Приложение №1 к протоколу заседания
Закупочной комиссии №___ от _____.

ЗАКУПОЧНАЯ ДОКУМЕНТАЦИЯ

на поставку, установку и запуск в эксплуатацию

Системы управления информацией и событиями безопасности (SIEM) и автоматизации реагирования (SOAR)

Заказчик: АКБ «Asia Alliance Bank»

Ташкент – 2026 г.

ИНСТРУКЦИЯ ДЛЯ УЧАСТНИКА КОНКУРСА

1. Общие положения

1.1. **Область действия конкурса:** настоящая Конкурсная документация разработана в соответствии с требованиями Порядка по закупкам АКБ «Asia Alliance Bank».

1.2. **Предмет Конкурса:** Внедрение системы управления информацией и событиями информационной безопасности (SIEM) и системы автоматизации реагирования на инциденты информационной безопасности (SOAR).

Для выполнения поставленной задачи, Поставщик должен осуществить:

- поставку программного обеспечения SIEM/SOAR;
- установку и настройку программного обеспечения;
- внедрение Системы;
- проведение интеграционных работ;
- ввод Системы в промышленную эксплуатацию.

Внедрение Системы SIEM/SOAR должно осуществляться Поставщиком совместно с ответственными представителями Заказчика без нарушения работоспособности действующей ИТ-инфраструктуры. Все работы выполняются на территории и в инфраструктуре Заказчика.

При этом, до начала внедрения Поставщик обязан провести предварительное обследование существующей ИТ-инфраструктуры, включая поверхностное обследование веб-ресурсов и веб-приложений Заказчика.

Также, Поставщик обязан провести обучение пользователей и администраторов Системы (до 10 человек) по вопросам эксплуатации внедренного решения.

1.3. **Наименование Заказчика:** АКБ «Asia Alliance Bank», 100047, г.Ташкент, Яшнабадский район, ул. Махтумкули, дом №2а Телефон: (+998 71) 231-60-00, факс: (+998 71) 289-55-33.

1.4. **Вид Конкурса:** Открытый.

1.5. **Ценовая часть:** для осуществления данной закупки определен бюджет в размере 2 700 000 000 сум

1.6. **Источник финансирования:** финансируется за счет собственных средств АКБ «Asia Alliance Bank».

1.7. **Условия платежа:**

- для организаций нерезидентов Республики Узбекистан: оплата производится 100% после поставки и установки ПО, а также предоставления требуемых подписок и лицензий, но не ранее 04.01.2027 года. При этом возможен авансовый платеж в размере 30% от общей стоимости контракта в замен предоставляемой поставщиком банковской гарантии авансового платежа на аналогичную сумму;

- для организаций резидентов Республики Узбекистан: авансовый платеж в размере 30% от общей стоимости контракта производится в течении 5 банковских дней с момента подписания контракта. Оплата 70% от общей стоимости контракта производится после поставки и установки ПО, а также предоставления требуемых подписок и лицензий, но не ранее 04.01.2027 года.

1.8. **Валюта платежа:**

- для организаций нерезидентов Республики Узбекистан: USD (Доллар США)
- для организаций резидентов Республики Узбекистан: UZS (узбекские суммы).

1.9. **Срок выполнения:** 30 календарных дней с даты подписания Договора.

1.10. **Процедура вскрытия конвертов с конкурсными предложениями порядок и критерии их оценки**: Вовремя, указанное в объявлении как время проведения конкурса, конкурсная комиссия для проведения оценки конкурсных предложений вскрывает конверты с предложениями, поданными участниками конкурса. Уполномоченный представитель участника конкурса вправе присутствовать при процедуре вскрытия конвертов. Полномочия представителя участника должны быть подтверждены доверенностью/приказом, которые должны быть представлены конкурсной комиссии. Оценка предложений производится в один этап. В случае установления недостоверности информации, содержащейся в документах, представленных

участником конкурса, конкурсная комиссия вправе отстранить такого участника от участия в конкурсе. Предложение признается надлежаще оформленным, если оно соответствует требованиям настоящей Конкурсной документации. Конкурсная комиссия отклоняет предложение, если подавший его участник конкурса не соответствует требованиям, установленным Конкурсной документации, либо расценен как организация с сомнительной репутацией, финансово неустойчивый либо санкционный. В процессе оценки конкурсных предложений Рабочая группа либо Конкурсная комиссия вправе направлять участникам письменные запросы по подтверждению или разъяснению той или иной информации, указанной в конкурсном предложении. При получении таких запросов участникам необходимо письменно ответить Заказчику и представить запрашиваемую информацию. В ходе таких переписок не допускается внесение каких-либо изменений в конкурсное предложение. Победителем признается участник конкурса, предложивший лучшие условия исполнения Договора на основе критериев, указанных в конкурсной документации. При наличии арифметических ошибок конкурсная комиссия вправе произвести перерасчет стоимости предложения исходя из стоимости за единицу. При этом по завершению корректировочных расчетов конкурсного предложение участнику отбора направляется уведомление по внесенным коррективам. В случае если участник отбора отказывается от корректировок, оценочная комиссия вправе отклонить предложение данного участника конкурса. Если участники конкурса представят предложения в разных валютах, суммы предложений при оценке будут пересчитаны в единую валюту по курсу Центрального банка Республики Узбекистан на дату вскрытия предложений. В целях корректного сравнения цен отечественных и иностранных участников конкурса, при оценке будут учтены соответствующие расходы (налоги, таможенные платежи и иные обязательные платежи), предусмотренные действующим законодательством Республики Узбекистан.

Конкурс может быть объявлен конкурсной комиссией не состоявшимся:

- если в конкурсе принял участие только один участник или никто не принял участие;
- если по результатам рассмотрения предложений конкурсная комиссия отклонила все предложения, на том основании, что все представленные конкурсные предложения не соответствуют требования конкурсной документации.

Невскрытые конкурсные пакеты участников, отстраненных от участия по решению конкурсной комиссии, возвращаются рабочим органом под роспись в 10-дневный срок после заседания конкурсной комиссии. По истечению указанного срока рабочий орган не несет ответственности за целостность и сохранность конкурсных пакетов.

1.11. **Заключение Договора:** По результатам конкурса Договор заключается на условиях, указанных в настоящей конкурсной документации и предложении, поданном участником конкурса, с которым заключается Договор по форме Приложения №3 настоящей Конкурсной документации.

Несвоевременное подписание Договора победителем может расцениваться как отказ от заключения Договора. В этом случае будет рассматриваться приемлемое предложение следующего (резервного - занявшее второе место по итогу оценки) участника конкурса. Заказчик имеет право вступать в переговоры с победителем конкурса о снижении цены Договора.

1.12. **Заинтересованным претендентам необходимо:**

- Подать соответствующим образом заполненную и подписанную Заявку на участие в Конкурсе, до истечения срока, по адресу: г.Ташкент, Яшнабадский район, ул.Махтумкули, дом №2А. Электронные предложения не принимаются.
- Сроки действия конкурсного предложения, предоставляемого Участником должен быть действительным не менее 50 дней с даты подачи Конкурсной Заявки.

2. Правила и требования для участников конкурса

2.1. Участники, представляющие предложения, должны нести все расходы, связанные с подготовкой и подачей конкурсной документации. АКБ «Asia Alliance Bank» не несет никакой материальной ответственности за расходы, понесенные участником конкурсных торгов по подготовке и предоставлению конкурсного предложения.

2.2. Участники, представляющие предложения, должны быть зарегистрированы в качестве юридического лица и быть правомочными к оказанию услуг/выполнению работ/реализации

товара в данной сфере, должны иметь соответствующие разрешительные документы, если таковые документы требуются в соответствии с законодательством страны регистрации Участника.

2.3. Технические требования к товарам, услугам и технологическим решениям, указаны в Техническом задании к Конкурсной документации, являющейся ее неотъемлемой частью.

2.4. К участию в Конкурсе не допускаются организации (компании):

- не предоставившие в установленный срок необходимые документы для отбора;
- предоставившие документы, не соответствующие требованиям Конкурсной документации;
- предоставившие технические решения, не соответствующие требованиям Технического Задания к Конкурсной документации, являющимся его неотъемлемой частью;
- находящиеся на стадии реорганизации (разделения, слияния), ликвидации или банкротства, а также организации на имущество которых наложен арест;
- находящиеся в состоянии судебного или арбитражного разбирательства с Заказчиком;
- имеющие задолженность по уплате налогов и сборов;
- представившие более одного предложения.

2.5. Конкурсное предложение должно быть представлено в одном опечатанном конверте, содержащем перечень документов, указанных в Приложении №1 (Квалификационная часть) и Приложении №2 (Ценовая часть) настоящей Конкурсной документации. Визирование уполномоченным представителем участника Конкурса, а также опечатывание конверта производится в местах склейки. Конверты должны быть опечатаны штампом или печатью участника (при наличии). В случае осуществления деятельности без печати и штампа, необходимо указать об этом на конверте следующей надписью: «деятельность организации осуществляется без печати/штампа».

На конвертах указываются наименование и адрес Заказчика, контактные телефоны, а также:

- название (предмет) конкурса;
- наименование Участника конкурса, контактные данные, ИНН участника;
- пометка - «Не вскрывать до установленного времени проведения конкурса».

Конверты не опечатанные и не помеченные в соответствии с вышеуказанными требованиями не принимаются и не рассматриваются.

Заказчиком к Участникам Конкурса предъявляются следующие квалификационные требования:

А. иметь подтвержденный опыт поставки и внедрения аналогичных программных решений не менее 2 (два) года;

Б. обладать статусом авторизованного партнера производителя предлагаемого программного обеспечения, подтвержденным соответствующими документами;

В. иметь право на поставку, внедрение и предоставление конечным пользователям прав использования программного обеспечения;

Г. не находиться в стадии ликвидации, банкротства или реорганизации, не иметь ограничений, препятствующих осуществлению хозяйственной деятельности;

Д. соблюдать требования законодательства Республики Узбекистан, а также внутренних нормативных документов Заказчика при работе с конфиденциальной информацией и обеспечивать ее неразглашение.

Е. Наличие действующего сертификата соответствия ГУ «Центр кибербезопасности» Республики Узбекистан на предлагаемую систему является преимуществом.

2.6. Конкурсное предложение и вся связанная с ним корреспонденция, и документация, которые осуществляются Участником и Заказчиком, могут быть на узбекском или русском языке. Прилагаемая к Конкурсному предложению документация может быть на другом языке при условии, что к нему будет приложен точный перевод на узбекский или русский язык. В случае наличия разночтений между редакциями на другом языке и переводом текста конкурсного предложения на узбекский или русский язык, переводом текста будет превалирующим.

2.7. При необходимости Конкурсная комиссия может дополнительно потребовать от Участников конкурса предоставления дополнительной информации касательно представленных ими Конкурсных предложений или других дополнительных документов, необходимых для выполнения данного заказа.

2.8. Никакие вставки между строками, подтирки или приписки в документах конкурсного предложения не допускаются, а при наличии их в документах, заявка не подлежит рассмотрению и отклоняется.

2.9. Участники конкурса должны представить Конкурсное предложение строго в соответствии с формами, предлагаемыми в Конкурсной документации. В случае предоставления Конкурсного предложения не по формам настоящей конкурсной документации, Конкурсная комиссия вправе отклонить данное предложение.

2.10. Предложения должны подаваться цельно и в количествах, указанных в Конкурсной документации.

2.11. Участник в представляемой заявке на участие должен указывать цену предложения с учетом НДС или без учета НДС (обязательно требуется указать).

2.12. Полномочия представителя Участника должны быть подтверждены доверенностью/приказом, которые должны быть представлены Конкурсной комиссии. Доверенность должна быть оформлена по Форме №2

2.13. При оценке предложения Заказчиком будут учитываться следующие критерии:

По квалификационной части Конкурса:

- соответствие предлагаемых работ и услуг техническим требованиям, изложенным в Конкурсной документации (качество);
- соответствие участника квалификационным требованиям, указанным в пункте 2.5 данной документации;
- деловая репутация участника конкурса учитывая условия пункта 1.11 данной документации.

По ценовой части Конкурса:

- цена;
- условия и сроки выполнения работ/услуг, поставки товара;
- условия платежа и гарантии;
- предоставление финансовой скидки. При этом механизм применения скидки должен быть точно описан.

Приложение №1 к Конкурсной документации

Перечень документов, предоставляемых участниками Конкурса (Квалификационная часть)

1. Заявка на участие в Конкурсе по Форме №1;
2. Доверенность (при участии доверенного лица участника) на фирменном бланке организации по форме №2 (вне конверта);
3. Гарантийное письмо, свидетельствующее, о том, что участник не находится в стадии реорганизации, ликвидации или банкротства, в состоянии судебного или арбитражного разбирательства с Заказчиком, не имеет задолженности по налогам и сборам по Форме №3;
4. Документация подтверждающая наличие опыта участника согласно требованиям, указанным в пункте 2.5, такие как:

- иметь подтвержденный опыт поставки и внедрения аналогичных программных решений не менее 2 года (приложить свидетельство о регистрации юридического лица и перечень указывающий на требуемый опыт);
- обладать статусом авторизованного партнера производителя предлагаемого программного обеспечения, иметь право на поставку, внедрение и предоставление конечным пользователям прав использования программного обеспечения (приложить действующее партнёрское соглашение с производителем / авторотационное письмо от производителя, подтверждающего право поставки оборудования на территорию Республики Узбекистан;
- предоставить при наличии действующий сертификат соответствия ГУ «Центр кибербезопасности» Республики Узбекистан на предлагаемую систему.

5. Техническое предложение Участника по Форме №4 и №5.

Приложение №2 к Конкурсной документации

Перечень документов, предоставляемых участниками Конкурса (Ценовая часть)

1. Коммерческое предложение по Форме №6

Форма №1 (к Приложению № 1)

ФИРМЕННЫЙ БЛАНК

Председателю Конкурсной комиссии
АКБ « Asia Alliance Bank »
У.А. Абдуазимову

З А Я В К А
на участие в конкурсе

_____ имеет возможность поставить _____.:
(наименование товаров или услуг)

№	Наименование работ/товаров/услуг	Цена
1		

Изучив данные объявления об условиях конкурса на заключение договора на поставку _____, мы нижеподписавшиеся,
(наименование товаров или услуг)
уполномоченные на подписание конкурсного предложения от имени (полное наименование Участника конкурса) в соответствии с конкурсной документацией.

Мы обязуемся поставить товар в точном соответствии с условиями нашего предложения, а также условиями предусмотренными договором и действующим законодательством Республики Узбекистан.

В случае если наше предложение будет принято Банком, берем на себя обязательство заключить договор с АКБ «ASIA ALLIANCE BANK» в срок не позднее 5 дней с момента определения победителя конкурса.

Мы осознаем, что АКБ «ASIA ALLIANCE BANK» имеет право в любой момент приостановить процесс отбора либо анулировать процесс а также имеет право отобрать любого участника по своему усмотрению не неся перед нами какого либо обязательства.

Контактный телефон/факс: _____

Адрес электронной почты: _____

_____
Ф.И.О. и подпись руководителя или уполномоченного лица

Место печати (при наличии)

Форма №2 (к Приложению № 1)

НА ФИРМЕННОМ БЛАНКЕ УЧАСТНИКА

ДОВЕРЕННОСТЬ №_____

_____ _____2026 г.

ООО_____, именуемое в дальнейшем «Организация», в лице _____, действующего на основании _____, настоящей доверенностью уполномочивает представителя Организации – гражданина_(паспорт серии_№___, выданный от года) на:

а) представление конкурсных документов;

б) проведение переговоров с заказчиком конкурса и рабочим органом, подписания от имени компании любой документации причастной к данному процессу отбора;

в) присутствие на заседаниях конкурсной комиссии при вскрытии конвертов с конкурсным предложением;

г) предоставление разъяснений касательно технической и ценовой части конкурсного предложения, а также других вопросов.

Настоящая доверенность вступает в силу с момента её подписания, выдана без права передоверия, сроком до _____г.

Ф.И.О. и подпись руководителя

Ф.И.О. и подпись лица, на имя которого выдана доверенность

Место печати (при наличии)

Форма №3 (к Приложению № 1)

НА ФИРМЕННОМ БЛАНКЕ УЧАСТНИКА

№: Дата: _

Председателю Конкурсной комиссии

ГАРАНТИЙНОЕ ПИСЬМО

Настоящим письмом подтверждаем, что компания_

_____

(наименование компании)

- не находится в стадии реорганизации (разделения, слияния), ликвидации или банкротства,
имущество компании не арестовано;
- не находится в состоянии судебного или арбитражного разбирательства с «Заказчиком»;
- не находится в Едином реестре недобросовестных исполнителей;
- отсутствуют ненадлежащим образом исполненные обязательства по ранее заключенным договорам;
- не имеет задолженности по уплате налогов и других обязательных платежей;
- не находится в оффшорных зонах.

Подписи:

Ф.И.О. руководителя _____

Ф.И.О. главного бухгалтера _____

Ф.И.О. юриста *(при наличии)*

Место печати (при наличии)

Форма №4 (к Приложению №1)

НА ФИРМЕННОМ БЛАНКЕ УЧАСТНИКА

№: *Дата:*

Председателю Конкурсной комиссии

Общая информация об участнике Конкурса

	Полное наименование юридического лица, с указанием организационно-правовой формы	
	Сведения о регистрации (дата регистрации, регистрационный номер, наименование регистрирующего органа)	
	Юридический адрес	
	Контактный телефон, факс, e-mail	
	Полные банковские реквизиты	
	Основные направления деятельности	

Информация об опыте поставке товаров или услуги

№	Наименование товара или услуги	Наименование заказчика, его адрес и контактная информация	Дата поставки	Примечание

Подписи:

Ф.И.О. руководителя

Ф.И.О. главного бухгалтера

Ф.И.О. юриста *(при наличии)*

Место печати (при наличии)

Форма №5 (к Приложению №1)

НА ФИРМЕННОМ БЛАНКЕ ОРГАНИЗАЦИИ

Техническое предложение на Конкурс_____
(Указать номер и предмет Конкурса)

№:
Дата: _____

Председателю Конкурсной комиссии

Уважаемые дамы и господа!

Изучив Конкурсную документацию на приобретение_____
(наименование товаров или услуг)
мы, _____ нижеподписавшиеся, предлагаем к поставке
(полное наименование Участника)
_____
(Указать наименование товаров или услуг)

Мы обязуемся, в случае выигрыша Конкурса, поставить_____
(наименование товаров или услуг)
по договору, который будет заключен с Заказчиком.

Мы согласны придерживаться положений настоящего предложения в течение 60 дней, начиная с даты, установленной как день окончания приема конкурсных предложений. Это конкурсное предложение будет оставаться для нас обязательным и может быть принято в любой момент до истечения указанного периода.

Приложения:
- таблица технических характеристик, предлагаемых_____
(наименование товаров или услуг)
на ___ листах;

Ф.И.О. и подпись руководителя

Ф.И.О. и подпись лица, на имя которого выдана доверенность

Место печати (при наличии)

Сравнительная таблица технических характеристик оборудования

№	Наименование параметра	Показатель, согласно требованиям технического задания	Показатель, согласно предложению участника	Примечание соответствует/ не соответствует)
1				
2				

Перечень предоставляемых подписок и лицензии:

Наличие Технической поддержки производителя:

Ф.И.О. и подпись руководителя или уполномоченного лица участника

Место печати

Форма №6 (к Приложению №2)

НА ФИРМЕННОМ БЛАНКЕ ОРГАНИЗАЦИИ

КОММЕРЧЕСКОЕ ПРЕДЛОЖЕНИЕ

на поставку _____

(указать наименование товаров или услуг)

Изучив Конкурсную документацию на _____, мы, нижеподписавшиеся _____предлагаем

(полное наименование Участника)

поставить _____ в соответствии с условиями Конкурса.

(указать наименование товаров или услуг)

Согласно нашему предложению:

- условия оплаты _____
- сроки поставки _____
- Общая сумма поставки предлагаемых товаров _____

(цифрами и прописью, а также валюта платежа)

согласно прилагаемой таблице цен, которая является частью настоящего Конкурсного предложения.

Мы согласны придерживаться положений настоящего предложения в течение 50 дней, начиная с даты, установленной как день окончания приема Конкурсных предложений. Это Конкурсное предложение будет оставаться для нас обязательным и будет принято в любой момент до истечения указанного периода.

Мы понимаем, что Конкурсная комиссия не обязана принять наименьшее ценовое предложение, а примет наилучшее предложение по всем показателям и критериям оценки.

Мы обязуемся выполнить работы/оказать услуги/поставить товар в точном соответствии с условиями, предусмотренными контрактом/договором и действующим законодательством Республики Узбекистан.

В случае если наше предложение будет принято Банком, берем на себя обязательство заключить контракт/договор с АКБ «Asia Alliance Bank» в срок не позднее 5 дней с момента объявления победителя конкурса.

Ф.И.О. и подпись руководителя

Ф.И.О. и подпись лица, на имя которого выдана доверенность

Место печати (при наличии)

Разбивка стоимости предложения:

Предмет поставки	Стоимость
Внедрение в инфраструктуру Банка систем мониторинга и управления информацией и событиями информационной безопасности (SIEM), также предоставление сервисной поддержки производителя (12 месяцев) и гарантии на выполненные работы (12 месяцев) со сроком подписки (Subscription) на лицензии 12 месяцев.	
Внедрение в инфраструктуру Банка систем автоматизации реагирования на инциденты информационной безопасности (SOAR), также предоставление сервисной поддержки производителя (12 месяцев) и гарантии на выполненные работы (12 месяцев) со сроком подписки (Subscription) на лицензии 12 месяцев.	
Услуги по обучению и внедрению систем SIEM и SOAR, включая техническую поддержку сроком на 12 месяцев.	
ИТОГОВАЯ СУММА ПРЕДЛОЖЕНИЯ	

Приложение №3 к Конкурсной документации

ПРОЕКТ ДОГОВОРОВ

Проект договора не является окончательным, в него могут быть внесены изменения, дополнения в процессе переговоров

ДОГОВОР № _____

Проект договора не является окончательным, в него могут быть внесены изменения, дополнения в процессе переговоров

г. Ташкент «____» _____ 2026 г.

АКБ «ASIA ALLIANCE BANK», именуемый в дальнейшем **«Заказчик»,** в лице _____ действующего на основан_____ , с одной стороны, и _____ именуемый в дальнейшем **«Исполнитель»,** в лице _____, действующего на основани_____ с другой стороны, при совместном упоминании именуемые «Стороны», заключили настоящий договор (далее - Договор) о нижеследующем:

1. Предмет Договора

1.1. «Исполнитель» принимает обязательства поставить в адрес «Заказчика», а «Заказчик» оплатить продукцию в соответствии с условиями и положениями договора в количестве, по ценам и техническим требованиям, указанным в приложении №1 (спецификация), являющемся неотъемлемой частью настоящего Договора.

1.2. «Исполнитель», по согласованию Заказчика, имеет право досрочно или частями отгрузить продукцию.

1.3. Качество поставляемой продукции должно соответствовать требованиям нормативных документов по стандартизации (ГОСТ, O'zDSt, Ts и т.п.), техническим требованиям «Покупателя», эталону-образцу, утвержденному сторонами и иметь, а также другим нормам и правилам, установленным для поставляемой продукции в Республике Узбекистан.

2. Стоимость Договора и условия оплаты

2.1. Общая стоимость настоящего Договора составляет _ (_) долларов США/узбекских сум с учетом НДС;

2.2. Оплата по настоящему Договору осуществляется прямым банковским переводом, следующим образом: _____.

2.3 Основанием для проведения последующей оплаты являются следующие документы:

- счет-фактура, подписанные между «Заказчиком» и «Исполнителем».

3. Условия и сроки поставки

3.1. Срок поставки продукции указан в спецификации (приложение №1), в течение которого «Исполнитель» обязан своими силами и средствами поставить продукцию до склада «Заказчика», находящегося по адресу:

_____

3.2. Дата поставки считается на день поступления продукции в адрес «Заказчика».

4. Порядок сдачи-приемки

4.1. Право собственности на продукцию переходит к «Заказчику» в момент фактической передачи, после составления и подписания счета-фактуры, подписанных уполномоченными лицами.

4.2. Приемка продукции по качеству и количеству осуществляется в соответствии с требованиями нормативных документов по стандартизации (ГОСТ, O'zDSt, Ts и т.п.), а также других нормативных документов, действующих на момент поставки продукции. Поставляемая продукция по размерно-ростовочным данным должна соответствовать требованиям «Покупателя».

5. Имущественная ответственность сторон и качество продукции

5.1. В случае просрочки поставки, недопоставки продукции «Исполнитель» уплачивает «Заказчику» пеню в размере 0,1% от неисполненной части обязательства за каждый день просрочки (за исключением праздничных и выходных дней), но при этом общая сумма пени не должна превышать 20% стоимости недопоставленной продукции.

5.2. При несвоевременной оплате поставленной продукции «Заказчик» уплачивает «Исполнителю» пеню в размере 0,1% от суммы просроченного платежа за каждый банковский день просрочки, но не более 20% суммы просроченного платежа.

5.3. Если поставленная продукция не соответствует требованиям, изложенным в спецификации (приложении №1) к настоящему Договору и требованиям, указанным в пункте 1.3. настоящего договора, «Заказчик» вправе:

- отказаться от принятия и оплаты продукции; -

- если продукция оплачена, потребовать замены продукции на качественную или возврата уплаченной суммы, а также взыскать с «Продавца» штраф в размере 20 % от стоимости продукции ненадлежащего качества.

5.4. Уплата штрафа и пени, в случае ненадлежащего исполнения обязательств, не освобождает стороны от исполнения обязательств по договору.

5.5. «Исполнитель», согласно действующему законодательству Республики Узбекистан, предоставляет на товары гарантийные сроки (эксплуатации), согласно спецификации (приложение №1).

6. Рекламации

6.1. Рекламации могут быть заявлены по качеству поставленной продукции в случае несоответствия её требованиям нормативных документов стандартизации (ГОСТ, O'zDSt, Ts и т.п.), техническим требованиям «Покупателя» и эталону-образцу, утвержденному сторонами, а также техническим характеристикам, описанным в технической документации производителя.

6.2. «Заказчик» имеет право заявить «Исполнителю» рекламацию по качеству продукции в течение гарантийного срока носки (эксплуатации).

6.2.1. В случае, если в течение установленного гарантийного срока при соблюдении условий эксплуатации продукция станет непригодной к дальнейшему использованию или не будет соответствовать требованиям качества, «Исполнитель» обязуется за свой счет произвести:

полную замену продукции, вышедшей из строя при эксплуатации в первой половине гарантийного срока;

произвести полный ремонт и привести в качественное состояние, в соответствии с предъявляемыми требованиями, продукцию, вышедшую из строя при эксплуатации во второй половине гарантийного срока.

6.2.2. При выявлении некачественной продукции или продукции, не выдержавшей гарантийного срока носки (эксплуатации), представитель «Заказчика» должен письменно известить «Исполнителя» доступным видом связи (по факсу или иными способами) о назначении даты оформления совместного акта рекламации. Дата совместного оформления рекламационного акта должна быть назначена на срок, не более чем 10 дней с момента письменного извещения «Исполнителя».

В извещении должно быть указано:

наименование и количество изделий, подлежащих совместной проверке, номер, дата и условное наименование отправителя;

основные недостатки, выявленные по качеству изделия;

срок нахождения в эксплуатации;

срок и место прибытия представителя «Исполнителя» (с учетом времени на проезд).

6.2.3. При неявке представителя «Исполнителя» по вызову представителя «Заказчика» в установленный срок, проверка и оформление производятся при участии независимой экспертизы или представителя независимой организации по выбору «Исполнителя» или в одностороннем порядке.

6.2.4. В одностороннем порядке представитель «Заказчика» имеет право произвести проверку и составить акт рекламации также в следующих случаях:

при неявке представителя «Исполнителя» в назначенный срок;

при оставлении извещения без ответа;

при отсутствии независимой организации, а также при отказе выделить представителей или неявке представителей вышеуказанных организаций.

В таком случае акт рекламации считается принятым к исполнению.

6.3. В случае обнаружения при приемке «Заказчиком» несоответствия количества или качества поставляемой продукции, «Исполнитель» обязан за свой счет поставить недостающую продукцию или заменить продукцию ненадлежащего качества в течение 15 (пятнадцати) банковских дней.

7. Решение споров

7.1. Все споры и разногласия между «Заказчиком» и «Исполнителем» в связи с настоящим договором должны разрешаться сторонами путем переговоров. Если сторонам не удается достичь соглашения, все споры и разногласия, возникшие из данного договора или в связи с ним, должны рассматриваться Ташкентским межрайонным Экономическим судом в соответствии с порядком, предусмотренным действующим законодательством Республики Узбекистан.

8. Форс-мажор

8.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему договору, если оно явилось следствием пожара, наводнения, эпидемий, пандемии, землетрясения, войны, блокады и других общепризнанных обстоятельств непреодолимой силы, издания актов государственных органов. При наступлении форс-мажорных обстоятельств стороны обязаны проинформировать друг друга о наступлении подобных обстоятельств в письменной форме с предоставлением документов, удостоверяющих эти обстоятельства, выданных соответствующими органами.

8.2. В случае продления форс-мажорных обстоятельств на срок более 2 (двух) месяцев полученная предоплата (за исключением исполненных сторонами обязательств) по настоящему договору в течение 10 (десяти) банковских дней подлежит возврату.

9. Антикоррупционная оговорка

9.1. При исполнении своих обязательств по настоящему Договору. Стороны, их аффилированные лица, работники или посредники обязуются не осуществлять, прямо или косвенно, действий, квалифицируемых как дача/получение взятки, коммерческий подкуп, злоупотребление должностным положением, а также действий, нарушающих требования законодательства Республики Узбекистан, международных норм права и международных договоров Республики Узбекистан о противодействии легализации (отмыванию) доходов, полученных преступным путём, и иные коррупционные нарушения — как в отношениях между сторонами Договора, так и в отношениях с третьими лицами и государственными органами. Стороны также обязуются довести это требование до их аффилированных (взаимосвязанных) лиц, работников, уполномоченных представителей и посредников.

9.2. Каждая из сторон Договора, их аффилированные (взаимосвязанные) лица, работники и посредники отказываются от стимулирования каким-либо образом работников или уполномоченных представителей другой стороны, в том числе путем предоставления денежных сумм, подарков, безвозмездного оказания в их адрес услуг или выполнения работ, направленных на обеспечение выполнения этим работником или уполномоченным представителем каких-либо действий в пользу стимулирующей его стороны.

9.3. Под действием работника, осуществляемыми в пользу стимулирующей его стороны понимаются, в том числе:

a) предоставление неоправданных преимуществ по сравнению с другими контрагентами;

b) предоставление каких-либо гарантий;

c) ускорение существующих процедур;

d) иные действия, выполняемые работником в рамках своих должностных обязанностей, но не соответствующие принципам прозрачности и открытости взаимоотношений между сторонами.

9.4. В случае возникновения у Стороны оснований полагать, что произошло или может произойти нарушение другой Стороной, ее аффилированными (взаимосвязанными) лицами, работниками, уполномоченными представителями или посредниками каких-либо обязательств, предусмотренных данной статьей, , Сторона обязуется незамедлительно уведомить об этом другую Сторону в письменной форме и по адресу электронной почты, указанной в Договоре. В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что такое нарушение произошло или может произойти.

9.5. Сторона, получившая уведомление о нарушении каких-либо положений настоящей статьи, обязана рассмотреть уведомление и сообщить другой стороне об итогах его рассмотрения в течение 10 (десяти) рабочих дней с даты получения письменного уведомления.

9.6. Стороны гарантируют осуществление надлежащего разбирательства по фактам нарушения положений настоящей статьи оговорки с соблюдением принципов конфиденциальности и применение эффективных мер по предотвращению возможных конфликтных ситуаций. Стороны гарантируют отсутствие негативных последствий как для уведомившей стороны в целом, так и для конкретных работников уведомившей стороны, сообщивших о факте нарушений.

9.7. В случае подтверждения факта нарушения одной стороной положений настоящей статьи и/или неполучения другой стороной информации об итогах рассмотрения уведомления о нарушении, другая сторона имеет право расторгнуть настоящий Договор в одностороннем внесудебном порядке путем направления

‘-письменного уведомления не позднее чем за 30 (тридцать) календарных дней до даты прекращения действия настоящего Договора.

10. Порядок изменения и расторжения договора

10.1. Любые изменения и дополнения к настоящему договору являются действительными лишь при условии выполнения их в письменном виде и подписания уполномоченными лицами «Заказчика» и «Исполнителя».

10.2. Стороны имеют право одностороннего расторжения договора в следующих случаях:

- при невыполнении договора со стороны «Исполнителя» в течение срока действия настоящего договора;
- при однократном нарушении условий настоящего договора или несоответствии качества поставляемой продукции Исполнителем по договорным обязательствам.

10.3. Сторона, у которой возникло право на расторжение договора, обязана уведомить другую сторону о своем намерении письменно не менее чем за 30 дней до предполагаемой даты расторжения настоящего Договора.

11. Прочие условия

11.1. Ни одна из сторон не может передавать свои права или обязанности по данному договору какой-либо третьей стороне без письменного согласия другой стороны.

11.2. В случае изменения наименования платежных или иных реквизитов сторон, другая сторона незамедлительно должна быть об этом информирована в письменной форме.

11.3. Договор, включая приложение, составлен на 6 (шести) листах, в 2 (двух) экземплярах, идентичных по содержанию и имеющих одинаковую юридическую силу, скреплен подписями и печатями сторон.

11.4. В соответствии с действующим законодательством Республики Узбекистан Стороны признают соблюдение требований законодательства о конфиденциальности информации в отношении настоящего Договора, а также и иной информации (банковская тайна, коммерческая тайна), ставшей ему известной в ходе заключения и исполнения настоящего договора.

12. Юридические адреса, реквизиты Сторон:

Заказчик:
Адрес: Республика[1]Узбекистан, 100047
г. Ташкент, ул. Махтумкули 2А.
Код банка: 01095
Р/с: 29802840800001095002
SWIFT: ASACUZ22
ИНН 207018693
ОКПО 22921172
Тел: +998712316000

Руководитель

_____ _____

Исполнитель:
_____
_____
_____
_____

Руководитель

_____ _____

Приложение №1 к Договору №

Спецификация

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На поставку, установку и запуск в эксплуатацию
Системы управления информацией и событиями безопасности (SIEM) и автоматизации реагирования (SOAR)

1. ОБЩИЕ СВЕДЕНИЯ

Настоящее Техническое задание определяет требования Заказчика к Системе управления информацией и событиями информационной безопасности (SIEM) и системе автоматизации реагирования на инциденты информационной безопасности (SOAR) (далее — Система).

Техническое задание предназначено для подготовки и проведения тендера (конкурса) на поставку программного обеспечения, выполнение комплекса работ по внедрению и оказанию сопутствующих услуг по принципу «под ключ».

1.1. Наименование выполняемых работ и оказываемых услуг

Полное наименование проекта: «Внедрение системы управления информацией и событиями информационной безопасности (SIEM) и системы автоматизации реагирования на инциденты информационной безопасности (SOAR)».

Все работы выполняются на территории и в инфраструктуре Заказчика.

В рамках настоящего Технического задания Исполнитель обязан предоставить коммерческое предложение, предусматривающее:

- поставку программного обеспечения SIEM/SOAR;
- установку и настройку программного обеспечения;
- внедрение Системы;
- проведение интеграционных работ;
- ввод Системы в промышленную эксплуатацию.

1.2. Цели использования выполняемых работ и оказываемых услуг

Основной целью реализации проекта является внедрение в инфраструктуре Банка Системы мониторинга и управления событиями информационной безопасности (SIEM), а также Системы автоматизации реагирования на инциденты информационной безопасности (SOAR) для обеспечения функционирования Центра мониторинга кибербезопасности (SOC).

Внедряемая Система должна обеспечивать решение следующих основных задач:

- централизованный сбор, обработку и хранение событий информационной безопасности;
- непрерывный мониторинг ИТ- и сетевой инфраструктуры;
- выявление инцидентов информационной безопасности;
- анализ, расследование и сопровождение инцидентов;
- формирование единой картины состояния информационной безопасности;
- поддержку процессов реагирования на инциденты;
- автоматизацию и оркестрацию процессов реагирования на инциденты информационной безопасности;
- автоматическое обогащение инцидентов данными из внутренних и внешних источников;
- сокращение времени выявления, расследования и реагирования за счет использования сценариев Playbook и Runbook;
- подготовку аналитических материалов, отчетности и статистики;

- контроль соблюдения требований информационной безопасности и нормативных документов.

Основным назначением Системы является централизованный сбор, обработка, хранение, анализ и корреляция событий информационной безопасности, а также оркестрация и автоматизация процессов реагирования, обеспечивающих своевременное выявление, расследование, эскалацию и устранение инцидентов информационной безопасности, возникающих в инфраструктуре банка.

2. ПЕРЕЧЕНЬ РАБОТ, УСЛУГ И ИХ ОБЪЕМ

Внедрение Системы SIEM/SOAR должно осуществляться Исполнителем совместно с ответственными представителями Заказчика без нарушения работоспособности действующей ИТ-инфраструктуры.

До начала внедрения Исполнитель обязан провести предварительное обследование существующей ИТ-инфраструктуры, включая поверхностное обследование веб-ресурсов и веб-приложений Заказчика.

Все работы, выполнение которых требует временной остановки корпоративных информационных систем, должны предварительно согласовываться с Заказчиком.

В рамках реализации проекта Исполнитель обязан выполнить следующие этапы работ:

- подготовительный этап;
- пуско-наладочные работы;
- интеграционные работы.

2.1. Подготовительный этап

Подготовительный этап предусматривает совместную работу специалистов Исполнителя и представителей Заказчика по обследованию существующей ИТ-инфраструктуры.

По результатам обследования должны быть определены:

- особенности топологии сети Заказчика;
- зоны ответственности Заказчика и Исполнителя при реализации проекта;
- перечень и количество информационных ресурсов, подлежащих мониторингу средствами Системы.

2.2. Пуско-наладочные и интеграционные работы

Совместно с ответственными специалистами Заказчика Исполнитель обязан выполнить следующие работы:

- установку программных компонентов Системы;
- настройку программных компонентов;
- интеграцию Системы в существующую сетевую инфраструктуру;
- активацию необходимых функциональных модулей;
- активацию лицензий.

Кроме того, Исполнитель обязан обеспечить:

- развертывание и базовую настройку компонента SOAR для автоматизации и оркестрации процессов реагирования;

- интеграцию Системы с Core Banking System, Service Desk/ITSM, Active Directory/LDAP, XDR (EDR/NDR), DLP, сканерами уязвимостей, межсетевыми экранами, антивирусными средствами защиты, PAM, DAM, WAF, средствами защиты рабочих станций и серверов, сетевыми средствами защиты, почтовыми шлюзами, а также иными информационными системами Заказчика в соответствии с согласованным перечнем;
- настройку не менее десяти (10) базовых сценариев автоматизации (Playbook/Runbook), предусматривающих реагирование на следующие события:
    - компрометация учетной записи;
    - атаки типа Brute Force;
    - обнаружение вредоносного программного обеспечения;
    - подозрительная активность привилегированных пользователей;
    - утечка информации;
    - нарушение требований и политик информационной безопасности;
- проверку корректности выполнения сценариев автоматизации по результатам срабатывания правил корреляции, формирования оповещений и ручного запуска аналитиком SOC.

В случае выявления ошибок в работе Системы, не связанных с функционированием ИТ-инфраструктуры Заказчика, Исполнитель обязан устранить выявленные недостатки до подписания Акта выполненных работ.

2.3. Порядок контроля и приемки Системы

Приемка Системы осуществляется посредством проведения приемочных испытаний с участием представителей Заказчика и Исполнителя.

Целью приемочных испытаний является подтверждение работоспособности Системы и соответствия ее функциональных возможностей требованиям настоящего Технического задания.

Виды, состав, объем и методика проведения приемочных испытаний определяются Программой приемочных испытаний, разрабатываемой Исполнителем и предоставляемой Заказчику на согласование не позднее чем за один рабочий день до начала испытаний.

По результатам проведения испытаний оформляется Протокол приемочных испытаний, подписываемый членами приемочной комиссии.

При успешном завершении приемочных испытаний стороны подписывают Акт завершения приемочных испытаний.

В случае выявления недостатков, дефектов либо иных несоответствий требованиям настоящего Технического задания в Протоколе приемочных испытаний должны быть отражены:

- перечень выявленных недостатков;
- степень их влияния на работоспособность Системы;
- сроки устранения выявленных недостатков.

После устранения замечаний Исполнитель уведомляет Заказчика о готовности к повторным испытаниям.

Повторные приемочные испытания проводятся в течение пяти рабочих дней после устранения выявленных недостатков.

При успешном прохождении повторных испытаний Система принимается в промышленную эксплуатацию.

2.4. Обучение персонала

Обучение специалистов Заказчика осуществляется Исполнителем в соответствии с требованиями раздела 8 настоящего Технического задания.

3. МЕСТО ВЫПОЛНЕНИЯ РАБОТ И ОКАЗАНИЯ УСЛУГ

Исполнитель обязан выполнить поставку, установку, настройку и ввод в эксплуатацию программного обеспечения по адресу:

Срок поставки, внедрения и ввода Системы в эксплуатацию определяется договором, заключенным между Заказчиком и Исполнителем, и не должен превышать **60 (шестидесяти) календарных дней** с даты подписания договора.

4. ТРЕБОВАНИЯ

4.1. Общие требования

4.1.1 Предлагаемое решение должно относиться к классу систем **Security Information and Event Management (SIEM)** и **Security Orchestration, Automation and Response (SOAR)** и обеспечивать централизованный сбор, хранение, обработку, индексирование, поиск, корреляцию и анализ событий информационной безопасности и ИТ-инфраструктуры.

4.1.2 Система должна предоставлять единый пользовательский интерфейс и единое хранилище данных для выполнения задач управления журналами событий, мониторинга информационной безопасности, расследования инцидентов, формирования отчетности, визуализации данных и администрирования.

4.1.3 Система должна обеспечивать хранение событий в исходном либо максимально приближенном к исходному виде без обязательной предварительной нормализации, агрегации либо приведения данных к фиксированной схеме.

4.1.4 Система должна поддерживать модель хранения и поиска данных без жестко заданной реляционной структуры и обеспечивать обработку разнородных машинных данных, поступающих из различных источников, представленных в человекочитаемом формате.

4.1.5 Предлагаемое решение должно иметь подтвержденный опыт промышленной эксплуатации у крупных корпоративных заказчиков, а также развитую экосистему технической документации, профессиональных сервисов, обучения, технической поддержки и партнерской сети.

4.1.6 Модель лицензирования должна быть прозрачной и обеспечивать возможность масштабирования по объему обрабатываемых (индексируемых) данных и (или) функциональным модулям без необходимости изменения архитектуры решения.

4.2. Требования к архитектуре и масштабируемости

4.2.1 Предлагаемое решение должно являться программным продуктом и не должно требовать обязательного использования специализированных аппаратных комплексов производителя.

4.2.2 Система должна поддерживать развертывание в физической инфраструктуре, виртуальной среде, частном и публичном облаке, а также в гибридной модели эксплуатации.

4.2.3 Архитектура Системы должна поддерживать распределенное развертывание для центральной и удаленных площадок, включая централизованный сбор, буферизацию, передачу и обработку данных.

4.2.4 Архитектура должна обеспечивать возможность горизонтального масштабирования

компонентов сбора, индексирования, хранения и поиска данных без необходимости полной переустановки Системы.

4.2.5 Система должна обеспечивать распределенный поиск по нескольким узлам хранения и индексирования, а также поддерживать параллельную обработку поисковых запросов.

4.2.6 Система должна обеспечивать возможность размещения различных типов данных в отдельных логических индексах (хранилищах) для повышения производительности поиска, разграничения доступа и управления сроками хранения информации.

4.2.7 Решение должно обеспечивать обработку значительных объемов машинных данных и иметь документально подтвержденную возможность масштабирования до десятков терабайт данных в сутки при условии соответствующего проектирования инфраструктуры.

4.3. Требования к сбору, приему и интеграции данных

4.3.1 Система должна обеспечивать сбор данных посредством протоколов Syslog**,** TCP/UDP, защищенных каналов TLS/SSL**,** агентского программного обеспечения, REST API**,** WMI**,** SNMP Events, файлов журналов, форматов JSON**,** XML**,** CSV**,** баз данных, скриптовых механизмов и иных модульных источников данных.

4.3.2 Агентское программное обеспечение должно обеспечивать шифрование передаваемых данных, локальное кэширование при недоступности центральных компонентов, балансировку нагрузки между принимающими узлами и передачу данных по надежному транспортному протоколу.

4.3.3 Система должна поддерживать как агентский, так и безагентный способы сбора данных, включая прямое получение журналов по сети, прием данных от существующих Syslog-серверов и интеграцию посредством API.

4.3.4 Система должна обеспечивать индексирование многострочных и сложных событий без потери их структуры и исходной временной метки.

4.3.5 Система не должна требовать обязательного предварительного создания фиксированной схемы таблиц до начала приема и анализа событий.

4.3.6 Система должна обеспечивать прием, индексирование и хранение исходных неизмененных машинных данных, поступающих из любых источников, без обязательного предварительного преобразования в фиксированную реляционную модель данных.

4.3.7 Система должна корректно обрабатывать временные метки, поступающие из различных часовых поясов, с сохранением как исходного времени события, так и времени поступления события в Систему.

4.3.8 Система не должна зависеть исключительно от готовых коннекторов производителя. Должна быть обеспечена возможность подключения новых источников данных и адаптации к изменению форматов журналов без внесения изменений в исходный код продукта.

4.3.9 Система должна обеспечивать автоматический контроль доступности источников данных, контроль полноты поступающих событий, а также формирование уведомлений при прекращении поступления данных от критически важных источников.

4.3.10 Система должна поддерживать интеграцию с Active Directory/LDAP**,** системами аутентификации, межсетевыми экранами, IDS/IPS**,** WAF**,** VPN**,** EDR/XDR, антивирусными решениями, DLP, сканерами уязвимостей, почтовыми и веб-шлюзами, DNS/DHCP, сетевыми

устройствами, NetFlow/IPFIX, операционными системами, системами управления базами данных, платформами виртуализации, облачными сервисами, бизнес-приложениями, Service Desk/ITSM**,** CMDB**,** а также иными информационными системами Заказчика.

4.4. Требования к хранению, индексированию и жизненному циклу данных

4.4.1 Система должна обеспечивать индексирование исходных неизмененных машинных данных с возможностью последующего поиска, расследования инцидентов и формирования отчетности на их основе.

4.4.2 Система должна поддерживать автоматическое сжатие индексированных данных с целью оптимизации использования дискового пространства.

4.4.3 Система должна обеспечивать хранение оперативных, «теплых» и архивных данных с возможностью гибкой настройки сроков хранения в зависимости от типа источника, индекса, уровня критичности и требований нормативного соответствия (Compliance).

4.4.4 Система должна поддерживать управление жизненным циклом данных, включая автоматическое перемещение данных на менее производительные или внешние хранилища, архивирование и удаление данных в соответствии с политиками Заказчика.

4.4.5 Система должна поддерживать репликацию данных и индексов для обеспечения высокой доступности, сохранности информации, отказоустойчивости и повышения производительности поисковых операций.

4.4.6 Должна быть обеспечена возможность масштабирования подсистемы хранения данных без остановки функционирования Системы.

4.4.7 Система должна обеспечивать защиту журналов событий и аудиторских данных от несанкционированного изменения или удаления, включая применение механизмов контроля целостности информации.

4.5. Требования к нормализации, обогащению и контексту

4.5.1 Система должна поддерживать нормализацию событий к унифицированной модели данных для типовых сценариев информационной безопасности, при этом исходные («сырые») данные должны оставаться доступными для поиска, анализа и расследования инцидентов.

4.5.2 Изменение логики извлечения полей, справочников, правил нормализации или обогащения не должно требовать обязательной повторной загрузки ранее сохраненных событий.

4.5.3 Система должна поддерживать категоризацию событий и их обогащение дополнительными контекстными данными, включая справочники, списки активов, сведения о пользователях, данные CMDB, внешние и внутренние источники Threat Intelligence, IOC, Geo-IP и иные справочные источники.

4.5.4 Система должна поддерживать интеграцию с корпоративными службами каталогов для получения атрибутов пользователей, включая логин, Ф.И.О., подразделение, должность, руководителя, контактный телефон, местоположение, признак привилегированного пользователя, даты начала и окончания трудовой деятельности, а также иные необходимые атрибуты.

4.5.5 Система должна обеспечивать возможность корреляции нескольких учетных записей (логинов), принадлежащих одному сотруднику или иному субъекту.

4.5.6 Система должна поддерживать интеграцию с CMDB и иными базами данных активов для получения сведений об устройствах, включая имя узла (Hostname), IP-адрес, MAC-адрес, местоположение, владельца, уровень критичности, наличие чувствительных данных, соответствие регуляторным требованиям и иные атрибуты.

4.5.7 Система должна обеспечивать возможность применения новых справочников и контекстных данных к ранее проиндексированным событиям для выполнения поиска и формирования отчетности за исторические периоды.

4.5.8 Система должна поддерживать подход Schema-on-Read, при котором исходные события сохраняются в полном объеме, а извлечение полей, нормализация, обогащение и интерпретация данных могут выполняться на этапе поиска и анализа без необходимости изменения структуры ранее сохраненных данных.

4.5.9 Изменение логики извлечения полей, нормализации, справочников, источников Threat Intelligence или правил обогащения не должно требовать обязательной переиндексации либо повторной загрузки ранее сохраненных исторических данных.

4.5.10 Система должна поддерживать ведение и использование справочников активов и идентификационных данных пользователей для обогащения событий информационной безопасности, корреляции, приоритизации и расследования инцидентов.

4.5.11 Для активов должна поддерживаться возможность хранения и использования IP-адресов, DNS-имен, MAC-адресов, сведений о владельцах, местоположении, уровне критичности, принадлежности к сегментам сети, признаках соответствия требованиям информационной безопасности, а также иных атрибутов, согласованных с Заказчиком.

4.5.12 Для пользователей должна поддерживаться возможность хранения и использования логинов, адресов электронной почты, Ф.И.О., подразделений, должностей, руководителей, признаков привилегированности, статуса учетной записи и иных атрибутов, получаемых из корпоративных служб каталогов либо справочников.

4.5.13 Система должна поддерживать централизованное подключение, хранение и использование внутренних и внешних источников Threat Intelligence, включая IOC по IP-адресам, доменным именам, URL-адресам, hash-значениям, адресам электронной почты, именам файлов и иным индикаторам компрометации.

4.5.14 При добавлении новых индикаторов компрометации (IOC) Система должна обеспечивать возможность выполнения ретроспективного поиска совпадений по историческим данным за выбранный период хранения без необходимости повторной загрузки исходных событий.

4.6. Требования к поиску, аналитике и корреляции

4.6.1 Система должна поддерживать интерактивный полнотекстовый поиск по любому полю индексированных данных с использованием ключевых слов, временных интервалов, логических операторов, регулярных выражений и подстановочных символов.

4.6.2 Система должна поддерживать выполнение поисковых запросов в режиме реального времени, выполнение запланированных поисковых запросов, а также параллельное выполнение нескольких поисковых операций.

4.6.3 Система должна обеспечивать возможность выполнения поиска, расследования, корреляции и формирования отчетности непосредственно по исходным индексированным событиям без необходимости предварительной нормализации или загрузки данных в отдельную SQL-базу данных.

4.6.4 Система должна поддерживать механизм, при котором исходные события сохраняются в полном объеме, а извлечение полей, нормализация, обогащение и интерпретация данных могут

выполняться как на этапе приема данных, так и на этапе поиска и анализа ранее сохраненной информации.

4.6.5 Система должна обеспечивать возможность сохранения, редактирования, повторного использования и передачи поисковых запросов другим пользователям с учетом ролевой модели доступа.

4.6.6 Система должна поддерживать статистический анализ данных, включая подсчет количества событий, определение уникальных значений, вычисление суммы, минимального, максимального и среднего значения, медианы, моды, стандартного отклонения, дисперсии, процентилей, а также определение первого и последнего появления значения.

4.6.7 Система должна поддерживать выявление редких и аномальных значений, построение базовых моделей поведения и обнаружение отклонений, включая сценарии выявления неизвестных угроз и APT без жесткой зависимости от сигнатур.

4.6.8 Система должна поддерживать корреляцию событий на основе временных, логических, поведенческих и статистических правил, включая выявление многоэтапных сценариев атак.

4.6.9 Система должна поддерживать использование моделей Cyber Kill Chain**,** MITRE ATT&CK**,** NIST**,** PCI DSS, а также обеспечивать возможность создания собственных моделей, фреймворков и контролей для классификации и описания сценариев обнаружения угроз.

4.6.10 Система должна обеспечивать возможность создания собственных правил корреляции, внесения изменений в существующие правила, а также их тестирования до ввода в промышленную эксплуатацию.

4.6.11 Система должна предоставлять преднастроенный контент SIEM, включающий правила корреляции, панели мониторинга (дашборды), отчеты, модели данных, сценарии расследования и шаблоны мониторинга информационной безопасности с возможностью их адаптации под инфраструктуру Заказчика.

4.6.12 Система должна предоставлять единый поисково-аналитический язык для выполнения полнотекстового поиска, фильтрации, агрегации данных, статистического анализа, корреляции событий, формирования отчетности, выявления аномалий и расследования инцидентов.

4.6.13 Поисково-аналитический язык должен обеспечивать возможность определения первого и последнего появления события, пользователя, IP-адреса, узла (Host), процесса, доменного имени либо иного значения за заданный период времени.

4.6.14 Унифицированная модель данных должна охватывать как минимум следующие домены: аутентификация, сетевой трафик, сетевые сессии, DNS, Web, электронная почта (Email), действия пользователей, изменения конфигураций, конечные устройства, вредоносная активность, уязвимости, облачная активность и события средств защиты информации.

4.6.15 Система должна поддерживать риск-ориентированный подход к выявлению угроз, при котором отдельные события формируют накопительный риск для пользователей, учетных записей, узлов, IP-адресов, приложений и иных объектов.

4.6.16 Система должна обеспечивать формирование риск-событий и накопление риск-рейтинга по различным объектам риска, включая пользователей, учетные записи, узлы, IP-адреса, приложения и иные сущности.

4.6.17 Система должна обеспечивать возможность формирования инцидента информационной безопасности не только на основании отдельного события, но и на основе накопленного риск-рейтинга, сформированного несколькими независимыми событиями за установленный период времени.

4.6.18 Система должна обеспечивать выявление угроз на основании совокупности нескольких низкоприоритетных событий, которые по отдельности не являются критическими, однако при накоплении в рамках одной сущности формируют инцидент информационной безопасности.

4.6.19 Система должна поддерживать настройку весовых коэффициентов риска, объектов риска, риск-событий, категорий риска и пороговых значений, используемых для формирования инцидентов.

4.7. Требования к мониторингу, оповещениям и расследованию инцидентов

4.7.1 Система должна обеспечивать мониторинг событий в режиме, максимально приближенном к реальному времени, а также формирование оповещений на основании результатов поисковых запросов, правил корреляции и аналитических сценариев.

4.7.2 Механизм формирования оповещений должен поддерживать настройку уровней приоритета, подавление повторных срабатываний, ограничение частоты формирования уведомлений и маршрутизацию ответственным группам.

4.7.3 Система должна поддерживать отправку уведомлений по электронной почте, посредством интеграции с внешними системами, через Webhook/API, запуск пользовательских скриптов, а также с использованием иных механизмов автоматизации.

4.7.4 Система должна предоставлять функциональные возможности для расследования инцидентов, включая ведение карточки (объекта) инцидента, привязку исходных событий и контекстной информации, ведение истории расследования, изменение статусов, добавление комментариев, назначение ответственных лиц и документирование результатов расследования.

4.7.5 Система должна обеспечивать возможность перехода от агрегированного события, панели мониторинга (дашборда) либо результата срабатывания правила корреляции к исходным событиям для проведения детального расследования инцидента.

4.8. Требования к SOAR, оркестрации и автоматизации реагирования

4.8.1 Компонент SOAR должен поддерживать развертывание в инфраструктуре Заказчика без обязательной зависимости от облачных сервисов производителя, с возможностью функционирования в изолированном либо ограниченно подключенном контуре при наличии локальных интеграций.

4.8.2 Решение SIEM и SOAR должно быть от одного производителя либо иметь нативную интеграцию без промежуточного интеграционного слоя, с единым механизмом аутентификации, обменом контекстом и поддержкой производителя.

4.8.3 Компонент SOAR должен обеспечивать двустороннюю интеграцию с SIEM, включая получение результатов корреляции и значимых событий, создание карточек инцидентов, запуск сценариев автоматизации, а также передачу статусов, результатов обогащения, комментариев и ссылок на расследование обратно в SIEM.

4.8.4 SOAR должен поддерживать объектную модель расследования, включающую инциденты (контейнеры), артефакты, наблюдаемые индикаторы (IP-адрес, URL, доменное имя, hash, адрес электронной почты, Hostname, пользователь), задачи, комментарии, вложения, историю действий и результаты выполнения автоматизированных операций.

4.8.5 SOAR должен предоставлять графический конструктор Playbook/Runbook, обеспечивающий создание, изменение, тестирование и повторное использование сценариев автоматизации без необходимости внесения изменений в исходный код продукта.

4.8.6 Должна поддерживаться возможность использования пользовательской логики и сценариев, включая Python либо функционально эквивалентные механизмы, для реализации нестандартных действий, проверок, преобразования данных и интеграции со сторонними системами.

4.8.7 SOAR должен обеспечивать интеграцию со следующими системами: SIEM, EDR/XDR, межсетевыми экранами (NGFW), WAF, VPN, IDS/IPS, DLP, DAM, FIM, PAM, FortiMail, FortiSandbox, антивирусными решениями, системами управления уязвимостями, SAST, DAST, SCA, Active Directory/LDAP, MFA, DNS/DHCP, Proxy, CMDB, ITSM/Service Desk, системами резервного копирования, системами мониторинга, Threat Intelligence Platform, Core Banking, Internet/Mobile Banking, Card Management System, а также иными корпоративными информационными системами Заказчика.

4.8.8 Должна быть обеспечена возможность создания и доработки собственных коннекторов и приложений с использованием открытого **API/SDK** производителя без необходимости ожидания выпуска готового коннектора производителем.

4.8.9 SOAR должен обеспечивать автоматическое обогащение инцидентов сведениями о пользователях, активах, критичности информационных систем, принадлежности IP-адресов (Geo-IP), репутации IP-адресов, доменных имен и URL, результатах проверки hash-значений, данных **Threat Intelligence**, **IOC** и иных справочных источников.

4.8.10 SOAR должен поддерживать выполнение автоматизированных действий реагирования, включая блокировку IP-адресов, URL, доменных имен и hash-значений на средствах защиты информации, изоляцию рабочих станций, отключение или блокировку учетных записей, сброс паролей, помещение сообщений электронной почты в карантин либо их удаление, создание или обновление заявок в **ITSM**, уведомление ответственных подразделений и эскалацию инцидентов.

4.8.11 Для критически важных действий реагирования должна поддерживаться модель **Human-in-the-Loop**, предусматривающая обязательное ручное подтверждение аналитиком или руководителем SOC перед выполнением действий, способных оказать влияние на бизнес-процессы.

4.8.12 SOAR должен поддерживать ручной, автоматический и условный запуск **Playbook/Runbook** в зависимости от типа инцидента, уровня критичности, источника события, категории угрозы, техники **MITRE ATT&CK**, значений артефактов и иных параметров.

4.8.13 SOAR должен обеспечивать управление задачами расследования, включая назначение ответственных лиц, контроль статусов, соблюдение **SLA**, управление приоритетами, ведение комментариев, фиксацию результатов выполнения задач, закрытие инцидентов и документирование итогового решения.

4.8.14 SOAR должен обеспечивать ведение полного журнала аудита действий пользователей, системных операций и автоматизированных шагов **Playbook/Runbook** с указанием времени выполнения, инициатора, входных параметров, результатов выполнения, возникших ошибок и изменений, внесенных во внешние системы.

4.8.15 SOAR должен поддерживать ролевую модель управления доступом для аналитиков, администраторов, руководителей SOC и аудиторов, включая разграничение доступа к инцидентам, Playbook, коннекторам, учетным данным интеграций и административным функциям.

4.8.16 SOAR должен обеспечивать безопасное хранение учетных данных интеграций, токенов, ключей API и иных секретов с разграничением прав доступа и ведением журнала их использования.

4.8.17 Должна поддерживаться версионность, импорт, экспорт, резервное копирование и перенос сценариев автоматизации, приложений (коннекторов) и конфигураций между тестовой и промышленной средами.

4.8.18 SOAR должен обеспечивать формирование отчетов и показателей эффективности реагирования, включая количество инцидентов по категориям, время первого реагирования, **MTTR**, количество выполненных автоматизированных действий, успешность выполнения Playbook, количество ошибок интеграции, долю автоматизированных операций и уровень нагрузки на аналитиков SOC.

4.8.19 В рамках внедрения должны быть реализованы базовые сценарии **SOAR** для обработки типовых инцидентов, включая:

- фишинговые сообщения электронной почты;
- подозрительные IP-адреса, доменные имена и URL;
- вредоносные hash-значения и файлы;
- подозрительную активность учетных записей;
- события, поступающие от **EDR/XDR** или антивирусных решений;
- сетевые события, полученные от **IDS/IPS**, **WAF** и **VPN**.

4.9. Требования к визуализации и отчетности

4.9.1 Система должна поддерживать построение интерактивных панелей мониторинга (дашбордов) и отчетов, включая таблицы, временные диаграммы, линейные, столбчатые, площадные, круговые и точечные графики, индикаторы состояния, а также географическую визуализацию по данным **IP/Geo-IP**.

4.9.2 Средства визуализации должны обеспечивать обновление информации в режиме, максимально приближенном к реальному времени, поддерживать механизм **Drill-down** от агрегированных показателей к исходным событиям, а также выделение аномалий и выбросов.

4.9.3 Система должна обеспечивать возможность создания отчетов и панелей мониторинга как техническими, так и нетехническими пользователями, включая визуальное редактирование панелей, настройку заголовков, легенд, осей координат и фильтров.

4.9.4 Система должна поддерживать автоматическое формирование отчетов по расписанию, а также экспорт и рассылку отчетов в распространенных форматах, включая **PDF**, **CSV**, **XLS/XLSX**, а также иных форматах, поддерживаемых поставляемым решением.

4.9.5 Система должна поддерживать формирование отчетов и панелей мониторинга для контроля соответствия требованиям информационной безопасности и нормативных документов, включая **ISO/IEC 27002**, **NIST**, **PCI DSS** и иные применимые стандарты.

4.10. Требования к безопасности, управлению доступом и аудиту

4.10.1 Система должна поддерживать гибкую ролевую модель управления доступом (**RBAC**) для пользователей и **API** с возможностью разграничения доступа к источникам данных, типам данных, временным диапазонам, отчетам, панелям мониторинга, поисковым запросам и административным функциям.

4.10.2 Система должна поддерживать интеграцию с **Active Directory/LDAP** и корпоративными системами единой аутентификации (**SSO**).

4.10.3 Передача данных между компонентами Системы должна осуществляться по защищенным каналам связи с использованием современных криптографических протоколов.

4.10.4 Система должна обеспечивать ведение полного аудита действий пользователей и администраторов, включая регистрацию входов в систему, выполнения поисковых запросов, просмотра отчетов, изменения конфигурации, управления пользователями, создания и изменения правил корреляции, а также иных значимых действий.

4.10.5 Аудиторские события должны содержать сведения о дате и времени выполнения действия, пользователе (субъекте), источнике события, выполненном действии и результате его выполнения.

4.10.6 Система должна поддерживать механизмы контроля целостности индексированных событий, включая использование хеширования, цифровой подписи событий либо функционально эквивалентных механизмов подтверждения их подлинности.

4.10.7 Система должна обеспечивать мониторинг собственного состояния, конфигурации, доступности компонентов и состояния системных сервисов с возможностью формирования уведомлений о возникновении сбоев.

4.11. Требования к открытости архитектуры и интеграции со сторонними системами

4.11.1 **Система должна предоставлять открытые интерфейсы** API **для доступа к индексированным данным, выполнения поисковых запросов, управления объектами конфигурации и интеграции с внешними информационными системами.**

4.11.2 **Желательна поддержка** SDK **либо библиотек для наиболее распространенных языков программирования, включая** Python**,** Java**,** JavaScript**,** C# **либо функционально эквивалентные средства разработки.**

4.11.3 **Все параметры конфигурации Системы должны быть доступны для управления посредством веб-интерфейса,** CLI **и (или) конфигурационных файлов.**

4.11.4 Система должна поддерживать интеграцию с внешними системами визуализации, **BI**, **ITSM**, **SOAR**, **CMDB**, платформами **Threat Intelligence**, системами мониторинга и иными корпоративными информационными системами Заказчика.

4.11.5 Система должна обеспечивать возможность передачи исходных, преобразованных или обогащенных событий во внешние системы по протоколам **Syslog TCP/UDP**, **Raw TCP**, посредством файлового обмена, **API** либо иных поддерживаемых механизмов.

4.11.6 Система должна поддерживать использование публичных и (или) предоставляемых производителем приложений, пакетов интеграции и коннекторов для наиболее распространенных программных продуктов и сценариев информационной безопасности.

4.11.7 Для компонента **SOAR** должна поддерживаться интеграция посредством **REST API/Webhook**, включая возможность вызова внешних API, приема входящих событий, запуска автоматизированных действий и передачи результатов во внешние информационные системы.

4.11.8 Решение должно обеспечивать возможность дальнейшего развития библиотеки интеграций и сценариев реагирования без необходимости миграции на отдельную платформу и без изменения архитектурного подхода **SIEM/SOAR**.

4.11.9 Система должна поддерживать расширенную настройку отчетов, панелей мониторинга, поисковых объектов и интеграционного контента посредством интерфейса администратора и (или) конфигурационных файлов.

4.11.10 Не допускается необходимость повторного сбора либо дублирования хранения одних и тех же событий для реализации различных сценариев анализа в рамках единой платформы.

4.12. Требования к отказоустойчивости и режимам функционирования

4.12.1 Система должна поддерживать резервирование ключевых компонентов, кластеризацию, репликацию критически важных данных и исключать наличие единой точки отказа при построении целевой архитектуры по схеме N+1**.**

4.12.2 Система должна обеспечивать автоматическое восстановление работоспособности либо наличие документированной процедуры восстановления после отказа отдельных компонентов.

4.12.3 Основным режимом функционирования Системы должен являться непрерывный круглосуточный режим работы в автоматизированном режиме под управлением администратора.

4.12.4 Система должна поддерживать штатный, сервисный и автономный режимы функционирования, включая возможность локальной буферизации данных при временной недоступности центральных компонентов.

4.13. Требования к производительности и пропускной способности

Поставляемое решение должно соответствовать следующим требованиям:

№	Показатель	Требуемое значение
1.	Средняя производительность по приему событий (EPS)	не менее 80 000 EPS либо эквивалентный объем данных, рассчитанный по среднему размеру события
2.	Пиковая производительность по приему событий	не менее 150 000 EPS
3.	Возможность кратковременного burst-нагрузки	до 250 000 EPS без потери событий при корректно рассчитанной архитектуре и буферизации
4.	Суточный объем индексируемых данных	не менее 100 ГБ/сутки /250 серверов (без учета ПК 1000) с возможностью дальнейшего увеличения без смены платформы
5.	Объем хранения «горячих» данных (оперативный доступ)	не менее 180 суток
6.	Объем хранения «тёплых» данных	не менее 12 месяцев
7.	Общий срок хранения архивных данных	не менее 3 лет
8.	Максимальная задержка обработки события до оповещения	не более 3 секунд для критичных корреляционных сценариев при штатной нагрузке
9.	Потери событий при штатной нагрузке	0% при корректной настройке источников и каналов передачи
10.	Количество одновременно подключенных источников	не менее 2 000
11.	Поддержка распределённых коллекторов/агентов	не менее 10 удалённых площадок
12.	Количество одновременно работающих пользователей SOC	не менее 60
13.	Количество одновременно работающих пользователей	не менее 3

№	Показатель	Требуемое значение
	SOAR	
14.	Время выполнения поискового запроса по данным за 90 суток	не более 120 секунд для согласованных типовых поисковых запросов
15.	Время выполнения агрегационного отчета за 6 месяцев	не более 10 минут
16.	Масштабирование производительности	горизонтальное, без полной остановки системы
17.	Возможность увеличения EPS	минимум в 3 раза без смены архитектурного подхода
18.	Поддержка раздельного хранения (hot/warm/archive tiers)	обязательна
19.	Отказоустойчивость	отсутствие единой точки отказа (N+1)
20.	Количество одновременно исполняемых SOAR-сценариев	не менее 100 параллельных запусков playbook/runbook при корректно рассчитанной архитектуре
21.	Время автоматического создания инцидента SOAR по критичному срабатыванию SIEM	не более 10 секунд при штатной нагрузке и доступности интеграционных интерфейсов
22.	Время запуска SOAR-сценария после создания инцидента	не более 15 секунд для автоматических сценариев при штатной нагрузке
23.	Количество поддерживаемых интеграций SOAR	не менее 100 готовых приложений/коннекторов производителя либо возможность расширения через API/SDK
24.	Аудит и трассировка автоматизаций	100% выполненных действий playbook/runbook должны фиксироваться в журнале аудита

4.14. Дополнительные требования к функциональным возможностям Системы

4.14.1 Система должна обеспечивать возможность многократного использования единожды собранных и проиндексированных данных для решения различных задач, включая мониторинг информационной безопасности, обеспечение соответствия требованиям регуляторов (Compliance), расследование инцидентов, выявление мошеннической активности, мониторинг ИТ-инфраструктуры, контроль функционирования приложений, цифровую аналитику и анализ бизнес-процессов.

4.14.2 Архитектура решения должна предусматривать возможность расширения функциональных возможностей путем подключения дополнительных модулей, приложений и интеграционных компонентов без необходимости миграции накопленных данных или изменения базовой архитектуры платформы.

4.14.3 Решение должно обеспечивать возможность дальнейшего развития функциональности в направлении автоматизации процессов реагирования на инциденты, интеграции с платформами **SOAR**, **ITSM**, средствами аналитики поведения пользователей и сущностей (**UEBA**), а также построения полного жизненного цикла процессов **SOC** — от регистрации события безопасности до завершения расследования, документирования принятых мер и закрытия инцидента.

5. Требования к Исполнителю

5.1. Состав информации, предоставляемой Исполнителем

В рамках участия в закупочной процедуре Исполнитель обязан предоставить следующие сведения:

- подробную спецификацию предлагаемого программного обеспечения;
- сроки поставки, установки и ввода программного обеспечения в эксплуатацию;
- условия предоставления и стоимость сервисной технической поддержки после окончания гарантийного периода;
- условия лицензирования (подписки), сроки действия и стоимость лицензий;
- описание предлагаемого технического решения, включая архитектуру, основные функциональные возможности и особенности внедрения.

5.2. Квалификационные требования к Исполнителю

Исполнитель должен соответствовать следующим требованиям:

- иметь подтвержденный опыт поставки и внедрения аналогичных программных решений не менее 2 **(два) года**;
- обладать статусом авторизованного партнера производителя предлагаемого программного обеспечения, подтвержденным соответствующими документами;
- иметь право на поставку, внедрение и предоставление конечным пользователям прав использования программного обеспечения;
- не находиться в стадии ликвидации, банкротства или реорганизации, не иметь ограничений, препятствующих осуществлению хозяйственной деятельности;
- соблюдать требования законодательства Республики Узбекистан, а также внутренних нормативных документов Заказчика при работе с конфиденциальной информацией и обеспечивать ее неразглашение.

5.3. Документы, подтверждающие квалификацию Исполнителя

В состав конкурсного предложения Исполнитель должен включить:

- копию документа, подтверждающего статус авторизованного партнера производителя;
- копии не менее **двух действующих сертификатов** инженерного состава, выданных производителем предлагаемого решения;

- перечень типовых сценариев автоматизации **SOAR (Playbook/Runbook)**, предлагаемых к реализации в рамках проекта, с описанием условий запуска, входных данных, выполняемых действий и ожидаемых результатов;
- перечень реализованных проектов по внедрению аналогичных решений за последние 2 **(два) года**.

5.4. Требования к Производителю

Производитель предлагаемого программного обеспечения должен:

- осуществлять деятельность на рынке соответствующих решений не менее 2 **(два) года**;
- иметь официальное представительство либо официально авторизованных партнеров на территории Республики Узбекистан;
- обеспечивать техническую поддержку и развитие предлагаемого программного продукта.

6. Требования к обеспечению безопасности при выполнении работ

При выполнении работ по внедрению Системы Исполнитель обязан соблюдать требования информационной безопасности, действующие на объектах Заказчика.

Поскольку в рамках настоящего проекта предусматривается поставка и внедрение исключительно программного обеспечения, специальные требования по промышленной или технической безопасности не предъявляются.

Все работы должны выполняться в соответствии с внутренними нормативными документами Заказчика, а также требованиями законодательства Республики Узбекистан в области информационной безопасности и защиты информации.

7. Требования к передаче технической и эксплуатационной документации

По завершении внедрения и ввода Системы в промышленную эксплуатацию Исполнитель обязан подготовить и передать Заказчику комплект исполнительной документации, отражающий фактически реализованную архитектуру, конфигурацию и параметры функционирования Системы.

Документация должна быть предоставлена:

- в двух экземплярах на бумажном носителе;
- в электронном виде в форматах **DOCX** и **PDF**.

В состав передаваемой документации должны входить:

- общее описание архитектуры Системы;
- архитектурные и сетевые схемы;
- перечень аппаратных и программных компонентов с указанием их конфигурации;
- описание реализованных интеграций с информационной инфраструктурой Заказчика;
- описание реализованных интеграций **SOAR**, используемых коннекторов, сервисных учетных записей и порядка их применения;
- описание реализованных сценариев **Playbook/Runbook**, включая алгоритмы автоматизации, условия запуска, механизмы ручного подтверждения, выполняемые действия и порядок внесения изменений;
- сведения о сетевой адресации (IP-адреса, используемые порты и сетевые протоколы);
- руководство по эксплуатации и администрированию Системы;
- описание реализованных мер по обеспечению информационной безопасности.

Передаваемая документация должна быть актуальной, полной и соответствовать фактической конфигурации внедренной Системы, обеспечивая возможность ее дальнейшей эксплуатации и сопровождения без обязательного привлечения Исполнителя.

8. Требования к обучению персонала Заказчика

В рамках реализации проекта Исполнитель обязан провести обучение пользователей и администраторов Системы по вопросам эксплуатации внедренного решения.

Обучение должно предусматривать ознакомление с выполненными настройками, архитектурой решения и основными функциональными возможностями Системы.

Количество слушателей — **до 10 человек**.

Форма проведения обучения — теоретическая демонстрация функциональных возможностей Системы с обязательным выполнением практических занятий.

Основной целью обучения является приобретение пользователями необходимых знаний и практических навыков для самостоятельной эксплуатации Системы.

Дополнительно Исполнитель обязан провести специализированное обучение аналитиков **SOC** и администраторов по работе с компонентом **SOAR**, включая следующие темы:

- работа с карточками инцидентов, артефактами и задачами;
- запуск, сопровождение и контроль выполнения сценариев **Playbook/Runbook**;
- применение механизма ручного подтверждения (**Human-in-the-Loop**);
- анализ результатов автоматизированного реагирования;
- внесение базовых изменений в сценарии автоматизации;
- работа с журналами аудита;
- анализ показателей эффективности процессов реагирования.

Программа обучения, его продолжительность и расписание должны быть предварительно согласованы с Заказчиком.

9. Гарантийные обязательства

Исполнитель гарантирует соответствие качества выполненных работ требованиям настоящего Технического задания при условии соблюдения Заказчиком требований производителя по эксплуатации программного обеспечения и отсутствия несанкционированного вмешательства в его функционирование.

Гарантийный срок на выполненные работы по внедрению Системы должен составлять **12 (двенадцать) месяцев** с даты подписания Сторонами Акта сдачи-приемки выполненных работ.

Срок действия подписки (**Subscription**) на поставляемые лицензии программного обеспечения также должен составлять **12 (двенадцать) месяцев**, если иное не предусмотрено договором.

10. Требования к сервисной поддержке и техническому сопровождению

Исполнитель обязан обеспечить сервисную поддержку поставляемого программного обеспечения в течение **12 (двенадцати) месяцев** с даты поставки лицензий.

Техническая поддержка должна предоставляться как Производителем программного обеспечения, так и Исполнителем.

Исполнитель обязан предоставить Заказчику доступ к официальным информационным ресурсам Производителя, обеспечивающим возможность самостоятельного получения технической документации, обновлений программного обеспечения, новых релизов и иной сопроводительной информации.

Исполнитель также обязан выполнить регистрацию и привязку лицензий программного обеспечения к учетной записи Заказчика на официальном портале Производителя.

10.1. Техническое сопровождение Системы

В рамках технического сопровождения Исполнитель должен обеспечить:

10.1.1. Поддержание работоспособности серверной инфраструктуры SIEM/SOAR

В состав работ должны входить:

- оптимизация параметров функционирования Системы с целью эффективного использования аппаратных и программных ресурсов;
- настройка параметров безопасности и эксплуатационных политик Системы;
- проведение проверки работоспособности Системы после установки обновлений и внесения изменений в конфигурацию.

10.1.2. Сопровождение интеграций

Исполнитель должен обеспечить:

- сопровождение интеграций с существующими информационными системами Заказчика;
- сопровождение и актуализацию SOAR-коннекторов;
- сопровождение сервисных учетных записей;
- корректировку сценариев автоматизации по согласованным заявкам Заказчика;
- анализ причин возникновения ошибок при выполнении Playbook/Runbook;
- восстановление работоспособности автоматизированных процессов;
- подготовку рекомендаций по повышению эффективности сценариев автоматизации.

10.1.3. Консультационная поддержка

Исполнитель должен предоставлять консультации по вопросам:

- масштабирования Системы;
- расширения функциональных возможностей;
- оптимизации производительности;
- внедрения дополнительных источников событий и интеграций.

10.1.4. Доступ к ресурсам Производителя

Заказчику должен быть обеспечен доступ к официальному порталу Производителя, включая:

- получение обновлений программного обеспечения;
- доступ к технической документации;
- использование базы знаний;
- доступ к техническому форуму и иным сервисным ресурсам.

10.1.5. Обучение при обновлении Системы

При выпуске новых версий программного обеспечения Исполнитель обязан провести дополнительный инструктаж не менее **двух администраторов** Заказчика по особенностям эксплуатации обновленной версии Системы.

10.1.6. Удаленная техническая поддержка

По запросу Заказчика Исполнитель должен обеспечивать возможность подключения специалиста посредством защищенного VPN-соединения для проведения диагностики, устранения неисправностей и оказания консультационной помощи.

10.1.7. Восстановление работоспособности Системы

Исполнитель обязан обеспечить:

- восстановление работоспособности Системы не позднее **2 (двух) рабочих дней** после возникновения программного сбоя;
- выполнение реконфигурирования, перенастройки, обновления либо полной переустановки программного комплекса при необходимости;
- устранение причин возникновения программных сбоев, связанных с поставляемым программным обеспечением;
- возможность временного перевода Системы в сервисный режим (Bypass) при выполнении восстановительных работ;
- восстановление функционирования Системы после аппаратных отказов, отключения электропитания и иных нештатных ситуаций;
- восстановление информации из резервных копий;
- предоставление Заказчику отчета о выполненных работах.

11. Требования к технической поддержке

Исполнитель обязан обеспечить локальную техническую поддержку поставляемого программного комплекса в течение **12 (двенадцати) месяцев** с момента ввода Системы в промышленную эксплуатацию.

Техническая поддержка должна предоставляться совместно Исполнителем и Производителем программного обеспечения с возможностью эскалации обращений на уровень технической поддержки Производителя (**L3**).

Поддержка должна распространяться на программные компоненты поставляемого решения.

11.1. Режим предоставления технической поддержки

Техническая поддержка должна предоставляться в следующем режиме:

- **24×7×365** — для критических инцидентов;
- **не ниже 8×5** — для инцидентов, не относящихся к критическим (по согласованию с Заказчиком).

11.2. Время реагирования на обращения

Исполнитель обязан обеспечить следующие показатели времени первичного реагирования:

Приоритет	Максимальное время реагирования
P1 (Критический)	не более **60 минут**
P2 (Высокий)	не более **2 часов**
P3 (Средний)	не более **4 часов**
P4 (Низкий)	не более **2 рабочих дней**

11.3. Сроки восстановления работоспособности

Исполнитель обязан обеспечить следующие сроки восстановления либо предоставления временного обходного решения:

Приоритет	Максимальный срок восстановления
P1	не более **24 часов**
P2	не более **48 часов**
P3	до **15 рабочих дней**
P4	по согласованию с Заказчиком

11.4. Каналы взаимодействия

Исполнитель обязан обеспечить единый механизм регистрации обращений пользователей, включающий:

- портал **Service Desk**;
- телефон службы технической поддержки;
- электронную почту.

12. Иные требования к выполнению работ и оказанию услуг

12.1. Организация выполнения работ

При выполнении работ Исполнитель обязан соблюдать требования внутреннего распорядка, нормативных документов, правил информационной безопасности и иных локальных нормативных актов Заказчика.

Заказчик предоставляет Исполнителю перечень уполномоченных сотрудников и их контактные данные для взаимодействия по вопросам внедрения, сопровождения и активации лицензий программного обеспечения.

12.2. Требования к комплектности поставки

Поставляемое решение должно включать полный комплект программных компонентов, лицензий и функциональных модулей, необходимых для реализации всех требований настоящего Технического задания.

Стоимость поставляемого решения должна учитывать полный состав программного обеспечения и не требовать приобретения дополнительных обязательных компонентов для обеспечения заявленного функционала.

12.3. Требования к интеграции

При выполнении интеграционных работ Исполнитель обязан учитывать архитектурные особенности, технические характеристики и требования существующей информационной инфраструктуры Заказчика.

12.4. Требования к поставляемому программному обеспечению

Поставляемое программное обеспечение должно являться актуальной версией, официально поддерживаемой Производителем, и поставляться с необходимыми лицензиями, подписками и иными компонентами, обеспечивающими полноценное функционирование решения в соответствии с требованиями настоящего Технического задания.