УТВЕРЖДАЮ
Заместитель председателя
государственного налогового
комитета _____ М.М.Махкамов
«___» _____ 2022 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на:

ПРИОБРЕТЕНИЕ СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ДЛЯ ГОСУДАРСТВЕННОГО НАЛОГОВОГО КОМИТЕТА

На 25 листах

Разработал
Заместитель директора ГУП
«Центр обработки налоговых
данных»
_____ К.Зубенко

Согласовано
Директор департамента
Информационных-
коммуникационных технологии ГНК
_____ А.Раббинов

Согласовано
Директор ГУП
«Центр обработки налоговых
данных»
_____ С.Хабибов

г. Ташкент

СОДЕРЖАНИЕ

1. Общие сведения

Государственный налоговый комитет Республики Узбекистан в целях минимизации рисков информационной безопасности, связанных со злоупотреблением доступа к системам ГНК планирует реализацию проекта на приобретение системы контроля привилегированных пользователей.

Настоящее Техническое задание описывает общие требования для специализированного программного обеспечения по обеспечению предотвращения утечек конфиденциальной информации.

1.1. Полное наименование ИС и ее условное обозначение

Полное наименование ИС: Система предотвращения утечек конфиденциальной информации Государственного Налогового Комитета

Условное обозначение ИС: СПУКИ (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. 40101086026277770113310930 01
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 тендерных торгов, либо иным путем согласно действующих законов, нормативных актов, постановлений и прочих нормативных документов по предмету приобретения программного обеспечения.

1.4. Основание для осуществления закупки

Основанием для разработки настоящего ТЗ на приобретение системы предотвращения утечек конфиденциальной информации является необходимость соответствия утвержденной политики информационной безопасности ГНК, распоряжение №112-РТ от 04.07.2022 г.

1.5. Плановые сроки начала и окончания работ

Плановый срок начала работ: Октябрь 2022 года.

Плановый срок выполнения работ: 80 рабочих дней (с даты заключения договора).

1.6. Порядок оформления и предъявления результатов работ

Работы по приобретению и внедрению системы предотвращения утечек конфиденциальной информации 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.

Оказанные услуги и работы считаются выполненными после подписания акта финальной приемки поставки программного обеспечения и выполненных работ.

2. Назначение и цели приобретения и внедрения ИС

2.1. Назначение ИС

Программное обеспечение предотвращения утечек конфиденциальной информации должно обеспечивать контроль над процессом передачи конфиденциальной информации за пределы сегментов вычислительных сетей Заказчика. ИС должна анализировать данные, передаваемые сотрудниками Государственного Налогового Комитета как внутри, так и за пределы информационной сети Заказчика.

2.2. Цели

Основной целью приобретения ИС является выявление фактов умышленной или неумышленной передачи конфиденциальной информации за пределы вычислительной сети Заказчика.

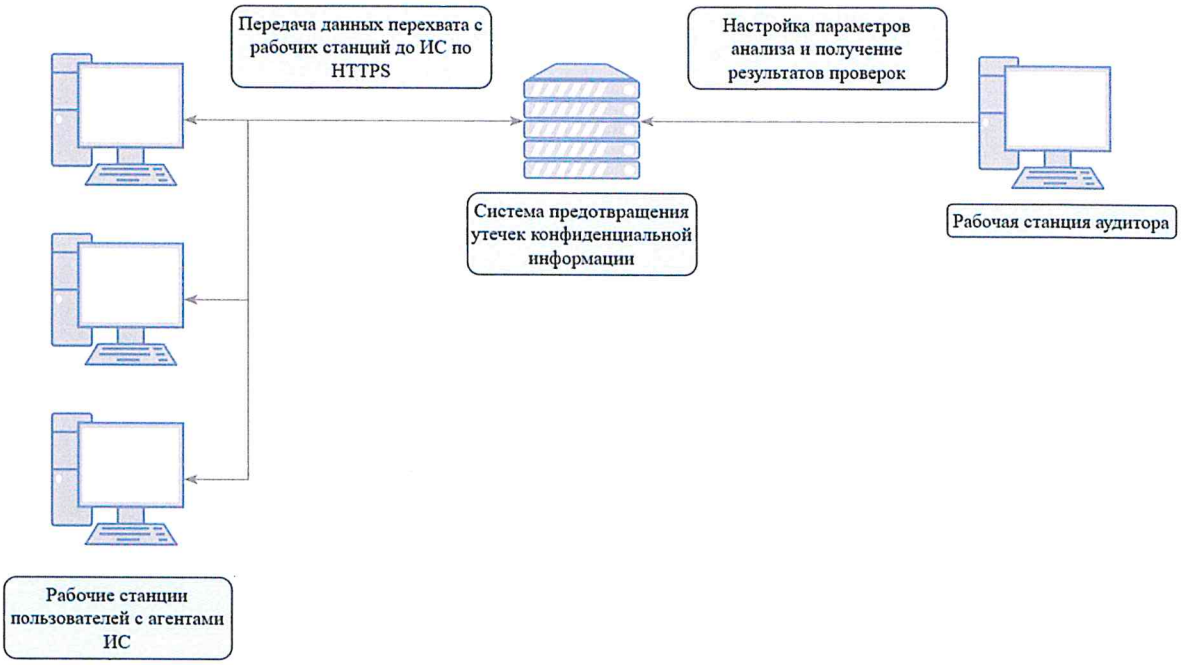
3. Требования к ИС

Настоящее техническое задание для приобретения системы предотвращения утечек конфиденциальной информации (далее ИС) описывает комплекс требований к программному обеспечению.

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 взаимо интегрированные), имеющихся в линейке разработчиков решения.

Общая (не детализированная) схема функционирования ИС должна выглядеть следующим образом:



3.1. Общие требования к ИС в целом

Дистрибутив программного обеспечения должен поставляться с документацией в электронном виде на русском языке и/или на узбекском языке. Документация должна включать в себя правила установки и использования программного обеспечения.

Техническая поддержка производителя должна включать в себя получение новых версий и обновлений ИС от производителя в течении одного года с момента активации лицензии.

ПО должно поддерживать одновременную работу с агентами ИС со всеми включенными (активированными) модулями в количестве 700 штук, не нарушая при этом как работоспособность ИС, так и лицензионную чистоту ИС.

Лицензия не должна иметь ограничений в количестве системных администраторов, офицеров безопасности.

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

3.2. Программные модули

Программное обеспечение должно включать следующее:

- возможность контроля электронной почты (в том числе передаваемой по защищенным каналам, а также входящей/исходящей почты через web-интерфейс);
- возможность контроля сервисов обмена мгновенными сообщениями;
- возможность контроля FTP-трафика;
- возможность контроля HTTP-трафика (POST- и GET-запросы)
- возможность контроля печати;
- возможность контроля и управления доступом съемных устройств;
- возможность контроля данных, вводимых с клавиатуры;
- возможность контроля активности пользователей и приложений;
- возможность контроля облачных хранилищ данных;
- возможность принятия решений;
- возможность администрирования;
- возможность контентного анализа;
- возможность индексации файлов рабочих станций;

3.3. Технические требования к ИС

Требования к ИС в целом:

ИС должна поддерживать контроль следующих данных:

- электронной почты, протоколы: IMAP, HTTP(S), SMTP;
- коммуникационных программ-клиентов Skype Desktop, Viber Desktop, WhatsApp Desktop и Telegram Desktop;
- FTP-трафика;
- HTTP-трафика;
- съемных устройств;
- отправленных на печать документов;
- данных, вводимых с клавиатуры;
- облачных хранилищ данных (Google Drive, OneDrive, Dropbox, Яндекс.Диск);
- активности пользователей в запускаемых ими приложениях;
- содержимого документов на рабочих станциях пользователей;

ИС должна предполагать возможность установки отдельного модуля на рабочие станции пользователей по каждому из вышеперечисленных каналов передачи данных.

ИС должна обеспечивать разграничение прав доступа к перехваченной информации и настройкам системы.

ИС должна обеспечивать перехват трафика на уровне рабочих станций.

ИС должна обеспечивать блокировку HTTP(S)-трафика согласно настраиваемым правилам с учетом таких атрибутов как: доменное имя пользователя, текст запроса.

Агент ИС, осуществляющий перехват на уровне рабочих станций, должен быть подписан цифровой подписью. Это обеспечивает его целостность и предотвращает возможность встраивания в него стороннего или вредоносного кода.

3.4. Требования к структуре и функционированию ИС

Структурно ИС должна включать следующие компоненты:

- сервер индексации;
- сервер перехвата на рабочих станциях;
- администрирования;
- принятия решений;

В состав ИС должны входить следующие основные логические компоненты:

- контроля почтового трафика;
- контроля сервисов обмена мгновенными сообщениями;
- контроля FTP-трафика;
- контроля HTTP-трафика;
- контроля печати;
- контроля съёмных устройств;
- контроля событий на мониторах и действий сотрудников;
- контроля разговоров сотрудников;
- контроля активности пользователей и приложений;
- контроля данных, вводимых с клавиатуры;
- контроля облачных хранилищ данных;
- индексации;
- индексации файлов рабочих станций;
- принятия решений;
- контентного анализа;
- модуль администрирования.

Компонент контроля почтового трафика должен обеспечивать контроль сообщений электронной почты (протоколы SMTP, IMAP, HTTP(S)).

Компонент контроля сервисов обмена мгновенными сообщениями должен обеспечивать перехват сеансов текстовой связи, файлов, переданных посредством коммуникационных клиентов Viber Desktop, WhatsApp Desktop и Telegram Desktop.

Компонент контроля FTP-трафика должен обеспечивать контроль исходящего FTP-трафика.

Компонент контроля HTTP-трафика должен обеспечивать контроль POST- и GET-запросов.

Компонент контроля печати должен обеспечивать контроль документов, отправленных на печать при помощи сетевых или локальных принтеров.

Компонент контроля съемных устройств должен обеспечивать контроль файлов, записываемых на USB-устройства.

Компонент контроля событий на мониторах и действий сотрудников должен обеспечивать контроль изображений с экранов пользователей, возможность вести видеозапись действий, создание снимков и записи видео посредством веб-камеры, а также предоставлять возможность просмотра содержимого мониторов и действий пользователей за рабочей станцией в режиме реального времени.

Компонент контроля разговоров сотрудников должен обеспечивать аудиозапись разговоров с помощью подключенного к рабочей станции микрофона.

Компонент контроля активности пользователей и приложений должен обеспечивать мониторинг активности пользователей и запускаемых ими процессов.

Компонент контроля данных, вводимых с клавиатуры, должен осуществлять логирование нажатий клавиш в приложениях.

Компонент контроля облачных хранилищ данных должен предоставлять возможности для контроля исходящих данных в облачные сервисы (Google Drive, OneDrive, Dropbox, Яндекс.Диск).

Компонент индексации должен обеспечивать индексирование документов, перехваченных модулями контроля, для быстрого поиска по ним в дальнейшем.

Компонент индексации файлов рабочих станций должен обеспечивать контроль документов, располагающихся на рабочих станциях с установленным агентом ИС.

Компонент администрирования должен обеспечивать управление настройками конфигурации ИС.

Компонент контентного анализа должен предоставлять возможности:

- проведения поиска перехваченной информации за определенный период в прошлом, учитывая возможность изменения правил проверки;
- просмотра активности пользователей в режиме реального времени.

3.5. Требования к способам и средствам связи для информационного обмена

ИС должна функционировать в составе информационно-вычислительной сети Заказчика.

ИС должна выполнять все, описанные в данном ТЗ, функции локально, т.е. ИС должна соответствовать, описанным в данном ТЗ, требованиям, не имея доступа к глобальной сети Интернет.

Все компоненты системы должны работать на платформе Windows. Модули перехвата на уровне рабочих станций могут работать на отдельных ОС семейства Linux (CentOS, RHEL, Ubuntu).

ИС при перехвате на уровне рабочей станции должен иметь возможность использования HTTPS для передачи данных на сервер ИС.

ИС должна корректно работать в сетях доменного типа.

ИС должна поддерживать виртуальную инфраструктуру (VMware ESX/ESXi).

Для информационного обмена между компонентами системы должны поддерживаться стандартные унифицированные протоколы семейства TCP/IP и интерфейсы (Ethernet/ Fast Ethernet /Gigabit Ethernet).

3.6. Требования к характеристикам взаимосвязей

ИС должна иметь возможность однозначного определения данных сотрудника компании, отправившего информацию, благодаря интеграции с Active Directory:

- учетной записи пользователя;
- информации об использованной рабочей станции (имени, IP-адреса).

3.7. Требования по диагностированию ИС

ИС должна обеспечивать возможность записи в журналы аудита информации по служебным событиям и сбоям. Записи в журналах должны содержать информацию, достаточную для установления причины неисправности.

Каждый модуль ИС должен иметь штатный и расширенный режим записи в журналы.

3.8. Перспективы развития и модернизации ИС

ИС должна быть реализована как открытая система и допускать наращивание производительности за счет улучшения характеристик технических средств.

ИС должна обеспечить возможность модернизации путем увеличения ресурсов технического обеспечения (аппаратных средств).

3.9. Требования к контролю почтовых сообщений

ИС должна предоставлять возможности для контроля сообщений и вложений, передаваемых по протоколам SMTP, IMAP, HTTP(S) (веб-почта: как исходящая, так и входящая).

ИС должна обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма.

3.10. Требования к контролю сервисов обмена мгновенными сообщениями

ИС должна обеспечивать перехват:

- чатов, файлов, переданных при помощи WhatsApp Desktop, Telegram Desktop, Viber Desktop;
- конференций Zoom;

3.11. Требования к контролю FTP-трафика

ИС должна обеспечивать перехват документов, загруженных или переданных по FTP-соединению.

ИС должна обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имен пользователей FTP-серверов, IP-адресов FTP-серверов.

3.12. Требования к контролю HTTP-трафика

ИС должна предоставлять возможности контроля файлов, отправленных посредством POST-запросов.

ИС должна поддерживать перехват GET-запросов, отправленных пользователями в поисковые системы Google, Яндекс.

ИС должна обеспечивать возможность блокировки передачи сообщений и файлов, соответствующих определенному контенту.

ИС должна обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста.

3.13. Требования к контролю печати

ИС должна осуществлять перехват документов, отправленных на печать при помощи локальных и сетевых принтеров.

ИС должна осуществлять перехват как графического представления, так и текстов, отправленных на печать.

ИС должна обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имен принтеров, количество распечатанных страниц.

ИС должна обеспечивать возможность блокировки печати файлов, соответствующих определенному контенту.

3.14. Требования к контролю съёмных устройств

ИС должна предоставлять возможность контроля доступа пользователя к внешним устройствам (съемные накопители USB, USB-устройства) и портам (USB).

ИС должна предоставлять возможность теневого копирования данных, передаваемых на внешнее устройство.

ИС должна предоставлять возможность фиксирования всех событий в журнале аудита: создание, чтение, запись, выполнение, переименование, форматирование, удаление файлов на съемном носителе.

ИС должна предусматривать следующие типы доступа пользователей к внешним устройствам: «запрет доступа», «полный доступ».

ИС должна предоставлять возможность контроля и блокировки буфера обмена на компьютере пользователя.

ИС должна предоставлять возможность использования «белых списков» устройств, доступ к которым в дальнейшем пользователь будет иметь неограниченный, а также «черных списков» устройств, доступ к которым будет заблокирован.

ИС должна обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств.

3.15. Требования к контролю активности пользователей и приложений

ИС должна обеспечивать контроль активности сотрудников в запускаемых ими приложениях или на сайтах.

ИС должна предоставлять возможность поиска перехваченных данных за указанный период времени применительно к заданным пользователям, компьютерам, IP-адресам, продолжительности активности пользователя/процесса, имени активного процесса.

ИС должна обеспечивать использование перехваченных данных для генерации отчетов.

3.16. Требования к контролю данных, вводимых с клавиатуры

ИС должна обеспечивать перехват нажатий клавиш в запущенных приложениях.

ИС должна обеспечивать перехват текстовой информации, помещенной пользователем в буфер обмена.

ИС должна обеспечивать возможность блокировки нажатий клавиши «PrintScreen».

ИС должна предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.

ИС должна предоставлять возможность поиска, вводимого с клавиатуры или помещаемого в буфер обмена содержимого за определенный период времени применительно к заданным пользователям, компьютерам, именам запущенных процессов, IP-адресам, продолжительности работы в приложении.

ИС должна предоставлять возможность экспорта перехваченных нажатий клавиш в отдельную папку.

3.17. Требования к контролю облачных хранилищ данных

ИС должна предоставлять возможности для контроля исходящих файлов в сервисы облачного хранения данных посредством Web браузера: Google Drive, Яндекс.Диск, Dropbox.

ИС должна предоставлять возможности для контроля исходящих файлов в сервисы облачного хранения данных посредством приложений: Dropbox, Яндекс.Диск, OneDrive.

ИС должна обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имени файла.

3.18. Требования к индексации

ИС должна обеспечивать индексирование баз данных ИС.

3.19. Требования к индексации файлов рабочих станций

ИС должна обеспечивать отслеживание изменений файлов.

ИС должна позволять ограничивать область сканирования файлов по их типу и расположению (пути)

ИС должна обеспечивать возможность сохранения теневой копии данных.

3.20. Требования к принятию решений

ИС должна использовать два пользовательских приложения: консоль сервера для задания настроек и клиентскую консоль для управления политиками безопасности и инцидентами.

ИС должна предоставлять возможности для ведения журнала инцидентов.

ИС должна предоставлять возможности для задания правил автоматического вынесения вердикта по объекту (инцидент / не инцидент). Должна обеспечиваться возможность применять правила автоматического вынесения вердикта на основании:

- формальных признаков перехваченного объекта (доменное имя, отправитель, получатель, хост, размер, расширение файла, канал передачи данных, протокол);
- факта защиты паролем файлов и архивов;
- результатов контентного анализа текста, извлеченного из перехваченных объектов (по словам, тематическим словарям, а также поиска с использованием регулярных выражений).

ИС должна предоставлять возможности для изменения существующих и применения новых правил автоматического вынесения вердикта (правил проверки).

ИС должна предусматривать возможность объединения политик безопасности (правил проверки) в группы.

ИС должна предоставлять возможность задания для каждой группы политик безопасности индивидуальных настроек: перечня индексов, по которым будет проводиться поиск, расписания проверки.

ИС должна предоставлять возможности для использования «белых» списков (списки пользователей, документы которых исключены из проверок) и «черных» списков (списки пользователей, только по документам, которых будет проводиться проверка).

ИС должна предоставлять возможность экспорта/импорта структуры настроек (политик безопасности, критериев поиска, списков исключений).

ИС должна поддерживать возможность категоризации инцидентов с помощью цветовых меток.

В случае отсутствия встроенной функции, ИС должна поддерживать возможность экспорта данных в информационные системы Заказчика посредством syslog и/или других механизмов для интеграции с имеющейся SIEM (Security information and event management) системой Заказчика (наименование SIEM системы: ArkSight) для корреляции событий информационной безопасности. SIEM обеспечивает анализ в реальном времени событий (тревог) безопасности, исходящих от ИС и позволяет реагировать на них до наступления существенного ущерба.

ИС должна предоставлять возможности для принятия решений в отношении следующих типов объектов, не защищенных паролем:

- сообщений, переданных по поддерживаемым системой каналам и протоколам;
- файлов форматов: MS Office (doc, docx, xls, xlsx, ppt, pptx, rtf и др.), дополнительные форматы документов (txt, xml, pdf, csv, log, bat, ini и др.);
- распознанных и проанализированных текстов в графических файлах форматов bmp, jpg, jpeg, png, tiff, gif и др.;
- документов, вложенных в сжатые файлы: rar, zip, 7z, tar, gz, gzip и др.

ИС должна обеспечить наличие следующих возможностей обнаружения критичной информации:

- по ключевым словам;
- по формальным признакам сообщений и файлов (доменный пользователь, имя компьютера, отправитель, получатель, размер, имя файла, формат), в том числе для файлов, из которых не может быть извлечен текст;
- по заранее заданному словарю с целью выявления определенных типов документов (резюме, финансовые и бухгалтерские отчеты);
- возможность создания комплексных поисковых запросов, включающих в себя несколько критериев (фразовый поиск, поиск по абзацам и целым документам и атрибутам), объединенных логическими операторами AND, OR, NOT;
- по регулярным выражениям – поиск сложных алфавитно-цифровых объектов (номера паспортов, индивидуальные номера налогоплательщиков, номера кредитных карт, договоров или счетов, кодов классификаторов и т.п.), с возможностью создания комплексных регулярных выражений (состоящих из нескольких простых). Должна быть возможность использования как стандартных выражений, включенных в дистрибутив, так и создание пользовательских, а также возможность проверки регулярного выражения на корректность;
- по количественным показателям статистических запросов (числу отправленных писем/распечатанных страниц/сообщений в WhatsApp, Telegram и Viber);
- возможность сузить результаты поиска путем дополнительного поискового запроса (фильтры по найденному).

ИС должна предусматривать наличие в дистрибутиве нескольких словарей.

ИС должна обеспечивать устойчивость к следующим видам манипуляции с информацией:

- импортирование фрагмента конфиденциальной информации в документы, не являющиеся конфиденциальными;
- изменения расстояний между словами;
- изменение форматирования документа;
- использование цифр вместо букв;
- изменение расширений файлов.

ИС должна предоставлять возможности для просмотра детальной информации по каждому инциденту.

3.21. Требования к администрированию

ИС должна обеспечивать возможность управления службами модулей ИС.

ИС должна предоставлять возможность управления всеми индексами и базами данных модулей контроля информации.

ИС должна обеспечивать возможность синхронизации с одним или более доменом Active Directory.

ИС должна обеспечивать возможность работы с пользователями рабочих групп.

ИС должна предоставлять возможность разграничения прав доступа сотрудников службы безопасности к функционалу консолей подсистем.

ИС должна предоставлять возможность указания настроек для подключения к базам данных, которые можно впоследствии использовать по умолчанию.

3.22. Требования к контентному анализу

ИС должна быть ориентирована на работу с индексами и базами данных модулей контроля информации.

ИС должна предоставлять возможность выполнять поиск всех перехваченных объектов за определенный период времени в прошлом:

- поиск по ключевым словам и фразам в базах перехваченных документов;
- выборка перехваченных данных по дате, доменному имени, адресам и хостам, адресам электронной почты, именам компьютеров, принтеров;

- поиск по набору слов (словарю), позволяющий находить документы, содержащие определенное количество либо процент таких слов. Набор слов может быть введен вручную, вставлен из буфера обмена либо загружен из внешнего текстового файла. При формировании каждого отдельного слова из словаря не должны использоваться логические операторы AND, OR, NOT.

ИС должна предоставлять возможность просмотра контентного маршрута перехваченного документа.

ИС должна предоставлять возможности экспорта выборки перехваченных данных (полного списка или набора файлов с оглавлением).

ИС должна обеспечивать возможность оперативного контроля за происходящим на рабочих местах пользователей в режиме реального времени: просмотр происходящего на экранах мониторов, прослушивание речи сотрудников, просмотр происходящего за компьютером посредством подключенной веб-камеры.

ИС должна поддерживать предоставление отчетов в табличном, диаграммном, в виде временного графика, а также в виде графа связей.

ИС должна генерировать отчеты по устройствам (перечень установленного оборудования на компьютерах пользователей).

ИС должна предусматривать представление связей между внутренними и внешними адресатами в виде интерактивного графа для получения наглядного представления о круге общения выбранного пользователя или нескольких пользователей, выявления общих контактов для данных пользователей, а также контактов внешних адресатов с сотрудниками компании.

ИС должна обеспечивать получение наглядного представления об адресах, с которых выбранный пользователь отправлял либо на которые получал сообщения.

ИС должна предусматривать возможность конвертации сгенерированных отчетов в PDF и/или других форматов, равно как и вывод их на печать.

ИС должна предоставлять функционал для расследования аудиторами инцидентов безопасности, позволяющий создавать задачи с прикрепленными к ним результатами поиска и файлами, назначать аудитора, ответственного за их решение, а также устанавливать приоритет и срок выполнения задач.

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 предотвращения утечек конфиденциальной информации ГНК

№	Наименование работ и их содержание	Плановые сроки выполнения работ	Исполнитель (организация, предприятие)	Ожидаемый результат
1.	Формирование списка участников проекта внедрения	Начало: октябрь 2022 г. Завершение: не более 80 дней (с даты заключения договора)	ГНК, Исполнитель	Список сформирован, ответственные участники утверждены
2.	Предпроектное обследование инфраструктуры, архитектурные сессии по внедрению ИС и обсуждению сценариев построения		ГНК, Исполнитель	Согласована схема развертывания и интеграции ИС
3.	Предоставление серверного оборудования для развертывания платформы предотвращения утечек конфиденциальной информации		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
4.	Развертывание платформы предотвращения утечек конфиденциальной		ГНК, Исполнитель	Платформа предотвращения утечек конфиденциальной информации

	информации в инфраструктуре ЦОДа, первоначальная настройка, обновление до актуальной версии			развернута и обновлена до актуальной версии в инфраструктуре ЦОДа
5.	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.
6.	Составление и утверждение списка сотрудников ГНК на чьи рабочие станции будут установлены модули и агент ИС. В списке присутствуют такие параметры как: имя компьютера в доменной среде Заказчика, IP-адрес.		ГНК	Список сотрудников ГНК на чьи рабочие станции будут установлены модули и агент ИС составлен, утвержден и передан Исполнителю. В списке присутствуют такие параметры как: имя компьютера в доменной среде Заказчика, IP-адрес.
7.	Установка 700 агентов ИС на рабочие станции сотрудников ГНК		ГНК, Исполнитель	700 агентов ИС установлены на рабочие станции сотрудников ГНК
8.	Написание несоставных правил (до 10) в ИС на базе политик Заказчика		ГНК, Исполнитель	Написаны несоставные правила (до 10) в ИС на базе политик Заказчика
9.	Функциональное тестирование и отладка, взаимодействие с		ГНК, Исполнитель	Решены оставшиеся проблемы интеграции с

	технической поддержкой производителя			инфраструктурными сервисами Заказчика, установки агентов на рабочие станции и написания несоставных правил (до 10)
10.	Приемочные испытания		ГНК, Исполнитель	Акт выполненных работ
11.	Ввод ИС в эксплуатацию		ГНК, Исполнитель	Акт финальной приемки ИС в промышленную эксплуатацию

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;
- Ввод ИС в эксплуатацию.

7. Требования к документированию

Исполнитель должен предоставить комплект документов, необходимых для эксплуатации системы.

Комплекты документации должны быть предоставлены на русском 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 в следующем составе:

Общее описание системы и подсистем;

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: г. Ташкент, 100011, 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.

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.

8.5. Требования к лингвистическому обеспечению интерфейса ИС

Интерфейс ИС должен иметь поддержку русского, английского и желательно узбекского языков (приветствуется).

8.6. Требования к техническому обеспечению

Технические средства для поставляемой ИС будет предоставлены силами и средствами Заказчика.

При этом, Исполнитель должен предоставить информацию о системных требованиях к аппаратным средствам (без привязки к определенному производителю), необходимых для полноценного функционирования 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
FTP	-	File Transfer Protocol (протокол передачи файлов) протокол прикладного уровня передачи файлов по сети
HTTP	-	Hyper Text Transfer Protocol (протокол передачи гипертекста) - протокол прикладного уровня передачи данных в виде текстовых сообщений
HTTPS	-	Hyper Text Transfer Protocol Secure - расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL или TLS, тем самым обеспечивается защита этих данных
IMAP	-	Internet Message Access Protocol - протокол прикладного уровня для доступа к электронной почте
SMTP	-	Simple Mail Transfer Protocol - (простой протокол передачи почты) - сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
USB	-	Universal Serial Bus - последовательный интерфейс для подключения периферийных устройств к вычислительной технике
POST, GET	-	Одни из многих методов запроса, поддерживаемых HTTP протоколом, используемым во Всемирной паутине
ОС	-	Операционная система
Syslog	-	Стандарт отправки и регистрации сообщений о происходящих в системе событиях, использующийся в компьютерных сетях, работающих по протоколу IP.
Несоставное правило	-	Правило написания политики работы ИС при котором не используются такие логические операторы как AND, OR и /или NOT