«УТВЕРЖДАЮ»
Заместитель Председателя
Правления АО «Узнацбанк»

_____ Жалилов Б.А.

«___» _____2022г.

II. ТЕХНИЧЕСКАЯ ЧАСТЬ

Техническое задание

по проекту:

Модернизация существующей инфраструктуры комплекса корпоративной защиты информации в АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан».

Ташкент - 2022г.

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование проекта

Модернизация существующей инфраструктуры комплекса корпоративной защиты информации в АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан».

1.2. Заказчик

АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан (далее Заказчик).

Реквизиты:

- Почтовый адрес: Республика Узбекистан 100084, г. Ташкент, проспект А.Темура, 101
- Р/с: No 29802840800000450391 в Межбанковском расчетном центре АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан»
- МФО: 00450
- ИНН: / КПП 200836354
- ОКОНХ: 96120
- Тел.: +99878 147-15-27
- E-mail: AMansurov@nbu.uz

1.3. Требования к участнику

Участник должен предоставить информацию по реализации аналогичных проектов (не менее 3-х) в течение последних 3 (трех) лет до начала настоящего проекта.

Участник должен представить свое Техническое предложение по поставке оборудования и программного обеспечения, удовлетворяющие всем требованиям данного документа.

Участник должен произвести все необходимые действия по нативной миграции существующих конфигураций и правил для расширяемого оборудования, без простоя и прерывания работы действующей системы в целом.

В рамках выделенного бюджета Участник должен поставить полностью укомплектованный и работоспособный программно-аппаратный комплекс в рамках технический требований настоящего Технического задания.

Участник и предлагаемое им решение должны отвечать следующим требованиям:

- участник должен предоставить авторизационное письмо от производителя предлагаемого оборудования и программного обеспечения, подразделение которого имеет все полномочия осуществлять деятельность непосредственно в стране Заказчика.
- участник должен предоставить официальные документы производителя, либо ссылки на официальные документы производителя подтверждающие полное техническое соответствие предлагаемого решения - требованиям к комплексу, представленным в данном Техническом задании. Участник также может предложить решение, превосходящее их, по каждому из пунктов технических требований, указанных в данном Техническом Задании. Частичное соответствие техническим требованиям - не допускается.
- приобретаемое решение должно покрываться официальной гарантией производителя на территории республики Узбекистан сроком на 5 лет.
- участник должен иметь в собственном штате не менее одного сертифицированного производителем инженера уровня professional и опытом работ по интеграции приобретаемых решений, квалификация которого подтверждается соответствующим сертификатом.

Участник может предложить решение, характеристики которого превосходят требования, указанные в техническом задании.

1.4. Основание для реализации проекта

Основанием для реализации проекта является:

1. Положение «Об организации защиты электронной информации в банках Республики Узбекистан» №492 от 23.06.2001г. (Рег. №1047 от 09.07.2001 г.);
3. Положение «О защите информации в электронных системах Центрального банка и ответственности должностных лиц» (Рег. № 633 от 17.01.2006 г.);
4. Положение «О защите информации в электронных системах коммерческих банков Республики Узбекистан» (Рег. № 1552 от 13.03.2006 г.);
5. Постановление Президента Республики Узбекистан № ПП-3270 от 12.09.2017 г. «О мерах по дальнейшему развитию и повышению устойчивости банковской системы Республики Узбекистан»;

6. Постановление Президента Республики Узбекистан № ПП-3620 от 23.03.2018г. «О дополнительных мерах по повышению доступности банковских услуг»;

7. Постановление Президента Республики Узбекистан от 02.02.2017 г. № ПП-2751 "О мерах по созданию благоприятных условий для дальнейшего развития в республике системы безналичных расчетов на основе банковских пластиковых карточек"

8. Рапорт на имя Председателя Правления.

1.5. Плановые сроки начала и окончания поставки

Плановые сроки реализации проекта:
Срок поставки - 120 календарных дней
Срок выполнения интеграционных работ - 60 календарных дней

Все поставляемое оборудование должно быть новым, ранее неиспользованным и со сроком производства не ранее 2021 года.

1.6. Источники финансирования и условия оплаты

Источником финансирования проекта являются собственные средства АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан».

Условия оплаты с иностранной компанией:

- Товар: предоплата в размере 30% от суммы товара, остальные 70% от суммы после поставки товара на условиях DAP Ташкент и предоставления всех необходимых документов в течение 5 банковских дней.
- Услуги: предоплата в размере 30% от суммы услуг, остальные 70% от суммы оказанных услуг в течении 5 банковских дней после подписания акта выполненных услуг.

Условия оплаты с местной компанией:

- Товар: предоплата в размере 30% от суммы товара, остальные 70% от суммы после поставки товара на территорию заказчика и предоставления всех необходимых документов в течение 5 банковских дней.
- Услуги: предоплата в размере 30% от суммы услуг, остальные 70% от суммы оказанных услуг в течении 5 банковских дней после подписания акта выполненных услуг.

2. НАЗНАЧЕНИЕ ПРОЕКТА

Основным назначением Комплекса корпоративной защиты информации АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан» является защита вычислительных ресурсов текущей ИТ-инфраструктуры и сервисов в АО «Узнацбанк».

Целью реализации проекта является увеличение вычислительных мощностей текущего комплекса корпоративной защиты информации основного и резервного центра, повышение надежности и безопасности информационной среды АО «Узнацбанк».

3. ХАРАКТЕРИСТИКА ОБЪЕКТА МОДЕРНИЗАЦИИ

3.1. Краткие сведения об объекте модернизации

Комплекс корпоративной защиты информации АО «Национальный банк внешнеэкономической деятельности Республики Узбекистан» представляет собой систему из двух географически разнесённых подсистем – Основной центр (Головной офис) и Резервный Центр (МБРЦ). Каждый из объектов состоит из межсетевых экранов следующего поколения стоечного типа.

В состав комплексов защиты информации инфраструктуры для АО «Национального Банка внешнеэкономической деятельности Республики Узбекистан» входят следующие компоненты:

№	Наименование	Количество
1	Межсетевой экран следующего поколения	4
2	Система централизованного управления межсетевыми экранами	1

В головном офисе также развернута система централизованного управления межсетевыми экранами.
Состав комплекса можно разделить по принципу размещения целевых систем:

3.2. Состав подсистемы Головного офиса

В состав комплекса защиты информации инфраструктуры Головного офиса АО «Национального Банка внешнеэкономической деятельности Республики Узбекистан» входят следующие компоненты:

№	Наименование	Количество
1	Межсетевой экран следующего поколения	2
2	Система централизованного управления межсетевыми экранами	1

3.3. Состав подсистемы Резервный офиса

В состав комплекса защиты информации инфраструктуры Резервного офиса АО «Национального Банка внешнеэкономической деятельности Республики Узбекистан» входят следующие компоненты:

№	Наименование	Количество
1	Межсетевой экран следующего поколения	2

3.4. Обоснование выбора архитектуры

Текущий комплекс корпоративной защиты информации АО «Узнацбанк» функционирует на базе оборудования Check Point, который является масштабируемой системой. Модернизация может быть проведена за счет добавления межсетевых экранов к существующим межсетевым экранам. Учитывая, что основная часть комплекса корпоративной защиты информации уже сформирована, то целесообразно в дальнейшем наращивать инфраструктуру корпоративной защиты информации Банка путем добавлением межсетевых экранов совместимых с имеющимися сетевыми экранами, что позволит:

- Сохранить ресурсы благодаря исключению перехода инфраструктуры на иную аппаратную и программную платформу;
- Сохранить ресурсы на обучение персонала новым технологиям при работе с кардинально новой платформой;
- Продолжить использование всех преимуществ высокотехнологичной платформы;
- Проводить своевременную аналитику и мониторинг аппаратно-программной платформы;
- Сохранить гибкое управление серверной инфраструктурой, построенной на базе одного производителя;
- Снизить время устранения различных неполадок, благодаря своевременным аналитическим данным мониторинга.

В связи с чем, комплекс корпоративной защиты информации должен быть расширен путем добавления межсетевых экранов совместимых с имеющимися межсетевыми экранами Check Point.

4. ТРЕБОВАНИЯ К КОМПЛЕКСУ

4.1. Требования к межсетевому экрану

4.1.1. Межсетевой экран должен использовать контроль состояния соединений на основе детализированного анализа связи и состояния приложения для отслеживания и управления сетевым потоком.

4.1.2. Решение должно поддерживать DHCP, сервер и relay.

4.1.3. Решение должно поддерживать HTTP & HTTPS proxy.

4.1.4. Решение должно поддерживать функционал reverse proxy.

4.1.5. Решение должно поддерживать работу в режиме Mail Transfer Agent.

4.1.6. Решение должно иметь встроенный модуль анти-спам и безопасность электронной почты.

4.1.7. Решение должно предоставлять возможность глубокой инспекции пакетов (DPI)

4.1.8. Решение должно поддерживать отправку файлов и URL на анализ в cloud sandbox для обнаружения неизвестных угроз класса “0-day”.

4.1.9. Решение должно включать в себя возможность работы в режиме Transparent/Bridge.

4.1.9.1. Решение должно поддерживать работу на 2 уровне модели OSI (режим bridge).

4.1.9.2. Решение должно поддерживать функционал Firewall, IPS, URL-фильтрацию, DLP, Antibot, Antivirus, базовый функционал Web Application Firewall (SQL Injection, Cross Site Scripting, OWASP Top 10 и т.д.), управление приложениями, инспекцию HTTPS, Identity Awareness и Sandboxing в режиме bridge.

4.1.9.3. Решение должно поддерживать кластеризацию Active/Standby в режиме bridge.

4.1.10. Решение должно поддерживать высокую доступность шлюза и распределение нагрузки с синхронизацией состояний сетевых соединений. В связи с планируемым расширением межсетевых экранов, в режиме высокой доступности или режиме распределения нагрузки должно поддерживаться до 20 узлов кластера, с возможностью линейного увеличения пропускной способности кластера (включая пропускную способность со всеми включенными инспекциями IPS, AV, App Control, Url filter и т.д), путем добавления аналогичного межсетевого экрана в кластер.

4.1.11. Решение должно поддерживать виртуализацию шлюза безопасности для консолидации нескольких виртуальных шлюзов на одном физическом устройстве.

4.1.11.1. Решение должно иметь лицензию на 20 виртуальных систем.

4.1.11.2. Сетевые возможности: решение должно поддерживать виртуальные коммутаторы и виртуальные маршрутизаторы для конфигурирования сетевых коммуникаций между виртуальными системами (виртуальными шлюзами).

4.1.11.3. Эффективное обеспечение безопасности: каждый виртуальный шлюз должен иметь возможность запуска своего собственного набора сервисов безопасности. Например, один виртуальный шлюз работает как Firewall, второй – как Firewall и IPS, третий – Firewall, IPS, Application Control, URL Filtering, и так далее.

4.1.11.4. Выделение ресурсов: решение должно обеспечивать управление вычислительными мощностями, гарантируя, что каждая виртуальная система получит то количество процессорной мощности и оперативной памяти, которая необходима для выполнения ее задач.

4.1.12. Решение должно обеспечивать поддержку IPv6.

4.1.13. Решение должно поддерживать политику, основанную на QoS.

4.1.13.1. Решение должно позволять гарантировать или ограничивать пропускную способность и управлять задержкой для определенного IP источника, IP пункта назначения или сервиса.

4.1.13.2. Решение должно иметь возможность произвольного применения правил QoS для VPN трафика.

4.1.14. Решение должно обеспечивать функционал IPS (системы предотвращения вторжений).

4.1.14.1. Система IPS должна основываться на следующих механизмах обнаружения: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение на основе поведения.

4.1.15. Решение должно обеспечивать функционал Идентификации пользователей.

4.1.15.1. Должно быть способно к сбору идентификаторов пользователей посредством запроса Microsoft Active Directory на основе событий безопасности.

4.1.15.2. Должно иметь метод аутентификации идентификатора пользователя на основе браузера для недоменных пользователей или компьютеров.

4.1.15.3. Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности.

4.1.16. Решение должно обеспечивать функционал Управления приложениями и URL-фильтрации.

4.1.16.1. База данных управления приложениями должна содержать свыше 9900 известных приложений, включая приложения используемые в СНГ. Участник должен предоставить перечень приложений используемых в предлагаемом им решении.

4.1.16.2. Решение должно обеспечивать детальный контроль безопасности минимум для 250000 Web 2.0 виджетов.

4.1.17.3. Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL.

4.1.17. Решение должно обеспечивать функционал Anti-Bot и Anti-Virus.

4.1.17.1. Приложение Anti-bot должно быть способно обнаружить и остановить подозрительное анормальное сетевое поведение.

4.1.17.2. Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи.

4.1.17.3. Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам и останавливать входящие вредоносные файлы.

4.1.17.4. Приложение Anti-virus должно быть способно проверять шифрованный SSL трафик.

4.1.18. Решение должно поддерживать инспекцию многоканального SMBv3.

4.1.19. Решение должно обеспечивать функционал инспекции SSL (входящего / исходящего трафика).

4.1.20. Решение должно предоставлять возможность глубокой инспекции пакетов (DPI).

4.1.21. Решение должно обеспечивать функционал «песочницы» Sandboxing (инспекция – в облаке или на выделенном локальном устройстве).

4.1.21.1. Функционал «песочницы» должен обеспечивать защиту от атак нулевого дня.

4.1.21.2. Топология внедрения песочницы:

- Поддержка режима сетевой песочницы (network based);
- Поддержка режима инлайн (bridge mode);
- Поддержка режима почтового агента (mail transfer agent).
- Поддержка режима зеркального порта (TAP/SPAN порт).

4.1.21.3. Решение не должно содержать раздельную инфраструктуру для защиты почты и веба.

4.1.21.4. Решение должно эмулировать исполняемые файлы, архивы, документы, включая Java и flash.

4.1.21.5. Движок эмуляции должен поддерживать различные операционные системы, например, XP и Windows 7, в том числе специально настроенные образы (customized images).

4.1.21.6. Движок эмуляции должен инспектировать, эмулировать, предотвращать и передавать события в инфраструктуру защиты от зловредного ПО.

4.1.21.7. Решение должно обеспечивать эмуляцию файлов как небольшого размера, так и размером свыше 10Мбайт.

4.1.21.8. Решение должно детектировать атаки на стадии выполнения экслойта (exploitation) – т.е. до того как запускается шелл-код (shell code) и осуществляется загрузка/исполнение самого кода зловредного ПО.

4.1.21.9. Решение должно детектировать ROP (return oriented programming) и другие техники эксплойтов (а том числе эскалацию привилегий – privilege exploitation) посредством мониторинга выполнения последовательности инструкций центрального процессора.

4.1.21.10. Решение должно обеспечивать сканирование ссылок внутри почтовых сообщений для защиты от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО.

4.1.21.11. Решение должно содержать средства борьбы с методиками детектирования исполнения в песочнице.

4.1.21.12. Решение должно обеспечивать возможность управления им с централизованного менеджмента.

4.1.21.13. Решение должно генерировать детальный отчет по результатам анализа каждого зараженного файла.

4.1.21.14. Решение должно поддерживать мгновенную доставку безопасной копии потенциально опасного документа.

4.1.21.15. Решение должно поддерживать следующие технологии очистки документа от потенциальных угроз:

4.1.21.16. Конвертация в PDF с сохранением исходного форматирования, нейтрализацией ссылок, возможностью выделения и копирования текста;

4.1.21.16.1. Конвертация с сохранением исходного формата и удалением активного контента: скрипты, макросы, активные ссылки, вложенные объекты, нестандартные и стандартные поля.

4.1.21.17. Решение должно поддерживать Веб-портал самообслуживания для запроса исходных файлов пользователями после проверки их в «песочнице».

4.1.21.18. Решение должно обеспечивать гибкие настройки по поддержке оригинального формата файлов и указания тех видов контента, который должен быть удален.

4.1.21.19. Решение должно обеспечивать функционал Anti-Spam и безопасности электронной почты.

4.1.22. Решение должно обеспечивать сканирование ссылок внутри почтовых сообщений для защиты от атак нулевого дня, решение должно поддерживать возможность блокировки ссылок с отложенной атакой.

4.1.23. Решение должно обеспечивать функционал IPSEC VPN.

4.1.23.1. Должна быть поддержка внутреннего CA (Certificate Authority), а также внешних сторонних CA.

4.1.23.2. Решение должно поддерживать 3DES и AES-256 шифрование для IKE фазы I и II IKEv2, а также "Suite-B-GCM-128" и "Suite-B-GCM-256" для фазы II.

4.1.23.3. Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5 (1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20

4.1.23.4. Решение должно поддерживать обеспечение целостности данных средствами md5, sha1 SHA-256, SHA-384 и AES-XCBC

4.1.23.5. Решение должно включать в себя поддержку для VPN типа site-to-site в следующих топологиях:

4.1.23.6. Полносвязная сеть (все-со-всеми),

4.1.23.7. Звездообразная сеть (удаленные офисы к центральному сайту)

4.1.23.8. Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт)

4.1.23.9. Иметь возможность приобретения лицензии на функционал DLP. Функционал DLP должен обеспечивать контроль за утечкой конфиденциальной информации по протоколам SMTP, FTP, HTTP, HTTPS, TLS и веб-почте, должна поддерживаться возможность расшифровки SSL-трафика. Должна поддерживаться возможность определения конфиденциальных документов по преднастроенным шаблонам или по метке документов водяными знаками. Система должна поддерживать более 500 типов данных

4.1.24. Удаленный мобильный доступ

4.1.24.1. Решение должно обеспечивать функционал Удаленного мобильного доступа минимум для 5 одновременных соединений пользователей.

4.1.24.2. Решение должно поддерживать управляемые и неуправляемые устройства доступа, такие как BYOD (принеси собственное устройство)

4.1.24.3. Решение должно обеспечивать Мобильный VPN-Клиент: VPN-приложение, обеспечивающее безопасный доступ к корпоративным ресурсам через SSL или IPsec туннель.

4.1.24.4. Решение должно обеспечивать SSL VPN-Портал: механизм для безопасного подключения к корпоративным ресурсам через портал из веб-браузера.

4.1.24.5. Решение должно обеспечивать функционал безклиентного VPN: плагин, который обеспечивает удаленный доступ с предоставлением полной возможности сетевого соединения для IP-приложений. Решение должно обеспечивать функционал SSL VPN 3-уровня по запросу для подключения к корпоративным ресурсам. Решение должно поддерживать любое IP-приложение, включая ICMP, TCP и UDP, не требуя сложной конфигурации для поддержки каждого приложения. Он должен работать на удаленных компьютерах, не требуя прав администратора.

4.1.24.6. Решение должно обеспечивать технологию виртуального рабочего стола, которая позволяет защищать данные во время сеансов пользователей и позволяет чистить кэш после окончания сеансов. Технология виртуального рабочего стола должна защищать все данные конкретной сессии на стороне клиента, а также:

- Создавать безопасную виртуальную среду, изолированную от хоста,
- Шифровать и удалять кэш, файлы и т.д. браузера и приложений, когда сеанс окончен.

4.1.24.7. Решение должно поддерживать интеграцию с решениями двухфакторной аутентификации.

4.1.24.8. Решение должно реализовать функционал интегрированной системы предотвращение вторжений от вредоносного кода, передаваемого в веб-приложениях. Решение должно быть способно блокировать червей, различные атаки, такие как переполнение буфера, SQL и инъекции команд, межсайтовый скриптинг, настраиваемый модуль блокирования HTTP червей, защиту от обход каталога (directory traversal), защиту от отклонения заголовков (header rejection),защиту от вредоносного HTTP-кода.

4.1.24.9. В целом, решение должно обеспечивать следующие функции:

- Безопасный SSL VPN доступ
- Ассоциирование мобильных устройств с конечными пользователями
- Обеспечение соответствия конечных точек соединения корпоративной политике

4.1.25. Аппаратные и рабочие требования для каждого межсетевого экрана:

4.1.25.1. Размер каждого межсетевого экрана не должен превышать 1 RU.

4.1.25.2. Продуктивные сетевые интерфейсы (минимальные требования):

- 8 x 1 Гбит/с медных Ethernet
- 4 x 1 Гбит/с оптических SFP
- 1 x Ethernet консольный порт
- 1 x 1 Гбит/с выделенный порт управления
- 2 x USB порта
- 2 x блока питания

4.1.25.3. Пропускная способность Firewall: минимум 12 Гбит/с. (Real condition traffic)

4.1.25.4. Пропускная способность IPS: минимум 6.5 Гбит/с.

4.1.25.5. Пропускная способность NGFW (с активированным функционалом Firewall, Application Control и IPS): минимум 5.5 Гбит/с.

4.1.25.6. Пропускная способность Threat Prevention (с активированным функционалом Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot и облачный Sandbox): минимум 2.5 Гбит/с.

4.1.25.7. Решение должно иметь встроенную лицензию на 20 виртуальных систем.

4.1.25.8. Одновременные соединения: минимум 8 миллионов.

4.1.25.9. Новые соединения: минимум 90 000 в секунду.

4.1.25.10. Локальное дисковое пространство: не менее 1x240 Гб SDD.

4.1.25.11. Объем оперативной памяти: не менее 32Gb

4.1.26. Поддержка и подписка.

4.1.26.1. Гарантийный период, техническая поддержка и подписка на обновления программного обеспечения и всех модулей должна составлять 5 лет и оказываться производителем предлагаемого решения. Уровень сервиса не ниже чем 24x7x365;

4.2. Требования к системе централизованного управления межсетевыми экранами.

4.2.1. Решение должно обеспечивать функционал централизованного управления безопасностью.

4.2.1.1. Все приложения безопасности межсетевых экранов следующего поколения должны быть управляемыми с центральной консоли GUI.

4.2.1.2. Система централизованного управления межсетевыми экранами должна управлять минимум 4 межсетевыми экранами .

4.2.1.3. Система централизованного управления межсетевыми экранами должна поддерживать учетные записи администраторов на основе ролей. Например, только роли для управления политикой брандмауэра или только роль для просмотра журнала.

4.2.1.4. Решение должно обеспечивать возможность обеспечения высокой доступности системы управления, используя резервный сервер управления, который автоматически синхронизируется с активным сервером.

4.2.1.5. Решение должно включать возможность централизованного распространения и применения новых версий программного обеспечения на межсетевые экраны.

4.2.1.6. Решение должно включать инструмент для централизованного управления лицензиями всех межсетевых экранов, контролируемых системой управления.

4.2.2. Решение должно обеспечивать механизм обновлении всех модулей, включая IPS, Контроль приложений, URL-фильтрацию, Anti-Bot и Anti-Virus.

4.2.3. Решение должно обеспечивать функционал Централизованного Протоколирования & Мониторинга.

4.2.3.1. Система централизованного протоколирования событий должна быть частью системы управления.

4.2.3.2. Решение должно протоколировать все правила.

4.2.3.3. У средства просмотра журналов событий должна быть возможность индексированного поиска.

4.2.3.4. Решение должно иметь возможность протоколирования событий во всех интегрированных модулях безопасности на межсетевых экранах (включая виртуальные межсетевые экраны), включая Firewall, IPSEC VPN, IPS, Идентификация пользователей, Мобильный доступ, DLP, Управление приложениями, URL-фильтрацию, Anti-Bot, Anti-Virus, Sandboxing.

4.2.3.5. У системы протоколирования должен быть безопасный канал для передачи данных для предотвращения подслушивания, канал передачи должен быть зашифрован и проходить проверку подлинности.

4.2.3.6. Журналы событий должны безопасно передаваться между шлюзом и управлением или выделенным сервером журналов.

4.2.3.7. Решение должно включать опцию динамического блокирования активного соединения в графическом интерфейсе системы протоколирования событий без необходимости внесения изменений в базу правил.

4.2.3.8. Решение должно включать настраиваемую установку пороговых значений параметров для выполнения действий при достижении определенных пороговых значений на межсетевом экране. Действия должны включать: запись события, оповещение, отправка SNMP trap, отправка электронного письма и выполнение определенного пользователем предупреждения.

4.2.3.9. Решение должно включать предварительно настроенные графики для мониторинга трафика во времени и системных счетчиков: главные правила безопасности, основные пользователи P2P, VPN туннели, сетевой трафик и другая полезная информация. Решение должно обеспечивать возможность создания новых графиков с различными типами диаграмм.

4.2.3.10. Решение должно поддерживать сегментирование политики безопасности по слоям с возможностью делегирования полномочий разным администраторам с точностью до блоков правил в общей политике.

4.2.3.11. Решение должно обеспечивать хранение ревизий политик для межсетевых экранов нового поколения с возможностью возврата изменений к предыдущим версиям ревизий.

4.2.4. Решение должно обеспечивать функционал Централизованной Корреляции событий и Отчетов.

4.2.4.1. Решение должно иметь возможность корреляции событий из всех модулей, включая Firewall, IPSEC VPN, IPS, Идентификация пользователей, Мобильный доступ, DLP, Управление приложениями, URL-фильтрация, Anti-Bot, Anti-Virus, Sandboxing.

4.2.4.2. Решение должно включать инструмент для корреляции событий из всех функций межсетевого экрана и сторонних устройств.

4.2.4.3. Приложение корреляции событий должно обеспечивать графическое представление событий на основе времени.

4.2.4.4. Решение должно включать возможность поиска внутри списка событий, углубления в детали для изучения и расследования инцидентов.

4.2.4.5. Решение должно включать предопределенные ежечасные, ежедневные, еженедельные и ежемесячные отчеты, в том числе, как минимум, Основные события, Основные источники, Основные пункты назначения, Основные сервисы, Основные источники и их основные события, Основные пункты назначения и их основные события, и Основные сервисы и их основные события.

4.2.4.6. Решение должно поддерживать автоматическое распространение отчетов по электронной почте, загрузку на FTP/Веб-сервер и скрипт рассылки внешних пользовательских отчетов.

4.2.4.7. Технические требования, поддержка и подписка. Система централизованного управления должна быть предоставлена в виде виртуальной машины и быть развернута в инфраструктуре заказчика. Требования к необходимым ресурсам должны быть предоставлены на этапе интеграции.

4.2.4.8. Решение должно обеспечивать функционал управления рисками и соответствия требованиям (GRC) – лучших практик безопасности на первый год использования.

4.2.4.8.1. Решение должно обеспечивать оценку соблюдения основных регуляторных требований в режиме реального времени (поддержка стандартов ISO 27001/27002, PCI-DSS,HiPPA,SOX и т.д.).

4.2.4.8.2. Решение должно предоставлять рекомендации по реализации лучших практик безопасности.

4.2.4.8.3. Решение должно переводить регуляторные требования в инструкции для выполнения лучших практик безопасности.

4.2.4.8.4. Решение должно постоянно контролировать конфигурацию шлюза при помощи лучших практик безопасности.

4.2.4.8.5. Решение должно генерировать автоматические отчеты по оценке для

определения рейтинга соответствия регуляторным требованиям.

4.2.4.8.6. Решение должно полностью интегрироваться в Архитектуру программного обеспечения и Инфраструктуру управления.

4.2.4.8.7. Решение должно обеспечивать мгновенное уведомление об изменениях политики, влияющих на соответствие регуляторным требованиям.

4.2.5. Система централизованного управления безопасностью должна быть выполнена в виде программного обеспечения, устанавливаемого на сервера, входящие в список аппаратной совместимости производителя, а так же виртуальные машины, функционирующие в средах виртуализации VMWare, Microsoft, KVM.

4.2.6. Система централизованного управления межсетевыми экранами должна поставляться с технической поддержка от производителя и подписками сроком на 5 лет, 24x7x365; гарантийная замена оборудования и все необходимые подписки на сервисы безопасности должны быть активны на весь приобретаемых период времени.

5. ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕСЧЕНИЯ КОМПЛЕКСА

5.1. Требования к составу и содержанию работ по модернизации комплекса

Исполнитель должен произвести все необходимые действия по нативной миграции существующих конфигураций и правил для расширяемого оборудования, без простоя и прерывания работы действующей системы в целом. Участник должен подготовить планы тестирования и подробные планы приёмочных испытаний.

Приостановка действующих сервисов – недопустима.

Участник должен предоставить поэтапный план миграции оборудования с указанием сроков, перечня работ и состава привлекаемых специалистов.

5.2. Требования к обучению персонала

Участник должен предоставить очное обучение для двух инженеров Заказчика в сертифицированном производителем оборудования учебном центре. Обучение должно включать в себя темы по установке, базовой и расширенной настройке, конфигурированию дополнительных сервисов, поиска и устранения неисправностей.

5.3. Сроки поставки и гарантии на оборудование

Срок поставки оборудования – 120 календарных дней.

Гарантийный период, техническая поддержка и подписка на обновления программного обеспечения и всех модулей должна составлять 5 лет и оказываться производителем предлагаемого решения. Уровень сервиса не ниже чем 24x7x365.

5.4. Требования к гарантийному обслуживанию

5.4.1. На всё предлагаемое участником решение поддержка должна осуществляться производителем оборудования и поставляться сроком на не менее чем 5 лет;

5.4.2. Прием запросов и обеспечение реакции на инциденты должно производиться в режиме 24x7 (24 часа, 7 дней в неделю).

5.4.3. Возможность создавать запросы с наивысшим приоритетом.

5.4.4. Соглашение об уровне обслуживания (Service Level Agreement (SLA) должно соответствовать или превосходить значения указанные в таблице ниже:

Уровень критичности	Время Реагирования (в соответствии с Планом поддержки)	Описание

Приоритет 1	30 Минут	Выделенная техническая поддержка производителя круглосуточно, до решения проблемы, или предоставление временного решения что бы минимизировать время неработоспособности сервисов.
Приоритет 2	2 Часа	Выделенная техническая поддержка производителя в стандартные рабочие часы, до решения проблемы, или предоставление временного решения что бы минимизировать время неработоспособности сервисов в не стандартные рабочие часы.
Приоритет 3	4 Часа	Выделенная техническая поддржка производителя в стандартные рабочие часы, до решения проблемы, или предоставление временного решения что бы минимизировать время неработоспособности сервисов
Приоритет 4	4 Часа	Выделенная техническая поддержка производителя в стандартные рабочие часы

5.4.4.1. Приоритет 1

- Ошибка непосредственно влияющая на безопасность решения;
- Ошибка в Программном обеспечении или Устройстве, которая делает продукт неработоспособным или вызывает катастрофический сбой продукта; например, критическое воздействие на систему, сбой системы;
  Сообщение о дефекте лицензионного продукта в производственной среде, который невозможно обойти в разумных пределах, при котором существует аварийное состояние, существенно ограничивающее использование лицензионного продукта для выполнения необходимых бизнес-функций.

5.4.4.2. Приоритет 2

- Ошибка, относящаяся к Программному обеспечению или Устройству, которая существенно снижает производительность продукта или существенно ограничивает бизнес; например, серьезное воздействие на систему, временное зависание системы;
- дефект лицензионного продукта, который ограничивает использование одной или нескольких функций лицензионного продукта для выполнения необходимых бизнес-функций, но не ограничивает полностью использование лицензионного продукта.

5.4.4.3. Приоритет 3

- Ошибка, относящаяся к Программному обеспечению или Устройству, которая оказывает лишь умеренное влияние на использование продукта; например, умеренное влияние на систему, влияние на производительность/эксплуатацию;
- Ошибка, которая может привести к некоторым функциональным ограничениям, но не оказывает критического или серьезного влияния на работу.

5.4.4.4. Приоритет 4

- Аномалия в лицензионном продукте, которая существенно не ограничивает использование одной или нескольких функций лицензионного продукта для выполнения необходимых бизнес-функций; это незначительная проблема и не имеет существенного значения для работы;
- Аномалия, которую можно легко обойти или которую необходимо отправить в техническую поддержку в качестве запроса на улучшение.

5.4.5. Прием запросов должен осуществляться по прямой телефонной линии и адресу электронной почты.

5.4.6. Каждое обращение должно фиксироваться в базе автоматизированной системы управления инцидентами.

5.4.7. Количество обращений в службу поддержки должно быть неограниченным.

5.5. Требования к безопасности

Необходимый уровень безопасности должен обеспечиваться Заказчиком путем строгого соблюдения правил эксплуатации и технического обслуживания оборудования, рекомендованных Исполнителями и разработчиками средств информатизации.

Работы по монтажу и наладке системы, а также последующее ее техническое обслуживание не должны быть сопряжены с воздействием на персонал опасных значений электрического тока, электромагнитных полей, акустических шумов, вибраций и т.д.

Конструкция технических средств должна обеспечивать защиту обслуживающего персонала от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.003 и ГОСТ 12.2.007.0.

Помещения, где будут размещаться технические средства системы, должны соответствовать с требованиями руководящего документа RH 45-201:2011;

Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление в соответствии с ГОСТ 12.1.030-81;

Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в целях нагрузки, а также аварийное ручное отключение.

Конструкция технических средств должна обеспечивать свободный доступ к отдельным узлам и элементам для их технического обслуживания и ремонта, удобное подключение силовых кабелей.

Безопасность помещений, в которых будут размещаться технические средства системы должна обеспечиваться соответствующей рабочей группой при банке, ответственной как за эксплуатацию комплекса в целом, так и за реализацию настоящего Технического задания.

5.6. Требования к транспортированию

Все оборудование должно быть в заводской упаковке от производителя.

5.7. Требования к техническому обеспечению

Проект подразумевает поставку, установку и пуско-наладку, что включает в себя обеспечение доставки при условии всех требований по поставке, установке, монтажу, настройки и документирования Оборудования, пуско-наладки вычислительной системы, обучения, тестирования работоспособности поставляемого оборудования (проведения приемочных испытаний) и ввод в действие и начала полноценного функционирования. В техническом предложении должен быть представлен перечень, количество и технические характеристики предлагаемого оборудования.

Поставляемое оборудование и программное обеспечение должно соответствовать техническим требованиям, указанным в п. 3 и п. 4.

Предлагаемое и поставляемое оборудование и программное обеспечение должно иметь технические характеристики не ниже указанных в технических требованиях (п. 3 и п. 4.).

5.8. Требования к месту и условиям поставки закупаемого оборудования

Исполнитель должен обеспечить доставку закупаемого в рамках проекта оборудования:

- для отечественных поставщиков: по адресу Республика Узбекистан 100084, г. Ташкент, проспект А.Темура, 101.
- для иностранных поставщиков: DAP г. Ташкент (ИНКОТЕРМС 2020).

Поставка и погрузочно-разгрузочные работы товаров осуществляется автомобильным транспортом, воздушным транспортом либо любым иным способом за счет средств поставщика до места поставки.

Директор Департамента
информационной и банковской безопасности Мухамадкулов Ш.Н.