«УТВЕРЖДАЮ»

Первый Заместитель председателя ГНК РУз

Председатель закупочной комиссии

_____ М.М. Мирзаев

«____» _____ 2022 г

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на:

ПРИОБРЕТЕНИЕ СИСТЕМЫ КОНТРОЛЯ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ ГОСУДАРСТВЕННОГО НАЛОГОВОГО КОМИТЕТА

На ___ листах

Действует с «____» _____ 2022 г.

г. Ташкент

СОДЕРЖАНИЕ

1. Общие сведения 3
1.1. Полное наименование ИС и ее условное обозначение 3
1.2. Наименование организации заказчика 3
1.3. Исполнитель 4
1.4. Основание для разработки ТЗ 4
1.5. Плановые сроки начала и окончания работ 4
1.6. Порядок оформления и предъявления результатов работ 4
2. Назначение и цели приобретения и внедрения ИС 4
2.1. Назначение ИС 4
2.2. Цели 5
3. Требования к ИС 6
3.1. Общие требования к ИС в целом 6
3.2. Функциональные (технические) требования 7
3.3. Требования к функционалу контроля привилегированных пользователей 12
3.4. Требования к приобретению, внедрению и поддержке ИС 14
4. Состав и содержание работ 15
5. Порядок контроля и приемки ИС 17
6. Требования к составу и содержанию работ по подготовке ИС к вводу в действие 18
7. Требования к документированию 18
8. Дополнительные требования 18
8.1. Требования к месту выполнения работ 18
8.2. Требования к исполнителю 19
8.3. Требования к безопасности выполнения работ и оказания услуг 19
8.4. Требования к обучению персонала заказчика 19
Приложение 1. Термины, сокращения и их определения 20

1. Общие сведения

Государственный налоговый комитет Республики Узбекистан в целях реализации стратегии развития спектра электронных услуг и улучшения качества предоставляемых услуг для своих пользователей планирует реализацию проекта на приобретение системы контроля привилегированных пользователей.

Настоящее Техническое задание описывает общие требования для специализированного программного обеспечения по контролю привилегированных пользователей.

1.1. Полное наименование ИС и ее условное обозначение

Полное наименование ИС: Система контроля привилегированных пользователей Государственного Налогового Комитета

Условное обозначение ИС: СКПП (далее ИС)

1.2. Наименование организации заказчика

В рамках данного технического задания, Заказчиком информационной системы является Государственный налоговый комитет Республики Узбекистан

Государственный налоговый комитет Республики Узбекистан
Адрес: г. Ташкент, 100011, улица Абдулла Кадыри, дом 13-а
Телефон: (8-371) 244-97-16 Факс: (8-371) 244-89-12
E-mail: org@soliq.uz
л.сч. 40101086026277770113310930001 ИНН: 202883501 ОКОНХ: 97150
РКЦ Гл. упр. Центрального банка РУ по г. Ташкенту; МФО: 00014
Опер. Упр. Каз. Мин.Фин. РУ.

1.3. Исполнитель

Исполнитель выбирается на основании конкурсных и/или тендерных торгов, либо иным путем согласно действующих законов, нормативных актов, постановлений и прочих нормативных документов по предмету приобретения программного обеспечения.

1.4. Основание для разработки ТЗ

Основанием для разработки настоящего ТЗ на приобретение системы контроля привилегированных пользователей является необходимость соответствия утвержденной политики информационной безопасности ГНК,

1.5. Плановые сроки начала и окончания работ

Плановые сроки начала работ: октябрь 2022 года.

Плановые сроки окончания работ: декабрь 2022 года.

Срок выполнения работ: не более 50 рабочих дней.

1.6. Порядок оформления и предъявления результатов работ

Работы по внедрению системы контроля привилегированных пользователей должны осуществляться и приниматься в порядке, установленном в разделе 4 настоящего Технического задания.

Приемка результатов работ должна проводиться в порядке, установленном в разделе 5 настоящего Технического задания.

2. Назначение и цели приобретения и внедрения ИС

2.1. Назначение ИС

Программное обеспечение контроля привилегированных пользователей предназначено для мониторинга и контроля учётных записей, а также аудита выполняемых действий на подключенных к ИС системах ГНК.

2.2. Цели

Основной целью приобретения ИС является минимизация рисков информационной безопасности, связанных со злоупотреблением правами доступа к системам ГНК сотрудниками Заказчика, а также третьими лицами (подрядчики, производители) (далее - привилегированные пользователи). Минимизация рисков достигается за счет снижения вероятности несанкционированного доступа к управляемым системам, неконтролируемого доступа к управляемым ИС системам, неконтролируемого изменения их настроек, путем записи сессий работы сотрудников.

3. Требования к ИС

Настоящее техническое задание для приобретения системы контроля привилегированных пользователей (далее ИС) описывает комплекс требований к программному обеспечению.

3.1. Общие требования к ИС в целом

Общие требования к системе контроля привилегированных пользователей:

– ИС должна иметь встроенный механизм защиты от несанкционированного доступа к операционной системе контроля привилегированных пользователей. Данная защита должна обеспечивать использование специального ключа защиты (пароля) при каждом запуске ИС (после выключения или перезагрузки).

– Настройка и администрирование ИС должно осуществляться через отдельный веб-портал администрирования на базе HTML с помощью любого современного браузера (Edge, Firefox, Chrome и др.) без необходимости установки дополнительных компонентов (плагинов, приложений и т. п.). Использование веб-консоли на базе технологий Flash или Java (JRE) не допускается.

– Администрирование ИС должно поддерживать ролевую модель управления и надзора за привилегированными пользователями.

– ИС должна предоставлять привилегированным пользователям специальный дополнительный веб-портал(ы) для доступа к контролируемым (целевым) системам. Использование данного портала должно быть опциональным (необязательным), т. е. ИС должна обеспечивать доступ к контролируемым (целевым) системам в том числе и без такого портала (посредством использования специализированных приложений).

– ИС должна иметь возможность создания отказоустойчивых конфигураций на базе встроенных технологий, использование сторонних (внешних) средств для построения таких (отказоустойчивых) конфигураций - не допускается.

– ИС должна иметь встроенные системы диагностирования, связанные с ошибками доступа к контролируемым (целевым) системам.

– ИС должна иметь функционал хранения и обработки всех событий, связанных с работой ИС, а также - функционал автоматической передачи таких событий во внешние системы обработки событий.

– ИС должна иметь функционал управления различными объектами такими как пользователи, целевые системы, способы подключения как локально (с помощью веб-портала), так и удаленно (с помощью открытых API-интерфейсов).

– Интерфейс ИС должен быть доступен на английском и русском языках.

Требования к вендору ИС и поставщику:

- Поставщику услуг/сервиса необходимо иметь сертифицированных специалистов по внедрению и настройке ИС;
- Наличие квалифицированного персонала на территории РУз, имеющего успешный опыт внедрения предлагаемого решения и по услугам технической поддержки. Оказание технической поддержки на узбекском и русском языках;
- Информационная система, а также лицензии к ней должны быть переданы в электронном формате;

- Производитель информационной системы обязуется поддерживать поставляемое решение не менее чем на срок активной гарантийной поддержки лицензии с момента поставки.

Исполнитель, в рамках выделенного бюджета, может предложить аналогичное / альтернативное либо с превосходящими характеристиками решение, которое будет выполнять все поставленные цели и задачи, указанные в настоящем техническом задании (с учетом целевого назначение и показателей). Для соответствия техническому заданию допускается установка опциональных модулей (в том числе взаимоинтегрированные), имеющихся в линейке разработчиков решения.

Производитель гарантирует наступление даты окончания поддержки поставляемого решения не ранее чем через 5 лет с момента заключения договора на поставку решения.

3.2. Функциональные (технические) требования

Функциональные (технические) требования к ИС:

– ИС должна поддерживать запись действий привилегированных пользователей встроенными средствами без необходимости установки любого компонента (агента, сервиса, драйвера и т. д.) как на конечные рабочие точки привилегированных пользователей, так и на системы, к которым подключаются привилегированные пользователи (целевые системы).

– ИС должна иметь встроенный функционал распознавания текстовой информации в записанных графических сессиях (OCR механизм или аналог), в том числе - кириллические символы, с целью дальнейшего поиска такой информации. Данный функционал должен работать как в ручном режиме, так и в автоматическом (применяться к каждой сохраненной сессии без вмешательства администратора ИС).

– Функционал ИС должен поддерживать расширенные сетевые настройки, такие как:

- поддержка виртуальных сетей (VLAN);
- агрегация сетевых каналов;
- создание собственных таблиц ARP;
- настройки статической маршрутизации для отдельных сетей;

– ИС должна иметь встроенную панель информирования о статусе работоспособности и нагрузках на компоненты ИС, по меньшей мере: нагрузка на процессор, нагрузка на оперативную память. Такая панель информирования должна быть доступна только для администраторов ИС на соответствующем веб-портале администрирования.

– ИС должна иметь возможность работы с не менее чем двумя виртуальными сетевыми адаптерами. Каждому сетевому адаптеру ИС должна иметь возможность присваивать уникальный IP-адрес (в том числе - с различных сетевых сегментов) как в статическом режиме, так и динамическом

(с помощью DHCP сервиса). Для каждого такого уникального IP-адреса ИС должна иметь возможность присваивать привилегированным пользователям специальный отдельный веб-портал для доступа к контролируемым (целевым) системам. ИС должна иметь функционал сегментации доступа к таким веб-порталам на основе групп пользователей и целевых систем.

– Каждый веб-портал для привилегированных пользователей должен предоставлять привилегированным пользователям следующие возможности:

- перечень доступных для подключения целевых систем с возможностью открытия сессий с помощью стандартных клиентов;
- перечень доступных для подключения целевых систем с возможностью открытия сессий с помощью встроенного WEB клиента;
- перечень IP-адресов и портов целевых систем;
- тип протокола, который используется для подключения к целевой системе;
- просмотр пароля к целевой системе (в случае если такие права предоставлены привилегированному пользователю соответствующей парольной политикой);
- изменение пароля на веб-портале для учетной записи привилегированного пользователя (в случае если пароль хранится в собственном защищенном хранилище ИС);

– Возможность дополнительных настроек таких как вывод дополнительной информации для привилегированных пользователей, логотипов заказчика и т. д. будет дополнительным преимуществом;

– ИС должна иметь встроенное защищенное хранилище для хранения записанных сессий привилегированных пользователей, реквизитов доступа (логин, пароль, ключи) к ИС и целевым системам, и журналам событий. Защищенное хранилище должно использовать стандартные крипто алгоритмы уровня не ниже AES-256;

– Ролевая модель использования ИС должна обеспечивать следующие разграничения на базе различных типов учетных записей:

- полные права администрирования, в том числе, возможность конфигурирования ИС;
- частично ограниченные права администрирования - любого действия кроме конфигурирования ИС;
- ограниченные права администрирования - возможность настройки и дальнейшего наблюдения за конкретно заданными целевыми системами и привилегированными пользователями;
- права пользователя - возможность подключения к заданным целевым системам без возможности входа в веб-портал администрирования;

– ИС должна иметь функционал добавления администраторов через веб-портал администрирования ИС с возможностью выбора роли, срока

действия учетной записи, языка и образа аутентификации администратора. Для каждой учетной записи администратора должна быть поддержка одновременно нескольких способов аутентификации, по меньшей мере:

- с помощью статического пароля, что хранится в защищенном хранилище ИС;
- одноразового пароля, который генерируется внешними сервисами (например, RADIUS-сервером);
- с помощью внешнего каталога пользователей (AD/LDAP);
- с помощью SSH ключа;
- должен иметь функционал MFA (в том числе для доменных учётных записей) с возможностью таких методов аутентификации как OATH (TOTP и HOTP), DUO; для метода OATH должна присутствовать поддержка приложения Google Authenticator;

– ИС должна иметь функционал добавления привилегированных пользователей через веб-портал администрирования ИС с возможностью выбора роли, срока действия учетной записи, языка и образа аутентификации администратора

– ИС должна иметь функционал добавления привилегированных пользователей следующими способами:

- в ручном режиме;
- синхронизация с уже существующим каталогом пользователей (AD / LDAP);
- через API интерфейс;

– ИС должна поддерживать не менее трех одновременных систем внешней аутентификации привилегированных пользователей и администраторов ИС на базе серверов каталогов пользователей AD и LDAP. Для каждого сервера каталога пользователей (AD или LDAP) ИС должна иметь возможность задавать приоритет использования (по отношению к другим таким серверам) и иметь следующие параметры:

- имя и пароль пользователя, имеющего доступ на чтение групп пользователей на сервере каталога пользователей AD или LDAP;
- организационную группу (OU) в каталоге пользователей в которой нужно искать привилегированных пользователей;
- адрес (FQDN или IP) и порт сервера каталога пользователей;
- возможность использования шифрованного (безопасного) соединения с помощью сертификатов;

– ИС должна иметь функционал автоматического предоставления отдельным группам привилегированных пользователей доступа к пулу целевых систем на базе заданной группы на сервере каталога пользователей (AD или LDAP).

– ИС должна иметь функционал создания безопасных (шифрованных) каналов связи на основе сертификатов SSL между привилегированными пользователями и ИС и между ИС и целевыми системами. Создание таких безопасных (шифрованных) каналов связи должно создаваться на основе как самоподписных сертификатов (с помощью пары «открытый» - «закрытый» ключей), так и на основе сертификатов центра сертификации (CA).

– Добавление целевых систем, сессии привилегированных пользователей, которые будут контролироваться, должно выполняться с помощью соответствующего меню в веб-панели администрирования, при этом ИС должна иметь функционал:

- одиночного добавления целевых серверов (по IP-адресу или FQDN и порту);
- группового добавления целевых систем (с помощью сетевой маски, наложенной на IP-подсеть);
- группового добавления целевых систем с помощью открытых API-интерфейсов;

– ИС должна иметь функционал выбора нумерации портов, по которым подключаются привилегированные пользователи, то есть, администратор ИС должен иметь возможность принудительного изменения портов подключения для привилегированных пользователей к целевым системам.

– ИС должна поддерживать работу с целевыми системами, аутентификация привилегированных пользователей на которых выполняется следующим образом:

- посредством введения локальной учетной записи;
- посредством введения доменного учетной записи;
- с помощью SSH-ключа;

– ИС должна иметь следующие возможности работы с реквизитами доступа (логины, пароли, имя домена, ключи SSH) используемыми привилегированными пользователями для подключения к целевым систем:

- ручное создание и хранение реквизитов доступа в защищенном хранилище ИС;
- использование внешних систем аутентификации (в том числе - внешних специализированных хранилищ паролей);
- анонимный доступ (без необходимости ввода реквизитов доступа);

В случае ручного создания и хранения реквизитов доступа для подключения к целевым систем, ИС должна иметь функционал полной маскировки (до и во время этапа аутентификации) от привилегированных пользователей данных реквизитов (кроме случаев, где просмотр пароля разрешен настройками ИС).

– ИС должна обеспечивать функционал дополнительной (повторной) принудительной аутентификации на целевых системах даже, в случае если реквизиты доступа привилегированных пользователей в ИС и на целевых системах полностью совпадают.

– ИС должна иметь возможность принудительной смены паролей на отдельных целевых системах по завершении активных сеансов и заданной парольной политике для отдельно заданных реквизитов доступа для подключения к целевым систем. Такая парольная политика должна обеспечивать задание следующих параметров:

- длина пароля;
- сложность пароля (в том числе, требования к прописным буквам, цифровым символам, специальным символам);
- частота смены пароля;

Принудительная смена паролей в соответствии с заданной парольной политикой должна поддерживаться как минимум на таких целевых системах как:

- UNIX / Linux-based операционные системы (посредством SSH);
- Windows операционные системы (через WMI / LDAP);

Функционал безопасного обмена паролями между программными приложениями будет преимуществом.

– ИС должна иметь встроенный функционал оценки эффективности работы с целевыми системами как отдельных привилегированных пользователей, так и групп привилегированных пользователей. Функционал эффективности работы с целевыми системами должен предоставлять статистику активных действий привилегированных пользователей (время активной работы по отношению к общему времени работы с целевой системой) с возможностью детализации и экспорта статистики во внешней отчет.

– ИС должна иметь систему хранения и обработки событий в виде журналов, хранящихся в защищенном хранилище. Все журналы событий должны быть защищены от удаления, в том числе администраторами ИС с самыми высокими уровнями доступа (правами). Журналы событий должны включать как минимум следующую информацию:

- события, связанные с работоспособностью ИС (в том числе журналы настроек);
- события, связанные с работой привилегированных пользователей на целевых системах;
- события, связанные с администрированием ИС;

– ИС должна иметь возможность экспорта полного или частичного журнала событий во внешний файл текстового формата. Частичный экспорт должен осуществляться по различным критериям (таким как аккаунт привилегированного пользователя (-ей), тип события, имя целевой системы, дата).

– ИС должна иметь интеграцию с внешними системами обработки событий с помощью стандартных протоколов, таких как SNMP, syslog.

3.3. Требования к функционалу контроля привилегированных пользователей

Требования к функционалу контроля привилегированных пользователей:

– ИС должна обеспечить функционал подключения к сессии с возможностью перехвата управления действий привилегированных пользователей. То есть, ИС должна обеспечивать одновременную работу пользователя и администратора, который подключается к активной сессии и перехватывает управление конечной системой с фиксацией логов, кто и когда выполняет конкретные действия.

– ИС должна обеспечивать контроль привилегированных пользователей, которые подключаются к различным целевым системам для управления, внесения изменений и работе с ними, а также контролировать передачу файлов на данные системы без подключения к ним.

– ИС должна иметь возможность воспроизведения графического интерфейса при терминальном подключении.

– ИС должна иметь функционал по принудительному ограничению файловых операций с контролирующей станции к целевой системе. Результатом контроля привилегированных пользователей, которые подключаются к целевым системам должен быть записанный графический видеоматериал (видеоролик). ИС должна иметь функционал экспорта сохранившихся графических видеоматериалов (видеороликов) во внешние видео форматы.

– ИС должна иметь функционал экспорта сохранившихся текстовых журналов во внешние форматы с текстовой структурой.

– ИС должна иметь функционал создания политик относительно команд, которые вводят привилегированные пользователи при работе с целевыми системами. ИС должна поддерживать синтаксис регулярных выражений на базе стандарта POSIX.

– ИС должна иметь возможность задавать минимум следующих правил при срабатывании таких политик: блокировка пользователя, оповещение ответственного лица, разъединение сессии, приостановка сессии (постановка сессии на паузу).

– ИС должна иметь функционал создания политик относительно временных интервалов, в которые привилегированные пользователи имеют возможность доступа к целевым систем.

– ИС должна иметь возможность задавать минимум следующие правила для таких политик: дни недели, в которые привилегированные пользователи могут подключаться к целевым систем, часы и минуты, когда привилегированные пользователи могут подключаться к целевым систем, интервал действия такой политики (с указанием начальных и конечных дат и времени), разрыв активных сеансов по завершению времени, разрыв сеансов по причине неактивности пользователя в течении определённого времени

– ИС должна иметь встроенные механизмы пересмотра результатов действий привилегированных пользователей, а именно - просмотр записанных сессий, вводимых команд и ответов целевой системы на такие команды. Просмотр результатов должен обеспечиваться в веб-портале администрирования без необходимости установки каких-либо средств.

– ИС должна иметь встроенные фильтры поиска результатов действий привилегированных пользователей по различным критериям, по меньшей мере по имени привилегированного пользователя или пользователей, введенным командам, протоколам, именем целевой системы, а также в заданном диапазоне дат. ИС должна иметь возможность создания отчетов на базе полученных результатов с заданными фильтрами. Такие отчеты должны иметь возможность экспорта в виде файлов формата CSV, PDF, HTML и/или др.

– ИС должна иметь функционал создания политик о возможности просмотра отдельными привилегированными пользователями пароля (-ей) к целевым системам, к которым они подключаются, в случае если такой пароль им неизвестен.

– ИС должна иметь функционал принудительного запроса причин просмотра привилегированными пользователями пароля (-ей) к целевым системам, к которым они подключаются.

– ИС должна иметь функционал дополнительного подтверждения (одобрения) просмотра привилегированными пользователями пароля (-ей) к целевым системам, к которым они подключаются.

– ИС должна иметь встроенные механизмы просмотра таких паролей в любое нужное время (в прошлом) в случае, если они (пароли) изменялись с помощью соответствующего функционала ИС (парольной политики).

– ИС должна иметь функционал принудительного запроса причин подключения к целевой системе привилегированным пользователем с отображением соответствующего поля для ответа пользователя.

– ИС должна иметь функционал дополнительного подтверждения (одобрения) подключения к целевой системе привилегированных пользователей ответственным лицом.

– ИС должна иметь функционал оповещения с помощью канала электронной связи (email) ответственного лица о действии привилегированных пользователей (подключение к целевой системе, отключение от целевой системы, присоединение к сессии другого лица, срабатывание политики).

– ИС должна иметь функционал просмотра ответственными лицами сессий привилегированных пользователей в режиме реального времени без какого-либо явного информирования привилегированных пользователей во время такого просмотра.

– Дополнительно ИС должна предоставлять ответственному лицу информацию о сессии: имя и IP-адрес целевой системы, имя привилегированного пользователя, тип протокола, который используется, время начала сессии.

– ИС должна иметь функционал временного или полного принудительного прекращения работы сессий привилегированных пользователей ответственными лицами в режиме реального времени. Также ИС должна иметь возможность одновременно с прекращением сессии привилегированного пользователя блокировать учетную запись привилегированного пользователя сессия которого прекращается.

– ИС должна иметь возможность предоставлять доступ третьим лицам к сессиям привилегированных пользователей, подключенных в режиме реального времени так и к сессиям что были сохранены (записаны). Такой доступ должен предоставляться с помощью уникальной URL-ссылки с возможностью подключения третьего лица к заданной сессии без какой-либо дополнительной авторизации. При создании URL-ссылки обязательно должна быть возможность задания времени действия такой ссылки и режима доступа (полный доступ к сессии или доступ только в режиме просмотра).

– ИС должна иметь функционал добавления собственных меток (комментариев) к сессиям привилегированных пользователей. ИС должна иметь функционал добавления таких меток (комментариев) к любой части временной шкалы с возможностью дальнейшего поиска по таким объектам.

– ИС должна иметь функционал поведенческого анализа, позволять анализировать поведение работы пользователей по следующим критериям:

- анализ выполняемых действий с помощью компьютерной мыши
- анализ команд, которые пользователи вводят с клавиатуры.

3.4. Требования к приобретению, внедрению и поддержке ИС

Требования к приобретению, внедрению и поддержке ИС:

– ИС должна быть поставлена в виде виртуального устройства (VA - virtual appliance) в бессрочное владение с годовой поддержкой. Поставляемое виртуальное устройство должно быть установлено на платформе виртуализации VMware ESXi Заказчика.

– Количество интегрируемых целевых систем с ИС — 400 (четыреста).

– ИС не должна иметь ограничений по количеству привилегированных пользователей.

– ИС должна быть поставлена в виде отказоустойчивого решения на базе двух виртуальных устройств (VA - virtual appliance).

– ИС должна обеспечиваться сервисной поддержкой производителя в режиме 8x5, в рабочие часы в рабочие дни на стандартных условиях, предлагаемых производителем для данной ИС. Такая стандартная поддержка должна позволять бесплатное решение проблем, связанных с эксплуатацией ИС и бесплатное обновление программного кода (получение новых версий) к ИС.

– Производитель должен предоставлять открытый доступ (без какой-либо предварительной регистрации) к документации по администрированию ИС в сети Интернет. Такая документация должна быть доступна на английском языке.

– Производитель должен обеспечить техническую поддержку ИС в течении 1 года. Техническая поддержка должна включать в себя получение новых версий и обновлений ПО от производителя в течении одного года с момента активации лицензии.

4. Состав и содержание работ

Плановые сроки начала и окончания работ будут согласованы в момент подписания договора между Заказчиком и Исполнителем на основании работ, приведенных в Таблице 1.

Таблица 1. План работ по внедрению системы контроля привилегированных пользователей ГНК

№	Наименование работ и их содержание	Длительность работ	Исполнитель (организация, предприятие)	Ожидаемый результат
1.	Предпроектное обследование инфраструктуры, архитектурные сессии по внедрению ИС и обсуждению сценариев построения	Начало: октябрь 2022 г. Завершение: декабрь 2022 г.	ГНК, Исполнитель	Согласована схема развертывания и интеграции ИС
2.	Предоставление серверного оборудования для развертывания платформы контроля привилегированного доступа		ГНК	Серверное оборудование согласно требованиям вендора программного обеспечения готово к эксплуатации и развертыванию ИС. Сетевая связность между платформой и необходимыми компонентами ИС (включая рабочие станции сотрудников ГНК) предоставлена
3.	Развертывание платформы контроля привилегированного доступа в инфраструктуре ЦОДа,		ГНК, Исполнитель	Платформа контроля привилегированного доступа развернута и обновлена до

	первоначальная настройка, обновление до актуальной версии			актуальной версии в инфраструктуре ЦОДа
4.	Интеграция ИС с инфраструктурными сервисами Заказчика		ГНК, Исполнитель	ИС интегрирована с такими инфраструктурными сервисами Заказчика как Active Directory, SIEM-система. Интеграция подразумевает настройку необходимых параметров только в ИС.
5.	Подключение всех текущих целевых систем (ЦС) заказчика к ИС		ГНК, Исполнитель	К ИС подключены целевые системы в кол-ве до 400 штук. Подключение подразумевает настройку необходимых параметров только в ИС.
6.	Функциональное тестирование и отладка, взаимодействие с технической поддержкой производителя		ГНК, Исполнитель	Решены оставшиеся проблемы интеграции с инфраструктурными сервисами Заказчика и подключения целевых систем
7.	Приемочные испытания		ГНК, Исполнитель	Акт о приемке ИС

5. Порядок контроля и приемки ИС

Контроль, испытания и приемка ИС должны быть осуществлены на основании и в соответствии с ГОСТ 34.603-92.

В соответствии с ГОСТ 34.603-92 для ИС предусматриваются следующие виды проверок и испытаний:

1) приемочные испытания.

При вводе в эксплуатацию ИС должна быть подвергнута приемочным испытаниям в соответствии с «Программой и методикой испытаний». По

результатам приемочных испытаний ИС должна быть введена в эксплуатацию. Проверке на испытаниях должны быть подвергнуты:

1) ИС в целом;

2) состав эксплуатационной документации, регламентирующей деятельность персонала при функционировании ИС;

3) степень ознакомления персонала с эксплуатационной документацией и его подготовленность к эксплуатации ИС.

При испытаниях должны быть проверены:

1) полнота соответствия ИС функциональным требованиям, описанным в ТЗ;

2) соответствие количественных и (или) качественных характеристик выполнения функций согласно требованиям ТЗ.

При проверке эксплуатационной документации, регламентирующей деятельность персонала при функционировании ИС, должны быть проверены:

1) соответствие состава эксплуатационной документации требованиям настоящего Технического задания;

2) знание персоналом состава эксплуатационной документации и наличие у него навыков, необходимых для выполнения функций ИС согласно настоящего ТЗ;

3) полнота содержащихся в эксплуатационной документации указаний персоналу по выполнению им предписанных действий при работе с ИС, в рамках требований настоящего ТЗ.

Результаты проведения приемочных испытаний должны быть зафиксированы в актах. Положительные результаты испытаний, зафиксированные актами, являются основанием для подписания актов сдачи-приемки работ.

6. Требования к составу и содержанию работ по подготовке ИС к вводу в действие

В ходе выполнения проекта требуется выполнить работы по подготовке к вводу системы в действие. При подготовке к вводу в эксплуатацию ИС Заказчик должен обеспечить выполнение следующих работ:

- Определить место выполнения работ как на площадке заказчика, так и удаленно;
- Определить подразделение и должностных лиц, ответственных за внедрение и проведение испытаний ИС;
- Совместно с Исполнителем подготовить методику испытания ИС;
- Перевести ИС в эксплуатацию.

7. Требования к документированию

Исполнитель должен предоставить комплект документов, необходимых для эксплуатации системы.

Комплекты документации должны быть предоставлены на русском языке или английском языке.

Комплект документов технического проекта представляется Заказчику в трех экземплярах в печатном виде, а также в электронном виде (на компакт-дисках).

Электронный вид предоставляемых документов должен соответствовать формату Adobe Portable Document Format (PDF) версии не ниже 7.0.

Графические элементы должны быть выполнены как рисунки, вставленные в основной текстовый документ. В случае, если графический элемент не может быть вставлен в текстовый документ без потери его смыслового наполнения, элемент исполняется как отдельный графический документ с использованием программы Microsoft Visio 2013 и выше.

Комплекты документации должны быть предоставлены на русском языке или английском языке в следующем составе:

Общее описание системы;

Руководство администратора системы;

8. Дополнительные требования

8.1. Требования к месту выполнения работ

Местом проведения работ является Государственный налоговый комитет Республики Узбекистан, расположенный по адресу: 100011 Республика Узбекистан, г. Ташкент, Шайхантахурский район, улица Абдулла Кадыри, дом 13-а. При этом, допускается дистанционная работа по согласованию сторон.

8.2. Требования к исполнителю

Исполнитель должен иметь в штате как минимум двух сертифицированных специалистов по предлагаемой ИС.

Исполнитель в рамках проведения работ предоставляет информацию:

- по персональному составу проектной команды (подтверждение наличия в штате исполнителя специалистов (инженеров), квалификация которых подтверждена соответствующими сертификатами);
- по методам достижения минимального уровня TCO (Total Cost of Ownership) сроком на не менее 5 лет;

- по сервисам и подпискам (включая стоимость технической поддержки);
- по условиям лицензирования при наличии (объем предоставления, порядок взимания платы, срок действия лицензий и др.);
- по перечню осуществляемых работ (услуг) с конкретизацией объема и привлекаемых специалистов (обоснование формирования стоимости оказываемых услуг);

В рамках выделенного бюджета Исполнитель должен предоставить полностью укомплектованное и работоспособное решение по указанному функционалу, при необходимости предложить дополнительные модули, продукты, и услуги, по каким-либо причинам не учтенные заказчиком, но обязательные для обеспечения полноты использования запрашиваемой конфигурации.

гарантирует наступление даты окончания поддержки поставляемого решения не ранее чем через 5 лет с момента заключения договора на поставку решения;

8.3. Требования к безопасности выполнения работ и оказания услуг

Исполнитель должен предпринять все необходимые меры по обеспечению информационной безопасности и сохранности конфиденциальной информации, а также, предотвращению утечки информации.

8.4. Требования к обучению персонала заказчика

Исполнитель должен предоставить услуги по обучению персонала Заказчика в количестве не менее 4-х человек по работе с предложенной ИС.

Приложение 1. Термины, сокращения и их определения

ГНК	-	Государственный Налоговый Комитет
ИС	-	Информационная система
СУБД	-	Система управления базами данных
TCP	-	Высокоуровневый протокол обмена данными в сетях передачи данных
ЦОД	-	Центр обработки данных
ЦС	-	Целевая система. Инфраструктурный ресурс Заказчика, доступ к которому будет обеспечен через систему контроля привилегированных пользователей. Определяется таким параметром как IP-адрес
DHCP	-	Dynamic Host Configuration Protocol - прикладной протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP
VLAN	-	Virtual Local Area Network - виртуальная локальная компьютерная сеть
ARP	-	Address Resolution Protocol - протокол в компьютерных сетях, предназначенный для определения MAC-адреса другого компьютера по известному IP-адресу.
OCR	-	Optical character recognition - механический или электронный перевод изображений рукописного, машинописного или печатного текста в текстовые данные, использующиеся для представления символов в компьютере (например, в текстовом редакторе).
API	-	Application Programming Interface - описание способов, которыми одна компьютерная программа может взаимодействовать с другой программой.
Java	-	Строго типизированный объектно-ориентированный язык программирования общего назначения
JRE	-	Java Runtime Environment - минимальная реализация виртуальной машины, необходимая для исполнения Java-приложений
Flash	-	Adobe Flash - программный продукт, позволяющий разрабатывать интерактивные мультимедийные приложения.
HTML	-	HyperText Markup Language - стандартизированный язык гипертекстовой

		разметки документов для просмотра веб-страниц в браузере
IP	-	Internet Protocol - маршрутизируемый протокол сетевого уровня стека TCP/IP
RDP	-	Remote Desktop Protocol - протокол удалённого рабочего стола
VNC	-	Virtual Network Computing - система удалённого доступа к рабочему столу компьютера
SSH	-	Secure Shell - сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой
AES	-	Advanced Encryption Standard - симметричный алгоритм блочного шифрования.
RADIUS	-	Remote Authentication in Dial-In User Service) - протокол для реализации аутентификации
AD	-	Active Directory - службы каталогов корпорации Microsoft для операционных систем семейства Windows Server
LDAP	-	Lightweight Directory Access Protocol - протокол прикладного уровня для доступа к службе каталогов X.500
MFA	-	Multi-Factor Authentication - метод аутентификации основанный на использовании более чем одного метода аутентификации
OATH	-	Open Authentication - открытый стандарт аутентификации
FQDN	-	Fully Qualified Domain Name - имя домена, не имеющее неоднозначностей в определении
OU	-	Organizational Unit - субконтейнер в Active Directory, в который можно помещать пользователей, группы, компьютеры и другие объекты AD
SSL	-	Secure Sockets Layer - криптографический протокол, который подразумевает более безопасную связь
WMI	-	Windows Management Instrumentation - одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows
SNMP	-	Simple Network Management Protocol - стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP
Syslog	-	system log - стандарт отправки и регистрации сообщений о происходящих в системе событиях,

	-	использующийся в компьютерных сетях, работающих по протоколу IP
X11	-	X Window System — оконная система, обеспечивающая стандартные инструменты и протоколы для построения графического интерфейса пользователя