Приложение №1 к протоколу заседания
Закупочной комиссии №8 от 06.07.2026 г.

ЗАКУПОЧНАЯ ДОКУМЕНТАЦИЯ

На поставку, установку и запуск в эксплуатацию
Системы управления информацией и событиями безопасности (SIEM)
и автоматизации реагирования (SOAR) в АКБ «Asia Alliance Bank»

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:** Поставка, установка и запуск в эксплуатацию Системы управления информацией и событиями безопасности (SIEM) и автоматизации реагирования (SOAR) для обеспечения функционирования Центра мониторинга кибербезопасности (SOC).

Внедрение Системы SIEM/SOAR должно проводиться совместно с ответственными лицами Заказчика, без нарушения работоспособности существующей ИТ-инфраструктуры Заказчика, с предварительным поверхностным обследованием имеющихся Веб-ресурсов и Веб-приложений. Все работы, требующие остановку каких-либо корпоративных систем, должны быть предварительно согласованы с Заказчиком.

В рамках проекта Исполнителем должны быть выполнены следующие этапы работ:

- подготовительный этап;
- пуско-наладочные и интеграционные работы (детальное описание в прилагаемом техническом задании).

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 оборудования, а также предоставления требуемых подписок и лицензий. 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 в течении 180 дней после поставки, установки (программного обеспечения или оборудования) и подписание актов, а также предоставления требуемых подписок и лицензий.

1.9. **Валюта платежа:**

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

1.10. **Срок выполнения:** 60 календарных дней с даты подписания Договора.

1.11. **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.

1.12. **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.

1.13. **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 60 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 опыт внедрения обозначенных услуг (поставка ПО), либо схожих по сложности и характеру систем — не менее 3 лет;

Б. Наличие не менее 3 реализованных проектов по внедрению обозначенных услуг (поставка ПО), либо схожих по сложности и характеру систем за последние 3 года;

В. Наличие действующего партнёрского статуса производителя;

Г. Наличие авторотационного письма от производителя, подтверждающего право внедрение ПО на территорию Республики Узбекистан;

Д. Наличие в составе исполнителя не менее двух сертифицированных производителем инженеров.

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 Приложения №5 к Конкурсной документации (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:

- не менее 3 лет опыта по предоставлению обозначенных услуг (поставка ПО), либо схожих по сложности и характеру систем (приложить свидетельство о регистрации юридического лица и перечень указывающий на требуемый опыт);
- не менее 3 реализованных проектов по предоставлению обозначенных услуг (поставка ПО), либо схожих по сложности и характеру систем за последние 3 года (приложить копии контрактов с документацией, подтверждающей приемку);
- приложить действующее партнёрское соглашение с производителем и авторотационное письмо от производителя, подтверждающего право поставки оборудования на территорию Республики Узбекистан;
- Наличие в составе исполнителя не менее двух сертифицированных производителем инженеров (приложить копии минимум 2-х сертификатов инженеров от производителя).

5. Техническое предложение Участника по Форме №5
6. Приложить перечень типовых SOAR-сценариев (playbook/runbook), которые Исполнитель готов реализовать в рамках проекта, с описанием входных данных, действий реагирования и ожидаемого результата.

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 60 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.	
Автоматизация 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 внедрению Splunk Enterprise Security и техническая поддержка на один год	
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 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

В настоящем Техническом задании описаны требования к Системе управления информацией и событиями безопасности SIEM и автоматизации реагирования на инциденты информационной безопасности (SOAR) достаточные для описания требований Заказчика к составу ПО (далее - Система), с целью объявления тендера и/или конкурса на приобретение ПО и услуг для реализации проекта в целом на условиях «под ключ».

1.1 Наименование выполняемых работ и оказываемых услуг

Полное наименование проекта: Система управления информацией и событиями безопасности SIEM и автоматизации реагирования на инциденты информационной безопасности (SOAR).

Работы проводятся на инфраструктуре и площадке Заказчика.

В рамках данного Технического задания Исполнитель должен предоставить коммерческое предложение на поставку ПО, установку, внедрение и запуск в эксплуатацию программного комплекса SIEM/SOAR.

1.2 Цели использования выполняемых работ и оказываемых услуг

Основная цель проекта — внедрение в инфраструктуре Банка систем мониторинга и управления информацией и событиями информационной безопасности (SIEM) и автоматизации реагирования на инциденты информационной безопасности (SOAR) для обеспечения функционирования Центра мониторинга кибербезопасности (SOC).

Основные задачи, решаемые Системой:

- централизованный сбор и хранение событий безопасности;
- непрерывный мониторинг ИТ- и сетевой инфраструктуры;
- выявление инцидентов информационной безопасности;
- анализ и расследование инцидентов;
- формирование единой картины состояния ИБ;
- поддержка реагирования на инциденты;
- автоматизация и оркестрация процессов реагирования на инциденты;
- автоматическое обогащение инцидентов контекстом из внутренних и внешних источников;
- сокращение времени расследования и реагирования за счет сценариев playbook/runbook.
- подготовка отчетов и аналитики;
- контроль соблюдения требований информационной безопасности.

Основное назначение Системы – централизованный сбор, анализ и корреляция событий информационной безопасности, а также оркестрация и автоматизация реагирования с целью своевременного выявления, расследования, эскалации и устранения инцидентов, возникающих в компании _____.

2 Перечень работ, услуг и их объемы (количество), требуемые от Исполнителя

Внедрение Системы SIEM/SOAR должно проводиться совместно с ответственными лицами Заказчика, без нарушения работоспособности существующей ИТ-инфраструктуры Заказчика, с предварительным поверхностным обследованием имеющихся Веб-ресурсов и Веб-приложений. Все работы, требующие остановку каких-либо корпоративных систем, должны быть предварительно согласованы с Заказчиком.

В рамках проекта Исполнителем должны быть выполнены следующие этапы работ:

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

2.1 Подготовительный этап

Включает в себя взаимодействие с ответственным за Проект персоналом Заказчика и совместное обследование ИТ инфраструктуры Заказчика. На данном этапе сотрудники должны определить:

- наиболее важные детали топологии сети Заказчика;
- зоны ответственности Заказчика и Исполнителя в ходе развёртывания Системы;
- количество ИТ ресурсов, которые будет мониторить и защищать Система.

2.2 Пуско-наладочные и интеграционные работы

Во взаимодействии с ответственным за Проект персоналом Заказчика пуско-наладочные работы включают в себя:

- инсталляцию и конфигурацию программной части Системы;
- интеграцию в сетевую инфраструктуру Заказчика;
- активацию модулей необходимых для работы Системы;
- активацию необходимых лицензий.
- развертывание и базовую конфигурацию компонента SOAR для оркестрации и автоматизации реагирования;
- интеграцию с Core Banking System, Service Desk/ITSM, Active Directory/LDAP, XDR(EDR&NDR), DLP, сканерами уязвимостей, межсетевыми экранами, антивирусными решениями, PAM, DAM, WAF, средствами защиты рабочих станций/серверов, сетевыми средствами защиты, почтовыми шлюзами и иными системами Заказчика по согласованному перечню;
- настройку не менее 10 (десяти) базовых сценариев автоматизации реагирования (playbook/runbook) для следующих сценариев: компрометация учетной записи, Brute Force атаки, обнаружение вредоносного ПО, подозрительная активность привилегированных пользователей, утечка данных, нарушение политик информационной безопасности.
- проверку корректности запуска сценариев автоматизации по результатам корреляционных правил, оповещений и ручного запуска аналитиком SOC.

В случае обнаружения сбоев в работе Системы по причине ошибок, не связанных с объектами ИТ инфраструктуры Заказчика, Исполнитель обязуется внести коррективы в функционал продукта до подписания акта о выполненных работах.

2.3 Порядок контроля и приемка Системы

Приемка Системы должна производиться путем проведения приемочных испытаний. Приемочные испытания осуществляются представителями Заказчика и Исполнителя.

Цель приемочных испытаний состоит в подтверждении работоспособности компонентов Системы и соответствие их требованиям ТЗ.

Виды, состав, объем и методы испытаний должны определяться программой приемочных испытаний. Программа приемочных испытаний разрабатывается Исполнителем и согласовывается Заказчиком не позднее, чем за 1 день перед началом испытаний.

Результаты приемочных испытаний должны оформляться протоколом, который подписывается членами приемочной комиссии. По факту успешного проведения приемочных испытаний подписывается Акт завершения приемочных испытаний.

При обнаружении во время приемочных испытаний недостатков, дефектов или иных отклонений от требований ТЗ, соответствующие факты должны фиксироваться в протоколе, в котором в том числе указывается:

- перечень недостатков (дефектов);
- степень влияния отмеченных недостатков на работоспособность системы;
- требуемые сроки устранения недостатков (дефектов).

В течение пяти рабочих дней с момента устранения недостатков, дефектов или иных отклонений от требований к системе, приемочная комиссия должна провести повторные приёмочные испытания соответствующего компонента и принять Системы в постоянную

эксплуатацию.

2.4 Обучение персонала.

Обучение согласно п.9 данного ТЗ.

3 Место выполнения работ и оказания услуг

Исполнитель должен обеспечить поставку, инсталляцию и настройку ПО, по следующему адресу: _____

Сроки поставки Системы будут определены в Договоре между Заказчиком и Исполнителем, но не более 60 календарных дней, со дня подписания договорных отношений Заказчика с Исполнителем.

4 Технические требования к Системе

К Системе предъявляются следующие основные технические требования.

4.1 Общие требования

4.1.1 Предлагаемая система должна относиться к классу SIEM (Security Information and Event Management) и автоматизации реагирования на инциденты информационной безопасности (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 интерфейс и единое хранилище данных для задач логирования, мониторинга безопасности, расследования инцидентов, отчетности, визуализации и администрирования.

4.1.3 Система должна хранить события в исходном либо максимально близком к исходному виде, без обязательной предварительной нормализации, агрегации или редукции данных до фиксированной схемы.

4.1.4 Система должна поддерживать схему хранения и поиска без жестко заданной реляционной модели данных и позволять работать с разнородными машинными данными из любых источников, представленных в человекочитаемом формате.

4.1.5 Решение должно иметь подтвержденную практику промышленного применения у крупных корпоративных заказчиков и развитую экосистему документации, профессиональных сервисов, обучения, поддержки и партнеров.

4.1.6 Лицензирование решения должно быть прозрачным и позволять масштабирование по объему обрабатываемых/индексируемых данных и/или функциональным модулям без необходимости полной замены архитектуры.

4.2 Архитектура и масштабируемость

4.2.1 Решение должно быть программным и не должно требовать обязательного использования специализированных физических устройств производителя.

4.2.2 Система должна поддерживать развертывание в физической инфраструктуре, виртуальной среде, частном/публичном облаке либо в гибридной модели.

4.2.3 Система должна поддерживать распределенную архитектуру для центральной площадки и удаленных площадок, включая сбор, буферизацию, передачу и централизованную обработку данных.

4.2.4 Архитектура должна поддерживать горизонтальное масштабирование компонентов сбора, индексирования/хранения и поиска без полной переустановки системы.

4.2.5 Система должна обеспечивать распределенный поиск по нескольким узлам

хранения/индексации и поддерживать параллельную обработку поисковых запросов.

4.2.6 Система должна поддерживать размещение разных типов данных в отдельных логических хранилищах/индексах для оптимизации производительности поиска, разграничения доступа и управления сроками хранения.

4.2.7 Система должна поддерживать обработку крупных объемов машинных данных и иметь документально подтвержденную возможность масштабирования до десятков ТБ данных в сутки при соответствующем проектировании инфраструктуры.

4.3 Требования к сбору, приему и интеграции данных

4.3.1 Система должна обеспечивать сбор данных по протоколам Syslog, TCP/UDP, защищенным каналам TLS/SSL, через агентское ПО, API/REST, WMI, SNMP events, из файлов журналов, JSON, XML, CSV, баз данных, скриптовых и модульных источников.

4.3.2 Агентское ПО должно поддерживать шифрование передачи данных, кэширование при недоступности центральных компонентов, балансировку нагрузки между принимающими узлами и передачу данных по надежному транспортному протоколу.

4.3.3 Система должна поддерживать как агентские, так и безагентные методы сбора данных, включая прямой доступ к логам по сети, прием от существующих Syslog-серверов и интеграцию через API.

4.3.4 Система должна поддерживать индексирование многострочных и сложных событий без потери структуры события и исходной временной метки.

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

4.3.6 Система должна обеспечивать прием, индексирование и хранение исходных, немодифицированных машинных данных из любых источников без обязательного предварительного приведения к фиксированной реляционной схеме данных.

4.3.7 Система должна корректно обрабатывать временные метки из разных часовых поясов и сохранять оригинальное время события наряду со временем поступления в систему.

4.3.8 Система не должна зависеть исключительно от готовых коннекторов производителя: должна быть возможность подключать новые источники и адаптироваться к изменению форматов логов без изменения исходного кода продукта.

4.3.9 Должна поддерживаться автоматическая проверка доступности источников, контроль полноты поступающих событий и оповещение при прекращении поступления данных от критичных источников.

4.3.10 Система должна поддерживать интеграцию с Active Directory/LDAP, системами аутентификации, межсетевыми экранами, IDS/IPS, WAF, VPN, EDR/XDR/антивирусами, DLP, сканерами уязвимостей, почтовыми и веб-шлюзами, DNS/DHCP, сетевыми устройствами, NetFlow/IPFIX, операционными системами, базами данных, системами виртуализации, облачными сервисами, бизнес-приложениями, Service Desk/ITSM, CMDB и пользовательскими приложениями.

4.4 Требования к хранению, индексированию и жизненному циклу данных

4.4.1 Система должна индексировать исходные, немодифицированные машинные данные и обеспечивать последующий поиск, расследование и отчетность по этим данным.

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

4.4.3 Должна быть обеспечена возможность хранения оперативных, теплых и архивных данных с гибкой настройкой сроков хранения по типам источников, индексам, критичности и требованиям комплаенса.

4.4.4 Система должна поддерживать детализированное управление данными по мере их устаревания: перенос на более дешевое/внешнее хранилище, архивирование и/или удаление согласно политикам Заказчика.

4.4.5 Система должна поддерживать репликацию данных/индексов для обеспечения доступности, целостности, устойчивости к сбоям и повышения производительности поиска.

4.4.6 Должна быть обеспечена возможность масштабирования хранилища без остановки всей системы.

4.4.7 Должна быть обеспечена защита журналов и аудиторских данных от несанкционированного изменения и удаления, включая механизмы проверки целостности.

4.5 Требования к нормализации, обогащению и контексту

4.5.1 Система должна поддерживать нормализацию событий к унифицированной модели данных для типовых сценариев безопасности, при этом исходные сырые данные должны оставаться доступными для поиска и расследования.

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 обогащение событий дополнительными данными (контекст: справочники, списки активов, информация о пользователях, данные CMDB, внешние и внутренние фиды угроз).threat intelligence, IOC, Geo-IP и иные справочные источники.

4.5.4 Должна поддерживаться интеграция с корпоративными директориями для получения атрибутов пользователей: логин, ФИО, подразделение, должность, руководитель, телефон, местоположение, признак привилегированности, даты начала/окончания работы и иные атрибуты.

4.5.5 Должна поддерживаться корреляция нескольких учетных записей/логинов с одним сотрудником или субъектом.

4.5.6 Должна поддерживаться интеграция с CMDB/базами активов для получения информации об устройствах: hostname, IP, MAC, местоположение, владелец, критичность, наличие чувствительных данных, соответствие регуляторным требованиям.

4.5.7 Система должна позволять применять новые справочники и контекстные данные к ранее проиндексированным событиям для поиска и отчетности за прошлые периоды.

4.5.8 Система должна поддерживать подход schema-on-read, при котором исходные события сохраняются в полном виде, а извлечение полей, нормализация, обогащение и интерпретация данных могут выполняться на этапе поиска и

анализа без обязательного изменения структуры ранее сохраненных данных.

4.5.9 Изменение логики извлечения полей, нормализации, справочников, threat intelligence-фидов или правил обогащения не должно требовать обязательной переиндексации или повторной загрузки ранее сохраненных исторических данных.

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

4.5.11 Для активов должна поддерживаться привязка IP-адресов, DNS-имен, MAC-адресов, владельцев, местоположений, критичности, принадлежности к сегменту сети, признаков соответствия требованиям ИБ и иных атрибутов, согласованных с Заказчиком.

4.5.12 Для пользователей должна поддерживаться привязка логинов, email-адресов, ФИО, подразделений, должностей, руководителей, признаков привилегированности, статуса учетной записи и иных атрибутов, получаемых из корпоративных директорий или справочников.

4.5.13 Система должна поддерживать централизованное подключение, хранение и использование внешних и внутренних источников threat intelligence, включая IOC по IP-адресам, доменам, URL, hash-значениям, email-адресам, именам файлов и иным индикаторам.

4.5.14 При добавлении новых индикаторов компрометации система должна позволять выполнять ретроспективный поиск совпадений по историческим данным за выбранный период хранения без 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 как поиски в реальном времени, так и запланированные поиски, а также параллельное выполнение нескольких поисковых запросов.

4.6.3 Система должна позволять выполнять поиск, расследование, корреляцию и построение отчетности непосредственно по исходным индексированным событиям, без необходимости предварительной нормализации или загрузки данных в отдельную SQL-базу данных.

4.6.4 Система должна поддерживать подход, при котором исходные события сохраняются в полном виде, а извлечение полей, нормализация, обогащение и интерпретация данных могут выполняться как на этапе приема, так и на этапе поиска и анализа ранее сохраненных данных.

4.6.5 Система должна позволять сохранять, редактировать, повторно использовать и передавать поисковые запросы другим пользователям с учетом ролевой модели доступа.

4.6.6 Система должна поддерживать статистический анализ: подсчет, уникальные значения, сумма, минимум, максимум, среднее, медиана, мода, стандартное отклонение, дисперсия, перцентили, первое/последнее появление значения.

4.6.7 Система должна поддерживать выявление редких и аномальных значений, построение базовых профилей поведения и выявление отклонений, включая

сценарии неизвестных угроз и APT без жесткой зависимости от сигнатур.

4.6.8 Система должна поддерживать корреляцию событий по временным, логическим, поведенческим и статистическим правилам, включая многошаговые сценарии атак.

4.6.9 Система должна поддерживать использование моделей kill chain, MITRE ATT&CK, NIST, PCI DSS, а также возможность создавать собственные фреймворки/контроли для классификации и описания сценариев выявления.

4.6.10 Система должна позволять создавать собственные правила корреляции, изменять существующие правила и тестировать их до ввода в промышленную эксплуатацию.

4.6.11 Система должна предоставлять преднастроенный SIEM-контент: корреляционные правила, дашборды, отчеты, модели данных, сценарии расследования и шаблоны мониторинга безопасности с возможностью адаптации под инфраструктуру Заказчика.

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

4.6.13 Поисково-аналитический язык должен поддерживать выявление первого и последнего появления значения события, пользователя, IP-адреса, хоста, процесса, домена или иного поля за заданный период времени.

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

4.6.15 Система должна поддерживать риск-ориентированный подход к выявлению угроз, при котором отдельные события могут формировать накопительный риск по пользователям, учетным записям, хостам, IP-адресам, приложениям или иным сущностям.

4.6.16 Система должна поддерживать формирование риск-событий и накопление риск-рейтинга по различным объектам риска: пользователям, учетным записям, хостам, IP-адресам, приложениям и иным сущностям.

4.6.17 Система должна позволять формировать инцидент не только по одиночному событию, но и на основании накопленного риск-рейтинга, сформированного несколькими независимыми событиями за заданный период времени.

4.6.18 Система должна позволять выявлять угрозы на основании совокупности нескольких низкоприоритетных событий, которые по отдельности не являются критичными, но при накоплении в рамках одной сущности формируют инцидент безопасности.

4.6.19 Должна поддерживаться возможность настройки весов риска, риск-объектов, риск-событий, категорий риска и пороговых значений для формирования инцидентов.

4.7 Требования к мониторингу, оповещениям и расследованию инцидентов

4.7.1 Система должна поддерживать мониторинг в режиме, близком к реальному времени, и формирование оповещений по результатам поисков, корреляционных правил и аналитических сценариев.

4.7.2 Оповещения должны поддерживать настройку приоритетов, подавление повторных срабатываний, ограничение частоты срабатывания и маршрутизацию ответственным группам.

4.7.3 Система должна поддерживать отправку уведомлений по электронной почте, через интеграции с внешними системами, Webhook/API, запуск пользовательских скриптов либо иные механизмы автоматизации.

4.7.4 Система должна предоставлять рабочие процессы расследования инцидентов: карточка/объект инцидента, привязка исходных событий и контекста, история расследования, статусы, комментарии, назначение ответственных и возможность документирования результатов.

4.7.5 Система должна обеспечивать переход от сводного события/дашборда/корреляционного срабатывания к исходным событиям для детального расследования.

4.8 Требования к SOAR, оркестрации и автоматизации реагирования

4.8.1 Компонент SOAR должен поддерживать развертывание в инфраструктуре Заказчика без обязательной зависимости от облачного сервиса производителя, с возможностью работы в изолированном или ограниченно подключенном контуре при наличии локальных интеграций.

4.8.2 SOAR должен обеспечивать двустороннюю интеграцию с SIEM: получение корреляционных срабатываний/значимых событий, создание карточек инцидентов, запуск сценариев автоматизации и передачу статусов, результатов обогащения, комментариев и ссылок на расследование обратно в SIEM.

4.8.3 SOAR должен поддерживать объектную модель расследования, включающую инциденты/контейнеры, артефакты, наблюдаемые индикаторы (IP, URL, домен, hash, email, hostname, user), задачи, комментарии, вложения, историю действий и результаты выполненных автоматизированных шагов.

4.8.4 SOAR должен предоставлять графический конструктор playbook/runbook для создания, изменения, тестирования и повторного использования сценариев автоматизации без необходимости изменения исходного кода продукта.

4.8.5 Должна поддерживаться возможность использования пользовательской логики и скриптов, включая Python или функционально эквивалентный механизм, для реализации нестандартных действий, проверок, преобразований данных и интеграций.

4.8.6 SOAR должен обеспечивать интеграцию со следующими системами: EDR/XDR, межсетевыми экранами, WAF, VPN, DLP, антивирусами, почтовыми шлюзами, sandbox, threat intelligence, сканерами уязвимостей, Active Directory/LDAP, DNS/DHCP, CMDB, ITSM/Service Desk, SIEM и иными корпоративными системами.

4.8.7 Должна быть обеспечена возможность создания и доработки собственных коннекторов/приложений через открытый API/SDK производителя, без ожидания выпуска готового коннектора производителем.

4.8.8 SOAR должен обеспечивать автоматическое обогащение инцидентов данными о пользователях, активах, критичности систем, принадлежности IP/Geo-IP, репутации IP/доменов/URL, результатах проверки hash, данных threat intelligence, IOC и иных справочных источников.

4.8.9 SOAR должен поддерживать автоматизированные действия реагирования, включая блокировку IP/URL/домена/hash на средствах защиты, изоляцию

рабочей станции, отключение или блокировку учетной записи, сброс пароля, карантин/удаление письма, создание или обновление заявки в ITSM, уведомление ответственных групп и эскалацию инцидента.

4.8.10 Для критичных действий реагирования должна поддерживаться модель human-in-the-loop: ручное подтверждение аналитиком/руководителем SOC перед выполнением потенциально влияющих на бизнес действий.

4.8.11 SOAR должен поддерживать ручной, автоматический и условный запуск playbook/runbook на основании типа инцидента, критичности, источника, категории угрозы, MITRE ATT&CK техники, значений артефактов или иных параметров.

4.8.12 SOAR должен обеспечивать управление задачами расследования: назначение ответственных, контроль статусов, SLA, приоритетов, комментариев, результатов выполнения, закрытие инцидента и фиксацию итогового решения.

4.8.13 SOAR должен вести полный аудит действий пользователей, системных действий и автоматизированных шагов playbook/runbook с указанием времени, инициатора, входных параметров, результата, ошибок и выполненных изменений во внешних системах.

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

4.8.15 SOAR должен поддерживать безопасное хранение учетных данных интеграций, токенов, ключей API и секретов с разграничением прав доступа и аудитом использования.

4.8.16 Должна поддерживаться версионность, импорт/экспорт, резервное копирование и перенос сценариев автоматизации, приложений/коннекторов и конфигураций между тестовой и промышленной средой.

4.8.17 SOAR должен предоставлять отчеты и метрики эффективности реагирования: количество инцидентов по типам, время первого реагирования, MTTR, количество выполненных автоматизаций, успешность playbook, ошибки интеграций, доля автоматизированных действий и нагрузка на аналитиков SOC.

4.8.18 В составе внедрения должны быть реализованы базовые SOAR-сценарии для типовых инцидентов: фишинговое письмо, подозрительный IP/домен/URL, вредоносный hash/файл, подозрительная активность учетной записи, срабатывание EDR/XDR либо антивируса, сетевое событие от IDS/IPS/WAF/VPN.

4.9 Требования к визуализации и отчетности

4.9.1 Система должна поддерживать построение интерактивных дашбордов и отчетов, включая таблицы, временные диаграммы, линейные, столбчатые, площадные, круговые и точечные графики, индикаторы состояния и географические визуализации по IP/Geo-IP.

4.9.2 Визуализации должны поддерживать обновление в реальном времени, drill-down от агрегированных показателей к исходным событиям и выделение аномалий/выбросов.

4.9.3 Система должна позволять создавать отчеты и дашборды как техническим, так и нетехническим пользователям, включая визуальное редактирование панелей и настройку заголовков, легенд, осей и фильтров.

4.9.4 Система должна поддерживать формирование отчетов по расписанию и

экспорт/рассылку отчетов в распространенные форматы, включая PDF, CSV, XLS/XLSX и иные форматы, доступные в продукте.

4.9.5 Система должна поддерживать отчеты и панели мониторинга для задач соответствия требованиям ИБ и регуляторики, включая ISO 27002, NIST, PCI DSS и аналогичные стандарты.

4.10 Требования к безопасности, доступу и аудиту

4.10.1 Система должна поддерживать гибкую ролевую модель доступа (RBAC) для пользователей и API с возможностью ограничения доступа к источникам данных, типам данных, временным диапазонам, отчетам, дашбордам, поискам и административным функциям.

4.10.2 Система должна поддерживать интеграцию с Active Directory/LDAP и корпоративными системами единого входа (SSO).

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

4.10.4 Система должна вести полный аудит действий пользователей и администраторов: входы, поисковые запросы, просмотр отчетов, изменения конфигурации, управление пользователями, создание/изменение правил и иные значимые действия.

4.10.5 Аудиторские события должны содержать дату и время, пользователя/субъект, источник, выполненное действие и результат выполнения.

4.10.6 Система должна поддерживать механизмы подтверждения целостности индексированных событий, включая хеширование и/или цифровую подпись событий либо функционально эквивалентный механизм контроля подлинности.

4.10.7 Система должна обеспечивать мониторинг собственной конфигурации, доступности компонентов и состояния системных сервисов с возможностью оповещения о сбоях.

4.11 Открытость архитектуры и интеграция 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 системами.

4.11.2 Желательна поддержка SDK или библиотек для распространенных языков программирования, включая Python, Java, JavaScript, C# или аналогичные.

4.11.3 Все конфигурации системы должны быть доступны для управления через веб-интерфейс, CLI и/или конфигурационные файлы.

4.11.4 Система должна поддерживать интеграцию с внешними системами визуализации, BI, ITSM/SOAR, CMDB, threat intelligence, системами мониторинга и иными корпоративными платформами Заказчика.

4.11.5 Система должна иметь возможность пересылать сырые, преобразованные или обогащенные события во внешние системы по Syslog TCP/UDP, raw TCP, через файл, API или аналогичный механизм.

4.11.6 Система должна поддерживать использование публичных и/или предоставляемых производителем приложений/пакетов интеграции для популярных продуктов и сценариев безопасности.

4.11.7 Для SOAR-компонента должна поддерживаться интеграция через REST API/Webhook, возможность вызова внешних API, приема входящих событий, запуска автоматизированных действий и передачи результатов во внешние

системы.

4.11.8 Решение должно позволять развивать библиотеку интеграций и сценариев реагирования без миграции на отдельную платформу и без изменения архитектурного подхода SIEM/SOAR.

4.11.9 Должна поддерживаться возможность расширенной настройки отчетов, панелей мониторинга, поисковых объектов и интеграционного контента через интерфейс администратора и/или конфигурационные файлы.

4.11.10 Не допускается требование повторного сбора или дублирующего хранения одних и тех же событий для реализации разных сценариев анализа в рамках одной платформы.

4.11.11 Для SOAR-компонента должна поддерживаться интеграция через REST API/Webhook, возможность вызова внешних API, приема входящих событий, запуска автоматизированных действий и передачи результатов во внешние системы.

4.11.12 Решение должно позволять развивать библиотеку интеграций и сценариев реагирования без миграции на отдельную платформу и без изменения архитектурного подхода SIEM/SOAR.

4.12 Требования к отказоустойчивости и режимам функционирования

4.12.1 Система должна поддерживать резервирование ключевых компонентов, кластеризацию, репликацию критичных данных и отсутствие единой точки отказа при целевой архитектуре N+1.

4.12.2 Система должна обеспечивать автоматическое восстановление либо документированную процедуру восстановления при сбоях компонентов.

4.12.3 Основной режим функционирования Системы – непрерывная круглосуточная работа в автоматизированном режиме под управлением администратора.

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

4.13 Требования к производительности и пропускной способности

Поставляемое решение должно отвечать 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 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

№	Показатель	Требуемое значение
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 SOAR	не менее 3
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 Требования к дополнительным сценариям использования

4.14.1 Система должна позволять использовать один раз собранные и индексированные данные в различных сценариях: мониторинг ИБ, комплаенс, расследование инцидентов, выявление мошенничества, IT-операции, мониторинг приложений, цифровая аналитика и бизнес-аналитика.

4.14.2 Система должна поддерживать расширение функциональности за счет

дополнительных модулей, приложений или интеграций без необходимости миграции данных на отдельную платформу.

4.14.3 Система должна обеспечивать полноценное развитие в сторону автоматизации реагирования, интеграции с SOAR/ITSM, расширенной аналитики поведения пользователей и сущностей, а также создания единого процесса SOC от выявления события до документированного реагирования и закрытия инцидента.

5 Требования к Исполнителю

К Исполнителю предъявляются следующие требования:

5.1 В рамках закупочной процедуры Исполнитель должен предоставить информацию:

- детальную спецификацию поставляемого ПО;
- срокам поставки и инсталляции ПО;
- условия и стоимости послегарантийной сервисной технической поддержки;
- условия и стоимости лицензий (подписки) на программное обеспечение;
- особенностям предлагаемого технического решения.

5.2 Общие требования к Исполнителю

Исполнитель должен удовлетворять следующим требованиям:

- подтвержденный опыт работы по предоставлению обозначенных услуг (поставка ПО) не менее, чем 3 года;

- являться авторизованным партнёром, а также иметь документальное подтверждение на распространение конечным пользователям прав на использование и внедрение реализуемого/внедряемого программного обеспечения;

- не являться неплатежеспособным или банкротом, находится в процессе ликвидации, не должен быть наложен арест, экономическая деятельность Исполнителя не должна быть приостановлена;

Исполнитель обязан соблюдать требования, предъявляемые действующим законодательством Республики Узбекистан к работе с документами и сведениями, содержащими конфиденциальную информацию и не разглашать конфиденциальную информацию, ставшую ему известной в процессе оказания услуг.

5.3 Исполнитель должен включить в состав предложения следующие документы, подтверждающие его соответствие вышеуказанным требованиям:

- копию авторизированного письма о наличии партнерского статуса с компанией производителем;

- копии минимум 2-х сертификатов инженеров от компании производителя

- перечень типовых SOAR-сценариев (playbook/runbook), которые Исполнитель готов реализовать в рамках проекта, с описанием входных данных, действий реагирования и ожидаемого результата;

- перечень реализованных ИТ-проектов за последние 3 года.

5.4 Требования к производителю

Компания-Вендор должна существовать на рынке не менее 5 лет, иметь локальное представительство на территории Республики Узбекистан и иметь авторизованных партнеров на рынке Узбекистана.

6 Требования к безопасности выполнения работ и оказания услуг

Так как при реализации проекта будут использоваться только программные решения, то специальных требований по безопасности не предъявляется.

7 Требования по передаче технических и иных документов по результатам выполненных работ и оказанных услуг

После завершения внедрения и ввода Системы в промышленную эксплуатацию Исполнитель обязан подготовить **рабочую (исполнительную) документацию, отражающую фактически реализованное состояние Системы.**

Документация предоставляется:

- в **2 (двух) экземплярах** на бумажном носителе;
- в **электронном виде** (форматы: DOCX и PDF)

Обязательный состав документации:

- общее описание Системы;
- архитектурные и сетевые схемы;
- перечень и конфигурация аппаратных и программных компонентов;
- описание интеграций с инфраструктурой Заказчика;
- описание реализованных SOAR-интеграций, коннекторов, учетных записей сервисного доступа и правил их использования;
- описание реализованных playbook/runbook, логики автоматизации, условий запуска, ручных подтверждений, действий реагирования и процедур изменения сценариев;
- сетевая адресация (IP, порты, протоколы);
- краткая эксплуатационная документация;
- описание реализованных мер информационной безопасности.

Документация должна быть **актуальной, полной и соответствовать фактической реализации Системы**, а также достаточной для её эксплуатации без привлечения Исполнителя.

8 Требования к передаче знаний персоналу Заказчика

В рамках данного ТЗ Исполнитель обеспечивает проведение инструктажа пользователей системы по проделанным / выполненным настройкам;

Количество слушателей: до 10 человек.

Формат: демонстрационный + практический.

Цель: освоение функциональных возможностей системы.

Дополнительно Исполнитель должен провести инструктаж по работе с SOAR-компонентом для аналитиков SOC и администраторов системы.

Темы: работа с карточками инцидентов, артефактами и заданиями; запуск и контроль playbook/runbook; ручное подтверждение действий реагирования; анализ результатов автоматизации; базовое изменение сценариев автоматизации; просмотр журналов аудита и метрик эффективности реагирования.

Содержание и время инструктажа предварительно согласовать с Заказчиком.

9 Гарантийные обязательства

Исполнитель должен гарантировать, что качество выполненной работы будет соответствовать техническому заданию и требованиям указанными Заказчиком, при условии соблюдения правил эксплуатации программного (программно-аппаратного) обеспечения, установленных производителем в документации и отсутствия несанкционированного вмешательства в работу инсталлированного программного обеспечения.

Срок гарантии на выполненные работы по внедрению Системы, должен составлять **12 (двенадцать) месяцев** и исчисляется со дня подписания Сторонами акта сдачи – приемки работ.

Срок подписки (Subscription) на лицензии должен составлять **12 (двенадцать) месяцев.**

10 Условия сервисной поддержки и техническое сопровождение

Срок сервисной поддержки производителя – **12 (двенадцать) месяцев**, с момента поставки лицензии ПО. Сервисная поддержка на программные компоненты должна оказываться как производителем, так и Исполнителем.

Исполнитель обязан предоставить информацию об информационных ресурсах компании производителя ПО, для самостоятельного скачивания документации, обновлений, релизов.

Исполнитель осуществляет привязку идентификационных данных ПО в кабинете Заказчика, на сайте Производителя.

Работы по техническому сопровождению ПО должны включать в себя:

a) Обеспечение непрерывного функционирования серверной части Системы SIEM/SOAR:

- настройка параметров Системы для оптимизации использования аппаратных и программных ресурсов;
- настройка параметров Системы для управления политикой безопасности;
- тестирование работы Системы в штатном режиме после проведения обновлений.

b) Интеграция с существующими системами управления и мониторинга.

Сопровождение и корректировка SOAR-интеграций, коннекторов, учетных данных сервисного доступа и сценариев автоматизации по согласованным запросам Заказчика.

Анализ ошибок выполнения playbook/runbook, восстановление работоспособности автоматизированных сценариев и предоставление рекомендаций по их оптимизации.

c) Консультации по масштабированию Системы.

d) Доступ к порталу производителя ПО (возможность скачивать обновления, доступ к техническому форуму, доступ к документации).

e) Проведение инструктажа 2-х администраторов Системы в случае обновления Системы.

f) Подключение специалиста посредством VPN по требованию для решения возникших проблем, консультаций, связанных с функционированием Системы.

g) Восстановление работоспособности программного комплекса:

- восстановление работоспособности Системы в штатном режиме не позднее, чем через 2 рабочих дня после сбоя программных средств;
- перенастройка, реконфигурирование, обновление и/или полная переустановка программного комплекса, а также устранение причин, приведших к сбою (при условии сбоя, вызванного продуктами компании);
- возможность отключения Системы на время сбоя для проведения восстановительных работ (режим байпас);
- восстановление активности Системы, после аппаратных сбоев, потеря питания, и т.д.;
- операции восстановления данных из резервных копий.
- предоставление отчетов о проделанной работе.

11 Требования к технической поддержке

12.1 Исполнитель обязан обеспечить локальную техническую поддержку поставляемого программного комплекса в течение 12 месяцев.

12.2 Поддержка также должна оказываться производителем ПО.

12.3 Уровень поддержки должен предусматривать возможностью эскалации на уровень производителя (L3).

12.4 Поддержка должна распространяться на:

- программную часть (software).

12.5 Поддержка должна предоставляться в режиме:

- 24×7×365 – для критичных инцидентов;
- не ниже 8×5 – для некритичных (по согласованию с Заказчиком).

12.6 Время реакции на инциденты:
- Критический (P1): не более 60 минут;
- Высокий (P2): не более 2 часов;
- Средний (P3): не более 4 часов;
- Низкий (P4): не более 2 рабочих дней.

12.7 Время восстановления (или обходного решения):
- P1: не более 24 часов;
- P2: не более 48 часов;
- P3: до 15 рабочих дней;
- P4: по согласованию с Заказчиком.

12.8 Исполнитель должен предоставлен единый канал регистрации заявок на ТП:
- Service Desk (портал);
- телефон горячей линии;
- e-mail.

12 Иные требования к работам, услугам и условиям их оказания

12.1 Обязательным условием оказания услуг является соблюдение правил действующего внутреннего распорядка Заказчика, внутренних положений, инструкций и требований, о которых Заказчик уведомит Исполнителя. Заказчик предоставляет Исполнителю список и контактные данные персонала, уполномоченного им на контакты с Исполнителем по решению заявленных проблем, связанных с активацией подписки на ПО.

12.2 Требование к комплектации

Система должна иметь полную комплектацию, для полноценного функционирования предлагаемого решения в рамках текущего ТЗ. Стоимость ПО должна формироваться исходя из полной комплектации.

12.3 Требование к интеграции

Интеграция должна учитывать особенности работы инфраструктуры Заказчика.

12.4 Сведения о новизне

Поставляемое ПО должна быть актуальной последней версии, со всеми необходимыми лицензиями на продукт и его составляющими.