Дата: «12» августа 2026г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На проведение анализа рынка с целью приобретения 70 лицензий системы предотвращения утечек информации (DLP)

Наименование:

«Приобретение 70 лицензий системы предотвращения утечек информации (DLP)»

Заказчик: АО «Национальный Межбанковский Процессинговый Центр» (НМПЦ)

Контактное лицо: Тоиров А. (Главный специалист отдела по закупкам, +998781132407 / 7733, tender@nmpc.uz)

Согласовано:

Заместитель председателя правления
по ИТ и технологической инфраструктуре _____ Самигуллин Д.Р.

Директор департамента
информационной безопасности _____ Гафуров А.А.

Начальник отдела архитектурных решений _____ Володикова Е.О.

Разработал:

Заместитель директора Департамента
информационной безопасности _____ Содиков А.А.

Техническое задание на проведение анализа рынка

Наименование проекта: Приобретение 70 лицензий системы предотвращения утечек информации (DLP)

1. Оглавление

2. Общие сведения

2.1. Наименование системы

Система предотвращения утечек информации (Data Loss Prevention, DLP) с приобретением 70 пользовательских лицензи

2.2. Основания для проведения работ

1. Увеличение количества рабочих станций под управлением macOS активных агентов DLP
2. Необходимость обеспечения единых политик информационной безопасности на Windows и macOS.
3. Контроль обработки конфиденциальной информации независимо от используемой операционной системы.
4. Выполнение требований внутренних нормативных документов по предотвращению утечек информации.

3. Общие положения

3.1. 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.

3.2. 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. Часть Системы, осуществляющая контроль процесса передачи конфиденциальной информации на уровне рабочих станций пользователей, должна быть представлена программным Агентом.

3.3. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства Windows (версии x64): Windows 8, 8.1, Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022.

3.4. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства Linux (версии x64): Альт Рабочая станция 10, 11; Astra Linux Special Edition 1.7 Special Edition 1.8; RedOS 7.3.2, 8; Ubuntu 22.04, 24.04; Debian 12.11, 12.12.

3.5. Агенты Системы должны поддерживать работу, как минимум, на следующих ОС семейства MacOS: Sonoma 14.0, Sequoia 15.0, Tahoe 26.0.

3.6. В связи с существенной разницей архитектур операционных систем Windows, Linux, MacOS допускается разница между функциями Агента, реализованными для ОС Windows, Linux и MacOS. Требования к функциям Агента для каждого семейства ОС представлены в соответствующих разделах настоящего Технического задания.

3.7. Все серверные функции Системы должны выполняться в рамках единого решения, единой СУБД для архивирования данных. Исключением служат сторонние сервисы, с которыми Система имеет возможность интеграции.

3.8. 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).

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

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

4. Требования к поставке лицензионных программных средств

4.1. 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.

4.2. Поставщик должен предоставить Заказчику бессрочную лицензию на использование программного обеспечения (без ограничения срока действия). Право на получение обновлений и техническую поддержку (гарантийное сопровождение) программного обеспечения предоставляется на срок 12 (двенадцать) месяцев с момента поставки.

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

4.4. Подсистема контроля должна иметь лицензирование по конечным пользователям: это значит, что одна лицензия требуется для одной подконтрольной (защищаемой Системой) доменной или локальной учетной записи.

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

5. Программное обеспечение должно включать следующие модули и подсистемы:

№ п/п	Наименование	Количество
1.	**Подсистема контроля, состоящая из:**	-
1.1.	модуль контроля электронной почты	70
1.2.	модуль контроля сервисов обмена мгновенными сообщениями	70
1.3.	модуль контроля FTP-соединений	70
1.4.	модуль контроля HTTP-трафика (POST- и GET-запросы)	70
1.5.	модуль контроля печати	70
1.6.	модуль контроля и управления доступом съёмных устройств	70
1.7.	модуль контроля событий на мониторах и действий сотрудников	70
1.8.	модуль контроля разговоров сотрудников	70
1.9.	модуль контроля активности пользователей и приложений	70
1.10.	модуль контроля облачных хранилищ данных	70
2.	**Подсистема контентного анализа**	**1**
3.	**Подсистема принятия решений**	**1**

6. Технические требования к Системе

6.1. 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 предусматривать возможность использования двухфакторной аутентификации пользователей при доступе к пользовательскому интерфейсу Системы.

Пользователь Системы должен иметь выбор между «толстым» клиентом и веб-интерфейсом при работе с функциями и данными Системы, при этом разграничение доступа должно быть централизованным и индивидуальным как при работе в «толстом» клиенте, так и в веб-интерфейсе.

Допускается различие в интерфейсах и возможностях «толстого» клиента и веб-интерфейса, однако пользователь Системы должен иметь возможность использования описанного в настоящем Техническом задании функционала с использованием одной из консолей.

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.3.3 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.

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.

6.2. 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 как в сетях доменного типа, так и в одноранговых сетях (рабочих группах).

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).

6.3. 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).

6.4. 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.

6.5. 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.

6.6. 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 ра-

бот 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.

6.7. 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 позволять создание внутренних учетных записей Системы (без привязки к учетным записям Active Directory или рабочих групп). Для учетных записей должна быть предусмотрена возможность настройки надежности (сложности) используемых паролей по следующим параметрам:

- Использование букв и цифр;
- Использование букв разного регистра;
- Использование спецсимволов;
- Минимальная длина пароля.

Система должна обеспечивать защиту от перебора паролей внутренних учетных записей путем временной (не менее 1 минуты) или постоянной блокировки учетной записи после 3-х неудачных попыток ввода пароля.

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 обеспечивать возможность управления настройками функций сбора статистики и предоставления отчетов, настройками модуля принятия решения, служб распознавания графических изображений и аудиофайлов, а также обеспечивать возможность настройки просмотра отчетов посредством веб-интерфейса.

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.

Интерфейс администратора должен позволять задать расположение с дистрибутивами обновлений компонентов Системы для последующего автоматического обновления компонентов на локальных и удаленных серверах Системы.

6.8. 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.

Для снижения нагрузки на системы хранения данных, в рамках конкретных модулей подсистемы контроля, должны быть предусмотрены механизмы фильтрации контролируемых данных (по пользователю, компьютеру и т.д.), а также возможность отключения сохранения теневых копий перехватываемых данных модулями контроля (где это технически возможно реализовать).

6.9. Требования к надежности

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.

7. Требования к функциям (задачам), выполняемым Системой

7.1. 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 7.3. 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, учетные записи 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.

Подсистема должна отображать на карте мира расположение пользователей (ПК пользователей с установленным Агентом Подсистемы контроля), а также историю их перемещения с точностью до города.

Подсистема должна предоставлять возможность генерации отчетов по имеющимся базовым шаблонам, предусматривать возможность настройки формирования и отображения отчетов пользователем Системы.

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 активными/неактивными 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 файл (XLSX, HTML, TXT, XML, PDF форматы: по выбору пользователя Системы), вывод их на печать, отправку по расписанию на заданный адрес электронной почты или сохранение в указанную сетевую папку.

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.

7.2. Требования к подсистеме принятия решений

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 правил проверки.

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

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

Подсистема должна предоставлять возможность задания для каждой политики 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 разграничения прав доступа пользователей Системы к используемым политикам безопасности: наделения их правами просмотра и редактирования тех или иных политик безопасности, в том числе возможность выставления запрета на данные действия.

Подсистема должна предоставлять возможности протоколирования выявленных инцидентов.

Подсистема должна поддерживать возможность категоризации инцидентов и/или документов в рамках данных инцидентов с помощью цветовых меток.

Подсистема должна поддержать возможность экспорта данных об инцидентах и событиях посредством syslog протокола или через выгрузку событий в файл формата .CEF. Подсистема должна предоставлять пользователю выбор экспортируемых инцидентов: всех; отмеченных инцидентов; инцидентов, содержащих отмеченные документы.

Подсистема должна предоставлять возможность подбора паролей для перехваченных архивов, защищенных паролем. Словарь для перебора паролей должен поддерживать:

- ручной ввод вариантов паролей;
- загрузку перечня паролей из текстового файла;
- автоматически сгенерированную базу паролей, полученную от 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 Microsoft Teams (Lync), Viber, IM и пр.);
- возможность сузить результаты поиска путем дополнительного поискового запроса (фильтры по найденному);
- по тексту предварительно распознанных изображений с использованием технологии OCR, при этом в Системе должен быть предусмотрен выбор между коммерческим (приобретается отдельно) и бесплатным модулем OCR;
- по тексту предварительно распознанных записей микрофона, а также записей звонков в мессенджерах и системах конференцсвязи.

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.

7.3. Требования к подсистеме контроля

7.3.1. Общие требования к функциям Агента для ОС Windows

Агент Системы должен осуществлять аудит технических данных рабочих станций, на которых он установлен, а именно:

- перечень установленного ПО;
- аппаратная конфигурация;
- активный пользователь;
- статус агента;
- свободное место на диске;
- последняя активность агента.

Агент должен передавать на сервер Системы информацию о географических координатах рабочей станции с Агентом. Определение нахождения рабочей станции с Агентом должно осуществляться как в локальной сети компании, так и вне её.

Агент должен иметь возможность работы в двух режимах: скрытом (Агент скрывает своё присутствие в операционной системе) и открытом (Агент отображает собственный интерфейс в операционной системе для взаимодействия с пользователем).

Интерфейс Агента должен позволять:

- отображение уведомлений пользователя о заблокированных действиях;
- отправку запросов администратору Системы на получение доступа к заблокированным устройствам;
- просматривать статистику рабочего времени пользователя;
- блокировать сессии пользователей на выбранной рабочей станции или сервере.

7.3.1.1 Требования к модулю контроля электронной почты (ОС Windows)

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

7.3.1.2 Требования к модулю контроля сервисов обмена мгновенными сообщениями (ОС Windows)

Модуль должен обеспечивать контроль:

- входящих/исходящих сообщений и файлов, переданных пользователями по протоколам OSCAR, XMPP (Jabber) и др., на усмотрение Разработчика Системы;

- входящих и исходящих сообщений по протоколу HTTP в социальных сетях (Facebook[1], LinkedIn, ВКонтакте, Мой Мир@Mail.ru, Одноклассники.ru, Мамба.ru и прочее на усмотрение Разработчика Системы);
- чатов, файлов, переданных при помощи desktop-версий мессенджеров: Microsoft Teams (Lync), Viber, Telegram, WhatsApp, Rocket.chat, Mattermost, Squadus, TrueConf, Zoom, Line, Signal, Dion, Yandex Telemost, Контур Толк, Iva Connect;
- чатов, файлов, переданных при помощи Metro-версий мессенджеров: WhatsApp, Microsoft Teams (Lync);
- чатов, файлов веб-версий: Telegram (web.telegram.org), WhatsApp (web.whatsapp.com), Rocket.chat, Mattermost, Microsoft Teams (Lync), Bitrix24, Yandex Telemost, Iva Connect, Matrix;
- звонков в приложениях Zoom, TrueConf, Viber, Signal, Discord, Microsoft Teams (Lync), Telegram, WhatsApp;
- видеосообщений, переданных через Telegram Desktop;
- чатов и файлов, переданных в RedHelper;
- истории передачи файлов и чатов Instagram[2], 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 посредством приложений Slack, Zoom, Telegram, Microsoft Teams (Lync), TrueConf, Line, Viber, Signal, WhatsApp;
- доступа к Telegram Web;
- звонков в приложениях Viber, Signal, Zoom, WhatsApp, Microsoft Teams (Lync).

Блокировки должны предусматривать в качестве одного из критериев наличие на файле метки конфиденциальности модуля аудита файлов (функция может быть доступна при наличии установленного модуля аудита файлов).

Правила блокировки должны предусматривать возможность использования OCR для анализа содержимого передаваемых файлов. При использовании технологии OCR должна быть реализована возможность указания максимального временного периода, по истечении которого обработка графического файла прекращается.

С целью отладки создаваемых правил блокировки должен быть предусмотрен проверочный режим работы создаваемого правила. В данном режиме должен выполняться аудит передаваемых данных, без фактической блокировки.

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.

7.3.1.3 Требования к модулю контроля FTP-соединений (ОС Windows)

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

Модуль должен обеспечивать возможность блокировки передачи файлов, соответствующих определенному контенту и/или контексту, на заданные администратором FTP-серверы.

Правила блокировки должны предусматривать возможность использования OCR для анализа содержимого передаваемых файлов.

С целью отладки создаваемых контентных правил блокировки должен быть предусмотрен проверочный режим работы создаваемого правила. В данном режиме должен выполняться аудит передаваемых данных, без фактической блокировки.

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.

7.3.1.4 Требования к модулю контроля HTTP-трафика (ОС Windows)

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 вычитку сохраненных в браузерах авторизационных данных пользователей к интернет-ресурсам, а также позволять осуществление подбора мастер-пароля в случаях, если данные защищены.

Модуль должен предусматривать возможность блокировки посещения запрещенных интернет-ресурсов по протоколу HTTP(S) (конкретных адресов; адресов, указанных в виде регулярного выражения; указанных категорий сайтов), предусматривать возможность настройки выводимого оповещения при блокировке доступа к запрещенному интернет-ресурсу, а также возможность применения правил блокировки в зависимости от местонахождения рабочей станции (в корпоративной сети или за ее пределами).

Модуль должен обеспечивать возможность блокировки передачи сообщений и файлов, соответствующих определенному контенту и/или контексту. Блокировки должны предусматривать в качестве одного из критериев наличие на файле метки конфиденциальности модуля аудита файлов (функция может быть доступна при наличии установленного модуля аудита файлов).

Правила блокировки должны предусматривать возможность использования OCR для анализа содержимого передаваемых файлов.

С целью отладки создаваемых контентных правил блокировки должен быть предусмотрен проверочный режим работы создаваемого правила. В данном режиме должен выполняться аудит передаваемых HTTP-запросов, без фактической блокировки.

Модуль должен обеспечивать возможность блокировки расширений (всех или указанных администратором) актуальных версий браузеров Chrome, Edge, Firefox, Opera, Yandex, Chronium-gost.

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

7.3.1.5 Требования к модулю контроля печати (ОС Windows)

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 поддерживать контроль печати из виртуальных приложений App-V.

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 иметь возможность сохранения теневой копии оригинала документа, отправленного на печать.

Модуль должен обеспечивать возможность ограничения количества страниц документа выводимого на печать, или блокировки печати файлов, соответствующих определенному контенту и/или контексту, в т.ч. предусматривать в качестве одного из критериев наличие на файле метки конфиденциальности модуля аудита файлов (функция может быть доступна при наличии установленного модуля аудита файлов).

Правила блокировки должны предусматривать возможность использования OCR для анализа содержимого файлов, отправленных на печать.

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

7.3.1.6 Требования к модулю контроля съёмных устройств (ОС Windows)

Модуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (CD-/DVD-приводы, съемные накопители USB и FireWire, USB-устройства, Wi-Fi и Bluetooth) 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 контроля и теневого копирования данных, передаваемых через буфер обмена, а также блокировку передачи данных через буфер обмена по содержимому копируемых данных, в том числе через буфер обмена RDP-сессии. При этом должна быть возможность настройки раздельного запрета при отправке данных буфера обмена на сервер RDP и при получении данных буфера обмена с сервера RDP.

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 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. Блокировки должны предусматривать в качестве одного из критериев наличие на файле метки конфиденциальности модуля

аудита файлов (функция может быть доступна при наличии установленного модуля аудита файлов).

Правила блокировки должны предусматривать возможность использования OCR для анализа содержимого записываемых на USB-накопитель файлов.

Модуль должен предоставлять возможность блокировки запуска определенных процессов на компьютере пользователя с учетом местонахождения рабочей станции (в корпоративной сети или за ее пределами).

Модуль должен предоставлять возможность теневого копирования передаваемых файлов по каналу Bluetooth, а также блокировки выбранных Bluetooth-устройств и/или сервисов.

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

Модуль должен предоставлять возможность контроля и блокировки доступа пользователей к определенным сетевым папкам. Модуль должен позволять администратору Системы выбор операций с файлами в сетевой папке для записи событий аудита. Модуль должен позволять сохранять теневые копии записываемых в сетевую папку файлов.

Модуль должен предоставлять возможность блокировки передачи файлов в заданные администратором Системы приложения (процессы) с использованием технологии drag-and-drop (перетаскивание файлов с использованием манипулятора «мышь»).

Модуль должен предоставлять возможность создания «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 предоставлять возможность импорта списка USB-накопителей и переносных устройств из R-Vision.

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

7.3.1.7 Требования к модулю контроля событий на мониторах и действий сотрудников (ОС Windows)

Модуль должен обеспечивать создание снимков/видеозаписей экранов рабочих станций пользователей по заданному расписанию.

Модуль должен позволять скорректировать расписание снятия скриншотов при посещении определенных (настроенных заранее) интернет-узлов, запуске заданных процессов операционной системы рабочей станции, вводе пользователем определенных ключевых слов, звонке или активации видеоконференции Microsoft Lync, отсутствии активности от клавиатуры и мыши, нажатии клавиши «PrintScreen» или сочетания клавиш Win+Shift+S.

Модуль должен позволять скорректировать расписание видеозаписи экрана при посещении определенных (настроенных заранее) интернет-узлов, запуске заданных процессов операционной системы рабочей станции, вводе пользователем определенных ключевых слов.

При наличии нескольких подключенных к рабочей станции мониторов, модуль должен предоставлять возможности:

- создания снимков/видеозаписей только для основного экрана;
- объединения снимков/видеозаписей с нескольких экранов в один файл.

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 регистрации 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 в режиме реального времени.

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 добавления перманентных водяных знаков на изображения экранов мониторов пользователей с возможностью изменения прозрачности водяных знаков, угла наклона и размера шрифта. Администратору Системы должны быть доступны на выбор следующие данные для отображения в качестве водяного знака:

- Имя пользователя;
- Имя компьютера;
- Имя домена;
- Дата и время;
- Произвольный текст.

Должна быть предусмотрена возможность отображения водяных знаков только при запуске определенного процесса пользователем рабочей станции.

Модуль должен позволять распознавать лицо пользователя при входе в учетную запись операционной системы рабочей станции (при наличии подключенной веб-камеры).

Модуль должен позволять распознавать попытки съемки экрана рабочей станции на мобильный телефон (смартфон) (при наличии подключенной веб-камеры).

7.3.1.8 Требования к модулю контроля разговоров сотрудников (ОС Windows)

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 позволять принудительно повышать чувствительность микрофона до максимальных значений.

Модуль должен позволять вести запись разговоров со всех подключенных к рабочей станции микрофонов. При этом должна быть возможность сведения записи со всех микрофонов в один аудиофайл.

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.

7.3.1.9 Требования к модулю контроля активности пользователей и приложений (ОС Windows)

Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях или на сайтах. При этом должна быть доступа индивидуальная настройка параметров активности для указанных администратором Системы приложений и сайтов.

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.

Модуль должен иметь возможность определять фиктивную активность, вызванную программными средствами, без использования физической клавиатуры и манипулятора «мышь».

7.3.1.10 Требования к модулю контроля облачных хранилищ данных (ОС Windows)

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, AnyDesk, Ассистент 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.

7.3.2. Общие требования к функциям Агента для ОС Linux

Агент для ОС Linux должен осуществлять аудит аппаратной конфигурации рабочих станций, на которых он установлен.

Агент должен осуществлять определение географических координат рабочей станции с Агентом.

7.3.2.1. Требования к модулю контроля электронной почты (ОС Linux)

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 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.

7.3.2.2. Требования к модулю контроля сервисов обмена мгновенными сообщениями (ОС Linux)

Модуль должен обеспечивать контроль:

- входящих/исходящих сообщений и файлов, переданных пользователями по протоколам OSCAR, XMPP (Jabber);
- входящих и исходящих сообщений по протоколу HTTP в социальных сетях (Facebook[3], LinkedIn, ВКонтакте, Мой Мир@Mail.ru, Одноклассники.ru, Мамба.ru и прочее на усмотрение Разработчика Системы);
- чатов, звонков, исходящих файлов, переданных при помощи desktop-приложений Telegram, Viber, TrueConf;
- чатов, исходящих файлов веб-версий: Bitrix24, Telegram (web.telegram.org), WhatsApp (web.whatsapp.com), DION.

Модуль должен обеспечивать возможность блокировки:

- передачи сообщений и файлов, соответствующих определенному контенту и/или контексту, передаваемых посредством приложения TrueConf.

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.

7.3.2.3. Требования к модулю контроля FTP-соединений (ОС Linux)

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.

7.3.2.4. Требования к модулю контроля HTTP-трафика (ОС Linux)

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 вычитку сохраненных в браузерах авторизационных данных пользователей к интернет-ресурсам.

Модуль должен предусматривать возможность блокировки посещения запрещенных интернет-ресурсов по протоколу HTTP(S) (конкретных адресов), предусматривать возможность настройки выводимого оповещения при блокировке доступа к запрещенному интернет-ресурсу, а также возможность применения правил блокировки в зависимости от местонахождения рабочей станции (в корпоративной сети или за ее пределами).

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

предусматривать в качестве одного из критериев наличие на файле метки конфиденциальности модуля аудита файлов (функция может быть доступна при наличии установленного модуля аудита файлов).

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

7.3.2.5. Требования к модулю контроля печати (ОС Linux)

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 иметь возможность сохранения теневой копии оригинала документа, отправленного на печать.

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.

Модуль должен обеспечивать возможность ограничения количества страниц документа, выводимого на печать, или блокировки печати файлов на указанном принтере/указанным пользователем/на указанном компьютере.

7.3.2.6. Требования к модулю контроля и управления доступом съёмных устройств (ОС Linux)

Модуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (CD-/DVD-приводы, съемные накопители USB, Wi-Fi, сканерам, USB-токенам, модемам, сетевым адаптерам и переносным устройствам на базе Android и Apple iOS), сетевым папкам и портам (COM, LPT).

Модуль должен поддерживать работу в терминальной сессии.

Модуль должен обеспечивать определение авторизованных групп пользователей устройств и портов.

Модуль должен предоставлять возможность теневого копирования данных, записываемых и/или хранящихся на USB-накопителе (в т.ч. Android или Apple iOS устройства, подключенные в режиме накопителя) или CD-/DVD-диск.

Модуль должен предоставлять возможность теневого копирования файла, полученного в результате сканирования документа на локально подключенном сканере.

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». Для съемных накопителей USB и сетевых папок дополнительно должен быть предусмотрен тип доступа «Только на чтение».

Модуль должен предоставлять возможность импорта списка USB-накопителей из R-Vision.

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. Блокировки должны предусматривать в качестве одного из критериев наличие на файле метки конфиденциальности модуля аудита файлов (функция может быть доступна при наличии установленного модуля аудита файлов).

Модуль должен предоставлять возможность блокировки заданных администратором Bluetooth-сервисов.

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

7.3.2.7. Требования к модулю контроля событий на мониторах и действий сотрудников (ОС Linux)

Модуль должен обеспечивать создание снимков/видеозаписей экранов рабочих станций пользователей по заданному расписанию.

Модуль должен позволять скорректировать расписание снятия скриншотов при посещении заданных интернет-узлов, запуске заданных процессов и/или при вводе пользователем указанных ключевых слов, при нажатии клавиши «PrintScreen», отсутствии активности от мыши и клавиатуры.

Модуль должен позволять скорректировать расписание видеозаписи экрана при посещении определенных (настроенных заранее) интернет-узлов, запуске заданных процессов операционной системы рабочей станции, вводе пользователем определенных ключевых слов.

При наличии нескольких подключенных к рабочей станции мониторов, модуль должен предоставлять возможности:

- создания снимков/видеозаписей только для основного экрана;
- объединения снимков с нескольких экранов в один файл.

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

Модуль должен обеспечивать создание снимков/видеозаписей 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 экрана пользователя в режиме реального времени.

Модуль должен обеспечивать просмотр действий пользователей за рабочей станцией посредством веб-камеры в режиме реального времени.

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

Модуль должен предоставлять возможность контроля и теневого копирования данных, передаваемых через буфер обмена, а также блокировку передачи данных через буфер обмена по содержимому копируемых данных.

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

Модуль должен предоставлять возможность добавления перманентных водяных знаков на изображения экранов мониторов пользователей с возможностью изменения прозрачности водяных знаков, угла наклона и размера шрифта. Администратору Системы должны быть доступны на выбор следующие данные для отображения в качестве водяного знака:

- Имя пользователя;
- Имя компьютера;
- Имя домена;
- Дата и время;
- Произвольный текст.

Должна быть предусмотрена возможность отображения водяных знаков только при запуске определенного процесса пользователем рабочей станции.

Модуль должен позволять распознавать лицо пользователя при входе в учетную запись операционной системы рабочей станции (при наличии подключенной веб-камеры).

Модуль должен позволять распознавать попытки съемки экрана рабочей станции на мобильный телефон (смартфон) (при наличии подключенной веб-камеры).

7.3.2.8. Требования к модулю контроля разговоров сотрудников (ОС Linux)

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.

7.3.2.9. Требования к модулю контроля активности пользователей и приложений (ОС Linux)

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

Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.

7.3.2.10. Требования к модулю контроля облачных хранилищ данных (ОС Linux)

Модуль должен обеспечивать контроль загружаемых/скачиваемых документов следующих облачных сервисов при работе через web-интерфейс (не используя приложение): 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.

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

7.3.3. Общие требования к функциям Агента для ОС MacOS

Агент должен осуществлять определение географических координат рабочей станции с Агентом.

7.3.3.1. Требования к модулю контроля HTTP-трафика (MacOS)

Модуль должен предоставлять возможности для контроля посещаемых пользователем интернет-ресурсов с использованием интернет-браузера.

Модуль должен поддерживать работу с актуальными версиями браузеров Safari, Chrome, Firefox.

7.3.3.2. Требования к модулю контроля печати (MacOS)

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

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.

7.3.3.3. Требования к модулю контроля и управления доступом съёмных устройств (MacOS)

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

7.3.3.4. Требования к модулю контроля событий на мониторах и действий сотрудников (MacOS)

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 иметь возможность объединения изображений с нескольких экранов в один файл.

Модуль должен предусматривать возможность регистрации 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.

7.3.3.5. Требования к модулю контроля разговоров сотрудников (MacOS)

Модуль должен обеспечивать аудиозапись происходящих событий с помощью подключенного микрофона (в гарнитуре, ноутбуке, веб-камере и пр.).

Модуль должен предусматривать возможность активации записи голосов по расписанию, а также возможность настройки качества записываемого звукового файла.

7.3.3.6. Требования к модулю контроля активности пользователей и приложений (MacOS)

Модуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях.

Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером.

8. Дополнительные требования

8.1. Требования к исполнителю

- Производитель решения должен не менее 5 лет присутствовать на рынке.
- Обеспечить техническую поддержку 10/5 предоставляемого программного обеспечения сроком не менее 1 года.
  Техническая поддержка должна включать:

  - помощь в установке ПО.
  - консультирование по вопросам настройки ПО.
  - консультирование по вопросам эксплуатации клиентских приложений ПО.
  - консультирование по вопросам анализа перехваченной информации.
  - предоставление информации по новым версиям ПО.
  - консультирование по работе новых версий.
  - постановка задач и планирование работы с инженером технической поддержки в случае возникновения необходимости.
  - помощь при возникновении проблем в работе ПО.
- Поставщик должен обеспечить возможность установки и эксплуатации решения в локальной инфраструктуре Заказчика (On-Premise).

- Поставщик должен предоставить информацию о системных требованиях к серверной и клиентской части решения.
- Поставщик должен предоставить информацию о возможности интеграции DLP-системы с корпоративными системами Заказчика, включая Active Directory/LDAP, SIEM, системы электронной почты и другие необходимые системы.
- Поставщик должен предоставить условия и порядок получения обновлений программного обеспечения, исправлений безопасности и технической поддержки.
- Наличие авторизационного письма от производителя решения.

8.2. Требования к предоставляемой информации

- полное наименование и версию предлагаемого DLP-решения;
- описание функциональных возможностей DLP-системы;
- описание архитектуры решения и схему взаимодействия основных компонентов;
- количество и тип предоставляемых лицензий — **70 лицензий**;
- условия и срок действия лицензий;
- технические характеристики и системные требования;
- перечень поддерживаемых операционных систем;
- перечень поддерживаемых интеграций и протоколов;
- требования к серверной инфраструктуре;
- требования к сетевому взаимодействию, портам и протоколам;
- описание механизмов обновления и технической поддержки;
- документацию по установке и настройке;
- информацию о производителе программного обеспечения и поставщике;
- лицензионные условия и ограничения использования программного обеспечения.