификации

Разграничение зон ответственности на период оказания Услуги Мониторинг событий ИБ

№	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 Заказчика, входящих в Зону мониторинга.		+
1.2	Мониторинг и анализ событий ИБ, зарегистрированных или касающихся элементов инфраструктуры Заказчика, 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 развертывания 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	Обеспечение работоспособности защищенных каналов передачи информации между площадками Заказчика и Поставщика	+	+
1.10	Выполнение рекомендаций ОЦИБ и своевременное реагирование на инциденты ИБ	+	

№	Параметр	Заказчик	Поставщик
1.11	Предоставление актуального перечня серверного, коммуникационного и компьютерного оборудования, а также информационных систем, входящих в Зону мониторинга	+	
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 другие.	+	
1.14	Хранение получаемых данных (события, сетевые потоки) от Заказчика в период действия Договора		+

Приложение 6
к технической спецификации

Расширенная экспертиза ИТ-инфраструктуры Заказчика

Вид запроса	Краткое описание	Единица представления
Сканирование зоны мониторинга на наличие уязвимостей	Инструментальное сканирование узлов и информационных систем, входящих в зону мониторинга, для выявления угроз в приложениях и операционных системах, с предоставлением детального отчета по уязвимостям и рекомендациям по их устранению.	Не менее 512 уникальных IP-адресов, не реже 1 (одного) раза в месяц, согласно утвержденному плану работ. Стоимость включена в цену Договора.
Сканирование периметра на уязвимости (внешнее)	Инструментальное сканирование узлов и информационных систем периметра Заказчика из сети Интернет для выявления угроз в приложениях и операционных системах, с предоставлением детального отчета по уязвимостям и рекомендациям по их устранению.	Не менее 256 уникальных IP-адресов, не менее 1 раза в квартал, согласно утвержденному плану работ.
Тесты на проникновение в инфраструктуру Заказчика извне	Проведение тестов на проникновение в инфраструктуру Заказчика из сети Интернет. Сценарии и методы тестирования согласовываются с Заказчиком. По итогам тестов Поставщик предоставляет отчет.	Не менее 128 уникальных IP-адресов, 2 (два) теста в течение срока оказания Услуг по заявке Заказчика; стоимость включена в цену Договора.
Имитация целевых кибератак (Red Teaming)	Проведение имитаций целевых кибератак с последующим анализом и предоставлением рекомендаций по повышению уровня защищенности информационных систем. В отличие от тестов на проникновение, цель Red Teaming — оценить способности Заказчика по выявлению и предотвращению вторжений, а не найти максимальное количество уязвимостей.	1 (одно) мероприятие с применением 1 (одного) сценария атаки в течение срока оказания Услуг по запросу Заказчика; стоимость включена в цену Договора.

- При необходимости проведения расширенного расследования критичных инцидентов с привлечением специалистов по форензике (включая мероприятия по реагированию на площадке Заказчика, сбор и исследование образов жестких дисков, анализ вредоносного ПО, а также оказание помощи в устранении последствий инцидентов), данный сервис предоставляется только по запросу Заказчика.