e-mail: info@uzairways.com
e-xat: airways@exat.uz
tel: +998 (78) 140-46-23
www.uzairways.com

O'zbekiston, Toshkent,
Amir Temur shohko'chasi, 41
GSP-100060

Uzbekistan, Tashkent,
41, Amir Temur avenue
GSP-100060

UZBEKISTAN AIRWAYS

Joint-Stock Company | Aksiyadorlik jamiyati

УТВЕРЖДАЮ:
Вр.и.о. Первого Заместителя
Председателя Правления
АО «Uzbekistan Airways»

_____ Xusanov U.A.
«02» _____ 2026 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на приобретение и внедрение готовой системы управления информацией и событиями безопасности (SIEM) и автоматизации реагирования на инциденты (SOAR) для АО «Uzbekistan Airways»

РАСШИРЕННАЯ СПЕЦИФИКАЦИЯ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ

Программно-аппаратный комплекс системы управления инцидентами информационной безопасности

1. Зрелость решения

1.1 Отраслевое признание

№ треб.	Описание требования
1.1.1	Производитель должен входить в квадрант лидеров (Leaders Quadrant) Gartner Magic Quadrant для систем управления информацией и событиями безопасности.
1.1.2	Производитель должен быть лидером по всем сценариям использования в последнем отчете Gartner Critical Capabilities для систем управления информацией и событиями безопасности.
1.1.3	Производитель должен занимать лидирующее место в отчете IDC Worldwide Market Share для систем управления информацией и событиями безопасности на протяжении не менее четырех (4) лет подряд.
1.1.4	Производитель должен быть признан лидером в отчете IDC MarketScape для корпоративных систем управления информацией и событиями безопасности.

1.2 Единая архитектура платформы

№ треб.	Описание требования
1.2.1	Программно-аппаратный комплекс должен представлять собой единую интегрированную платформу, охватывающую управление журналами, управление инцидентами информационной безопасности, аналитику безопасности и ИТ-операции на основе единого хранилища данных, без необходимости использования отдельных баз данных или пользовательских интерфейсов.
1.2.2	Решение должно использовать архитектуру schema-on-read, позволяющую принимать данные без предварительно определенных схем и обеспечивающую индексирование и поиск любых машинно-генерируемых данных без предварительной нормализации.
1.2.3	Решение должно хранить необработанные, неизмененные данные в плоских файлах без сокращения данных, применения схем или нормализации на этапе приема данных.
1.2.4	Решение должно поддерживать неограниченное извлечение полей на этапе поиска, без ограничений на количество индексируемых или извлекаемых полей на одно событие.
1.2.5	Платформа должна поддерживать сценарии использования как в области безопасности, так и в ИТ-операциях на основе одной и той же инфраструктуры данных, позволяя выполнять единый поиск по событиям безопасности, журналам приложений, метрикам инфраструктуры и бизнес-данным.

2. ТРЕБОВАНИЯ К ЯЗЫКУ ОБРАБОТКИ ПОИСКОВЫХ ЗАПРОСОВ

2.1 Встроенные возможности языка поисковых запросов

№ треб.	Описание требования
2.1.1	Решение должно включать встроенный язык обработки поисковых запросов с не менее чем 140 командами для поиска данных, фильтрации, преобразования, статистического анализа и визуализации.
2.1.2	Язык запросов должен поддерживать конвейерный синтаксис (в стиле Unix pipe), позволяющий объединять несколько команд в одном поисковом запросе для последовательного преобразования и анализа данных.
2.1.3	Язык поисковых запросов должен поддерживать шесть отдельных типов команд: распределяемые потоковые (distributable streaming), централизованные потоковые (centralized streaming), преобразующие (transforming), генерирующие (generating), оркестрирующие (orchestrating) и команды обработки наборов данных (dataset processing).
2.1.4	Решение должно поддерживать подзапросы (вложенные поисковые запросы), позволяющие использовать результат одного поиска в качестве входных данных для другого поиска в рамках одного запроса.
2.1.5	Платформа должна поддерживать поисковые макросы для создания многократно используемых фрагментов поисковых запросов с параметризованными аргументами, которые можно использовать совместно в рамках организации.
2.1.6	Решение должно включать встроенные функции вычисления и преобразования полей, включая математические операции, обработку строк, функции работы с датой/временем, условную логику и преобразование типов данных.

2.2 Расширенные статистические и аналитические команды

№ треб.	Описание требования
2.2.1	Язык поисковых запросов должен включать встроенные функции статистического анализа, включая подсчет событий и уникальных значений, сумму, среднее значение, медиану, моду, стандартное отклонение, дисперсию, минимальное и максимальное значения, диапазон, а также первые и последние значения.
2.2.2	Решение должно поддерживать встроенные функции обнаружения аномалий, статистических выбросов и кластеризации с использованием машинного обучения без необходимости применения внешних инструментов.
2.2.3	Платформа должна включать функции предиктивной аналитики, использующие исторические паттерны данных для прогнозирования будущих значений с помощью встроенных алгоритмов.
2.2.4	Язык поисковых запросов должен поддерживать анализ транзакций, позволяющий группировать события на основе общих значений полей и временных интервалов для анализа последовательностей из нескольких событий как единых логических транзакций.

2.2.5	Решение должно включать встроенные функции анализа временных рядов для сравнения данных за несколько периодов времени в рамках одной визуализации.
2.2.6	Платформа должна поддерживать извлечение полей с помощью регулярных выражений и автоматизированное формирование регулярных выражений на этапе поиска.

2.3 Производительность и оптимизация поиска

№ треб.	Описание требования
2.3.1	Решение должно включать встроенный механизм диагностики выполнения поисковых запросов, предоставляющий подробные метрики производительности, включая время, затраченное на каждом этапе поиска, количество просканированных событий и использование ресурсов.
2.3.2	Платформа должна поддерживать механизм ускоренного поиска по предварительно агрегированным и сводным данным моделей данных, обеспечивая выполнение оптимизированных запросов по терабайтам исторических данных с минимальной задержкой.
2.3.3	Решение должно поддерживать суммарное индексирование (summary indexing), позволяющее хранить предварительно вычисленные результаты поиска в отдельных индексах для значительно более быстрой отчетности.
2.3.4	Платформа должна поддерживать ускорение моделей данных (data model acceleration), автоматически генерирующее высокопроизводительные сводки нормализованных данных для быстрого построения дашбордов и отчетов.

3. МЕХАНИЗМ ОПОВЕЩЕНИЙ НА ОСНОВЕ РИСКА (RBA)

3.1 Архитектура встроенного механизма оценки риска

№ треб.	Описание требования
3.1.1	Система управления инцидентами информационной безопасности должна включать встроенный механизм оповещений на основе риска (RBA), объединяющий несколько низкодостоверных событий безопасности в высокодостоверные агрегированные риск-оповещения на основе накопленных оценок риска.
3.1.2	Механизм RBA должен поддерживать присвоение оценки риска как активам (системам, серверам, конечным точкам), так и идентификационным данным (пользователям, сервисным учетным записям) как отдельным типам риск-объектов.
3.1.3	Решение должно включать выделенный индекс риска, хранящий все события риска вместе с соответствующими метаданными, включая оценку риска, риск-объект, тип риск-объекта, объект угрозы и аннотации фреймворков.
3.1.4	Платформа должна поддерживать динамическое изменение оценки риска на основе контекстных факторов, таких как критичность актива, уровень

	привилегий пользователя, бизнес-подразделение, известные уязвимости и внешние данные Threat Intelligence.
3.1.5	Механизм RBA должен поддерживать затухание оценки риска с течением времени, позволяя более старым событиям риска вносить меньший вклад в общий расчет риска.

3.2 Правила инцидентов риска и оповещения

№ треб.	Описание требования
3.2.1	Решение должно включать готовые правила инцидентов риска (Risk Incident Rules), генерирующие оповещения при превышении накопленной оценкой риска настраиваемых пороговых значений за определенный период времени (например, 100 баллов за 24 часа).
3.2.2	Платформа должна включать правила инцидентов риска, оповещающие при наблюдении нескольких тактик MITRE ATT&CK для одного риск-объекта на протяжении длительного периода времени (например, 3 и более тактик за 7 дней) для обнаружения медленных, скрытых атак.
3.2.3	Механизм RBA должен поддерживать оповещения на основе разнообразия источников данных, срабатывающие, когда риск-объект генерирует события из нескольких уникальных источников данных, указывающие на более широкую подозрительную активность.
3.2.4	Агрегированные риск-оповещения должны включать полный контекст с указанием всех событий риска, внесших вклад, их индивидуальных оценок, соответствующих аннотаций фреймворков и хронологии подозрительной активности.

3.3 Анализ и визуализация рисков

№ треб.	Описание требования
3.3.1	Решение должно включать выделенный дашборд анализа рисков, показывающий тренды оценки риска, наиболее рискованные объекты, вклад в риск по источникам и охват фреймворками с течением времени.
3.3.2	Платформа должна обеспечивать возможность детализации (drill-down) от агрегированных риск-оповещений к отдельным событиям риска, внесшим вклад, и от событий риска к исходным необработанным данным.
3.3.3	Механизм RBA должен поддерживать визуализацию паттернов поведения риск-объектов, показывающую динамику оценок риска и связанных техник с течением времени.

4. ИНТЕГРАЦИЯ С ФРЕЙМВОРКАМИ КИБЕРБЕЗОПАСНОСТИ

4.1 Встроенная поддержка фреймворка MITRE ATT&CK

№ треб.	Описание требования
4.1.1	Решение должно включать встроенную интеграцию с фреймворком MITRE ATT&CK с автоматической аннотацией обнаружений соответствующими тактиками, техниками и подтехниками.
4.1.2	Платформа должна поддерживать аннотации MITRE ATT&CK на уровне корреляционных поисковых запросов/правил обнаружения, автоматически проставляя всем результирующим событиям соответствующие идентификаторы техник.
4.1.3	Решение должно включать визуализацию покрытия MITRE ATT&CK, показывающую, какие техники охвачены текущими обнаружениями, и выявляющую пробелы в покрытии.
4.1.4	Платформа должна предоставлять интеграцию с MITRE ATT&CK Navigator или эквивалентную визуализацию для сопоставления обнаружений и инцидентов с матрицей ATT&CK.
4.1.5	Решение должно поддерживать оповещения на основе прогрессии тактик MITRE ATT&CK, обнаруживая ситуации, когда сущность демонстрирует поведение в рамках нескольких тактик, указывающее на развитие цепочки атаки.

4.2 Поддержка дополнительных фреймворков

№ треб.	Описание требования
4.2.1	Решение должно поддерживать встроенную интеграцию с фреймворком Lockheed Martin Cyber Kill Chain для сопоставления обнаружений с фазами атаки.
4.2.2	Платформа должна поддерживать сопоставление с фреймворком NIST Cybersecurity Framework, критическими средствами контроля безопасности CIS (CIS18/CIS20) и стандартом NIST 800-53.
4.2.3	Решение должно включать готовый контент соответствия требованиям PCI-DSS, SOX, HIPAA, GDPR и региональным нормативным требованиям.
4.2.4	Платформа должна позволять определять пользовательские фреймворки и аннотации для специфичных для организации фреймворков безопасности и сопоставлений средств контроля.

5. ЕДИНОЕ ОБНАРУЖЕНИЕ УГРОЗ, РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ (TDIR)

5.1 Единый центр управления расследованиями и реагированием

№ треб.	Описание требования
5.1.1	Система управления инцидентами информационной безопасности должна включать нативно интегрированный единый центр управления расследованиями и реагированием, предоставляющий единую рабочую область для обнаружения, расследования и реагирования без необходимости использования отдельных пользовательских интерфейсов.
5.1.2	Единый интерфейс управления расследованиями и реагированием должен обеспечивать непрерывный рабочий процесс от сортировки оповещений через расследование до реагирования в рамках одного пользовательского интерфейса.
5.1.3	Решение должно поддерживать стандартизированную терминологию TDIR, согласованную с отраслевыми подходами: оповещения/срабатывания, дела/расследования и планы реагирования/плейбуки.
5.1.4	Платформа должна включать единую очередь аналитика с расширенной фильтрацией, сортировкой и массовыми действиями для эффективной обработки оповещений и управления делами.
5.1.5	Решение должно поддерживать управляемые рабочие процессы расследования с рекомендациями на основе ИИ по следующим шагам, основанными на контексте находки и исторических паттернах.

5.2 Управление делами и совместная работа

№ треб.	Описание требования
5.2.1	Платформа должна включать встроенное управление делами, позволяющее аналитикам группировать связанные находки, добавлять доказательства, прикреплять заметки и отслеживать ход расследования.
5.2.2	Решение должно поддерживать временные шкалы расследования, отображающие хронологическую последовательность связанных событий, действий аналитика и изменений статуса дела.
5.2.3	Платформа должна поддерживать совместную работу нескольких аналитиков над делами с ролевыми разрешениями, журналами аудита и возможностями уведомлений.
5.2.4	Решение должно предоставлять метрики по делам и отслеживание SLA, включая среднее время обнаружения (MTTD), среднее время реагирования (MTTR) и время нахождения дела в работе.

5.3 Планы реагирования и автоматизация

№ треб.	Описание требования
5.3.1	Платформа должна поддерживать планы реагирования (плейбуки), которые могут быть привязаны к правилам обнаружения для автоматизированных или управляемых аналитиком рабочих процессов реагирования.
5.3.2	Решение должно включать готовые шаблоны планов реагирования для распространенных типов инцидентов, включая фишинг, вредоносное ПО, несанкционированный доступ и утечку данных.
5.3.3	Планы реагирования должны поддерживать условное ветвление на основе атрибутов находки, результатов обогащения и решений аналитика.

5.4 Интеллектуальный помощник аналитика и агентные технологии

№ треб.	Описание требования
5.4.1	Система управления инцидентами информационной безопасности должна обеспечивать использование функций искусственного интеллекта при локальном (on-premises) развертывании основной программной части Системы на вычислительной инфраструктуре Заказчика.
5.4.2	Интеллектуальный помощник должен быть интегрирован в пользовательский интерфейс Системы управления инцидентами информационной безопасности и обеспечивать взаимодействие с аналитиком информационной безопасности на естественном языке.
5.4.3	Интеллектуальный помощник должен обеспечивать автоматическое формирование краткого резюме события, обнаружения или инцидента информационной безопасности с учетом доступного контекста, включая затронутые активы, учетные записи, временную последовательность событий, индикаторы компрометации и результаты аналитической обработки.
5.4.4	Интеллектуальный помощник должен обеспечивать анализ контекста расследования и формирование рекомендаций по дальнейшим действиям аналитика, включая проведение дополнительных поисковых запросов, проверку связанных сущностей, анализ исторической активности и получение дополнительного контекста.
5.4.5	Решение должно обеспечивать возможность формирования поисковых и аналитических запросов на основании задания пользователя, сформулированного на естественном языке.
5.4.6	Интеллектуальный помощник должен обеспечивать возможность объяснения существующих поисковых и аналитических запросов на естественном языке, включая описание выполняемых операций и логики обработки данных.
5.4.7	Решение должно обеспечивать возможность использования интеллектуальным помощником контекста, доступного в Системе управления инцидентами информационной безопасности, включая события безопасности, результаты обнаружений, сведения об активах и учетных записях, индикаторы компрометации, результаты поисковых запросов и материалы расследований.
5.4.8	Решение должно поддерживать агентный режим работы, при котором интеллектуальный помощник способен самостоятельно определять последовательность аналитических операций, необходимых для выполнения задания пользователя, и выполнять несколько взаимосвязанных операций в рамках одного процесса расследования.

№ треб.	Описание требования
5.4.9	Агентные функции должны обеспечивать возможность автоматизированного выполнения отдельных задач аналитика информационной безопасности, включая: первичный анализ и триаж обнаружений; поиск связанной активности; анализ событий за требуемый период; формирование аналитических запросов; получение дополнительного контекста; подготовку рекомендаций по расследованию; формирование резюме и материалов расследования; подготовку рекомендаций по реагированию.
5.4.10	Решение должно предусматривать возможность применения специализированных интеллектуальных агентов для автоматизации отдельных процессов центра мониторинга информационной безопасности, включая анализ и триаж обнаружений, помощь в создании правил обнаружения и поддержку процессов автоматизированного реагирования.
5.4.11	Выполнение интеллектуальным агентом действий, способных привести к изменению конфигурации информационных систем, блокированию сетевого взаимодействия, изоляции конечных точек, изменению учетных записей либо иному активному воздействию на информационные системы Заказчика, должно предусматривать возможность обязательного предварительного подтверждения уполномоченным пользователем.
5.4.12	Все действия интеллектуального помощника и интеллектуальных агентов должны подлежать журналированию. Журнал должен содержать сведения о запросе пользователя, инициированных агентом операциях, полученных результатах и выполненных либо предложенных действиях.
5.4.13	Доступ к функциям искусственного интеллекта и агентным функциям должен регулироваться средствами ролевого управления доступом Системы.
5.4.14	Администратор Системы должен иметь возможность централизованно включать и отключать функции интеллектуального помощника и агентные функции.
5.4.15	Основные компоненты Системы управления инцидентами информационной безопасности, обеспечивающие сбор, хранение, индексирование, поиск, корреляцию и управление событиями и инцидентами информационной безопасности, должны размещаться в инфраструктуре Заказчика. Допускается использование внешней вычислительной инфраструктуры производителя для выполнения отдельных функций искусственного интеллекта при условии сохранения основной программной платформы и основного массива журналов и событий информационной безопасности в инфраструктуре Заказчика.
5.4.16	В случае использования внешних вычислительных ресурсов для выполнения функций искусственного интеллекта взаимодействие локальной инфраструктуры Заказчика с внешним сервисом должно осуществляться по защищенному шифрованному каналу связи с использованием протокола HTTPS/TLS либо эквивалентного защищенного протокола.
5.4.17	Архитектура решения должна обеспечивать возможность контролируемого сетевого взаимодействия с внешними сервисами искусственного интеллекта через определенные производителем сетевые адреса и порты, с возможностью применения межсетевого экранирования и/или прокси-сервера Заказчика.
5.4.18	Производитель должен документировать перечень информации, передаваемой во внешние сервисы искусственного интеллекта, назначение такой передачи, применяемые механизмы защиты информации и архитектуру обработки данных.

№ треб.	Описание требования
5.4.19	Использование интеллектуального помощника не должно требовать передачи полного массива хранимых Системой журналов и событий информационной безопасности во внешнюю инфраструктуру. Передача отдельных данных или контекста, необходимых для обработки конкретного запроса интеллектуального помощника, допускается в соответствии с документированной архитектурой решения и политиками информационной безопасности Заказчика.
5.4.20	Передача данных между локально развернутой Системой и внешними компонентами искусственного интеллекта должна осуществляться исключительно в зашифрованном виде.
5.4.21	Решение должно обеспечивать возможность отключения взаимодействия с внешними сервисами искусственного интеллекта без прекращения функционирования основных функций Системы управления инцидентами информационной безопасности, включая сбор, хранение, поиск, корреляцию, обнаружение и управление инцидентами.
5.4.22	Отключение функций искусственного интеллекта не должно приводить к потере либо недоступности ранее собранных журналов, событий, обнаружений, инцидентов и результатов расследований.
5.4.23	Использование функций искусственного интеллекта не должно требовать размещения основной базы событий информационной безопасности, журналов и индексов Заказчика во внешней облачной инфраструктуре.
5.4.24	Производитель должен обеспечивать возможность эксплуатации функций интеллектуального помощника из пользовательского интерфейса локально развернутой Системы управления инцидентами информационной безопасности без необходимости использования отдельного внешнего пользовательского интерфейса.
5.4.25	Архитектура использования искусственного интеллекта должна предусматривать возможность централизованного управления подключением к внешним сервисам, контроля доступности соединения, настройки параметров подключения и отключения соответствующей функциональности администратором Заказчика.

6. ВСТРОЕННАЯ ИНТЕГРАЦИЯ С SOAR

6.1 Интегрированная оркестрация, автоматизация и реагирование в области безопасности

№ треб.	Описание требования
6.1.1	Система управления инцидентами информационной безопасности должна включать встроенную интеграцию с SOAR-решением поставщика, позволяющую выполнять плейбуки непосредственно из интерфейса Системы управления инцидентами информационной безопасности без переключения контекста.
6.1.2	Интеграция с SOAR должна поддерживать как облачные, так и локальные развертывания SOAR с эквивалентной функциональностью.
6.1.3	Решение должно обеспечивать видимость статуса выполнения плейбуков, результатов действий и истории автоматизации непосредственно в интерфейсе

	управления делами Системы управления инцидентами информационной безопасности.
6.1.4	Платформа должна поддерживать автоматизированные действия по обогащению, собирающие дополнительный контекст из Threat Intelligence, баз данных активов и хранилищ идентификационных данных в ходе расследования.
6.1.5	Интеграция с SOAR должна включать не менее 300 готовых интеграций (приложений) с распространенными средствами безопасности, ИТ-системами и облачными сервисами.

6.2 Адаптивные действия реагирования

№ треб.	Описание требования
6.2.1	Решение должно поддерживать адаптивные действия реагирования, которые могут запускаться автоматически правилами корреляции или вручную аналитиками в ходе расследования.
6.2.2	Встроенные действия реагирования должны включать: присвоение оценки риска, создание события/оповещения безопасности, уведомление по электронной почте, выполнение внешнего скрипта и запрос данных Threat Intelligence.
6.2.3	Платформа должна поддерживать пользовательские действия реагирования, разработанные с использованием SDK поставщика для специфичных для организации требований автоматизации.

7. РАСШИРЕННЫЕ ВОЗМОЖНОСТИ ОБНАРУЖЕНИЯ

7.1 Механизм корреляционных поисковых запросов

№ треб.	Описание требования
7.1.1	Решение должно включать встроенный механизм корреляционных поисковых запросов, позволяющий определять правила безопасности с использованием языка поисковых запросов платформы с выполнением по расписанию или в реальном времени.
7.1.2	Корреляционные поисковые запросы должны поддерживать автоматическое извлечение полей, сопоставление с единой информационной моделью данных и нормализацию для межисточниковой корреляции.
7.1.3	Платформа должна поддерживать корреляцию по неограниченному числу источников данных в рамках одного правила, обеспечивая обнаружение сложных многоэтапных атак, охватывающих различные источники журналов.
7.1.4	Правила корреляции должны поддерживать настраиваемые временные окна, ограничение частоты (throttling) и подавление дублирующихся оповещений для предотвращения переполнения оповещениями и дублирующихся уведомлений.

7.1.5	Решение должно включать не менее 1400 готовых корреляционных поисковых запросов, охватывающих распространенные паттерны атак, требования соответствия и сценарии угроз.

7.2 Обновления контента

№ треб.	Описание требования
7.2.1	Поставщик должен предоставлять регулярные обновления контента (не реже одного раза в месяц), включая новые правила обнаружения, дашборды и планы реагирования, сопоставленные с новыми угрозами и новыми техниками MITRE ATT&CK.
7.2.2	Обновления контента должны разрабатываться и исследоваться выделенной командой поставщика по исследованию угроз с публикуемой информацией Threat Intelligence и рекомендациями по обнаружению.
7.2.3	Фреймворк обновления контента должен поддерживать выборочное развертывание, позволяющее организациям включать конкретные пакеты контента в зависимости от их среды и профиля риска.
7.2.4	Обновления контента должны включать подробную документацию, объясняющую логику обнаружения, необходимые источники данных и рекомендации по настройке.

7.3 Аналитика поведения пользователей и сущностей (UEBA)

№ треб.	Описание требования
7.3.1	Решение должно включать встроенные возможности UEBA, использующие машинное обучение для установления поведенческих базовых показателей и обнаружения аномальной активности пользователей и сущностей.
7.3.2	UEBA должна поддерживать модели машинного обучения без учителя (unsupervised), автоматически адаптирующиеся к паттернам поведения организации без создания правил вручную.
7.3.3	Платформа должна обеспечивать оценку риска сущностей, объединяющую поведенческие аномалии с обнаружениями на основе правил для комплексной оценки риска.
7.3.4	UEBA должна поддерживать анализ групп сравнения (peer group analysis), сопоставляющий поведение пользователя с поведением аналогичных пользователей по роли, подразделению или пользовательским группировкам.

8. АРХИТЕКТУРА ДАННЫХ И МАСШТАБИРУЕМОСТЬ

8.1 Распределенная архитектура

№ треб.	Описание требования
8.1.1	Решение должно поддерживать горизонтально масштабируемую распределенную архитектуру с отдельными уровнями централизованного

	сбора и предварительной обработки данных, хранения и индексирования данных, а также поиска и аналитической обработки.
8.1.2	Платформа должна поддерживать кластеризованное развертывание узлов хранения и индексирования данных с автоматической репликацией данных для обеспечения высокой доступности и аварийного восстановления.
8.1.3	Решение должно поддерживать возможность кластеризации узлов поиска и аналитической обработки для обеспечения высокодоступного поиска и отчетности с автоматическим переключением при отказе.
8.1.4	Архитектура должна поддерживать географически распределенные развертывания с настраиваемыми коэффициентами репликации и оптимизированным выбором узлов для выполнения поисковых запросов.

8.2 Сбор и пересылка данных

№ треб.	Описание требования
8.2.1	Поставщик должен предоставлять легковесные агенты сбора данных, которые можно развернуть на конечных точках, серверах и сетевых устройствах с минимальной нагрузкой на ресурсы.
8.2.2	Агенты и узлы сбора данных должны поддерживать зашифрованную передачу данных (TLS/SSL), локальное кеширование данных, балансировку нагрузки между несколькими получателями и автоматическое переключение при отказе.
8.2.3	Решение должно поддерживать выделенные узлы централизованного сбора и предварительной обработки данных, способные выполнять разбор, фильтрацию, маршрутизацию и обогащение данных перед передачей в кластер хранения и индексирования.
8.2.4	Платформа должна поддерживать высокопроизводительный прием событий по HTTP(S)/REST API с токенной аутентификацией от приложений и облачных сервисов.

8.3 Федеративный поиск и аналитика

№ треб.	Описание требования
8.3.1	Решение должно поддерживать федеративную аналитику (Federated Analytics), позволяющую выполнять поисковые запросы по данным, хранящимся во внешних озерах данных (например, Amazon Security Lake, Azure Data Lake), без перемещения данных.
8.3.2	Федеративные поисковые запросы должны использовать тот же язык поисковых запросов и обеспечивать согласованные результаты независимо от физического расположения данных.
8.3.3	Платформа должна поддерживать выборочный прием данных из федеративных источников, позволяя перемещать ценные данные в платформу для долгосрочного хранения, одновременно выполняя запросы к «холодным» данным на месте.

8.4 Многоуровневое хранение и удержание данных

№ треб.	Описание требования
8.4.1	Решение должно поддерживать несколько уровней хранения (горячий, теплый, холодный, замороженный) с настраиваемыми политиками хранения данных и автоматическим перемещением данных между уровнями.
8.4.2	Платформа должна поддерживать архитектуру объектного хранения данных, позволяющую хранить индексированные данные в совместимом объектном хранилище (S3, Azure Blob, GCS или эквивалент) при сохранении производительности поиска.
8.4.3	Решение должно поддерживать архивирование данных во внешнее хранилище с возможностью восстановления и поиска архивных данных по запросу.
8.4.4	Политики хранения данных должны настраиваться для каждого индекса отдельно, позволяя устанавливать разные сроки хранения для данных безопасности, соответствия требованиям и операционных данных.

9. АНАЛИТИКА АКТИВОВ И ИДЕНТИФИКАЦИОННЫХ ДАННЫХ

9.1 Обнаружение активов и управление ими

№ треб.	Описание требования
9.1.1	Решение должно включать встроенные возможности анализа активов и рисков, обеспечивающие непрерывное обнаружение активов на основе принимаемых источников данных без необходимости обязательной интеграции с внешней CMDB.
9.1.2	Платформа должна автоматически сопоставлять идентификаторы активов (IP-адрес, имя хоста, MAC-адрес) для поддержания единых записей об активах, несмотря на изменения идентификаторов.
9.1.3	Записи об активах должны поддерживать обогащение бизнес-контекстом, включая критичность, владельца, местоположение, бизнес-подразделение и область применения требований соответствия.
9.1.4	Решение должно поддерживать категоризацию и тегирование активов для фильтрации и приоритизации в рабочих процессах безопасности.

9.2 Корреляция идентификационных данных и контекст

№ треб.	Описание требования
9.2.1	Платформа должна поддерживать корреляцию идентификационных данных, связывая несколько имен учетных записей, адресов электронной почты и идентификаторов аутентификации в единые записи идентификационных данных.
9.2.2	Решение должно интегрироваться с корпоративными каталогами (Active Directory, LDAP, Azure AD) для обогащения идентификационных данных, включая подразделение, руководителя, местоположение и статус привилегий.

9.2.3	Записи идентификационных данных должны включать индикаторы риска, такие как статус в списке наблюдения, привилегированный доступ, недавние события безопасности и оценки поведенческих аномалий.
9.2.4	Платформа должна поддерживать переход к расследованию на основе идентификационных данных, позволяя аналитикам просматривать всю активность, связанную с идентификационными данными, по всем источникам данных.

10. ИНТЕГРАЦИЯ С THREAT INTELLIGENCE

10.1 Встроенная платформа Threat Intelligence

№ треб.	Описание требования
10.1.1	Решение должно включать встроенные возможности управления Threat Intelligence для агрегирования, нормализации и практического применения данных об угрозах из нескольких источников.
10.1.2	Платформа должна поддерживать протоколы STIX/TAXII для автоматизированного приема фидов Threat Intelligence от коммерческих и открытых поставщиков.
10.1.3	Решение должно включать встроенную интеграцию с Threat Intelligence мировых вендоров, предоставляющую данные об угрозах в реальном времени, информацию о глобальных вспышках и контекстные сведения.
10.1.4	Threat Intelligence должна автоматически обогащать события безопасности контекстом индикаторов, включая оценки достоверности, атрибуцию злоумышленника и связанные индикаторы.

10.2 Обнаружение на основе данных Threat Intelligence

№ треб.	Описание требования
10.2.1	Платформа должна поддерживать автоматизированную корреляцию принимаемых событий с индикаторами Threat Intelligence (IP-адресами, доменами, хешами файлов, URL-адресами) в реальном времени.
10.2.2	Совпадения с данными Threat Intelligence должны автоматически повышать оценку риска для затронутых активов и идентификационных данных в рамках механизма RBA.
10.2.3	Решение должно поддерживать загрузку пользовательских данных Threat Intelligence, включая внутренние индикаторы, отраслевые фиды и вручную составленные списки.
10.2.4	Платформа должна включать дашборды на основе данных Threat Intelligence, показывающие частоту срабатывания индикаторов, наиболее часто совпадающие индикаторы и тренды активности злоумышленников.

11. ЕДИНАЯ ИНФОРМАЦИОННАЯ МОДЕЛЬ И НОРМАЛИЗАЦИЯ ДАННЫХ

11.1 Нормализация по принципу schema-on-read

№ треб.	Описание требования
11.1.1	Решение должно включать единую информационную модель, обеспечивающую стандартизированные имена полей и модели данных для разрозненных источников данных с целью единого анализа.
11.1.2	Нормализация должна происходить на этапе поиска (schema-on-read), сохраняя целостность исходных данных при обеспечении межисточниковой корреляции.
11.1.3	Платформа должна включать готовые модели данных, для сценариев использования в области безопасности, включая аутентификацию, сетевой трафик, конечные точки, веб, электронную почту и вредоносное ПО.
11.1.4	Соответствие моделям данных должно достигаться за счет псевдонимов полей и вычисляемых полей без изменения исходных данных.

11.2 Интеграционные модули и коннекторы

№ треб.	Описание требования
11.2.1	Поставщик должен предоставлять готовые интеграционные модули и коннекторы для распространенных источников данных, автоматически выполняющие разбор, извлечение полей и сопоставление с единой информационной моделью данных.
11.2.2	Платформа должна включать не менее 1000 готовых интеграционных модулей и коннекторов, охватывающих корпоративную безопасность, сети, облако, конечные точки и источники данных приложений.
11.2.3	Интеграционные модули и коннекторы должны быть доступны через управляемый поставщиком каталог приложений и интеграций с отслеживанием версий и уведомлениями об обновлениях.
11.2.4	Решение должно поддерживать пользовательское извлечение полей и сопоставление с моделями данных для проприетарных или неподдерживаемых источников данных.

12. ЭКОСИСТЕМА ПРИЛОЖЕНИЙ И РАСШИРЯЕМОСТЬ

12.1 Магазин приложений

№ треб.	Описание требования
12.1.1	Поставщик должен управлять курируемым магазином приложений, содержащим не менее 2500 приложений, надстроек и интеграций, предоставленных поставщиком, партнерами и сообществом.
12.1.2	Магазин приложений должен включать программы сертификации приложений, обеспечивающие качество, безопасность и совместимость с текущими версиями платформы.
12.1.3	Приложения должны устанавливаться непосредственно из интерфейса платформы с управлением зависимостями и проверкой совместимости версий.
12.1.4	Магазин приложений должен включать готовые приложения для ведущих поставщиков решений безопасности, облачных платформ и корпоративных приложений.

12.2 Платформа разработки и API

№ треб.	Описание требования
12.2.1	Решение должно предоставлять комплексные REST API для всех функций платформы, включая поиск, администрирование, настройку и прием данных.
12.2.2	Платформа должна включать SDK для основных языков программирования (Python, Java, JavaScript, C#) для разработки пользовательских интеграций.
12.2.3	Решение должно поддерживать разработку пользовательской визуализации с использованием стандартных веб-технологий (JavaScript, D3, React).
12.2.4	Платформа должна поддерживать модульные входные данные (modular inputs), позволяющие разрабатывать пользовательские методы сбора данных и упаковывать их в виде приложений.

13. ВИЗУАЛИЗАЦИЯ И ДАШБОРДЫ

13.1 Встроенные возможности визуализации

№ треб.	Описание требования
13.1.1	Решение должно включать встроенные типы визуализации: таблицы, линейные диаграммы, диаграммы с областями, столбчатые диаграммы, круговые диаграммы, точечные диаграммы, одиночные значения, индикаторы (радиальные, заполняющие, маркерные) и географические карты.
13.1.2	Все визуализации должны поддерживать обновление данных в реальном времени с настраиваемыми интервалами обновления.

13.1.3	Визуализации должны поддерживать интерактивную детализацию (drill-down), позволяющую пользователям переходить от сводных данных к отфильтрованным представлениям и далее к необработанным событиям.
13.1.4	Платформа должна включать конструктор дашбордов с перетаскиванием (drag-and-drop), позволяющий нетехническим пользователям создавать дашборды без программирования.

13.2 Расширенные исполнительные дашборды

№ треб.	Описание требования
13.2.1	Решение должно поддерживать расширенные исполнительные дашборды с пользовательскими фоновыми изображениями, позиционированными индикаторами и наложениями статуса.
13.2.2	Расширенные исполнительные дашборды должны поддерживать динамические индикаторы, меняющие цвет, размер или видимость в зависимости от базовых условий данных.

14. БЕЗОПАСНОСТЬ И КОНТРОЛЬ ДОСТУПА

14.1 Ролевое управление доступом (RBAC)

№ треб.	Описание требования
14.1.1	Решение должно поддерживать детализированное ролевое управление доступом (RBAC) с настраиваемыми возможностями для поиска, отчетности, администрирования и доступа к данным.
14.1.2	RBAC должен поддерживать ограничения на уровне данных, ограничивающие доступ пользователей к определенным индексам, типам источников или значениям полей.
14.1.3	Платформа должна поддерживать интеграцию с корпоративными системами аутентификации, включая Active Directory, LDAP, SAML 2.0 и OAuth 2.0.
14.1.4	Решение должно поддерживать многофакторную аутентификацию (MFA) для всех способов доступа пользователей.

14.2 Аудит и соответствие требованиям

№ треб.	Описание требования
14.2.1	Платформа должна вести исчерпывающие журналы аудита всех действий пользователей, включая выполненные поисковые запросы, просмотренные отчеты, изменения конфигурации и доступ к данным.
14.2.2	Журналы аудита должны быть защищены от несанкционированного изменения с помощью цифровых подписей или эквивалентной защиты целостности.

14.2.3	Решение должно поддерживать пересылку журналов аудита во внешние Системы управления инцидентами информационной безопасности для централизованного мониторинга безопасности.

15. ВАРИАНТЫ РАЗВЕРТЫВАНИЯ

15.1 Модели развертывания On-premise

№ треб.	Описание требования
15.1.1	Программная часть программно-аппаратного комплекса должна поддерживать локальное развертывание на инфраструктуре, управляемой заказчиком, для организаций с требованиями суверенитета данных или нормативными требованиями.

15.2 Требования к платформе

№ треб.	Описание требования
15.2.1	Для локального развертывания решение должно поддерживать установку на основных дистрибутивах Linux (RHEL, CentOS, Ubuntu, Amazon Linux) и Windows Server.
15.2.2	Платформа должна поддерживать развертывание на основных платформах виртуализации (VMware, Hyper-V) и оркестрации контейнеров (Kubernetes, OpenShift).

16. Платформа SOAR

16.1 Оркестрация, автоматизация и реагирование в области безопасности (SOAR)

№ треб.	Описание требования
16.1.1	Решение должно предоставлять возможности автоматизированного реагирования и устранения последствий.
16.1.2	Решение должно обеспечивать возможности оркестрации и автоматизации (SOAR), работающие «из коробки» с бесшовной интеграцией с большинством средств безопасности, представленных на рынке.
16.1.3	Функции автоматизации и оркестрации должны быть разработаны с использованием широко известного языка программирования.
16.1.4	Расширенные функции и интеграции платформы должны быть реализуемы с использованием единого языка программирования.
16.1.5	Рабочие процессы автоматизации и процессы оркестрации должны создаваться через графический пользовательский интерфейс (GUI).
16.1.6	Решение должно предоставлять контроль версий для существующих плейбуков.

16.1.7	Плейбуки должны поддерживать вызов других плейбуков (субплейбуков).
16.1.8	Плейбуки должны поддерживать выполнение по расписанию в заранее заданное время.
16.1.9	Должен быть доступен визуальный отладчик плейбуков для быстрой разработки и тестирования.
16.1.10	Поставщик должен предоставлять новые приложения и плейбуки через экосистему, развиваемую сообществом.
16.1.11	Решение должно включать готовые плейбуки оркестрации «из коробки».
16.1.12	Платформа SOAR должна быть разработана исключительно для автоматизации задач безопасности, а не как инструмент автоматизации общего назначения.
16.1.13	Решение должно предоставлять контекстные рекомендации на основе действий, ранее предпринятых аналитиками в аналогичных случаях.
16.1.14	Решение должно интегрироваться с более чем 200 продуктами безопасности и поддерживать сотни встроенных действий.
16.1.15	Платформа SOAR должна использовать отраслевые стандартные фреймворки нормализации событий (например, Common Event Format - CEF).
16.1.16	Решение должно поддерживать обогащение данных путем получения информации из внешних источников Threat Intelligence для расширения контекста инцидента.
16.1.17	Пользователи должны иметь возможность выполнять поиск информации по IP-адресам непосредственно в плейбуках.
16.1.18	Плейбуки должны быть достаточно гибкими для включения действий с участием человека (human-in-the-loop), включая согласования и запросы к аналитику.
16.1.19	Платформа SOAR должна поддерживать прием событий на основе электронной почты.
16.1.20	Решение должно интегрироваться с платформами Threat Intelligence (TIP) с использованием протоколов TAXII/STIX.
16.1.21	Решение должно интегрироваться с Системами управления инцидентами информационной безопасности.
16.1.22	Решение должно поддерживать двунаправленную интеграцию, обеспечивающую обмен данными с существующими технологиями безопасности.

16.2 Управление инцидентами и делами

№ треб.	Описание требования
16.2.1	Решение должно предоставлять встроенные возможности управления инцидентами и делами.

16.2.2	Платформа должна поддерживать совместную работу в реальном времени между аналитиками безопасности.
16.2.3	Каждому инциденту должен присваиваться уникальный идентификатор (UUID).
16.2.4	Детализированные права доступа должны быть назначаемыми для обеспечения совместной работы между различными командами.
16.2.5	Уровень серьезности инцидента должен автоматически изменяться на основе предопределенных правил.
16.2.6	Инциденты должны поддерживать возможность автоматической эскалации на основе заданных критериев.
16.2.7	Решение должно предоставлять возможности расследования и корреляции дел.
16.2.8	Должен быть доступен дашборд, позволяющий аналитикам быстро искать и анализировать индикаторы компрометации (IOC) в рамках инцидента/контейнера.

16.3 Отчетность

№ треб.	Описание требования
16.3.1	Решение должно предоставлять настраиваемую отчетность.
16.3.2	Отслеживание SLA должно поддерживаться и отражаться в отчетах.
16.3.3	Платформа должна отражать в отчетах экономию времени и затрат, достигнутую благодаря процессам автоматизации и оркестрации.
16.3.4	Решение должно формировать отчеты уровня руководства, подходящие для CISO и руководства SOC.

16.4 Администрирование и безопасность

№ треб.	Описание требования
16.4.1	Решение должно предоставлять детализированное ролевое управление доступом (RBAC).
16.4.2	Все действия пользователей должны быть полностью подотчетны и регистрируемы.
16.4.3	Решение должно предоставлять высокую доступность (HA) и отказоустойчивость.
16.4.4	Решение должно поддерживать крупномасштабные корпоративные нагрузки.
16.4.5	Платформа должна поддерживать протокол Traffic Light Protocol (TLP).
16.4.6	Решение должно поддерживать многопользовательскую (multi-tenant) архитектуру, что делает решение подходящим для MSSP.

16.5 Единое управление SOAR и Системой управления инцидентами информационной безопасности в рамках единой платформы TDIR

№ треб.	Описание требования
16.5.1	Система управления инцидентами информационной безопасности и SOAR должны управляться из единой консоли управления (single pane of glass) в рамках единой платформы TDIR (обнаружение угроз, расследование и реагирование).
16.5.2	Процессы управления инцидентами, поиска угроз (threat hunting) и реагирования должны работать в интегрированном режиме между Системой управления инцидентами информационной безопасности и SOAR.
16.5.3	Данные Threat Intelligence, поступающие из Системы управления инцидентами информационной безопасности, должны быть напрямую доступны для использования плейбуками SOAR.
16.5.4	Все инциденты должны сопоставляться в рамках единого дашборда.
16.5.5	Система управления инцидентами информационной безопасности и SOAR должны поддерживать моделирование угроз в соответствии с фреймворком MITRE ATT&CK.

16.6 Преимущества коннектора SOAR

№ треб.	Описание требования
16.6.1	Коннектор SOAR должен работать с полной интеграцией в SOAR без необходимости оплаты дополнительных лицензионных сборов.
16.6.2	SOAR должен обеспечивать встроенную интеграцию с Системой управления инцидентами информационной безопасности.
16.6.3	События Системы управления инцидентами информационной безопасности должны автоматически передаваться в плейбуки SOAR для выполнения.
16.6.4	Должна поддерживаться двунаправленная интеграция между Системой управления инцидентами информационной безопасности и SOAR.
16.6.5	Уровень серьезности инцидента должен определяться с помощью аналитики на основе машинного обучения.
16.6.6	Коннектор SOAR должен автоматически обогащать артефакты Threat Intelligence, такие как IP-адреса, домены и хеши файлов.

17. ТРЕБОВАНИЯ К АППАРАТНОЙ ЧАСТИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА

17.1 Состав и минимальные вычислительные ресурсы

№ треб.	Описание требования
17.1.1	Аппаратная часть программно-аппаратного комплекса должна обеспечивать работу распределенной архитектуры в составе: одного узла централизованного сбора и предварительной обработки данных, трех узлов кластера хранения и индексирования данных, одного узла поиска и аналитической обработки и одного узла управления и администрирования.
17.1.2	Узел централизованного сбора и предварительной обработки данных должен иметь не менее 12 вычислительных ядер (vCPU при виртуальном развертывании), не менее 16 ГБ оперативной памяти и не менее 300 ГБ дискового пространства на SSD Enterprise-класса.
17.1.3	Кластер хранения и индексирования данных должен состоять не менее чем из трех узлов. Каждый узел должен иметь не менее 24 вычислительных ядер (vCPU при виртуальном развертывании), не менее 48 ГБ оперативной памяти и не менее 28 ТБ дискового пространства для хранения индексируемых данных.
17.1.4	Кластер хранения и индексирования должен обеспечивать автоматическую репликацию данных между узлами, сохранение доступности данных при отказе отдельного узла и срок оперативного хранения событий не менее 365 дней. Расчетный объем хранения - около 82 ТБ; совокупная установленная емкость кластера должна составлять не менее 84 ТБ.
17.1.5	Узел поиска и аналитической обработки должен иметь не менее 32 вычислительных ядер (vCPU при виртуальном развертывании), не менее 96 ГБ оперативной памяти и не менее 1 ТБ дискового пространства на SSD Enterprise-класса.
17.1.6	Узел управления и администрирования должен иметь не менее 12 вычислительных ядер (vCPU при виртуальном развертывании), не менее 16 ГБ оперативной памяти и не менее 300 ГБ дискового пространства на SSD Enterprise-класса.
17.1.7	Минимальный суммарный объем вычислительных ресурсов программно-аппаратного комплекса должен составлять не менее 128 вычислительных ядер/vCPU, 272 ГБ оперативной памяти и ориентировочно 85,6 ТБ установленного дискового пространства без учета дополнительного технологического резерва, системных разделов и резервных копий.
17.1.8	Допускается поставка серверов с характеристиками, превышающими указанные минимальные требования, при условии полной совместимости программной и аппаратной частей комплекса.

17.2 Общие требования к серверному оборудованию

№ треб.	Описание требования
17.2.1	Серверное оборудование должно быть построено на промышленной серверной платформе архитектуры x86-64 и предназначено для непрерывной эксплуатации в режиме 24/7.

17.2.2	Оперативная память серверов должна относиться к серверному классу и поддерживать коррекцию ошибок ECC. Объем оперативной памяти каждого узла должен быть не ниже значений, установленных в разделе 17.1.
17.2.3	Системные диски и дисковая подсистема хранения индексируемых данных должны быть логически или физически разделены. Для системных разделов и высоконагруженных операций должны применяться SSD/NVMe накопители Enterprise-класса либо эквивалентное по надежности и производительности решение.
17.2.4	Дисковая подсистема узлов хранения и индексирования должна обеспечивать производительность, достаточную для одновременного приема, индексирования, репликации и поиска данных. Конфигурация RAID и/или механизм защиты данных должны соответствовать рекомендациям производителя программной части комплекса и не снижать требуемую полезную емкость ниже значений раздела 17.1.
17.2.5	Каждый физический сервер должен иметь не менее двух резервируемых блоков питания Hot-Swap с возможностью подключения к независимым линиям электропитания.
17.2.6	Каждый сервер должен иметь не менее двух сетевых интерфейсов с пропускной способностью не менее 10 Гбит/с для технологического обмена данными между узлами комплекса, а также отдельный интерфейс удаленного аппаратного управления (BMC/IPMI или эквивалент).
17.2.7	Серверы должны поддерживать установку в стандартную 19-дюймовую серверную стойку и поставляться с комплектом направляющих, креплений и кабелей питания, необходимых для ввода в эксплуатацию.
17.2.8	Должна обеспечиваться возможность замены отказавших дисков и блоков питания без длительной остановки комплекса, если такая возможность предусмотрена конструкцией поставляемого серверного оборудования.

17.3 Требования к размещению, сети и отказоустойчивости

№ треб.	Описание требования
17.3.1	Три узла кластера хранения и индексирования должны размещаться в независимых отказоустойчивых доменах. При виртуальном развертывании указанные узлы не должны одновременно размещаться на одном физическом гипервизоре.
17.3.2	Между узлом централизованного сбора и предварительной обработки данных, кластером хранения и индексирования и узлом поиска и аналитической обработки должна быть обеспечена выделенная или гарантированная сетевая пропускная способность не менее 10 Гбит/с.
17.3.3	Сетевое подключение критичных узлов должно поддерживать резервирование каналов (teaming/bonding или эквивалентный механизм) и исключать наличие единой точки отказа на уровне сетевых интерфейсов.
17.3.4	При виртуальном развертывании вычислительные ресурсы, указанные в разделе 17.1, должны выделяться гарантированно. Не допускается использование механизмов динамического уменьшения оперативной памяти и

	чрезмерного перераспределения процессорных ресурсов, способного привести к снижению производительности комплекса.
17.3.5	Архитектура должна обеспечивать возможность последующего горизонтального масштабирования путем добавления узлов сбора, хранения/индексирования и поиска/аналитики без полной перестройки комплекса.
17.3.6	При расчете полезной дисковой емкости должны учитываться фактический суточный объем поступающих данных, срок хранения не менее 365 дней, коэффициент репликации, служебные данные, технологический запас свободного пространства и рост объема событий.

18. Общие требования

№ треб.	Описание требования
18.1	Срок лицензирования программной части программно-аппаратного комплекса - не менее 1 года с момента активации (требуется официальное письмо компании-производителя с указанием срока предоставления лицензий и технической поддержки).
18.2	Требования к новизне программной части - закупаемые лицензии должны быть новыми, ранее не использованными и не активированными.
18.3	Лицензирование программной части программно-аппаратного комплекса - по объему не менее 200 ГБ / день
18.4	Условия оплаты - 100% постоплата в течение 10 дней с момента подписания сторонами акта выполненных работ/приема-передачи и подтверждения счета-фактуры.
18.5	Закупаемые лицензии должны быть оформлены на АО «Uzbekistan Airways» без права третьих лиц на поставляемые лицензии.
18.6	Требования к новизне аппаратной части - поставляемое серверное оборудование должно быть новым, не бывшим в эксплуатации, не восстановленным, поставляться в заводской комплектации и иметь действующую гарантию производителя.

19. Требования, предъявляемые к участникам отбора

№ треб.	Описание требования
19.1	Авторизация производителя - наличие у поставщика письменного разрешения от производителя на право продаж на территории Республики Узбекистан (требуется официальное письмо компании-производителя об авторизации поставщика).
19.2	Гарантия и техническая поддержка - гарантийное письмо от производителя о легальной сервисной гарантии на программную и аппаратную части программно-аппаратного комплекса и технической поддержке в режиме 24/7 в

	течение не менее 1 года с момента активации лицензий и подписания акта приема-передачи оборудования.
19.3	Сертификат соответствия -поставляемое программное обеспечение и серверное оборудование при необходимости должны иметь сертификаты соответствия, выданные уполномоченными органами Республики Узбекистан, если это требуется законодательством Республики Узбекистан.
19.4	Сроки поставки программно-аппаратного комплекса, лицензий и оказания услуг - в течение 90 рабочих дней после подписания договора.
19.5	Требования к патентной и лицензионной чистоте - программная часть комплекса должна состоять из экземпляров программного обеспечения, которые распространяются и используются в объемах и на условиях, определенных соответствующими лицензиями.

РАЗРАБОТАНО:

Врио директора департамента
ИТ инфраструктуры, цифровизации
и кибербезопасности **Kirillov A.A.**

С О Г Л А С О В А Н О:

Врио Первого заместителя Председателя правления по вопросам трансформации, финансов и приватизации **Sattarov A.A.**