«УТВЕРЖДЕНО»

Председатель Конкурсной комиссии
АКБ «ASIA ALLIANCE BANK»

_____ Норкулов О.О.

ДОКУМЕНТЫ

конкурсных торгов
на поставку DLP-системы Falcongaze SecureTower
АКБ «ASIA ALLIANCE BANK»

Заказчик: Акционерно-коммерческий банк «ASIA ALLIANCE BANK»

ТАШКЕНТ-2021 год

Общие сведения

1. **Область действия конкурса:** настоящая Конкурсная документация разработана в соответствии с требованиями "Положения Акционерного коммерческого банка «ASIA ALLIANCE BANK» о порядке организации установления рыночной стоимости имущества и собственных ценных бумаг, а также определения поставщика товаров, работ и услуг" и регулирует порядок проведения и участия участников конкурса в конкурсе.

2. **Наименование Заказчика:** АКБ «ASIA ALLIANCE BANK», 100047, г.Ташкент, Яшнабадский район, ул. Махтумкули дом №2а Телефон: (+998 71) 231-60-00, факс: (+998 71) 289-55-33

3. **Предмет конкурса:** Поставка DLP-системы Falcongaze SecureTower для АКБ «ASIA ALLIANCE BANK»

4. **Вид конкурса** - открытый.

5. **Источник финансирования:** Финансируется за счет собственных средств АКБ «ASIA ALLIANCE BANK»

6. **Условия платежа:** условия оплаты – предоплата в размере 50% от размера вознаграждения перечисляется на расчетный счет Лицензиата в течение 5 банковских дней с даты подписания настоящего договора. Оставшиеся 50% от размера вознаграждения выплачиваются после подписания Сторонами Акта предоставления права на использование ПО и счет-фактуры.

7. **Тип поставки:** электронная.

8. **Валюта платежа:** сум

1. Правила и требования для участников

1. Участники, представляющие предложения, должны нести все расходы, связанные с подготовкой и подачей конкурсной документации. АКБ «ASIA ALLIANCE BANK» не несет никакой материальной ответственности за расходы, понесенные участником конкурсных торгов по подготовке и предоставлению конкурсного предложения.

2. Участники, представляющие предложения, должны быть зарегистрированы в соответствии с законодательством РУз, и быть правомочными к оказанию услуг/выполнению работ/реализации товара в данной сфере, должны иметь соответствующие разрешительные документы.

3. Требования к Участнику:

- Авторизация от производителя поставляемого ПО.
- Технический специалист участника должен иметь сертификат от производителя ПО.
- Участник должен иметь сертификат о партнёрстве от производителя ПО действующего на территории Республики Узбекистан.
- Участник должен быть представлен на рынке Узбекистана как одна из ведущих компаний в области ПО в течении последних 5 лет;

4. К участию в конкурсе не допускаются организации (компании):

- не предоставившие в установленный срок необходимые документы для отбора;
- предоставившие документы, не соответствующие требованиям конкурсной документации;
- находящиеся на стадии реорганизации (разделения, слияния), ликвидации или банкротства, на имущество которых наложен арест;
- находящиеся в состоянии судебного или арбитражного разбирательства с Заказчиком;
- имеющие задолженность по уплате налогов и сборов.

5. Требования к поставляемому ПО и гарантии:

- Приобретаемое ПО должно иметь гарантийную поддержку не менее 12 месяцев.
- Срок гарантийной поддержки ПО начинается со дня подписания Акта установки и сдачи в эксплуатацию.
- ПО должно быть завезено в Узбекистан в установленном Законодательством порядке.
- Количество лицензий – на 200 пользователей

6. Конкурсное предложение и вся связанная с ним корреспонденция, и документация, которые осуществляются Участником и Заказчиком, могут быть на узбекском, русском или английском языке. Конкурсное предложение может быть на другом языке при условии, что к нему будет приложен точный перевод на узбекский, русский или английский язык. В случае наличия разночтений между редакциями на другом языке и переводом текста конкурсного предложения на узбекский, русский или английский язык, узбекский, русский или английский будет превалирующим.

7. Конкурсное предложение должно быть представлено в одном опечатанном конверте. Визирование уполномоченным представителем Участника конкурса, а также опечатывание конверта производится в местах склейки. Конверты должны быть опечатаны штампом или печатью Участника (при наличии). В случае осуществления деятельности без печати и штампа, необходимо указать об этом на конверте следующей надписью: «деятельность организации осуществляется без печати/штампа».

В конверте должны содержаться документы, указанные в Приложении №1 к настоящей Конкурсной документации. На конверте указываются наименование и адрес Заказчика, контактные телефоны, а также:

- название (предмет) конкурса;
- наименование Участника конкурса, контактные данные, ИНН участника;
- пометка - «Не вскрывать до установленного времени проведения конкурса».

Конверты не опечатанные и не помеченные в соответствии с вышеуказанными требованиями не принимаются и не рассматриваются.

8. При необходимости Конкурсная комиссия может дополнительно потребовать от Участников конкурса предоставления дополнительной информации касательно представленных ими конкурсных предложений или других дополнительных документов, необходимых для выполнения данного заказа.

9. Никакие вставки между строками, подтирки или приписки в документах конкурсного предложения не допускаются, а при наличии их в документах, заявка не подлежит рассмотрению и отклоняется.

10. Участники конкурса должны представить конкурсное предложение строго в соответствии с формами, предлагаемыми в Конкурсной документации. В случае предоставления конкурсного предложения не по формам настоящей конкурсной документации, Конкурсная комиссия вправе отклонить данное предложение.

11. Предложения должны подаваться цельно и в количествах, указанных в конкурсной документации.

12. Участник в представляемой заявке на участие должен указывать цену предложения с учетом НДС или без учета НДС.

13. Полномочия представителя участника должны быть подтверждены доверенностью/приказом, которые должны быть представлены конкурсной комиссии. Доверенность должна быть оформлена по форме Приложения № 3.

14. При оценке предложения Заказчиком будут учитываться следующие критерии:

- соответствие предлагаемого товара/работы/услуги техническим требованиям, изложенным в конкурсной документации (качество);
- цена;
- условия и сроки выполнения работ/услуг, поставки товара;
- условия платежа и гарантии;
- наличие собственной производственно-технической базы и квалифицированного сертифицированного персонала;
- предоставление финансовой скидки;
- деловая репутация участника конкурса.

2. Объявление о проведении конкурса

АКБ «ASIA ALLIANCE BANK» объявляет конкурс на поставку DLP-системы Falcongaze SecureTower АКБ «ASIA ALLIANCE BANK».

Технические требования к программному обеспечению (ПО)

1. **Требования к системе в целом:**

- мониторинг событий случайной или преднамеренной пересылки пользователями за пределы сегментов вычислительных сетей Заказчика конфиденциальной информации по следующим каналам:
  - электронная почта (протоколы POP3, SMTP, IMAP, MAPI, HTTP, в т.ч. шифрованные аналоги);
  - электронная почта, защищенная по стандарту S/MIME;
  - электронная почта, переданная через почтовые веб-службы (gmail.com, mail.ru, rambler.ru, yandex.ru и т.д.);
  - двунаправленный перехват сообщений в чатах, статусов, комментариев к публикациям и на форумах социальных сетей: Facebook, Odnoklassniki, Vk, Twitter;
  - средства мгновенного обмена сообщениями – Telegram, Skype, SIP, Viber (с возможностью перехвата и архивирования вложенных файлов, текстовых и голосовых данных, распознавания голосовых коммуникаций), Microsoft Lync (голосовые и текстовые сообщения, распознавания голосовых коммуникаций), ICQ, AIM, Mail.Ru Агент, Miranda, WhatsApp, Google Hangouts, QIP Infium, PSI, Yahoo! Messenger, и др., в т.ч. использующие шифрование;
  - запись файлов на внешние накопители;
  - запись файлов на локальные сетевые ресурсы;
  - отправка файлов в облачные сервисы хранения информации (Dropbox, OneDrive, Google Drive, Яндекс.Диск, Apple iCloud, облако Mail.Ru);
  - отправка файлов на печать на локальные и сетевые принтеры;
  - передача файлов в компьютерных сетях по протоколам FTP и FTPS;
- мониторинг событий разглашения конфиденциальной информации в разговорной речи путем контроля аудио потока с микрофона контролируемой рабочей станции в режиме реального времени;
- поддержка удаленного доступа к просмотру видеоизображения рабочего стола компьютера пользователя в режиме реального времени;
- мониторинг в режиме реального времени наличия или появления в файловой системе контролируемой рабочей станции конфиденциальных документов;
- сбор и хранение всех исходящих и входящих электронных сообщений, с возможностью полнотекстового поиска по архиву, в том числе и в присоединенных к письмам файлах;
- контроль использования периферийных устройств (доступ и копирование на внешние накопители, аудит подключения и доступ к внешним устройствам различного назначения);
- контроль эффективности использования рабочего времени и ресурсов персоналом компании путем снятия снимков экрана, сбора информации по времени работы/простоя ПК, используемым приложениям (в том числе WinRT (Metro) и виртуальные рабочие столы), а также статистического и событийного анализа перехваченной информации;
- запрет запуска отдельных программных приложений;

- возможность блокирования доступа к определенным веб-ресурсам и их функционалу (на основании заданных политик безопасности);
- блокирование сетевого трафика отдельных процессов;
- возможность блокирования передачи исходящих сообщений по протоколам SMTP, HTTP и MAPI (в т.ч. с использованием шифрования), содержащих определенную информацию на основе контентного и атрибутивного анализа сообщений и вложенных данных.

Функциональные требования к системе

Реализация перехвата данных

Система должна поддерживает несколько схем перехвата трафика данных в контролируемой сети. Перехват на базе системы DLP должно быть реализован как одним из приведенных ниже способов в отдельности, так и их комбинацией:

- централизованный перехват сетевого трафика путем зеркалирования трафика на SPAN-порт сетевого коммутатора;
- перехват агентами, установленными на рабочие станции пользователей;
- перехват электронной почты, переданной через почтовые сервера;
- перехват HTTP(S)-трафика, переданного через прокси-сервера.

Гибридные способы контроля представлены различными сочетаниями, в том числе:

- перехват агентами и перехват почты, переданной через почтовые сервера;
- перехват агентами и централизованный перехват (только протокол HTTP).

Централизованный перехват данных

Весь внешний трафик контролируемой локальной сети с помощью управляемого коммутатора должно зеркалироватся на специально выделенный сервер, на котором установлен компонент системы Сервер перехвата. Сервер перехвата должен обеспечиват следующие возможности:

- централизованный перехват данных, отправляемых по протоколам, не использующим шифрование (POP3, SMTP, IMAP, MAPI (MAPI over RPC, MAPI over RPC over HTTP), OSCAR, XMPP (Jabber), HTTP, FTP, MMP (Mail.Ru Агент), YIM;
- фильтрация для анализа данных, отправляемых по протоколу HTTP;
- гибкая настройка исключений из перехвата по IP-адресам (отдельным и диапазону) и отдельным MAC-адресам, протоколам, учетным записям и адресам электронной почты, учетным записям систем мгновенного обмена сообщениями, процессам.

Перехват данных агентским модулем

Агент контроля рабочих станций - независимый программный модуль, который устанавливается на рабочие станции в сети (максимум один агент на рабочую станцию). Помимо перехвата нешифрованного сетевого трафика, агентский модуль выполняет перехват SSL-трафика и данных, переданных по использующим шифрование протоколам, а также фиксирует активности пользователя на контролируемой рабочей станции. Контроль сети, реализованный на базе агентских модулей, обеспечивает следующее:

- возможность как централизованной установки – из консоли администратора либо средствами групповых политик домена (с использованием MSI-пакета), так и установки вручную (с использованием отдельного EXE-инсталлятора агента с графическим интерфейсом);
- централизованная настройка дистрибутива агента для установки вручную;

- возможность перехвата данных, отправляемых по нешифрованным протоколам (POP3, SMTP, MAPI (MAPI over RPC, MAPI over RPC over HTTP, MAPI over HTTP), OSCAR, XMPP (Jabber), HTTP, FTP, MMP (Mail.Ru Агент), YIM);
- возможность перехвата данных, отправляемых по шифрованным протоколам (с использованием SSL/TLS-шифрования), включая шифрованные протоколы передачи электронной почты и мгновенного обмена сообщениями, HTTPS, FTPS, Skype, SIP, а также данные, переданные в приложениях Viber, WhatsApp, Google Hangouts, Telegram и Microsoft Lync;
- перехват данных, отправляемых по протоколам с использованием SSL/TLS-шифрования, осуществляется путем подмены цифрового сертификата. При этом имеется возможность указания произвольного имени удостоверяющего центра в генерируемых системой сертификатах, а также возможность гибкой настройки подмены для использования различных сертификатов при перехвате различных SSL/TLS-соединений;
- возможность перехвата и автоматического дешифрования зашифрованных почтовых сообщений, содержащих цифровую подпись (включая вложенные в письма файлы), защищенных по стандарту S/MIME;
- возможность установки режима перехвата: только шифрованный либо нешифрованный трафик, весь трафик (шифрованный и нешифрованный);
- возможность фильтрации для анализа данных, отправляемых по протоколу HTTP/ HTTPS;
- возможность гибкой настройки исключений из перехвата по IP-адресам (отдельным и диапазону), протоколам, системным учетным записям пользователей, учетным записям и адресам электронной почты, учетным записям систем мгновенного обмена сообщениями, атрибутам процессов, вешним устройствам и локальным сетевым ресурсам;
- возможность блокирования передачи исходящих сообщений по протоколу SMTP(S), содержащих определенную информацию (на основании заданных политик безопасности с использованием контентного и атрибутивного анализа сообщений и вложенных данных);
- возможность указания адресов электронной почты пользователей, активных в текущий момент, на компьютерах с установленными агентами.
- возможность блокирования передачи почтовых сообщений по протоколу MAPI (в том числе с использованием шифрования), содержащих определенную информацию (на основании заданных политик безопасности с использованием контентного и атрибутивного анализа сообщений и вложенных данных);
- возможность блокирования передачи исходящих сообщений по протоколу HTTP(S), содержащих определенную информацию (на основании заданных политик безопасности с использованием контентного и атрибутивного анализа данных);
- возможность блокирования посещения веб-ресурсов, использование отдельных интерактивных элементов веб-ресурсов, поиск запрещенной информации в сети Интернет;
- возможность блокирования паразитного HTTP(S) трафика вредоносных и служебных программ;
- блокирование сетевого трафика процессов на основании анализа их атрибутов и значения хеш-функций исполнительных файлов;
- опциональное уведомление пользователя о сработках блокировки устройств, запуска процессов, сетевого трафика процессов и MAPI-трафика;
- возможность задавать произвольный текст сообщений о блокировании устройств, запуска процессов, сетевого трафика процессов, HTTP- и MAPI-трафика;
- перехват web-коммуникаций пользователей в социальных сетях Facebook, Odnoklassniki, Vk, Twitter, при этом реализуется: двунаправленный перехват

сообщений в чатах; перехват статусов; перехват комментариев к публикациям и изображениям, перехват комментариев на форумах социальных сетей с контролем всего блока комментариев;

- перехват входящей и исходящей web-почты (gmail, mail.ru, rambler, yandex, yahoo, hotmail);
- контроль данных (путем создания и передачи в централизованное хранилище теневых копий файлов), отправляемых на внешние накопители, принтеры, облачные хранилища и локальные сетевые ресурсы пользователей и терминальных серверов;
- аудит файловых операций, контроль записи информации и блокирование доступа пользователей к локальным сетевым ресурсам;
- аудит файловых операций, контролировать передачу информации и блокирование доступа пользователей к облачным сервисам хранения информации при использовании веб-интерфейса и десктоп- приложений (Dropbox, OneDrive, Google Drive, Яндекс.Диск, Apple iCloud, облако Mail.Ru);
- аудит файловых операций, контроль записи информации и блокирование доступа пользователей к различным классам внешних накопителей информации с учетом их параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер);
- аудит использования и контроль доступа для внешних устройств, подключенных к рабочей станции, и блокирование доступа с учетом их параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);
- возможность сбора статистики по времени работы/простоя компьютера;
- контроль запуска приложений на компьютерах пользователей, а также длительность работы в каждом приложении (например, для контроля использования нежелательного или запрещенного программного обеспечения в корпоративной сети);
- запрет запуска пользователем отдельных программных приложений на контролируемой рабочей станции на основании имени процесса, атрибутов исполнительного файла и значения хеш-функции;
- возможность снятия снимков экрана рабочего стола пользователя с заданным интервалом, а также по событию (нажатие клавиши PrintScreen, смена окна активного приложения либо вкладки браузера, запуск определенного приложения);
- перехват данных, помещаемых в буфер обмена, позволяет исключить активность отдельных процессов из перехвата;
- контроль данных, вводимых пользователем с клавиатуры («кейлоггер») с возможностью исключения активности отдельных процессов из перехвата;
- прослушивание аудиопотока, поступающего с микрофонов, подключенных к рабочим станциям в режиме реального времени;
- подключение к видеопотоку, поступающему с монитора рабочей станции с возможностью удаленного просмотра видеоизображения рабочего стола пользователя в режиме реального времени;
- автоматическую запись аудиопотока с микрофона и системных звуков, а также видеоизображения с рабочего стола и подключенной веб-камеры компьютера по расписанию;
- автоматический поиск конфиденциальных файлов на дисках рабочей станции пользователя и отправлять уведомления офицеру безопасности о случаях их обнаружения в местах, для этого не предназначенных (несанкционированное владение);
- инструменты поиска определенных файлов, а также файлов по заданным атрибутам или значениям хеш-функций в файловых системах контролируемых компьютеров;

- возможность установки агентов с разными настройками применительно к различным объектам AD, отдельным компьютерам (группам компьютеров) и пользователям с указанным SID путем использования различных профилей настроек агентов;
- выбор условий активации профилей: наличие соединения с сервером, наличие активного VPN-подключения, пользовательское условие на основе LUA-скрипта;
- возможность защиты агента на рабочей станции от несанкционированного удаления пользователем;
- возможность скрытия агента на рабочей станции (включая скрытие процессов, служб, установочных файлов и папок агента);
- опциональное отображение иконки программы в панели задач;
- возможность использования агентами локального хранилища данных на рабочей станции (например, в случае выноса ноутбука за пределы корпоративной сети, агент сохраняет все собираемые данные во временное хранилище на локальном компьютере с последующей передачей данных на сервер для анализа – при восстановлении подключения агента к серверу);
- возможность настройки параметров локального хранилища данных (ограничение максимального размера и времени хранения);
- система отслеживает и отображает статистику по состоянию агентских модулей на рабочих станциях пользователей (с цветовой индикацией состояний «агент работает успешно», «агент устанавливается/удаляется», «компьютер не присылает данные», «компьютер недоступен», «компьютер отклонен лицензией», «компьютер с предупреждениями», «компьютер с ошибками»), а также отображает статистику по поступлению данных на сервер в разрезе агентов, пользователей, подключенных внешних устройств и типов данных (протоколов). Данные статистики доступны для экспорта в CSV и TXT- форматы.

Перехват HTTP-трафика, переданного через прокси-сервера

Перехват данных, переданных по протоколам HTTP и HTTPS через прокси-сервера, выполняется путем интеграции с прокси-сервером по ICAP-протоколу. При этом обеспечивается:

- возможность перехвата и фильтрации для анализа данных, отправляемых по протоколам HTTP/HTTPS;
- возможность блокирования передачи исходящих сообщений по протоколу HTTP(S), содержащих определенную информацию (на основании заданных политик безопасности с использованием контентного и атрибутивного анализа данных).

Перехват электронной почты, переданной через почтовые сервера

Перехват почты, отправляемой через почтовые сервера, развернутые на базе Microsoft Exchange Server, IBM Lotus and Domino, Sendmail, hMailServer и другого программного обеспечения, выполняется путем интеграции с почтовыми серверами по протоколам POP3, IMAP или SMTP. При этом обеспечивается перехват всех почтовых сообщений, переданных и полученных с помощью почтовых серверов компании по протоколам POP3, SMTP, IMAP и MAPI.

Описание возможностей хранения и обработки данных:

- встроенная СУБД SQLite в комплекте поставки;
- хранение всех перехватываемых данных вне зависимости от срабатывания политик безопасности;

- возможность централизованного хранения всех собираемых системой данных в СУБД Microsoft SQL Server, Oracle, PostgreSQL версии 9.3 и выше, MySQL версии 5.7.09 и выше, SQLite (на выбор);
- возможность объединять одиночные базы данных в группы, поддерживающие кольцевую ротацию баз. Поисковые операции выполняются по всем базам данных в группе. Для событий запуска ротации можно настроить выполнение скриптов (перед и/или после ротации);
- поддержка работы с базами данных, расположенных на разных серверах;
- возможность настройки правил записи данных в базы для регуляции, в какую базу или группу баз записывать информацию в зависимости от типа данных, источника данных, пользователя, IP-адреса и другой атрибутной информации;
- возможность балансировки нагрузки по двум и более группам баз данных либо базам данных согласно алгоритму "round robin": все поступающие в систему данные записываются в базы данных поочерёдно;
- возможность автоматической репликации поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;
- возможность перенаправления поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;
- возможность настройки расписания для репликации данных;
- возможность хранения очереди репликации данных на диске для обеспечения сохранности и целостности реплицируемых данных в случае отказа системы;
- отображение статистики репликации данных;
- возможность сохранения файловых объектов большого размера на диск сервера, а не в базу. В базу данных при этом помещаются относительные пути к файлам;
- возможность настройки длительности хранения информации в базе данных в группе ротации, в том числе установки различной длительности хранения для различных типов данных (например, хранить почтовую переписку за последние 60 дней, а переписку через программы мгновенного обмена сообщениями – за последние 30 дней);
- возможность очистки базы данных вручную через Консоль администратора;
- возможность выбора режима очистки и обновления поисковых индексов (ручной и автоматический режимы);
- возможность архивирования баз данных с последующим подключением к системе для осуществления поиска в них критичной информации;
- поддержка режима параллельной обработки данных, перехваченных по различным каналам передачи информации, что позволяет повысить производительность системы при выполнении операций обновления, удаления и поиска данных;
- возможность настройки резервного хранилища агентского модуля в части ограничения размера и максимального периода хранения информации;
- настройка максимальной скорости передачи перехваченных данных от агента на сервер;
- возможность осуществления асинхронного поиска по перехваченным данным (при проведении параллельного поиска по нескольким каналам передачи информации, отображение результатов выполняется по мере их получения).
- возможность выборочного удаления пользователем перехваченной информации.

Система должна индексировать файлы следующих форматов:

- Adobe Acrobat (*.pdf)
- Ami Pro (*.sam)
- Ansi Text (*.txt)
- ASCII Text

- ASF (метаданные) (*.asf)
- CSV (Comma-separated values) (*.csv)
- DBF (*.dbf)
- DjVu
- DWG
- DXF
- EBCDIC
- EML files (электронные письма, сохраненные Outlook Express) (*.eml)
- Enhanced Metafile Format (*.emf)
- Eudora MBX файлы сообщений (*.mbx)
- Flash (*.swf)
- GZIP (*.gz)
- HTML (*.htm, *.html)
- JPEG (метаданные) (*.jpg)
- Lotus 1-2-3 (*.wk?, *.123)
- MBOX архивы электронных писем (включая Thunderbird) (*.mbx)
- MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (*.mht)
- Microsoft Access (*.mdb)
- Microsoft Access 2007 (*.accdb)
- Microsoft Document Imaging (*.mdi)
- Microsoft Excel (*.xls)Microsoft Excel 2003 XML (*.xml)
- Microsoft Excel 2007 (*.xlsx)
- Microsoft Open XML Paper Specification (*.oxps)
- Microsoft Outlook (OST)
- Microsoft Outlook Express 5 и 6: базы сообщений (*.dbx)
- Microsoft PowerPoint (*.ppt)
- Microsoft Rich Text Format (*.rtf)
- Microsoft Searchable Tiff (*.tiff)
- Microsoft Word 2003 XML (*.xml)
- Microsoft Word 2007 (*.docx)
- Microsoft Word for DOS (*.doc)
- Microsoft Word for Windows (*.doc)
- Microsoft Works (*.wks)
- MIME-сообщения
- MP3 (метаданные) (*.mp3)
- MSG files (электронные письма, сохраненные Outlook) (*.msg)
- Multimate Advantage II (*.dox)
- Multimate version 4 (*.doc)
- OpenOffice версий 1, 2 и 3: документы, электронные таблицы и презентации (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (включая OASIS Open Document Format для офисных приложений)
- OST(внутренний формат Microsoft Outlook)
- Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw)
- TAR (*.tar)
- TIFF (*.tif)
- TNEF (winmail.dat)
- Treepad HJT (*.hjt)
- Unicode (UCS16, порядок байтов Mac или Windows, или UTF-8)
- Windows Metafile Format (*.wmf)
- WMA видео (метаданные) (*.wma)

- WMV видео (метаданные) (*.wmv)
- WordPerfect (5.0 и выше) (*.wpd, *.wpf)
- WordPerfect 4.2 (*.wpd, *.wpf)
- WordStar 2000
- WordStar версий 1, 2, 3, 4, 5, 6(*.ws)
- Write (*.wri)
- XBase (включая FoxPro, dBase и другие совместимые с XBase форматы) (*.dbf)
- XML Paper Specification (*.xps)
- XSL
- XyWrite
- ZIP (*.zip)

Кроме того, система должна обеспечивать возможность извлечения текстовой информации из файлов графических форматов (BMP, JPEG, PNG, TIFF, GIF и другие), а также из файлов формата PDF, DjV, OXPS путем оптического распознавания символов (OCR).

Программа должна обеспечивает распознавание печатей на изображениях по заданным эталонам.

Возможность выбора встроенного средства распознавания Nicomsoft OCR или ABBYY FineReader.

Описание возможностей управления данными пользователей:

- отсутствие ограничений по количеству профилей пользователей в базе программы;
- создание внутренних профилей (карточек) пользователей, содержащих всю идентификационную информацию пользователей локальной сети;
- интеграция с Active Directory (возможность импорта всех идентификационных данных пользователя, хранящихся в Active Directory, в профиль пользователя; возможность автоматического создания (удаления) профилей пользователей при добавлении (удалении) записей в (из) Active Directory, автоматическое создание карточек при обнаружении ранее неизвестной пользовательской информации, а также автоматическая синхронизация изменений идентификационных данных пользователей в Active Directory с их профилями с возможностью настройки расписания синхронизации);
- возможность выборочной интеграции с Active Directory с указанием доменов (объектов доменов) и контроллеров доменов, с которыми будет выполняться синхронизация;
- возможность автоматической привязки идентификационных данных пользователя, отсутствующих в Active Directory (используемые учетные записи Skype, Telegram, Viber, Yahoo, WhatsApp, Google Hangouts, номера ICQ, ID социальных веб-сетей, SIP, адреса электронной почты, включая учетные записи XMPP и Lync, а также IP-адреса и фотографии), к профилю пользователя для последующей идентификации;
- возможность создания пользовательских карточек без выделения лицензий на соответствующих пользователей (например, создание карточки для внешнего пользователя с целью отслеживания его общения с внутренними абонентами; в случае увольнения сотрудника – возможность сохранения карточки пользователя для контроля его последующего общения с сотрудниками компании);
- возможность создания и редактирования пользовательских карточек как в клиентской консоли системы, так и в консоли администратора;
- возможность отображения пользовательских карточек как в виде линейного списка, так с разбивкой на группы и подгруппы на основании информации из Active Directory (с учетом Organizational Units), либо на основании произвольно

задаваемых параметров в карточках пользователей (произвольная группировка по организациям/отделам);
- возможность разграничения прав доступа к системе и ее компонентам для различных пользователей с назначением ролей (например, «системный администратор» - доступ только к изменению технических параметров системы – без доступа к просмотру перехваченной информации; «руководитель подразделения» - доступ только к просмотру информации об активности определенных сотрудников – без доступа к просмотру информации об инцидентах или об активности других сотрудников; «офицер безопасности» - доступ только к политикам безопасности и инцидентам – без доступа к просмотру информации об активности сотрудников, и т.п.) с использованием системы аутентификации пользователей;
- возможность аутентификации пользователей, работающих с системой, на основании их учетных записей Windows;
- возможность аутентификации пользователей, работающих с системой, на основании внутренних учетных записей (с запросом имени и пароля пользователя при входе в систему);
- политика сложности и срока действия паролей в режиме внутренней аутентификации;
- возможность отправки администратору уведомлений по электронной почте о системных событиях (системные ошибки, предупреждения и т.д.);
- ведение журнала (лога) действий пользователей, работающих с системой.

Контролируемые каналы утечки

Контроль отправки информации посредством электронной почты, включая следующие возможности:

- централизованный перехват почтовых сообщений посредством зеркалирования трафика на сетевом коммутаторе (для нешифрованных протоколов – POP3, SMTP, IMAP, MAPI);
- перехват почтовых сообщений агентами, установленными на рабочие станции пользователей (для нешифрованных и шифрованных (SSL) протоколов – POP3, SMTP, MAPI плюс шифрованные аналоги);
- перехват агентами почтовых сообщений, переданных посредством почтовых программ с поддержкой стандарта защищённой электронной почты S/MIME, при этом обеспечивается автоматическая расшифровка содержимого письма;
- перехват почтовых сообщений путем интеграции с почтовыми серверами по протоколам POP3, SMTP, IMAP (на выбор), при этом система обеспечивает возможности интеграции с почтовыми серверами на базе Microsoft Exchange, IBM Lotus Domino, Postfix, Sendmail и др.;
- перехват почтовых сообщений между Microsoft Outlook и Microsoft Exchange Server по протоколу MAPI (в том числе с использованием шифрования) путем интеграции с Microsoft Outlook;
- перехват и анализ почтовых сообщений, отправленных либо полученных при помощи почтовых веб-сервисов по протоколу HTTP(S) (yandex, mail.ru, rambler, gmail, yahoo, hotmail и т.д.);
- перехват и анализ файлов-вложений почтовых сообщений;
- автоматическое обнаружение почтовых сообщений и почтовых вложений, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

- блокировка агентским модулем исходящих почтовых сообщений по протоколу SMTP(S), HTTP(S), MAPI на основании заданных политик безопасности с использованием контентного и атрибутивного анализа сообщений;
- возможность сохранения электронных писем в HTML-формате и в формате, совместимом с Microsoft Outlook;
- возможность поиска по тексту и атрибутам почтовых сообщений и файлов.

Контроль отправки информации посредством IM клиентов, включая следующие возможности:

- возможность централизованного перехвата сообщений и файлов посредством зеркалирования трафика на сетевом коммутаторе (для протоколов OSCAR, XMPP, MRA, YIM, не использующих шифрование);
- возможность перехвата текстовых сообщений агентами, установленными на рабочие станции пользователей (Skype, Telegram, WhatsApp, Google Hangouts, SIP, Viber, MS Lync, OSCAR, XMPP, MRA, YIM – как шифрованных (SSL), так и нешифрованных);
- возможность перехвата файлов агентами (Skype, Telegram, Viber, OSCAR, XMPP, MRA, YIM – как шифрованных (SSL), так и нешифрованных);
- возможность перехвата голосовых разговоров, осуществляемых через Skype (в том числе звонки Skype-to-Skype, Skype-to-phone), а также через Viber, Microsoft Lync и по протоколу SIP с сохранением разговоров в файлы формата MP3;
- возможность распознавания (перевода в текстовый формат) голосовых разговоров (коммуникаций) Viber, Skype, SIP, Lync;
- возможность перехвата голосовых сообщений Telegram;
- возможность воспроизведения сохраненных разговоров Skype, Viber, Microsoft Lync и SIP;
- возможность ограничения перехвата по отдельным учетным записям пользователей;
- автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность осуществления поиска по тексту и атрибутам сообщений и файлов, переданных через IM-клиенты.

Контроль отправки информации по HTTP протоколу, включая:

- возможность централизованного перехвата данных посредством зеркалирования трафика на сетевом коммутаторе (для протокола HTTP);
- возможность перехвата посредством интеграции с прокси-серверами по протоколу ICAP (для протоколов HTTP и HTTPS);
- возможность перехвата данных агентами, установленными на рабочие станции пользователей (для протоколов HTTP и HTTPS);
- возможность создания и гибкой настройки фильтров для исключения из перехвата определенной исходящей и входящей информации по ряду предустановленных правил и правил, созданных пользователем;
- возможность настройки фильтрации перехвата данных по MIME-типам;
- перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы;
- перехват входящих и исходящих данных веб-коммуникаций (переписки в чатах, публикация статусов, комментарии) на веб-ресурсах: Facebook, Odnoklassniki, Vk, Twitter;

- перехват входящих и исходящих электронных писем и вложений, переданных либо полученных через почтовые веб-сервисы (yandex, mail.ru, rambler, gmail, yahoo, hotmail и т.д.);
- перехват сообщений, переданных в веб-клиентах Skype и ICQ;
- перехват и анализ поисковых запросов пользователя;
- сохранение адресов всех страниц (URL), посещенных пользователем;
- автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам сообщений и файлов, переданных по протоколу HTTP(S);
- возможность блокирования посещений веб-ресурсов, исходящих сообщений и файлов определенного содержания (HTTP и HTTPS) агентским модулем и посредством интеграции с прокси-серверами по протоколу ICAP;
- контроль браузер-активности (посещения веб-сайтов с помощью веб-браузера): фиксируются переходы между страницами веб-сайтов и ведется комплексная статистика времени, проведенного на различных веб-ресурсах;
- возможность сохранения различных типов отчетов о браузер-активности (рейтинг посещенных сайтов за день, хронология событий) за выбранный временной интервал для отдельного пользователя или для нескольких пользователей в виде PDF-файла.

Контроль информации, передаваемой по протоколу FTP, включая возможности:

- перехвата файлов, загруженных или переданных по простому FTP-соединению, а также переданных по зашифрованному SSL-соединению;
- возможность централизованного перехвата данных посредством зеркалирования трафика на сетевом коммутаторе (для протокола FTP);
- возможность перехвата данных агентами, установленными на рабочие станции пользователей (для протоколов FTP и FTPS);
- возможность настройки ограничения по размеру перехватываемых файлов;
- автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам файлов, переданных по протоколу FTP(S).

Возможности контроля информации, отправляемой на печать:

- перехват отправляемых на печать документов агентами, установленными на рабочих станциях пользователей;
- возможность перехвата документов, отправляемых на сетевые и локальные принтеры (в том числе подключенные к COM-, LPT-портам);
- возможность перехвата печати в XPS-формат;
- возможность настройки исключений из перехвата по отдельным принтерам;
- возможность ограничения перехвата печати по количеству страниц и по размеру документа;
- возможность исключения процессов для модуля перехвата печати на принтерах.
- извлечение и анализ текста отправленных на печать документов;
- автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу,

ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам отправленных на печать файлов;
- сохранение в PDF- и HTML-формате.

Возможности контроля информации, отправляемой на внешние накопители:
- теневое копирование файлов, отправляемых на внешние накопители (съемные жесткие диски, карты памяти, съемные накопители, CD/DVD и флоппи-диски);
- возможность настройки исключений из теневого копирования по размеру и расширению файлов;
- возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
- возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
- возможность настройки исключений из теневого копирования для определенных внешних накопителей информации (по типам устройств, идентификаторам, производителям, названиям, серийным номерам);
- контроль доступа к внешним накопителям информации, с возможностью запрета на использование устройств с определенными параметрами (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);
- управление правами записи на внешние накопители с возможностью запрета записи на определенные устройства (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства), а также запрета записи файлов с определенным расширением;
- возможность контроля копирования информации на внешние накопители как в локальных, так и терминальных пользовательских сессиях;
- аудит событий копирования файлов на внешние накопители: фиксируется имя файла, пользователь, дата, время и данные устройства;
- контроль доступа и аудит использования внешних устройств любого типа, подключаемых к рабочей станции, по набору параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства);
- автоматическое обнаружение случаев использования внешних устройств с указанными параметрами (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- автоматическое обнаружение случаев передачи на внешние накопители файлов в целом и, в частности, содержащих определенную информацию (на основании заданных политик безопасности), с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту и атрибутам отправленных на внешние накопители файлов.

Возможности контроля информации, передаваемой в облачные хранилища (Dropbox, OneDrive, Google Drive, Яндекс.Диск, Apple iCloud, облако Mail.Ru):
- теневое копирование файлов, отправляемых в облачные хранилища пользователем либо процессом;
- возможность настройки исключений из аудита, теневого копирования и контроля доступа по расширениям файлов;
- возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);

- возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
- контроль доступа к отдельным облачным хранилищам с возможностью запрета доступа для определенных пользователей;
- управление правами передачи данных в облачные хранилища с возможностью запрета отправки файлов определенных форматов;
- автоматическое обнаружение переданных в облачные хранилища файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, имя пользователя, дата, время и имя облачного сервиса хранения;
- возможность поиска по тексту и атрибутам отправленных файлов.

Возможности контроля информации, отправляемой на локальные сетевые ресурсы:

- теневое копирование файлов, отправляемых на сетевые ресурсы;
- возможность настройки исключений из теневого копирования по расширениям файлов;
- возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
- возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
- контроль доступа к сетевым ресурсам с возможностью запрета доступа для определенных пользователей;
- управление правами записи на сетевые ресурсы с возможностью запрета записи определенных форматов файлов;
- возможность теневого копирования файлов, передаваемых на сетевые ресурсы терминальных серверов;
- автоматическое обнаружение переданных на сетевые ресурсы файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- аудит событий копирования файлов на локальные сетевые ресурсы: фиксируется имя файла, пользователь, дата, время и сетевой путь к ресурсу;
- возможность поиска по тексту и атрибутам отправленных на сетевые ресурсы файлов.

Описание возможностей мониторинга действий пользователей на ПК

Скриншоты (снимки экрана рабочего стола пользователя):

- возможность снятия скриншотов с заданным интервалом с точностью до секунды;
- возможность снятия скриншотов при смене активного окна и вкладки браузера, запуске нового процесса;
- возможность снятия скриншотов при нажатии клавиши PrintScreen;
- возможность настройки качества скриншотов (в т.ч. сохранения в черно-белом формате);
- возможность настройки размера скриншотов (в процентах от оригинала);
- возможность настройки формата скриншотов (JPEG, PNG);
- сохранение специальной отметки в случае невозможности снятия скриншота (сессия пользователя отключена, заблокирована и т.п.);
- возможность отключения захвата снимков при простое рабочей станции.

- возможность экспорта снимков экранов во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к просмотру перехваченных данных через веб-браузер;
- возможность сохранения скриншотов отдельного пользователя за день (или за выбранный временной интервал) в виде набора графических файлов либо объединенных в один PDF- или видео-файл.

Статистика по активности ПК:

- ведение статистики по времени работы и простоя (отсутствия действий пользователя) ПК с представлением собранной информации в виде графика;
- ведение статистики по времени работы пользователя в приложениях с представлением собранной информации в виде графика (при этом учитывается время не от запуска до завершения процессов, а время работы пользователя в активном окне);
- возможность настройки исключений отдельных процессов из мониторинга;
- возможность автоматического анализа собранной статистики для выявления определенных событий (например, запуск несанкционированных приложений), контроля длительности работы пользователей с конкретными приложениями и длительности периодов работы/простоя компьютера – с отправкой соответствующего уведомления ответственному лицу;
- возможность сохранения отдельных отчетов по активности (активность пользователя за ПК, активность приложений, хронология событий) за выбранный временной интервал для отдельного пользователя или нескольких пользователей в виде PDF-файла.

Контроль буфера обмена:

- теневое копирование помещаемой в буфер обмена текстовой информации с фиксацией приложения, из которого данная информация была помещена в буфер обмена, и времени события;
- возможность ограничения максимального объема текста, перехватываемого из буфера обмена;
- автоматическое обнаружение определенной информации (на основании заданных политик безопасности), помещаемой в буфер обмена, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту, помещаемому пользователями в буфер обмена.

Кейлоггер:

- регистрация нажатий пользователем клавиш на клавиатуре с фиксацией приложения, в котором пользователь вводил данную информацию, и времени, возможность отображения/скрытия нажатий служебных клавиш (Shift, Enter, Backspace и т.п.);
- автоматическое обнаружение определенной информации (на основании заданных политик безопасности), вводимой пользователем с помощью клавиатуры, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- возможность поиска по тексту, вводимому пользователями с клавиатуры.

Аудиомониторинг:

- подключение к микрофонам контролируемых рабочих станций с возможность прослушивания аудио-потока в режиме реального времени;
- прослушивание микрофонов нескольких пользователей одновременно;

- автоматическая запись поступающего с микрофона аудио-потока и системных звуков компьютера по расписанию;
- запись вручную;
- возможность сохранения записей нескольких пользователей одновременно;
- возможность воспроизведения файла записи средствами системы и в любом из медиа-проигрывателей.

Видеомониторинг:

- подключение к монитору компьютера пользователя и просмотра изображения рабочего стола в режиме реального времени;
- мониторинг рабочих столов нескольких пользователей одновременно;
- возможность вывода окна просмотра на отдельный экран;
- автоматическая запись видеоизображения рабочего стола и подключенной веб-камеры по расписанию;
- запись вручную;
- возможность сохранения записей нескольких пользователей одновременно;
- возможность воспроизведения файла записи средствами системы и в любом из медиа-проигрывателей.

Контроль файловых систем:

- формирование банков конфиденциальных документов, поиск которых должен выполняться во время сканирования;
- автоматическое сканирование дисков контролируемых компьютеров на предмет наличия определенных документов, которые носят статус конфиденциальных либо представляют интерес в рамках обеспечения информационной безопасности;
- возможность выбора компьютеров и пользователей, чьи файловые системы будут контролироваться;
- гибкая настройка правил выбора файлов и папок, подлежащих автоматической проверке;
- возможность создавать индивидуальные политики контроля за содержимым файловых систем для отдельных пользователей и рабочих станций;
- возможность удаленного поиска документов в файловых системах контролируемых рабочих станций на основе атрибутов файлов и значения их хеш-функций.

Анализа перехваченной информации

При работе с политиками безопасности пользователю должно предоставлятся доступ к следующим функционалам:

- автоматическая доставка уведомлений по электронной почте ответственному лицу в случае срабатывания политики безопасности (выявления инцидента); уведомление содержит общую информацию об инциденте (название политики безопасности, пользователь, допустивший нарушение, тип перехваченных данных, дата/время инцидента), а также ссылку на открытие соответствующего инцидента в пользовательской консоли либо вложения с документами, вызвавшими сработку;
- возможность настройки периодичности отправки уведомлений на электронную почту (немедленная отправка уведомления по выявлению инцидента либо накопление и порционная отправка уведомлений с заданной периодичностью – раз в час, раз в сутки и т.д.);
- возможность просмотра всех инцидентов по выбранной политике безопасности в клиентской консоли (с индивидуальным выделением просмотренных/непросмотренных инцидентов для каждого офицера безопасности, работающего с системой);

- при просмотре информации об инциденте в клиентской консоли доступна следующая информация:
  - пользователь, допустивший нарушение;
  - дата и время инцидента;
  - тип документа, вызвавшего срабатывание политики безопасности (электронное письмо, файл, отправленный на печать и т.д.);
  - содержание документа (электронного письма, переписки в IM-клиенте, файла и т.д.), вызвавшего срабатывание политики безопасности;
  - другая дополнительная информация.
- возможность назначения статуса для инцидента (инцидент не расследован, расследование инцидента отложено, инцидент расследован, важный инцидент, неважный инцидент, ложное срабатывание);
- возможность гибкого выборочного просмотра инцидентов по политике безопасности (например, показать только новые (непросмотренные) инциденты; показать только последние 100 инцидентов; показать инциденты за ближайший месяц, но не более 20 последних; показать инциденты, имеющие статус «Важный» и зарегистрированные в течение последней недели и т.д.);
- возможность полного или выборочного удаления записей об инцидентах по политике безопасности (например, удалить все инциденты старше 10 дней; удалить последние N инцидентов; удалить все инциденты, имеющие статус «Расследован»; удалить инциденты по данным, удаленным из БД, и т.д.);
- возможность сортировки списка инцидентов по различным параметрам (по релевантности, по дате/времени, по локальному/удаленному пользователю, по типу/размеру перехваченных данных, по статусу инцидента и т.д.);
- возможность фильтрации списка инцидентов по различным параметрам: по статусам (например, отобразить только важные), по типам данных (например, отобразить только инциденты, вызванные пересылкой информации по почтовым протоколам), по состоянию (например, отобразить только непросмотренные) – и по комбинациям этих параметров;
- возможность экспорта списка инцидентов в файл форматов MS Excel, CSV, XML, PDF (при этом сохраняется следующая информация об инцидентах – тип перехваченных данных, локальный/удаленный пользователь, дата/время перехвата, размер, статус инцидента, прочая информация);
- возможность экспорта перехваченных данных, вызвавших срабатывание политики безопасности, в файлы соответствующих форматов;
- ведение журнала (лога) действий офицера безопасности.

При анализе информации используются следующие возможности (аналитические возможности системы одинаковы для всех поддерживаемых языков анализируемой информации – включая анализ информации на русском, белорусском, казахском, английском, немецком, испанском, китайском, корейском, арабском и других языках):

Контентный анализ

- поиск по словам и словосочетаниям с учетом морфологии (возможность отключения), расстояния между словами и порядка слов, транслитерации кириллических символов латинскими, а также с возможностью нечеткого поиска (для поиска ключевых слов, в т.ч. написанных с ошибками и опечатками);
- технология поиска регулярных выражений, используемая для обнаружения фиксированных последовательностей символов, например, номеров паспортов, номеров банковских карт и т.п.;

- ручной и автоматический поиск по тематическим словарям с возможностью настройки порога срабатывания (например, при обнаружении любых 3 из 10 слов или выражений, содержащихся в словаре);
- возможность использования встроенных словарей и создания пользовательских;
- поиск документов с умышленно измененным расширением;
- поиск документов, защищенных паролем;
- цифровые отпечатки документов: возможность создания цифровых отпечатков документов или папок с документами для последующего обнаружения в перехваченных данных похожих документов – с возможностью указания процента совпадения);
- цифровые отпечатки баз данных: возможность настройки подключения системы к базе данных, содержащей конфиденциальную информацию, для создания цифровых отпечатков определенных полей выбранных таблиц с целью последующего обнаружения утечки информации из этой БД (например, при одновременном обнаружении персональных данных из связки полей «ФИО + паспортные данные»). Создание и обновление цифровых отпечатков баз данных осуществляется без промежуточных действий (таких как выгрузка базы данных в файл-источник цифрового отпечатка). При внесении изменений в базу данных система автоматически обновляет соответствующие цифровые отпечатки.
- ручной и автоматический поиск по цифровым отпечаткам;
- комбинирование нескольких простых запросов при помощи логических операторов «И», «ИЛИ», «НЕ».
- возможность поиска данных по DNS-имени и SID компьютера, по имени и SID домена среди данных, перехваченных агентами.

Анализ по атрибутам

- анализ по атрибутам пользовательских документов, таким как «имя документа», «адрес получателя электронной почты», «пользователь», «учетная запись IM-клиента», «дата», «время», «размер» и пр.;
- анализ атрибутов документа по статусам, таким как пересылка документа по защищенному протоколу, шифрованного или защищенного документа, поврежденных данных, отправка вызвавших блокирование данных либо переданных в индивидуальном порядке данных
- анализ атрибутов процессов: имя исполняющего файла, полный путь к файлу, заголовок окна процесса.

Статистический анализ

- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по отправленным/полученным пользователем электронным письмам (например, «пользователь получил более 10 писем за час» или «пользователь отправил менее 20 писем за день» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по отправленным/полученным пользователем файлам (например, «пользователь получил более 10 файлов за час» или «пользователь отправил более 20 файлов за день» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по голосовым переговорам в IM-клиентах (например, «время голосовых переговоров пользователя в IM-клиентах за день превысило 1 час» или «пользователь совершил более 10 звонков за день» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по переписке пользователя в IM-клиентах (например, «пользователь провел более 10 сессий переписки за день» или «пользователь отправил более 100 сообщений за день» и т.д.);

- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по посещенным пользователем URL (например, «пользователь посетил более 100 URL за день», «пользователь посетил более 1000 URL за неделю» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по поисковым запросам пользователя (например, «пользователь отправил более 100 поисковых запросов в период с 13:00 до 15:00» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по данным, отправленным пользователем на печать (например, «пользователь распечатал более 10 документов за день» или «пользователь распечатал более 1000 страниц за неделю» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности/простоя ПК (например, «ПК бездействовал в течение более 3 часов за день», «начало активности ПК зафиксировано позже 10:30» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени работы пользователя с определенными приложениями (например, «пользователь работал в Microsoft Word в течение более 5 часов за день» или «пользователь работал в приложении “Пасьянс Косынка” в течение более 70% рабочего времени» и т.д.);
- возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности пользователя в браузере (например, «Время пребывания пользователя на определенном сайте через браузер превысило 1 час за день» и т.д.);

Событийный анализ

Возможность настройки автоматических уведомлений в следующих случаях:

- запуск (завершение работы) пользователем определенного приложения;
- обнаружения пересылки зашифрованного вложения (например, защищенный паролем документ MS Office или архив);
- копирования файлов с контролируемых компьютеров на внешние накопители, облачные хранилища и сетевые диски с определенными параметрами;
- подключения и использования на контролируемых рабочих станциях устройств с определенными параметрами;
- посещение определенных web-ресурсов;
- блокирования пересылки данных по протоколам SMTP, HTTP, MAPI;
- обнаружения конфиденциальных файлов на компьютерных дисках пользователей;
- выявления факта пересылки документа с измененным расширением (например, при переименовании пользователем файла .doc в .jpg и последующей отправкой, система должна быть в состоянии определить оригинальный формат файла и извлечь из него текст для контентного анализа, дополнительно уведомив ответственного сотрудника о самом факте изменения расширения).

Независимо от используемого типа анализа, система предоставляет возможность выполнять ретроспективный анализ всех перехваченных данных для выявления фактов нарушения вновь созданной политики безопасности в прошлом (за весь период наблюдения).

Отчетность

Все перехваченные данные представляются в форме отчетов следующих видов:

Отчет об активности пользователя

a) Фотография рабочего дня пользователя содержит:
- информацию о количестве отправленных и полученных пользователем писем с разбивкой по часам;
- информацию о количестве сессий переписки пользователя в IM-клиентах с указанием длительности и количества сообщений в каждой сессии переписки;
- информацию о количестве файлов, полученных и отправленных пользователем по электронной почте, через IM-клиенты, по протоколам HTTP(S) и FTP(S), скопированных на внешние устройства, сетевые ресурсы, в облачные хранилища или распечатанных на локальных/сетевых принтерах – с разбивкой по часам;
- информацию о количестве посещенных URL и отправленных запросов – с разбивкой по часам;
- информацию о количестве сделанных системой снимков экрана рабочего стола пользователя – с разбивкой по часам;
- информацию о времени работы/простоя компьютера пользователя, детальную статистику активности приложений и данные о процентном соотношении времени работы в различных приложениях;
- информацию о количестве документов, помещенных в буфер обмена – с разбивкой по часам;
- информацию о посещении веб-сайтов с помощью веб-браузера с разбивкой по часам с предоставлением комплексной и детальной статистики времени, проведенного на различных веб-ресурсах;
- информацию о количестве символов, введенных пользователем с клавиатуры с разбивкой по часам.

Фотография рабочего дня пользователя является интерактивным и динамическим отчетом, что позволяет осуществлять переход по ссылкам непосредственно к просмотру содержимого перехваченных документов либо веб-ссылок.

Обеспечивается возможность экспорта фотографии рабочего дня во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к перехваченным данным через веб-браузер. Также поддерживается возможность экспорта в Outlook-файл либо в файл исходного формата.

b) Графики по типам информации

Система обладает возможностью представления данных, собранных по определенному пользователю за конкретный интервал времени, в виде графиков по отдельным типам информации (график по отправленным/полученным письмам, по количеству сессий/сообщений переписок в IM-клиентах, по количеству полученных и отправленных файлов, количеству посещенных URL и веб-запросов).

Графики по типам информации являются интерактивными и динамическими, что позволяет осуществлять переход по ссылкам (точкам на графике) непосредственно к просмотру содержимого перехваченных документов.

c) Граф-анализатор взаимосвязей пользователей

Система обладает возможностью графического отображения взаимосвязей пользователя (в виде графа либо матрицы) на основании собранной по нему информации для наглядного представления круга абонентов (как внутренних, так и внешних), с которыми данный пользователь обменивался какой-либо информацией в течение выбранного интервала времени.

Поддержка группировки контактов пользователя по принадлежности к установленным и не распознанным контактам.

Возможность просмотра взаимосвязей внешнего абонента с пользователями сети организации после предварительного создания карточки внешнего пользователя.

Возможность выбора масштаба отображения отчета при просмотре в клиентской консоли (с указанием % размера от оригинала).

Возможность интерактивного перехода от просмотра схемы взаимосвязей к содержимому документов (письма, переписки, файлы и т.д.), которыми пользователь обменивался с конкретным абонентом.

Поддержка сохранения отчета о взаимосвязях в виде графа во внешний файл формата PNG.

d) Сводная отчетность

Ежедневное автоматическое обновление отчетов с поддержкой перестроения отчетов вручную пользователем.

Автоматическая рассылка отчетов согласно расписанию на электронную почту указанным подписчикам.

Экспорт отчетов во внешний файл.

Поддержка интерактивности количественных данных - возможность прямого перехода к списку результатов по выбранному показателю.

Отчет по пользователю

Возможность построения сводного интерактивного отчета по определенному пользователю за все время наблюдения (или за выбранный интервал времени), включающего следующую информацию:

a) статистику перехвата данных, в т.ч.:
   - количество переданной и полученной пользователем информации по всем каналам передачи, включая почту и мессенджеры;
   - количество посещенных сайтов и поисковых запросов;
   - количество файлов, переданных/принятых по FTP;
   - количество распечатанных документов и страниц;
   - количество операций копирования в буфер обмена;
   - количество снятых скриншотов;
   - количество файлов, переданных на внешние накопители/сетевые ресурсы/облачные хранилища;
   - количество нажатых клавиш клавиатуры;
b) информацию об активности пользователя за компьютером, в т.ч.:
   - общее время активной работы пользователя за ПК;
   - среднесуточное время активной работы пользователя за ПК;
   - общее время простоя ПК;
   - среднесуточное время простоя ПК;
   - общее время присутствия сотрудника на работе;
   - среднесуточное время присутствия сотрудника на работе;
   - среднее время начала работы;
   - среднее время окончания работы;
   - общее количество рабочих дней;
   - календарь учета рабочих дней сотрудника с указанием времени начала/окончания работы, времени активности/простоя компьютера за каждый день (с цветовым

выделением фактов раннего начала работы, начала работы с опозданием, раннего окончания работы, окончания работы с задержкой);
- гистограмму по времени активности/простоя компьютера пользователя за каждый день;

c) информацию об активности приложений на компьютере пользователя, в т.ч.:
- процентное соотношение времени работы в различных приложениях (с построением круговой диаграммы)
- полный список запускавшихся приложений с указанием абсолютного времени работы в каждом из них;

d) информацию о браузер-активности:
- рейтинг посещенных веб-ресурсов;
- хронология активности в веб-браузере.

e) информацию о количестве зафиксированных инцидентов безопасности, инициированных пользователем, и соответствующих им правилах с различной степенью детализации.

Возможность пакетного сохранения отчетов для групп пользователей с предварительной настройкой единой формы отчета.

«ТОП-отчеты»

Возможность построения сводных интерактивных отчетов по контролируемым каналам передачи данных за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, наиболее активно использующих этот канал.

Возможность создания ТОП-отчета для сотрудников, входящих в группы пользователей системы либо в группы пользователей Active Directory.

Например, отчеты вида «ТОП-10 пользователей по количеству исходящих писем» или «ТОП-20 пользователей по количеству распечатанных страниц» и т.д.

Возможность построения сводных отчетов по количеству инцидентов безопасности за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, активность которых привела к срабатыванию правил безопасности большее количество раз.

При этом обеспечена возможность учета как общего суммарного, так и среднесуточного значения соответствующих параметров при составлении таких отчетов (например, отчет вида «ТОП-10 пользователей по среднесуточному количеству посещенных сайтов»).

«Отчеты по Центру безопасности»

Возможность построения сводных интерактивных отчетов о статистике срабатывания правил безопасности, заданных в Центре обеспечения безопасности.

При этом система обеспечивает просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям с выбором детализации по дням, месяцам, за произвольный временной промежуток и просмотр итогового количества срабатываний по каждому правилу в отдельности и по всем существующим правилам безопасности.

Сводный отчет

Возможность построения сводных интерактивных отчетов о статистических показателях сетевой и локальной активности выбранных пользователей.

При этом система обеспечивает просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям с выбором детализации по дням, месяцам, за произвольный временной промежуток и просмотр сводной статистики для выбранных статистических показателей.

Организация документов при проведении расследований

Специальный модуль Центр расследований должно предоставлять следующие возможности:

a) в целях сбора доказательств по инцидентам безопасности -- создавать документы (дела), которые могут включать в себя:
- информацию об инциденте;
- перечень вовлеченных лиц и их реквизиты;
- перечень проводимых (проведенных) мероприятий по расследованию инцидента и их результаты;
- выводы по результатам расследований;
- материалы расследований – внутренние документы (результаты перехвата) системы;
- реквизиты внутренних документов: тип данных, локальный пользователь, удаленный пользователь, дата перехвата, размер документа;
- материалы расследований – внешние документы;
- внешние документы, содержащие аналитические записки, рапорты и т.п.

b) в целях комплексного аудита результатов перехвата обеспечивать функции:
- просмотр содержания документов в расширенном виде напрямую из дела;
- фильтрацию документов при просмотре в деле;
- представление включенных в дело документов в режимах просмотра карточки, список;
- возможность экспорта дела в форматы *.pdf, *.xps.
- возможность распечатки дела на принтере.

c) в целях контроля за внесением изменений в дело наличие журнала событий, включающего в себя информацию о всех вносимых правках:
- имя пользователя, который совершил операцию в деле;
- совершенное действие;
- дату и время совершенного действия;
- прочую дополнительную информацию, которая может быть полезна для контроля за ведением дела.

d) в целях упрощения работы лиц, ведущих расследование, система должна обеспечивать:
- ведение списка дел;
- возможность сортировки дел в группы;
- возможность создания групп и подгрупп с количество уровней иерархии не менее 20;
- возможность переноса дел из группы в группу простым перетаскиванием «мышкой»;
- возможность переноса подгрупп из группы в группу простым перетаскиванием «мышкой»;

- возможность удаления дел и групп;
- возможность исправления дел;
- возможность просмотра: всех дел, только открытых дел, только закрытых дел;
- возможность глубокой пользовательской настройки просмотра дел: всех дел за определенный период; дел, открытых в определенный период; дел, закрытых в определенный период;
- возможность закрепления и открепления поля списка дел;
- возможность переноса поля списка дел к любой стороне окна программы.

Система также должна обеспечивать возможность удобного присоединения документов к делу в центре расследований из других модулей системы: например, через контекстное меню.

Мониторинг работоспособности системы

Сервис мониторинга работоспособности серверных компонентов должна контролировать состояние системы в режиме реального времени. При этом обеспечивать следующие возможности:

- ведение журнала событий серверных компонентов системы;
- просмотр журнала, а также детальной информации и рекомендаций по каждому событию в консоли администратора;
- фильтрация событий в журнале по рабочей станции, серверному компоненту, уровню, дате;
- выбор определенных рабочих станций для ведения мониторинга;
- автоматическое уведомление администратора системы о новых событиях серверных компонентов через консоль администратора и по почте;
- настройка правил отправки уведомлений по почте (выбор адресата, серверного компонента, уровня события или конкретных событий).

Помимо прочего, сервис должен обеспечивать фиксацию сведений о всех наиболее существенных событиях в работе серверных компонентов DLP в журнале операционной системы рабочей станции, на которой они установлены.

Прочие требования

Масштабируемость системы

В зависимости от конфигурации сети, от объема обрабатываемых перехваченных данных и других параметров, система должна гибко масштабироваться для обеспечения контроля большой и сложно организованной сети, а также распределения нагрузки на сетевые и аппаратные ресурсы:

- возможность установки нескольких серверов перехвата данных– для распараллеливания перехвата нескольких контролируемых каналов выхода в интернет;
- возможность установки нескольких серверов контроля агентов– для контроля разных сегментов сети или разных групп компьютеров;
- возможность организации кластера для горизонтального масштабирования больших нагрузок по множеству серверов;
- возможность установки нескольких серверов индексирования– для оптимизации и распределения нагрузки на сервер и базу данных;
- возможность установки нескольких серверов обработки почты – для работы с несколькими почтовыми серверами (MS Exchange, Lotus Domino и др.).

Ориентация работы всех компонентов системы на много-поточность

Система должен обеспечивать полную поддержку распределения нагрузки в многоядерных и многопроцессорных системах.

При использовании модуля распознавания ABBYY существует возможность распознавания одновременно нескольких PDF-документов.

Удобство администрирования

Централизованное управление компонентами системы из двух консолей: единая консоль администратора и единая консоль пользователя (сотрудника службы ИБ).

Система должна обеспечивать возможность шифрования трафика между консолями администратора и пользователя и сервером.

При работе с консолью пользователя система должна выполнять автоматическое переподключение к серверу при разрыве соединения.

Централизованное подключение и настройка хранилищ информации для всех серверных компонентов системы.

Возможность отключения автоматического управления системным брандмауэром.

Возможность при настройке профилей для агентов добавлять компьютер в профиль из схемы агентов, а также копировать/перемещать объекты между профилями.

Система автоматически должна фиксировать пользователей, которые проводят авторизацию или отклонении сервера-компонента на центральном сервере.

Возможность настройки автоматического запуска программ и скриптов при срабатывании правил безопасности.

Предельная стоимостью для проведения конкурса по приобретению DLP-системы Falcongaze SecureTower составляет 713 000 000 (семьсот тринадцать миллионов) сум.

Заинтересованные претенденты должны подать соответствующим образом заполненную и подписанную Заявку на участие в конкурсе по адресу: г.Ташкент, Яшнабадский район, ул. Махтумкули, дом №2А.

Конкурсные предложения, поступившие после указанного срока, не будут рассмотрены и будут отклонены. Электронные предложения не принимаются.

В конкурсных торгах могут принимать участие предприятия и организации, независимо от форм собственности.

Финансирование данной закупки будет осуществлено за счет собственных средств АКБ «ASIA ALLIANCE BANK».

Имя и должность ответственного лица заказчика и контакты:

Главный специалист Филатов Владимир Олегович,

Главный специалист Максудханова Алёна Олеговна,

адрес: г.Ташкент, Яшнабадский район, ул. Махтумкули, дом №2а. Телефон: (+998 71) 231-60-00, факс: (+998 71) 289-55-33

Приложение №1
к Конкурсной документации

ПЕРЕЧЕНЬ ДОКУМЕНТОВ, ПРЕДОСТАВЛЯЕМЫХ УЧАСТНИКАМИ КОНКУРСА.

Участник конкурса должен представить в запечатанном конверте следующие документы:

1. Заявка на участие в конкурсе по форме Приложение № 2 к Конкурсной документации.

2. Документы, подтверждающие правоспособность (документы о регистрации, копия паспорта руководителя, выписки из торгового реестра).

3. Гарантийное письмо, свидетельствующее, о том, что участник не находится в стадии реорганизации, ликвидации или банкротства, в состоянии судебного или арбитражного разбирательства с Заказчиком по форме, не имеет задолженности по налогам и сборам № 2 по форме Приложения № 3.

4. Доверенность на фирменном бланке организации по форме Приложения №4 к Конкурсной документации

5. Технические характеристики поставляемой DLP-системы Falcongaze SecureTower.

Приложение № 2
ФОРМА КОНКУРСНОГО ПРЕДЛОЖЕНИЯ

ФИРМЕННЫЙ БЛАНК

Председателю Конкурсной комиссии
АКБ «ASIA ALLIANCE BANK»
Норкулову О.О.

_____ имеет возможность поставить DLP-систему Falcongaze SecureTower в АКБ «ASIA ALLIANCE BANK»:

Производитель	**Продукт**	**Кол-во**	**Цена за ед. без НДС**	**Общая сумма без НДС**	**НДС**	**Цена за ед. с НДС**	**Общая сумма с НДС**
		200	0,00	0,00	0,00	0,00	0,00
	Итого:						**0,00**

Изучив данные объявления об условиях конкурса, мы, нижеподписавшиеся, уполномоченные на подписание заявки, (полное наименование Участника конкурса), намерены участвовать в конкурсных торгах (указать предмет конкурса) в соответствии с конкурсной документацией.

Мы обязуемся выполнить работы/оказать услуги/поставить товар в точном соответствии с условиями, предусмотренными договором и действующим законодательством Республики Узбекистан.

В случае если наши предложения будут приняты банком, берем на себя обязательство заключить договор с АКБ «ASIA ALLIANCE BANK» в срок не позднее 5 дней с момента направления в наш адрес извещения о принятии наших предложений.

Руководитель Участника конкурса _____

Дата _____ Место печати

Приложение № 3
к Конкурсной документации

НА ФИРМЕННОМ БЛАНКЕ УЧАСТНИКА

Кому: Конкурсной комиссии

_____

(указать предмет конкурса)

Дата: _____

ГАРАНТИЙНОЕ ПИСЬМО

Настоящим письмом подтверждаем, что компания

_____

(наименование компании)

- не находится в стадии реорганизации (разделения, слияния), ликвидации или банкротства, имущество компании не арестовано;
- не находится в состоянии судебного или арбитражного разбирательства;
- не имеет задолженности по налогам и сборам.

Подписи:

Ф.И.О. руководителя _____

Ф.И.О. главного бухгалтера _____

Ф.И.О. юриста _____

Место печати

Приложение № 4
к Конкурсной документации

НА ФИРМЕННОМ БЛАНКЕ ОРГАНИЗАЦИИ

ДОВЕРЕННОСТЬ №_____

г. _____ _____20__г.

ООО_____,
именуемое в дальнейшем «Организация», в лице _____,
действующего на основании _____, настоящей доверенностью уполномочивает представителя Организации – гражданина _____(паспорт серии__№____, выданный _____ от _____ года) на:
а) представление конкурсных документов;
б) проведение переговоров с заказчиком конкурса и рабочим органом;
в) присутствие на заседаниях конкурсной комиссии при вскрытии конвертов с конкурсным предложением;
г) предоставление разъяснений, касательно технической и ценовой части конкурсного предложения, а также других вопросов.

Настоящая доверенность вступает в силу с момента её подписания, выдана без права передоверия, сроком до _____г.

Ф.И.О. и подпись руководителя

Ф.И.О. и подпись лица, на имя которого выдана доверенность

Место печати (при наличии)

Приложение № 5
к Конкурсной документации

ПРОЕКТ ДОГОВОРА

Настоящий проект Договора является предварительным, его условия могут подлежать изменению по согласованию сторон в частях, не противоречащих действующему законодательству Республики Узбекистан.

Сублицензионный договор № _____
на поставку лицензии

г. Ташкент **«____»_____2021г.**

_____ именуемое в дальнейшем «**Лицензиат**», в лице _____, действующего на основании Устава, с одной стороны, и _____, именуемое в дальнейшем «**Сублицензиат**», в лице _____, действующий на основании _____, с другой стороны, совместно по тексту также именуемые «Стороны», а по отдельности «Сторона», заключили настоящее Лицензионный договор (далее «**Договор**») о нижеследующем:

1. ОПРЕДЕЛЕНИЯ

«**Программное обеспечение**» (или «**ПО**») – любые программы и их модификации в объекте коде, их обновленные версии и копии, включая все пакеты приложений, ассемблеры, компиляторы, такие как машинно-считываемая, объектно-кодированная версия загружаемых пользователем приложений и операционных программ.

«**Право использования**» (или «**Лицензия**») - неисключительное, ограниченное право на воспроизведение (установку и запуск Программного обеспечения на аппаратных средствах Сублицензиата в соответствии с лицензионными требованиями правообладателя) Программного обеспечения и его использование на условиях, установленных в настоящем Договоре

2. ПРЕДМЕТ ДОГОВОРА

2.1. Лицензиат обязуется предоставить Сублицензиату неисключительное, безотзывное и ограниченное право на использование (Лицензию) программного обеспечения, указанного в Спецификации в Приложении № 1 к настоящему Договору на территории Республики Узбекистан.

Лицензию на такое Программное обеспечение Лицензиат обязуется предоставлять на условиях, согласованных Сторонами в настоящем договоре, а Сублицензиат осуществит соответствующий лицензионный платеж в пользу Лицензиата за предоставление право (Лицензию) использования такого Программного обеспечения.

2.2. Настоящий Договор вступает в силу с даты его подписания Сторонами и действует до полного исполнения Сторонами своих обязательств.

3.ЦЕНЫ И ОБЩАЯ СУММА ДОГОВОРА

3.1. Общая сумма Договора составляет **0,00 (_____) сум с учетом НДС.**

3.2. Цена, указанная в Спецификации (Приложение № 1) представляет собой лицензионное вознаграждение за предоставление право использования (Лицензии) Программного обеспечения.

3.3. Лицензиат обязан заблаговременно (не менее чем за 5 (пять) рабочих дней), предупреждать Сублицензиата о прекращении выпуска правообладателем старых версий ПО и о начале выпуска новых версий ПО, равнозначных по цене и функциональности, Лицензии на которые Сублицензиат может приобрести у Лицензиата.

4.УСЛОВИЯ И ПОРЯДОК РАСЧЕТОВ

4.1. Сублицензиат производит предоплату в размере 50% (пятьдесят процентов) от общей суммы Договора, в течение 10 (десяти) банковских дней от даты подписания Договора. Оставшиеся 50% (пятьдесят процентов) от суммы настоящего Договора перечисляются не позднее 10 (десяти) банковских дней с даты подписания Сторонами Акта приема-передачи Лицензий.

4.2. Оплата производится в национальной валюте Республики Узбекистан, «СУМ».

Датой платежа и, соответственно, исполнения Сублицензиатом своих обязательств по оплате по настоящему Договору считается день поступления денежных средств на расчетный счет Лицензиата.

5. СРОКИ И УСЛОВИЯ ПЕРЕДАЧИ ЛИЦЕНЗИЙ

5.1. Дистрибутив ПО и Документацию к ПО Сублицензиат самостоятельно устанавливает с сайта Правообладателя, для чего Лицензиат передает Сублицензиату по электронным каналам передачи данных ссылки на электронный портал правообладателя.

5.2. Лицензии передаются по электронным каналам передачи данных или на электронных носителях.

5.3. При необходимости в срок не позднее 3-х (трех) рабочих дней до даты предоставления (передачи) Лицензий Лицензиат направляет Сублицензиату посредством электронных (e-mail) средств связи уведомление, содержащее информацию о номенклатуре, количестве и дате предстоящей передачи Лицензий в соответствии со Спецификацией.

5.4. Лицензиат обязуется произвести передачу Лицензий согласно Спецификации, в течение 30 (тридцати) рабочих дней со дня поступления предоплаты согласно пункту 4.1. настоящего Договора.

6. ПРОЦЕДУРА ПРИЕМКИ

6.1. Одновременно с передачей Лицензии Лицензиат обязан предоставить Сублицензиату передаточные документы (счет фактуру, акты выполнения работ и\или приема передачи и т.п.). Сублицензиат обязуется в течение 3 (трех) рабочих дней со дня получения передаточных документов подписать и оформить их, либо представить мотивированный отказ от их подписания.

6.2. Лицензии считаются предоставленными Сублицензиату в день подписания передаточных документов обеими Сторонами. В случае непредставления Сублицензиатом подписанных передаточных документов на Лицензии или мотивированного отказа от подписания в течение 3 (трех) рабочих дней, Лицензии считаются принятыми и подлежащими оплате Сублицензиатом.

7. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

7.1. Лицензиат гарантирует, что он обладает необходимыми правами и полномочиями (включая разрешение правообладателя ПО на передачу права использования Лицензии (ПО) по настоящему договору) для надлежащего исполнения своих обязательств по Договору. Лицензионный договор № _____ от _____ с правообладателем _____.

7.2. Гарантийное обслуживание предоставляется правообладателем ПО в соответствии со стандартными условиями производителя (правообладателя) ПО, изложенными на официальном сайте правообладателя ПО.

7.4. Настоящая гарантия действительна только при надлежащем использовании и обслуживании ПО Сублицензиатом в соответствии с условиями правообладателя.

8. ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

8.1.Все авторские, и иные права интеллектуальной собственности на ПО принадлежат и будут принадлежать правообладателям.

8.2.Ничто в настоящем Договоре не будет рассматриваться как нарушающее или затрагивающее права интеллектуальной собственности, принадлежащее одной из Сторон или разработанное и приобретенное за рамками настоящего Договора.

8.3. По условиям передаваемых Лицензий Сублицензиат получает неисключительные права на использование ПО, воспроизведение ПО, ограниченное правом инсталляции, копирования и запуска ПО;

8.4 Лицензиат несет полную имущественную ответственность за соблюдение авторских прав (в том числе исключительных имущественных прав на использование и пр.) при выполнении обязательств по настоящему Договору и гарантирует, что обладает всеми необходимыми правами и разрешениями от фирм производителей ПО и владельцев имущественных прав на ПО для выполнения своих обязательств по настоящему Договору и предоставит полную защиту и освободит Сублицензиата от любых претензий и исков, или проведении иных процессуальных действий против Сублицензиата если в ходе таких разбирательств заявлено, что передача Лицензий по настоящему Договору нарушает интеллектуальные права третьих лиц, а также незамедлительно возместит ему все убытки, которые могут быть предъявлены или причинены Сублицензиату, связанные с нарушением авторских, имущественных третьих лиц и вытекающие из выполнения Лицензиатом своих обязательств по настоящему Договору.

Лицензиат оплачивает Сублицензиату все убытки, которые он может понести в связи с окончательным решением, принятым судом соответствующей юрисдикции в связи с таким нарушением. При этом Лицензиат:

a) должен быть незамедлительно уведомлен Сублицензиатом в письменной форме обо всех претензиях и судебном преследовании в связи с таким нарушением, и получить полную возможность и право самостоятельно организовать защиту и урегулирование подобных споров

b) должен получить от Сублицензиата всю информацию и посильную помощь для организации такой защиты либо для урегулирования спорного вопроса.

8.5. Если принятое окончательное решение устанавливает факт нарушения Лицензиатом авторских прав при использовании ПО и распространение такого ПО запрещается, Лицензиат вправе, по своему усмотрению и за свой счет:

(i) обеспечить Сублицензиату право далее на законных основаниях использовать ту часть ПО, использование которой считается ущемлением прав третьих лиц, или

(ii) изменить такую часть ПО таким образом, что его использование не будет являться ущемлением прав, если только изменение этой части не делает ПО непригодным в целях, для которых оно предназначено; или

(iii) удалить такую часть и компенсировать Сублицензиату заплаченную им за эту часть цену в полном объеме, если только удаление этой части не делает ПО непригодным в целях, для которых оно предназначено;

(iv) компенсирует Сублицензиату заплаченную им цену за такие Лицензии.

9. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

9.1.Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему Договору, если это неисполнение явилось следствием обстоятельств непреодолимой силы, возникших после заключения Договора в результате обстоятельств чрезвычайного характера, которые Стороны не могли предвидеть или предотвратить. Под обстоятельствами непреодолимой силы понимаются: наводнение, пожар, землетрясение, эпидемия и другие явления природы, война или военные действия, а также решения органов государственной власти или управления и т.п.

9.2.При наступлении обстоятельств, указанных в п. 9.1 Договора, каждая из Сторон должна в течение 5 (пяти) рабочих дней известить о них в письменном виде другую Сторону. Сторона,

ссылающаяся на обстоятельства непреодолимой силы должна незамедлительно предоставить другой Стороне официальные документы, другие подтверждения, удостоверяющие наличие этих обстоятельств и, по возможности, дающие оценку их влияния на возможность исполнения Стороной своих обязательств по Договору.
9.3.Если Сторона, подвергшаяся воздействию обстоятельств непреодолимой силы, не направит в течение 5 (пяти) рабочих дней извещение, предусмотренное в п. 9.2 Договора, то такая Сторона лишается права ссылаться на такие обстоятельства как на основание освобождения ее от ответственности за неисполнение или ненадлежащее исполнение обязательств по Договору.
9.4.В случаях наступления обстоятельств, предусмотренных в п. 9.1. Договора, срок выполнения Стороной обязательств по Договору отодвигается соразмерно времени, в течение которого действуют эти обстоятельства и их последствия.
9.5.Если наступившие обстоятельства, перечисленные в п. 9.1. Договора, и их последствия продолжают действовать более 1 (одного) месяца, Стороны проводят дополнительные переговоры для выявления приемлемых альтернативных способов исполнения Договора.

10. ОТВЕТСТВЕННОСТЬ СТОРОН ПРИ ПРЕКРАЩЕНИИ ДЕЙСТВИЯ ДОГОВОРА

10.1. В случае если Лицензионный договор между Лицензиаром и Лицензиатом будет прекращен или расторгнут, и Лицензиат своевременно не сообщит Сублицензиату о данном факте, и Сублицензиат в связи с этим понесет какие-либо убытки, то Лицензиат будет нести ответственность и обязан выплатить Сублицензиату полную действительную стоимость понесенных Сублицензиатом убытков.
10.2. Стороны несут ответственность за неисполнение или ненадлежащее исполнение обязательств по настоящему Договору в порядке и на условиях, определенных настоящим Договором и предусмотренных законодательством Республики Узбекистан.
10.3. Сторона, нарушившая свои обязательства по настоящему Договору, обязуется незамедлительно известить об этом другую Сторону и сделать все от нее зависящее для устранения нарушения, а также возместить другой Стороне причиненные убытки.
10.4.В случае нарушения Лицензиатом срока предоставления (передачи) Лицензий по вине Лицензиата, Сублицензиат имеет право требовать от Лицензиата уплаты неустойки в виде пени в размере 0,1 % от цены Лицензии на Программное обеспечение за каждый день задержки его предоставления при этом общая сумма пени не может превышать 25% (двадцать пять процентов) от цены такой Лицензии.
10.5.В случае просрочки платежа Сублицензиатом, Лицензиат имеет право требовать от Сублицензиата уплаты неустойки в виде процентов в размере **0,1%** от суммы недоплаты за каждый день задержки, при этом общая сумма пени не может превышать 25% (пятнадцать процентов) от суммы задержанного платежа. Уплата пени не освобождает Стороны от исполнения своих обязательств по настоящему Договору.

11. ВСТУПЛЕНИЕ ДОГОВОРА В СИЛУ И СРОК ДЕЙСТВИЯ

11.1. Настоящий Договор между Лицензиатом и Сублицензиатом вступит в силу с даты его подписания уполномоченными представителями обеих Сторон.
11.2. Договор будет действовать до тех пор, пока Стороны не исполнят свои обязательства по настоящему Договору в полном объеме.
10.3. Расторжение Договора не прекращает действие предоставленной и оплаченной Лицензии.
10.4. Положения настоящего Договора, которые по своему смыслу или в определенном контексте должны быть действительны после прекращения настоящего Договора или окончания срока его действия, сохранят свою силу после такого окончания или прекращения.

12. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

12.1. Все споры, возникающие между Сторонами в связи с исполнением, изменением или прекращением настоящего Договора, должны быть урегулированы путем переговоров и предъявлением официальных претензий. Срок рассмотрения претензий 20 дней со дня

получения его стороной. Если возникшие споры не урегулированы мирным путем, то спор подлежит разрешению в Ташкентском межрайонном экономическом суде (для юридических лиц и физических лиц частных предпринимателей) либо в соответствующем гражданском суде (для физических лиц). Решение суда является окончательным и обязательным для обеих Сторон.

12.2. Настоящий Договор регулируется материальным и процессуальным правом Республики Узбекистан.

13. КОНФИДЕНЦИАЛЬНОСТЬ

13.1. Стороны обмениваются информацией, обоснованно необходимой каждой из сторон для выполнения своих обязательств по настоящему Договору. Вся письменная или устная информация, относящаяся к выполнению обязательств по настоящему Договору, предоставляемая одной стороной другой стороне, в отношении которой законами предусмотрен режим ограниченного доступа, либо информация, о которой сторона, передающая информацию, уведомила другую сторону явным образом, что такая информация является конфиденциальной, будет считаться и настоящим определяться как конфиденциальная информация ("Конфиденциальная информация"). К Конфиденциальной информации относятся, в том числе, персональные данные и сведения, составляющие коммерческую, профессиональную, служебную, а также иные виды тайн, определенные законодательством, бухгалтерские и финансовые данные, информация о проведении платежных операций, управляющая информация для настройки информационных, телекоммуникационных и платежных систем. Конфиденциальная Информация подлежит защите от несанкционированного доступа к ней, обеспечению её целостности, сохранности и своевременного предоставления.

13.2.Сторона, получающая Конфиденциальную информацию в соответствии с настоящим Договором ("Получающая сторона»") без предварительного получения письменного согласия стороны, предоставляющей такую информацию ("Передающая сторона"), не будет использовать какую-либо часть Конфиденциальной информации для целей, не предусмотренных настоящим Договором, предоставлять Конфиденциальную информацию или ее часть каким-либо лицам или организациям, не относящимся к работникам и консультантам Получающей стороны (а также к субподрядчикам), которым обоснованно необходимо иметь доступ к Конфиденциальной информации в целях, предусмотренных настоящим Договором, и которые соглашаются обеспечивать сохранность Конфиденциальной информации как в том случае, если бы они были стороной по настоящему Договору, не допускать неправомерного использования Конфиденциальной информации.

13.3. Получающая сторона не будет нести ответственность за разглашение Конфиденциальной информации или ее части, если она сможет доказать, что такая Конфиденциальная информация являлась всеобщим достоянием во время ее получения или стала таковой впоследствии не по вине Получающей стороны;

была известна Получающей стороне или находилась в ее распоряжении до ее получения;

стала известна Получающей стороне из источника, не являющегося Передающей стороной, при отсутствии нарушения обязательств по обеспечению сохранности Конфиденциальной информации.

13.4. Если Получающая сторона будет обязана по закону раскрыть какую-либо Конфиденциальную Информацию органам государственной власти, уполномоченным законодательством требовать раскрытия Конфиденциальной Информации, такая Сторона обязана немедленно письменно уведомить об этом факте Передающую сторону. При этом, в случае надлежащего уведомления Передающей стороны, Получающая сторона, раскрывающая Конфиденциальную Информацию в соответствии с настоящим пунктом, не считается нарушившей своего обязательства о неразглашении Конфиденциальной Информации. В случае такого раскрытия Получающая сторона обязуется сделать все от нее зависящее для того, чтобы обеспечить защиту Конфиденциальной Информации.

13.5. Конфиденциальная информация остается собственностью Передающей стороны, и по требованию последней после того, как она становится не нужна для целей, предусмотренных

настоящим Договором, подлежит немедленному возвращению такой стороне или уничтожается вместе со всеми копиями, сделанными Получающей стороной или какой-либо другой стороной, которой такая Конфиденциальная информация была предоставлена Получающей стороной, в соответствии с положениями настоящего раздела.

14. ПРОЧИЕ УСЛОВИЯ

14.1. Взаимоотношения сторон, прямо не урегулированные настоящим Договором, регламентируются действующим законодательством Республики Узбекистан.

14.2. Настоящий Договор заключен в письменной форме, в двух оригинальных экземплярах, тексты которых имеют одинаковую юридическую силу: один из которых находится у Сублицензиата, второй – у Лицензиата. Стороны договорились, что письменная форма Договора считается соблюденной при обмене подписанными уполномоченными представителями Сторон экземплярами Договора по электронной почте, факсу или посредством других средств связи. При этом каждая из Сторон обязуется предоставить оригинал подписанного Договора в течение 3 (трех) рабочих дней с даты его направления по электронной почте, факсу или посредством других средств связи.

14.4. Все соглашения, переговоры и переписка между Сторонами по вопросам, изложенным в настоящем Договоре, и имевшие место до его подписания, теряют силу с даты вступления Договора в силу.

14.5. Все изменения и дополнения к настоящему Договору являются неотъемлемой частью Договора и действительны лишь в том случае, если они совершены в письменной форме, имеют подписи уполномоченных лиц и печати Сторон.

14.6. Ни одна из Сторон не имеет право передать третьему лицу права и обязательства по настоящему Договору без письменного согласия другой Стороны.

14.7. Под уполномоченными представителями Сторон в целях настоящего Договора понимаются лица, действующие в интересах одной из Сторон на основании доверенности, уполномочивающей совершать определенные фактические и/или юридические действия в пользу доверителя. При этом уполномоченные представители обязаны предоставить доверенность при совершении каких-либо действий в пользу доверителя в рамках настоящего Договора.

15. АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

«ЛИЦЕНЗИАТ»	«СУБЛИЦЕНЗИАТ»
_____ _____ Тел: _____ Р/с _____ _____ МФО _____ ИНН _____ ОКЭД Код НДС: _____ _____ _____ М.П	_____ _____ Тел: _____ Р/с _____ _____ МФО _____ ИНН _____ ОКЭД Код НДС: _____ _____ _____ М.П

Приложение № 1

к Сублицензионному договору № _____ от «___» _____ 2021г.

Спецификация на лицензии

Производитель	Продукт	Кол-во	Цена за ед. без НДС	Общая сумма без НДС	НДС	Цена за ед. с НДС	Общая сумма с НДС
		200	0,00	0,00	0,00	0,00	0,00
	Итого:						**0,00**

Общая стоимость: **0,00**

«ЛИЦЕНЗИАТ»

_____

_____

_____

_____

М.П

«СУБЛИЦЕНЗИАТ»

_____

_____

_____

М.П