«ПОДТВЕРЖДАЮ»
АКБ «Банк развития бизнеса»
Заместитель председателя правления:
Б.Бобожонов

«20» август 2025 г.
№ 169

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
«Программное обеспечение для защиты информации»

Ташкент 2025г.

Приложение № _
к Тендерной документации

Т Е Х Н И Ч Е С К А Я С П Е Ц И Ф И К А Ц И Я

«Программное обеспечение для защиты информации»

1. Общие положения

1.1. Программное обеспечение для защиты информации (Далее – Система) должно обеспечивать контроль над процессом передачи конфиденциальной информации за пределы сегментов вычислительных сетей. Система должна поддерживать работу на уровне рабочих станций (Endpoint), на уровне сети (получение теневой копии трафика от сетевого оборудования либо прокси-сервера) и на уровне интеграций со сторонними системами (пр. технологий - SMTP, ICAP, API). Система должна предоставлять возможность работы в одном или нескольких перечисленных режимах одновременно.

1.2. Система должна быть построена на базе клиент-серверной архитектуры, где сервер выполняет роли администрирования, обработки, хранения и анализа данных, а клиент выполняет роль пользовательского интерфейса. Клиентская часть Системы, осуществляющая контроль процесса передачи конфиденциальной информации на уровне рабочих станций пользователей, должна быть представлена программным Агентом.

1.3. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства Windows: Windows 8, 8.1 x32/x64, Windows 10 x32/x64, Windows 11 x64, Windows
Server 2016, Windows Server 2019, Windows Server 2022.

1.4. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства Linux: Alt Linux 8 СП x64, 9 x64, 10 x64; CentOS 8 x64; RedOS 7.3 x64; Ubuntu 20.04 x64, 22.04 x64,
24.04 x64.

1.5. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства MacOS: Monterey 12.1, Ventura 13.3, Sonoma 14.0, Sequoia 15.0.

1.6. В связи с существенной разницей архитектур операционных систем Windows, Linux, MacOS допускается разница между функциями Агента, реализованными для ОС Windows, Linux и MacOS, а также между разными ядрами или версиями ОС Linux. Требования к функциям Агента для ОС Windows представлены в п. 5.3.1, требования к функциям Агента для ОС Linux представлены в п. 5.3.2, требования к функциям Агента для ОС MacOS представлены в п. 5.3.3.

1.7. Все серверные функции Системы должны выполняться в рамках единого решения, единой СУБД для архивирования данных и работать в рамках одной линейки ОС. Исключением служат сторонние сервисы, с которыми Система имеет возможность интеграции.

1.8. Система должна поддерживать работу в замкнутом контуре, то есть в локальной сети Заказчика без выхода в сеть Интернет. Исключением служат отдельные опциональные функции, выключенные по умолчанию и активируемые только по желанию Заказчика (такие как передача данных агентами через Интернет, подключение к облачным корпоративным сервисам и другие функции, в явном виде требующие интернет-соединения).

1.9. Все сетевые соединения, протоколы связи и направления соединений должны быть указаны в технической документации на Систему.

1.10. Система должна обеспечивать защиту данных, передаваемых агентскими или клиентскими компонентами по линиям связи.

2. Требования к поставке лицензионных программных средств

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

2.2. Исполнитель должен предоставить Заказчику лицензионные (сублицензионные) соглашения, подтверждающие права на обновление и поддержку (гарантийное сопровождение) программного обеспечения в течение 12 (двенадцати) месяцев.

2.3. Подсистемы контентного анализа и принятия решений должны лицензироваться за единицы (одна лицензия на каждую подсистему).

2.4. Модули подсистемы контроля должны иметь лицензирование по конечным пользователям: это значит, что одна лицензия требуется для одной подконтрольной (защищаемой Системой) доменной или локальной учетной записи. Исключением служит модуль аудита файлов, где лицензирование происходит по количеству рабочих станций (в случае использования Агента Системы на клиентских версиях (workstation) операционных систем) или по объему сканируемых данных (в случае сетевого сканирования или использования Агента на серверных версиях (server) операционных систем).

2.5. Лицензии модулей подсистемы контроля должны быть конкурентными. Это значит, что одну лицензию можно использовать для контроля разных пользователей (учетных записей) / рабочих станций только в разные периоды времени.

3. Программное обеспечение должно включать следующие модули и подсистемы:

№	Наименование
1.	Подсистема контроля, состоящая из:
1.1.	модуль контроля электронной почты
1.2.	модуль контроля сервисов обмена мгновенными сообщениями
1.3.	модуль контроля FTP-соединений
1.4.	модуль контроля HTTP-трафика (POST- и GET-запросы)
1.5.	модуль контроля печати
1.6.	модуль контроля и управления доступом съёмных устройств
1.7.	модуль контроля событий на мониторах и действий сотрудников
1.8.	модуль контроля разговоров сотрудников
1.9.	модуль контроля активности пользователей и приложений
1.10.	модуль контроля облачных хранилищ данных
1.11.	модуль аудита файлов
2.	Подсистема контентного анализа
3.	Подсистема принятия решений

3.1. Количество лицензий

№	Наименование лицензии	Количество, шт.
1.	Лицензия на программное обеспечение DLP	200 рабочих станций

Тип лицензирования – бессрочные лицензии.

Гарантийная поддержка разработчика/правообладателя на весь программный комплекс

– 1 календарный год с даты подписания акта передачи лицензий.

Также решение должно включать Модуль DLP для аудита файлов АРМ на 200 рабочих станций, а также Модуль DLP для аудита файлов на сервере на 10 ТБ сетевого хранилища файлов.Технические требования к Системе

3.2. Требования к Системе в целом

Система должна поддерживать контроль и защиту передачи конфиденциальной информации в рамках каналов, описанных в настоящем техническом задании, а также ее автоматизированный анализ в рамках технологий, указанных в настоящем техническом задании.

Система должна предполагать возможность выборочной активации модулей контроля для вышеперечисленных каналов передачи данных.

Система должна обеспечивать разграничение прав доступа к архиву информации, политикам безопасности и настройкам Системы.

Система должна иметь удобный и понятный пользовательский интерфейс, где все сообщения и документация должны быть на русском языке.

Система должна обеспечивать контроль веб-трафика на уровне рабочих станций, на уровне интеграций с прокси-серверами по протоколу ICAP и на уровне передачи теневой копии трафика (SPAN) с сетевых шлюзов.

Система должна обеспечивать контроль почтового трафика как на уровне рабочих станций, так и на уровне интеграции с корпоративным почтовым сервером.

Система должна обладать возможностью оптимизации нагрузки на ресурсы территориально разделенных сетей с «узким» каналом передачи данных благодаря предварительному сжатию информации, настройке расписания, маршрутов передачи и ограничения скорости передачи, а также за счет возможности задействовать промежуточные серверы обработки и временного хранения данных.

Система должна обеспечивать блокировку HTTP(S)-трафика на рабочих станциях согласно настраиваемым атрибутивно-зависимым правилам. Тематическая категория блокируемого HTTP(S) ресурса также должна являться атрибутом.

Система должна обеспечивать полноценный контроль пользователей, работающих на терминальных серверах ОС Windows для всех указанных в п.1.3 операционных систем.

Агент Системы, осуществляющий контроль на уровне рабочих станций с ОС Windows,

должен быть подписан цифровой подписью.

Подсистема контентного анализа должна предоставлять возможности:

- проведения ретроспективного анализа архива информации, учитывая возможность изменения правил проверки;
- генерации отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности;
- просмотра активности пользователей в режиме реального времени.

Подсистема принятия решений должна предоставлять возможности для автоматического вынесения вердикта по перехваченному объекту – нарушает или не нарушает он существующие правила.

Модуль контроля электронной почты должен обеспечивать контроль сообщений электронной почты (протоколы SMTP/ESMTP/SMTPS, POP3/POP3S, IMAP, MAPI), а также иметь подключаемую функцию автоматической остановки отправки сообщения в случае возникновения инцидента, зарегистрированного данным модулем на конечных станциях.

Модуль контроля сервисов обмена мгновенными сообщениями должен обеспечивать контроль сообщений и файлов, переданных при помощи популярных интернет-мессенджеров. В частности, обеспечивать контроль сеансов текстовой и голосовой связи, файлов и SMS- сообщений, контроль чатов, звонков и файлов коммуникационных клиентов Microsoft Lync, Viber Desktop, Telegram Desktop и Zoom

Chat.

Модуль контроля FTP-соединений должен обеспечивать контроль входящего и исходящего FTP-трафика. В случае контроля на уровне рабочих станций также необходима поддержка FTP через SSL (FTPS).

Модуль контроля HTTP-трафика должен обеспечивать контроль POST- и GET-запросов при использовании пользователями Заказчика интернет-сервисов, а также иметь подключаемую функцию автоматической остановки трафика в случае возникновения инцидента, зарегистрированного данным модулем.

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

Модуль контроля и управления доступом съемных устройств должен обеспечивать контроль файлов, записываемых на USB-устройства, CD-/DVD-матрицы и др. типы съемных устройств.

Модуль контроля событий на мониторах и действий сотрудников должен обеспечивать контроль изображений с экранов пользователей, предоставлять возможность осуществления видеозаписи действий, создания снимков и записи видео посредством веб-камеры, а также предоставлять возможность просмотра содержимого мониторов и действий пользователей за рабочей станцией в режиме реального времени. Модуль должен осуществлять контроль данных, вводимых с клавиатуры, логирование нажатий клавиш в любых приложениях (в том числе нажатия системных клавиш и их сочетаний). В целях обеспечения конфиденциальности, модуль, при наличии технической возможности, должен выделять ввод пароля и давать возможность исключить пароли из аудита. Техническая возможность и методика реализации в данном случае определяется Разработчиком Системы.

Модуль контроля разговоров сотрудников должен обеспечивать аудиозапись разговоров с помощью подключенного к рабочей станции микрофона. В целях обеспечения конфиденциальности третьей стороны важно, чтобы модуль позволял выбирать различные настройки своей работы для случаев, когда сотрудник находится в офисе и за его пределами.

Модуль контроля активности пользователей и приложений должен обеспечивать мониторинг активности пользователей и запускаемых ими процессов с учетом длительности в течение рабочего дня.

Модуль контроля облачных хранилищ данных должен предоставлять возможности для контроля входящих и исходящих данных облачных сервисов (Google Drive, OneDrive, Office 365, Dropbox, Evernote, Яндекс Диск, cloud.mail.ru и др.), а также позволять контролировать файлы, передаваемые в программах удаленного доступа (TeamViewer, RealVNC, Radmin, LiteManager).

Модуль аудита файлов должен обеспечивать аудит всех файловых операций, обеспечивать сканирование содержимого файлов в локальных и сетевых файловых системах в соответствии с настроенными правилами сканирования, производить индексацию файлов рабочей станции, производить аудит прав доступа к объектам файловой системы.

В Системе должны быть реализованы функции, обеспечивающие управление настройками конфигурации Системы и осуществляющие автоматизированный контроль штатного функционирования Системы. Под управлением понимается комплекс действий, позволяющих сотрудникам Заказчика изменять заданные настройки Системы самостоятельно, без привлечения сторонних специалистов. Под автоматизированным контролем штатного функционирования подразумевается мониторинг штатной работы всех компонентов Системы и автоматическое уведомление администратора в случае нештатных ситуаций.

3.3. Требования к способам и средствам связи для информационного обмена

Система должна функционировать в составе информационно-вычислительной сети Заказчика.

Модули контроля на уровне рабочей станции должны иметь возможность использования HTTPS для передачи данных на сервер Системы для защиты соединения и/или использовать альтернативные алгоритмы шифрования передаваемых данных.

Система должна корректно работать в сетях доменного типа.

Система должна поддерживать работу в виртуальной инфраструктуре. Перечень сред виртуализации, прикладного ПО и его версий, поддерживаемых Системой, должен передаваться Исполнителем в составе технической документации.

Для информационного обмена между компонентами Системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP и интерфейсы (Ethernet/ Fast Ethernet /Gigabit Ethernet) и\или беспроводные сетевые соединения.

Для информационного обмена между Системой и корпоративной почтовой системой должен использоваться протокол SMTP.

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

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

3.4. Требования к режимам функционирования Системы

Система должна обеспечивать возможность работы в следующих режимах:

- штатный режим (основной режим функционирования, предусматривающий автоматизированную работу Системы под управлением администратора, при которой обеспечивается непрерывное круглосуточное выполнение всех функций Системы);
- сервисный режим (используется для проведения обслуживания, реконфигурации и модернизации компонентов);
- автономный режим (используется в случае отсутствия связи между компонентами Системы или с внешними сетями, для доступа к конфигурационной и архивной информации).

3.5. Требования по диагностированию Системы

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

Каждый модуль Системы должен иметь штатный и расширенный режим записи в журналы. В случае программных сбоев должен быть предусмотрен отладочный режим принудительной записи в системные журналы. Отладочный режим включается автоматически без участия пользователя при наступлении программного сбоя.

В случае многопользовательской работы модуль должен автоматически создавать раздельные журналы для каждого пользователя.

3.6. Требования к численности и квалификации персонала Исполнителя

Для обеспечения поставки и ввода в эксплуатацию Системы в составе персонала Исполнителя должна присутствовать минимум одна штатная единица инженера технической поддержки.

Инженер технической поддержки должен обладать знаниями в объеме, необходимом для выполнения штатного технического и аварийного обслуживания Системы у Заказчика.

3.7. Перспективы развития и модернизации Системы

Система должна допускать наращивание производительности за счет улучшения характеристик технических средств.

Система должна обеспечивать возможность модернизации путем замены технического и/или программного обеспечения.

Исполнитель может привлекаться для консультаций Заказчика для согласования минимально достаточного или рекомендуемого оборудования при планировании внедрения Системы. Консультации должны носить формализованный вид и быть построены на базе типового анкетирования Заказчика.

3.8. Требования к характеристикам, при которых сохраняется целевое назначение Системы

Целевое назначение Системы должно сохраняться на протяжении всего срока эксплуатации Системы. Срок эксплуатации Системы определяется сроком устойчивой работы технических средств вычислительных комплексов, своевременным проведением работ по замене (обновлению) технических средств, по сопровождению и обновлению программного обеспечения Системы (в рамках гарантийного и послегарантийного обслуживания) и его модернизации.

Целевое назначение Системы должно сохраняться на протяжении всего срока эксплуатации Системы для заранее оговоренного ИТ-окружения. Поддержка новых версий системного или прикладного ПО, не оговоренных отдельно с Исполнителем и вышедших в будущем не может быть гарантирована.

3.9. Требования к функциям администрирования

Интерфейс администратора должен предоставлять возможность контроля работоспособности Системы.

Интерфейс администратора должен предоставлять возможность отображения статистики работы Агентов, серверных подсистем перехвата данных с рабочих станций, сервера индексации, служб контроля почтовой переписки (на уровне интеграции с корпоративным почтовым сервером), службы блокировки почты, СУБД MS SQL Server и PostgreSQL, служб распознавания графических изображений и аудиофайлов, операционной системы. Для всех указанных статистических данных должна быть реализована возможность обеспечения резервного копирования.

Интерфейс администратора должен обеспечивать возможность управления службами подсистем.

Интерфейс администратора должен предоставлять возможность управления базами данных модулей контроля информации.

Интерфейс администратора должен предоставлять возможность мониторинга дискового пространства на серверах Системы.

Интерфейс администратора должен предоставлять возможность автоматического оповещения о важных событиях (сбои в работе, нехватка свободного места, превышение количества лицензий и другие).

Интерфейс администратора должен обеспечивать возможность синхронизации с одним или более доменом Active Directory.

Интерфейс администратора должен обеспечивать возможность работы с пользователями рабочих групп.

Интерфейс администратора должен предоставлять возможность разграничения прав доступа сотрудников службы безопасности к функциям консолей подсистем и к данным по тем или иным пользователям, группам пользователей, и источникам данных. Под данными подразумеваются зафиксированные подсистемой принятия решений инциденты, а также доступное к просмотру в подсистеме контентного анализа содержимое документов и почтовых сообщений, попавших в карантин.

Интерфейс администратора должен предоставлять возможность указания настроек для подключения к базам данных (для случаев, когда они используются), которые можно впоследствии использовать по умолчанию.

Интерфейс администратора должен предоставлять возможность автоматического переноса «старых» баз данных, индексов, хранилищ на новое место хранения (с целью

разгрузки быстрых дисков), а также осуществление автоматического архивирования баз данных, индексов, хранилищ с последующей возможностью их восстановления.

3.10. Требования к хранению данных

Для эффективной работы с большими массивами данных Система, когда это технически возможно, должна хранить оригиналы теневых копий файлов в специальном файловом хранилище, адаптированном и оптимизированном для работы с Системой. Техническая возможность определяется Разработчиком Системы.

Система должна иметь опцию хранения текстовой и атрибутивной информации в специализированных индексах для ускорения поисковых выборок. В случае, когда информация содержится в индексе, любой поисковый запрос такой информации также должен сначала выполняться по индексу.

Система должна быть совместима с Microsoft SQL Server 2012 SP4 и выше, а также с PostgreSQL 14 и выше для хранения информации в структурированной табличной форме и дальнейшей ее обработки в сторонних системах анализа.

Система должна архивировать все перехваченные объекты, а не только те, по которым зафиксированы инциденты.

3.11. Требования к надежности

На всех серверах Системы должно быть предусмотрено наличие массива RAID.

Должен быть предусмотрен типовой регламент действий по восстановлению работоспособности в случае отказов Системы. Процедуры восстановления работоспособности Системы должны быть описаны и задокументированы в соответствующей эксплуатационной документации на Систему.

Система должна быть реализована таким образом и/или определен комплекс мер и мероприятий, обеспечивающих восстановление ее работоспособности и данных при сбоях силами штатного обслуживающего персонала.

В случае возникновения сбоя технического или программного обеспечения Системы должна быть обеспечена возможность восстановления ее данных и настроек.

4. Требования к функциям (задачам), выполняемым Системой

4.1. Требования к подсистеме контентного анализа

Подсистема контентного анализа должна быть ориентирована на работу с данными, получаемыми от модулей подсистемы контроля.

Подсистема должна предоставлять возможность выполнять ретроспективный анализ всех перехваченных или запротоколированных объектов, обозначенных в разделе 5.3. По объектам, для которых в Системе настроена индексация данных, должны поддерживаться следующие поисковые возможности:

- поиск, по ключевым словам, и фразам в базах перехваченных документов;
- выборка перехваченных данных по дате, доменному имени пользователя, адресам и хостам электронной почты, именам компьютеров, принтеров и др. атрибутам;
- поиск по образцу текста, схожему по смыслу или содержанию с искомым. Данный тип поиска не должен подразумевать никаких манипуляций с настройками поискового механизма и подключения дополнительных словарей, кроме задания процента релевантности (схожести) документов;
- поиск по набору слов (словарю), позволяющий находить документы, содержащие определенное количество либо процент таких слов. Набор слов может быть введен вручную, вставлен из буфера обмена либо загружен из внешнего текстового файла. При формировании каждого отдельного слова из словаря не должны использоваться логические операторы.

Анализ текстового содержимого должен производиться с учетом морфологических особенностей и синонимов русского языка. При этом словоформы

должны образовываться без использования логических операторов и специальных символов.

Подсистема должна предоставлять возможности для просмотра детальной информации по каждому перехваченному объекту, в том числе возможность просмотра записи действий на экранах пользователей во встроенном видеоплеере, а также соотношения видеозаписи с активностью приложений и нажатиями клавиш.

Подсистема должна предоставлять возможность просмотра контентного маршрута перехваченного документа.

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

Подсистема должна предоставлять возможность формирования и отображения

«Карточки пользователя», включающей в себя: общую информацию по выбранному пользователю (с возможностью добавления дополнительных полей), используемые им учетные записи из Active Directory, его контактные данные (e-mail адреса и других IM-клиентов), а также информацию по связям текущего пользователя за указанный период времени.

Подсистема должна предоставлять возможность просмотра информации по активности сотрудников в режиме реального времени с возможностью фильтрации по категориям активности пользователя.

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

Подсистема должна предоставлять возможность генерации отчетов по имеющимся базовым шаблонам (не менее 30 штук), а также предусматривать возможность добавления пользовательских шаблонов.

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

Подсистема должна производить сбор статистики и генерацию отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности.

Подсистема должна отображать информацию по активности пользователей в запускаемых ими приложениях в течение рабочего дня. При нарушениях сотрудниками установленного в компании трудового распорядка (поздний приход, ранний уход, недостаточная активность; длительная работа в приложениях, не связанных с рабочей деятельностью), должна быть предусмотрена возможность формирования оповещения по данному факту с последующей отправкой его на электронный адрес сотрудника службы информационной безопасности.

Подсистема должна генерировать краткие и детальные отчеты по продуктивности работы пользователей за выбранный период времени.

Подсистема должна генерировать отчеты по программам: количеству установок и удалений программ, установке/удалении агентов, перечню компьютеров с (не)установленными заданными программами и истории их изменений на компьютерах.

Подсистема должна генерировать отчеты по устройствам: перечень установленного оборудования на компьютерах пользователей и отчет по изменениям в устройствах (комплектующих) компьютеров.

Подсистема должна генерировать системные отчеты, отображающие:

- операции с агентами/протоколами, совершенные любым либо указанным пользователем;
- список компьютеров с нерабочими агентами;
- список компьютеров без агентов;
- информацию о количестве сообщений по выбранным компьютерам за

заданный промежуток времени.

Подсистема должна предоставлять возможность быстрого перехода к поиску и просмотру найденных документов.

Подсистема должна предоставлять возможность переходов по связанным отчетам.

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

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

Подсистема должна предусматривать возможность конвертации сгенерированных отчетов в PDF-файл, равно как и вывод их на печать.

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

4.2. Требования к подсистеме принятия решений

Подсистема должна использовать клиентскую консоль для управления политиками безопасности и инцидентами. Для консоли должно работать изолированное разграничение прав доступа.

Подсистема должна выносить единый вердикт (инцидент / не инцидент) для каждого перехваченного объекта.

Подсистема должна предоставлять возможности для ведения журнала инцидентов с возможностью рубрикации по каналам передачи данных, протоколам, пользователям, правилам проверки.

Подсистема должна предоставлять возможность уведомления ответственных лиц об инцидентах по электронной почте.

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

- формальных признаков перехваченного объекта (доменное имя, отправитель, получатель, хост, размер, расширение файла, канал передачи данных, протокол и т.д.);
- защищенных паролем архивов;
- результатов контентного анализа текста, извлеченного из перехваченных объектов (по словам и образцам текстов, тематическим словарям, путем сравнения с базой эталонных документов, путем поиска текстов, близких по смыслу или содержанию с эталоном, поиска алфавитно-цифровых объектов, а также поиска с использованием регулярных выражений).

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

Подсистема должна предусматривать возможность применения пользовательских шаблонов политик безопасности (правил проверки).

Подсистема должна предоставлять возможность выполнения ретроспективного контроля перехваченных документов с учетом обновленных правил проверки.

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

Подсистема должна предоставлять возможность задания для каждой группы политик безопасности индивидуальных настроек: перечня источников данных, по

которым будет проводиться опрос, расписания проверки, списка получателей оповещений об инцидентах, списка исключений.

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

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

Подсистема должна предоставлять возможность добавления пользователей и наделения их правами просмотра и редактирования тех или иных политик безопасности и списков исключений, в том числе возможность выставления запрета на данные действия.

Подсистема должна предоставлять возможности протоколирования выявленных инцидентов.

Подсистема должна поддерживать возможность категоризации инцидентов с помощью цветовых меток.

Подсистема должна поддержать возможность экспорта данных об инцидентах и событиях посредством syslog.

Подсистема должна предоставлять возможность подбора паролей для перехваченных архивов, защищенных паролем. База (словарь) для перебора паролей генерируется автоматически на базе данных модуля контроля данных, вводимых с клавиатуры.

Подсистема должна предоставлять возможности для принятия решений в отношении следующих типов объектов:

- сообщений, переданных по поддерживаемым Системой каналам и протоколам;
- файлов форматов: MS Office (doc, docx, dot, xls, xlsx, xlsb, xlsm, xlt, xltx, xltm, ppt, pptx, rtf, pot, vsd, vst, vsdx), Open Office (sxw, stw, odt, ods), HTML-файлы (htm, html, shtml, mht, css, js, maff), файлы почтовых сообщений (eml, msg), базы данных (mdb), дополнительные форматы документов (txt, xml, pdf, djvu, csv, lst, log, bat, ini, wri);
- распознанных и проанализированных текстов в графических файлах форматов bmp, jpg, jpeg, png, tif, tiff, gif;
- документов, вложенных в сжатые файлы: rar, zip, 7z, jar, tar, arj, gz, gzip, cab, iso, chm, hlp, 001.

Подсистема должна обеспечить наличие следующих возможностей обнаружения критичной информации:

- по ключевым словам, в том числе с возможностью ограничений по взаимному расположению искомых слов и с учетом морфологических особенностей и синонимии русского языка;
- возможность обнаружения похожих документов на основе образца, схожего по содержанию с искомым;
- по формальным признакам сообщений и файлов (доменный пользователь, имя компьютера, отправитель, получатель, размер, имя файла, формат и др.), в том числе для файлов, из которых не может быть извлечен текст;
- по заранее заданному словарю с целью выявления определенных типов документов (резюме, финансовые и бухгалтерские отчеты);
- возможность создания комплексных поисковых запросов, включающих в себя несколько критериев (фразовый поиск, поиск по абзацам и целым документам и атрибутам), объединенных логическими операторами AND, OR, NOT;
- по регулярным выражениям PCRE – поиск сложных алфавитно-цифровых объектов (номера паспортов, индивидуальные номера налогоплательщиков, номера кредитных карт, договоров или счетов, кодов классификаторов и т.п.), с возможностью создания комплексных регулярных выражений

(состоящих из нескольких простых), задания порога срабатывания по суммарному количеству регулярных выражений, количеству вхождений регулярного выражения в документ и количеству промежуточных символов между регулярными выражениями, возможностью использования как стандартных выражений, включенных в дистрибутив, так и создание пользовательских, а также с возможностью проверки полученных результатов;

- по цифровым отпечаткам конфиденциальных документов с возможностью указания порога срабатывания;
- по значениям атрибутов (как общих атрибутов, так и уникальных для отдельных каналов связи);
- по количественным показателям статистических запросов (числу отправленных писем/распечатанных страниц/сообщений в Lync, Viber, IM и пр.);
- возможность сузить результаты поиска путем дополнительного поискового запроса (фильтры по найденному).

Подсистема должна предусматривать наличие в дистрибутиве нескольких словарей.

Подсистема должна обеспечивать устойчивость к следующим видам манипуляции с информацией:

- импортирование фрагмента конфиденциальной информации в документы, не являющиеся конфиденциальными;
- изменение порядка слов;
- изменения расстояний между словами;
- изменение форматирования документа;
- изменение словоформ;
- замены букв на символы другого алфавита;
- использование цифр вместо букв;
- изменение расширений файлов.

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

4.3. Требования к подсистеме контроля

4.3.1. Общие требования к функциям Агента для ОС Windows

5.3.1.1. Требования к модулю контроля электронной почты

Модуль должен предоставлять возможности для контроля сообщений и вложений, передаваемых по протоколам SMTP, POP3, IMAP, MAPI, HTTP (веб-почта: как исходящая, так и входящая), при помощи почтовых клиентов или браузеров. Модуль должен иметь подключаемую функцию автоматической остановки исходящих почтовых сообщений по протоколам SMTP и HTTP, а также блокировки исходящих электронных сообщений, передаваемых с помощью почтового клиента Outlook по протоколам IMAP и MAPI, на основе контентного и/или контекстного анализа как почтовых сообщений, так и вложений.

Модуль должен предоставлять возможность блокировки исходящей почты по контентным и/или контекстным критериям.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.

5.3.1.2. Требования к модулю контроля сервисов обмена мгновенными сообщениями

Модуль должен обеспечивать контроль:

- входящих/исходящих сообщений и файлов, переданных пользователями по протоколам OSCAR (ICQ/QIP), XMPP (Jabber), MMP (Агент Mail.ru), и

др, на усмотрение Разработчика Системы;

- входящих и исходящих сообщений по протоколу HTTP в социальных сетях (Facebook, LinkedIn, ВКонтакте, Мой Мир@Mail.ru, Одноклассники.ru, Мамба.ru и прочее на усмотрение Разработчика Системы);
- чатов, файлов, переданных при помощи desktop-версий мессенджеров: Lync, Viber, Telegram, WhatsApp, Rocket.chat, Mattermost;
- чатов, файлов веб-версий мессенджеров: Telegram (web.telegram.org), WhatsApp (web.whatsapp.com), Rocket.chat, Mattermost, Teams, Bitrix24;
- чатов, звонков и файлов, переданных при помощи Zoom Chat, TrueConf Client, а также конференций Zoom;
- истории передачи файлов и чатов Instagram, LINE, Output Messenger;
- сообщений и файлов ресурса slack.com.

Модуль должен обеспечивать возможность блокировки передачи сообщений и файлов, соответствующих определенному контенту и/или контексту, передаваемых по протоколу HTTP в социальных сетях, посредством Slack, Zoom Chat, Telegram, а также возможность блокировки файлов, передаваемых посредством WhatsApp Desktop, WhatsApp Web и полной блокировки доступа к Telegram Web.

Модуль должен осуществлять контроль сеансов текстовой и голосовой связи (в том числе, звонки на телефонные номера и звуковые дорожки сеансов видеосвязи), файлов.

Модуль должен обеспечивать контроль входящих/исходящих сообщений, звонков и файлов коммуникационных программ-клиентов Microsoft Lync, Viber и Telegram.

Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN'ов отправителя и получателей, количества сообщений и др.

5.3.1.3. Требования к модулю контроля FTP-соединений

Модуль должен обеспечивать контроль документов, загруженных или переданных через
FTP-соединения, в том числе с применением SSL-шифрования.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др.

Модуль должен обеспечивать помещение перехваченных документов в специальное файловое хранилище.

5.3.1.4. Требования к модулю контроля HTTP-трафика

Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).

Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Internet Explorer; Mozilla Firefox; Opera; Google Chrome.

Модуль должен поддерживать контроль GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo.

Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB).

Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение.

Модуль должен обеспечивать контроль нажатий клавиш с фильтрацией по приложениям и браузерам в которых они набирались.

Модуль должен предусматривать возможность блокировки посещения запрещенных интернет-ресурсов по HTTP(S), создание «белых» и «черных» списков исключений, а также использование категорий сайтов для блокировки и/или разрешения посещения интернет- ресурсов, предусматривать возможность настройки выводимого оповещения при блокировке доступа к запрещенному интернет-ресурсу.

Модуль должен обеспечивать возможность блокировки передачи сообщений и файлов, соответствующих определенному контенту и/или контексту.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др.

5.3.1.5. Требования к модулю контроля печати

Модуль должен осуществлять контроль документов, отправленных на печать при помощи локальных и сетевых принтеров.

Модуль должен осуществлять контроль как графического представления, так и текстов отправленных на печать документов.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имен принтеров, количества распечатанных страниц и др.

Модуль должен поддерживать возможность исключения из контроля отдельных принтеров (в том числе по их описанию и месту расположения), пользователей, документов (по именам) и процессов.

Модуль должен обеспечивать возможность блокировки печати файлов, соответствующих определенному контенту и/или контексту.

Модуль должен позволять блокировку Escape-функций для PostScript/PCL принтеров, при активации которых контроль распечатанных документов невозможен.

5.3.1.6. Требования к модулю контроля съёмных устройств

Модуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (CD-/DVD-приводы, съемные накопители USB и FireWire, USB-устройства) и портам (USB, FireWire, COM, LPT, IRDA, SCSI и прочее на усмотрение Разработчика Системы).

Модуль должен поддерживать работу в терминальной сессии.

Модуль должен обеспечивать определение авторизованных групп пользователей устройств и портов.

Модуль должен предоставлять возможность теневого копирования данных, передаваемых на внешнее устройство.

Модуль должен обеспечивать возможность теневого копирования данных, хранящихся на подключаемом внешнем USB-устройстве.

Модуль должен предоставлять возможность теневого копирования данных, передаваемых через буфер обмена, в том числе буфер обмена RDP-сессии.

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

Модуль должен предусматривать следующие типы доступа пользователей к внешним устройствам: «запрет доступа», «полный доступ» и «только чтение».

Модуль должен предоставлять возможность блокировки записи на подключаемые внешние USB-устройства, исходя из формальных признаков файлов (имя файла, формат), а также по содержимому передаваемых данных.

Модуль должен предоставлять возможность запрета копирования данных, передаваемых через RDP-сессию.

Модуль должен позволять ограничение установки RDP-подключения как на удаленные рабочие станции или серверы, так и на рабочую станцию или сервер с

работающим модулем.

Модуль должен предоставлять возможность блокировки запуска определенных процессов на компьютере пользователя.

Модуль должен предоставлять возможность контроля буфера обмена на компьютере пользователя, а также блокировку передачи данных через буфер обмена по содержимому копируемых данных.

Модуль должен предоставлять возможность блокировки доступа пользователей к определенным локальным папкам и/или логическим дискам (за исключением системных).

Модуль должен предоставлять возможность использования «белых списков» устройств, к которым в дальнейшем пользователь будет иметь неограниченный доступ либо доступ «только чтение», а также «черных списков» устройств, доступ к которым будет заблокирован.

Модуль должен обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств и др.

5.3.1.7. Требования к модулю контроля событий на мониторах и действий сотрудников

Модуль должен обеспечивать снятие снимков экранов рабочих станций пользователей по заданному расписанию, в том числе в привязке к заданному интернет-узлу, процессу операционной системы рабочей станции и/или при вводе пользователем ключевых слов.

Модуль должен позволять скорректировать расписание снятия скриншотов при посещении определенных (настроенных заранее) интернет-узлов, звонке или активации видеоконференции, отсутствии активности от клавиатуры и мыши, нажатии клавиши «PrintScreen» или сочетания клавиш Win+Shift+S.

Модуль должен обеспечивать видеозапись происходящего на экранах мониторов согласно настроенному расписанию или событиям, в том числе в привязке к заданному интернет-узлу, процессу операционной системы рабочей станции и/или при вводе пользователем ключевых слов.

Модуль должен обеспечивать создание снимков, видеозаписи посредством подключенной к рабочей станции веб-камеры по заданному расписанию, в том числе в привязке к заданному процессу операционной системы рабочей станции, с возможностью использования нескольких веб-камер.

Модуль должен позволять скорректировать расписание создания снимков при посещении определенных (настроенных заранее) интернет-узлов, авторизации в операционной системе, отсутствии пользовательских сессий.

Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент снятия экрана и видеозаписи.

Модуль должен обеспечивать одновременный просмотр активности экрана одного или нескольких пользователей в режиме реального времени.

Модуль должен обеспечивать просмотр действий пользователей за рабочей станцией посредством веб-камеры.

Модуль должен предоставлять возможность экспорта перехваченных снимков экрана и видеозаписей в отдельную папку.

Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.

Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена.

Модуль должен обеспечивать возможность блокировки нажатий клавиши «PrintScreen».

Модуль должен выделять и позволять исключать из аудита набранные символы, если они являются вводом пароля для всех случаев, когда это технически возможно. Техническая возможность определяется Разработчиком Системы.

Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.

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

Модуль должен предоставлять возможность экспорта перехваченных нажатий клавиш в отдельную папку.

5.3.1.8. Требования к модулю контроля разговоров сотрудников

Модуль должен обеспечивать аудиозапись происходящих событий как внутри офиса, так и за его пределами, с помощью подключенного микрофона (в гарнитуре, ноутбуке, веб-камере и пр.), а также иметь возможность аудиозаписи с выхода звуковой карты.

Модуль должен предусматривать возможность активации записи голосов по расписанию, при запуске определенных процессов, внутри офиса/за его пределами (в командировке), при отсутствии авторизованных пользователей в операционной системе, автоматической активации микрофона при деактивации его пользователями в настройках ОС, а также возможность настройки качества записываемого звукового файла.

Модуль должен обеспечивать возможность прослушивания подключенного к рабочей станции микрофона в режиме реального времени.

Модуль должен обеспечивать помещение записанных звуковых файлов в базу данных либо использовать для хранения бинарных данных файловое хранилище.

Модуль должен предоставлять возможность экспорта перехваченных разговоров в отдельную папку.

5.3.1.9. Требования к модулю контроля активности пользователей и приложений

Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях или на сайтах.

Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.

Модуль должен иметь подключаемую возможность автоматической категоризации любых посещенных сайтов на тематические группы, используя заранее загруженную и регулярно пополняемую базу классификации сайтов.

5.3.1.10. Требования к модулю контроля облачных хранилищ данных

Модуль должен предоставлять возможности для контроля входящих и исходящих данных облачных сервисов Google Drive, Google Docs, OneDrive, SkyDrive, Office 365, DropBox, Evernote, Яндекс.Диск, Cloud.mail.ru, Amazon S3, iCloud, DropMeFiles, OwnCloud, Pcloud, OziBox, MediaFire, OpenDrive, 4shared, Box, Syncplicity, CloudMe, MiMedia, My-Files, Nextcloud, Seafile, SharePoint, Acronis File Advanced, Cloudian S3 storage, Disk Bitrix24, Диск-О и другие на усмотрение Разработчика Системы.

Модуль должен обеспечивать контроль файлов, передаваемых в программах удаленного доступа TeamViewer, RealVNC, Radmin, LiteManager и другие на усмотрение Разработчика Системы.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имени файла, IP-адресов и др.

Модуль должен обеспечивать возможность блокировки передачи в облачные хранилища посредством веб-браузера файлов, соответствующих определенному контенту и/или контексту, за исключением трафика вне спецификации HTTPS.

5.3.1.11. Требования к модулю аудита файлов

Требование аудита файлов в DLP: Система должна позволять выполнять аудит

операций с файлами и папками на рабочей станции, а также на сетевых папках. При этом должно отслеживаться следующие операции с файлами: создание, чтение, записать, удаление, переименование, открытие изменения прав доступа.

Система должны отслеживать следующие операции с папками: создание, удаление, переименование, открытие, изменение прав доступа.

4.3.2. Общие требования к функциям Агента для ОС Linux

Агент для ОС Linux должен осуществлять контроль данных, передаваемых посредством электронной почты, сервисов обмена мгновенными сообщениями, FTP-соединений, протокола HTTP, сервисов облачных хранилищ, контроль и управление доступом к данным на внешних устройствах, контроль печати данных, событий на мониторах и их действий, разговоров сотрудников и их активности в приложениях, а также контроль файлов, статически хранящихся на рабочих станциях сотрудников.

4.3.2.1. Требования к модулю контроля электронной почты

Модуль должен предоставлять возможности для контроля сообщений и вложений, передаваемых по протоколам SMTP, POP3, IMAP, MAPI, HTTP (веб-почта: как исходящая, так и входящая) при помощи любых почтовых клиентов или браузеров. Иметь подключаемую функцию автоматической остановки исходящих почтовых сообщений по протоколам SMTP, на основе контентного и/или контекстного анализа как почтовых сообщений, так и вложений.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.

4.3.2.2. Требования к модулю контроля сервисов обмена мгновенными сообщениями

Модуль должен обеспечивать контроль:

- входящих и исходящих сообщений по протоколу HTTP(S) в социальных сетях (Facebook, LinkedIn, ВКонтакте, Мой Мир@Mail.ru, Одноклассники.ru, Мамба.ru и прочее на усмотрение Разработчика Системы);
- чатов, звонков, исходящих файлов, переданных при помощи desktop-версии Telegram;
- чатов, исходящих файлов веб-версий мессенджеров: Bitrix24;
- чатов веб-версий мессенджеров: Telegram (web.telegram.org), WhatsApp (web.whatsapp.com).

Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN’ов отправителя и получателей, количества сообщений и др.

4.3.2.3. Требования к модулю контроля FTP-соединений

Модуль должен обеспечивать контроль документов, загруженных или переданных через FTP-соединение, в том числе с применением SSL-шифрования.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др.

4.3.2.4. Требования к модулю контроля HTTP-трафика

Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).

Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Mozilla Firefox; Opera; Google Chrome.

Модуль должен поддерживать контроль GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo.

Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB).

Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др.

4.3.2.5. Требования к модулю контроля печати

Модуль должен осуществлять контроль документов, отправленных на печать при помощи локальных и сетевых принтеров.

Модуль должен осуществлять контроль как графического представления, так и текстов отправленных на печать документов.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имен принтеров, количества распечатанных страниц и др.

Модуль должен поддерживать возможность исключения из контроля отдельных принтеров (в том числе по их описанию и месту расположения), пользователей.

4.3.2.6. Требования к модулю контроля и управления доступом съёмных устройств

Модуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (съемные накопители USB и сетевым адаптерам) и портам (COM, LPT).

Модуль должен поддерживать работу в терминальной сессии.

Модуль должен обеспечивать определение авторизованных групп пользователей устройств и портов.

Модуль должен обеспечивать возможность теневого копирования данных, записываемых на внешнее USB-устройство.

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

Модуль должен предусматривать следующие типы доступа пользователей к внешним устройствам: «запрет доступа», «полный доступ» и «только чтение».

Модуль должен обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств и др.

4.3.2.7. Требования к модулю контроля событий на мониторах и действий сотрудников

Модуль должен обеспечивать снятие снимков экранов рабочих станций пользователей по заданному расписанию, в том числе в привязке к заданному интернет-узлу, процессу операционной системы рабочей станции.

Модуль должен позволять скорректировать расписание снятия скриншотов при посещении определенных (настроенных заранее) интернет-узлов, запуске определенных (настроенных заранее) процессов, отсутствии активности от клавиатуры и мыши, нажатии клавиши «PrintScreen».

Модуль должен обеспечивать видеозапись происходящего на экранах мониторов.

Модуль должен позволять останавливать запись экрана при отсутствии активности от клавиатуры и мыши рабочей станции.

Модуль должен обеспечивать создание снимков посредством подключенной к рабочей станции веб-камеры по заданному расписанию, в том числе при входе пользователя в операционную систему, с возможностью использования нескольких веб-камер.

Модуль должен обеспечивать просмотр активности экрана пользователя в режиме реального времени.

Модуль должен обеспечивать просмотр действий пользователей за рабочей станцией посредством веб-камеры.

Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент создания снимка экрана.

Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.

Модуль должен обеспечивать контроль текстовой информации, помещенной пользователем в буфер обмена.

Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.

4.3.2.8. Требования к модулю контроля разговоров сотрудников

Модуль должен обеспечивать аудиозапись происходящих событий как внутри офиса, так и за его пределами, с помощью подключенного микрофона (в гарнитуре, ноутбуке, веб-камере и пр.).

Модуль должен обеспечивать возможность прослушивания подключенного к рабочей станции микрофона в режиме реального времени.

Модуль должен предусматривать возможность активации записи голосов по расписанию, внутри офиса/за его пределами (в командировке), а также возможность настройки качества записываемого звукового файла.

4.3.2.9. Требования к модулю контроля активности пользователей и приложений

Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях или на сайтах.

Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.

4.3.3. Общие требования к функциям Агента для ОС MacOS

Агент для ОС MacOS должен осуществлять контроль событий на мониторах и действий сотрудников, их активности в приложениях.

4.3.3.1. Требования к модулю контроля событий на мониторах и действий сотрудников

Модуль должен обеспечивать снятие снимков экранов рабочих станций пользователей по заданному расписанию, в том числе в привязке к заданному процессу операционной системы рабочей станции.

Модуль должен предусматривать возможность просмотра процессов (с разделением на фоновые и активные), которые выполнялись операционной системой компьютера на момент создания снимка экрана.

Модуль должен обеспечивать контроль нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.

Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов.

4.3.3.2. Требования к модулю контроля активности пользователей и приложений

Модуль должен обеспечивать контроль активности сотрудников в запускаемых

ими приложениях.

Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.

4.3.4. Требования к функциям контроля данных на уровне сетевого перехвата (при интеграции с прокси-сервером (по протоколу ICAP) либо сетевым оборудованием через зеркалирование трафика (SPAN))

4.3.4.1. Требования к модулю контроля электронной почты

Модуль должен предоставлять возможности для контроля сообщений и вложений, передаваемых по протоколам SMTP, POP3, IMAP, HTTP (веб-почта: как исходящая, так и входящая), при помощи почтовых клиентов или браузеров. При этом нешифрованный трафик HTTP доступен в как в режиме зеркалирования, так и в режиме интеграции с прокси-сервером. Нешифрованный SMTP, POP3 и IMAP трафик доступен только в режиме зеркалирования. Шифрованный HTTP(S) трафик доступен только в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.

4.3.4.2. Требования к модулю контроля сервисов обмена мгновенными сообщениями

Модуль должен обеспечивать контроль в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата:

- входящих и исходящих сообщений по протоколу HTTP (S) в социальных сетях (Facebook, LinkedIn, ВКонтакте, Мой Мир@Mail.ru, Одноклассники.ru, Мамба.ru и других, на усмотрение Разработчика Системы);
- чатов, файлов веб-версий мессенджеров: Telegram (web.telegram.org), WhatsApp (web.whatsapp.com), Rocket.chat, Mattermost;
- истории передачи файлов и чатов Instagram, VK Teams;
- сообщений и файлов ресурса slack.com.

Модуль должен обеспечивать возможность блокировки передачи сообщений и файлов, передаваемых по протоколу HTTP в социальных сетях и веб-мессенджерами (Rocket.chat, Mattermost и др.), соответствующих определенному контексту.

Модуль должен обеспечивать контроль трафика сервисов обмена мгновенными сообщениями, переданного с применением пользователем HTTP-туннелирования.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, UIN’ов отправителя и получателей, количества сообщений и др.

4.3.4.3. Требования к модулю контроля FTP-соединений

Модуль должен обеспечивать контроль документов, загруженных или переданных через FTP-соединения, в том числе с применением SSL-шифрования в режиме интеграции с прокси- сервером, на котором выполняется подмена сертификата

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, целевых URL-адресов, имен пользователей FTP-серверов и др.

Модуль должен обеспечивать помещение перехваченных документов в специальное файловое хранилище.

4.3.4.4. Требования к модулю контроля HTTP-трафика

Контроль защищенного HTTPS трафика может быть доступен только в режиме интеграции с прокси-сервером, на котором выполняется подмена сертификата.

Контроль незащищенного HTTP трафика может быть доступен как режиме

интеграции с прокси-сервером, так и в режиме зеркалирования трафика.

Модуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).

Модуль должен поддерживать фильтрацию запросов, генерируемых современными браузерами, в том числе Internet Explorer; Mozilla Firefox; Opera; Google Chrome.

Модуль должен поддерживать контроль GET-запросов, отправленных пользователями в популярные поисковые системы, в том числе Google, Яндекс, Рамблер, Yahoo.

Модуль должен поддерживать фильтрацию запросов, генерируемых популярными службами блогов, веб-чатов и популярными форумными движками (vBulletin, Invision Power Board, phpBB).

Модуль должен предусматривать возможность поисковой выдачи только тех перехваченных POST-запросов, набор символов которых несет смысловое значение.

Модуль должен предусматривать возможность блокировки посещения запрещенных интернет-ресурсов по HTTP(S), создание «белых» и «черных» списков исключений, а также использование категорий сайтов для блокировки и/или разрешения посещения интернет- ресурсов, предусматривать возможность настройки выводимого оповещения при блокировке доступа к запрещенному интернет-ресурсу.

Модуль должен обеспечивать возможность блокировки передачи запросов, соответствующих определенному контексту.

Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, тела запроса, имени хоста и др.

5. Прочие требования ко всему программному обеспечению

5.1. Требования к услугам по установке и настройке

Поставщик должен выполнить установку каждой составной части приобретенного решения в течение до тридцати (30) дней после поставки. Услуги выполняются на условиях
«под ключ».

5.2. Требования к лицензированию программного обеспечения

Все лицензии должны быть выданы на бессрочное использование, то есть по истечении
36 (тридцати шести) месяцев обновления и гарантии продукты будут продолжать
использоваться контрагентом, независимо от того, приобретаются ли пакеты обновлений и техническая поддержка для последующего использования.

Участник конкурса должен представить доказательство, выданное производителем каждого предлагаемого компонента программного обеспечения, информирующее о том, что поставщик может и уполномочен продавать продукты и услуги на территории Республики Узбекистан.

Программно-техническиесредства защиты информации, используемые в системе обеспечения информационной безопасности, должны быть лицензированными и сертифицированными. (Пункт 18 Положения №3224 от 10 марта 2020 года «О защите информации в автоматизированных банковских системах коммерческих банков Республики Узбекистан».)

Участник конкурса должен представить сертификат выданный программному обеспечению, выполняющему функции DLP и файлового аудита, со стороны организации
«Центр Кибербезопасности» Узбекистана, согласно требованиям нормативной документации
O’z DSt 2816:2014 п. 5.3 (3 уровень отсутствия НВД) и O’z DSt 2814:2014 п.9.1, п.9.2, п.9.4.

Участник конкурса должен предоставить подтверждение об освобождении от налога на доходы нерезидента в соответствии с законодательством Республики Узбекистан:

- Участник должен подтвердить, что является резидентом *указать страну резидентства*, как компания, зарегистрированная в *указать страну резидентства*, и юридическим лицом *указать страну резидентства*, имеющим право на льготы по Соглашению между *указать страну резидентства* и Правительством Республики Узбекистан об избежание двойного налогообложения в отношении налогов на доходы, ратифицированному *указать дату и номер межправительственного соглашения*.
- Участник конкурса в составе пакета квалификационных документов должен предоставить сертификаты, оформленные должным образом, подтверждающие, что он является налоговым резидентом *указать страну резидентства*.
- Участник конкурса в составе пакета квалификационных документов должен предоставить сертификаты, оформленные должным образом, подтверждающие, что правообладатель предлагаемых программных продуктов является налоговым резидентом *указать страну резидентства*.
- Освобождение от уплаты налога на доходы (прибыль) нерезидента в применимых в соответствии с законодательством РУз производится на основании следующих документов:
  - справка (сертификат) о резидентстве участника конкурса в одном экземпляре;
  - справка (сертификат) о резидентстве правообладателя предлагаемых программных продуктов в одном экземпляре.
- В случае непредоставления Исполнителем вышеуказанных Справок о резидентстве, Заказчик производит оплату по настоящему договору с удержанием налога на доходы нерезидентов в размере 20% по тому программному продукту, на который не был предоставлен соответствующий Сертификат резидентства правообладателя и Сертификат резидентства участника конкурса.

5.3. Дополнительные требования

В состав предложения участника конкурса должно быть включено авторизованное обучение по всем программным продуктам– 2 сотрудника.

Внедрение всех систем на условиях «под ключ» и поддержка в течение срока действия гарантии.

Техническая поддержка правообладателя/производителя на все программное обеспечение, предлагаемое в рамках текущего конкурса – 1 год.