**Техническое задание**

|  |
| --- |
| **1. Наименование товаров (прав на использование программ для ЭВМ), их количество (объем).** |
| **Наименование программ для ЭВМ** | **Ед. изм.** | **Количество (объем)** |  |
| Права на использование программного обеспечения (программного комплекса) для предотвращения утечек информации  | усл. ед. | 1 |
| **2. Требования к товару (программе для ЭВМ)** |
| **Передача прав на использование программ для ЭВМ** | 2.1. Нормативные документы, согласно которым установлены требования | ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель (в действующей ред.);Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (в действующей ред.);Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (в действующей ред.). |
| 2.2. Технические и функциональные характеристики товара (программ для ЭВМ) | Программное обеспечение для защиты информации (Далее – Система) должно обеспечивать контроль над процессом передачи конфиденциальной информации за пределы сегментов вычислительных сетей. Система должна анализировать все данные, передаваемые работниками как внутри, так и за пределы информационной сети заказчика. Заказчик на основании лицензионного/сублицензионного договора, получает право на использование Системы (неисключительное право использовать Систему (программное обеспечение, программный комплекс) бессрочно).Обновления Системы в рамках версии должны быть доступны в автоматическом режиме внутри приложения. Обновления Системы / программных модулей системы включают в себя все обновления в рамках версии в течение предоставляемого гарантийного срока обслуживания Системы.Система должна быть передана Заказчику в объеме, соответствующем информационной сети Заказчика, то есть, иметь возможность его установки на рабочих станциях пользователей Заказчика в количестве не менее 160 ед.1. Требования к системе в целом1.1. Система должна поддерживать контроль следующих данных: - электронной почты, протоколы: POP3, IMAP, MAPI, веб-почта, SMTP с возможностью активации/деактивации функции остановки;- сервисов обмена мгновенными сообщениями (ICQ, QIP, Mail.ru Agent, Jabber и т.п.), коммуникационных программ-клиентов Microsoft Lync, Viber Desktop, WhatsApp Desktop и Telegram Desktop, а также чаты социальных сетей (Facebook, Одноклассники, LinkedIn, ВКонтакте и др.); - FTP-трафика; - веб-запросов интернет-форумов, блогов, чатов, служб веб-почты, браузерных IM-клиентов; - Skype (чаты, файлы, звонки, SMS, конференции); - съемных устройств;- отправленных на печать документов; - событий на мониторах и действий сотрудников посредством веб-камер;- данных, вводимых с клавиатуры (в том числе нажатия системных клавиш и их сочетаний);- разговоров сотрудников как внутри офиса, так и за его пределами;- облачных хранилищ данных (Google Drive, OneDrive, Office 365, Dropbox, Evernote, Яндекс Диск, cloud.mail.ru и др.);- аудит файлов и папок в локальных и сетевых файловых системах;- активности пользователей в запускаемых ими приложениях;- содержимого документов на рабочих станциях пользователей.Система должна предполагать возможность установки отдельного модуля по каждому из вышеперечисленных каналов передачи данных.Система должна иметь удобный и понятный пользовательский интерфейс, где все сообщения и документация должны быть на русском языке.Система не должна накладывать ограничений на нормальное функционирование серверов и рабочих станций заказчика.Система должна обеспечивать разграничение прав доступа к перехваченной информации и настройкам системы.Система должна обеспечивать перехват шифрованного трафика как на уровне рабочих станций, так и на уровне сетевых шлюзов.Система должна обладать возможностью оптимизации нагрузки на ресурсы территориально разделенных сетей с «узким» каналом передачи данных благодаря предварительному сжатию информации, настройке расписания и скорости ее передачи.Система должна обеспечивать блокировку HTTP(S)-трафика согласно настраиваемым правилам с учетом таких атрибутов как: дата, доменное имя пользователя, IP-адрес, HTTP-метод, текст запроса и др., а также содержать набор предустановленных правил блокировки.Агент Системы, осуществляющий перехват на уровне рабочих станций, должен быть подписан цифровой подписью. Это обеспечивает его целостность и предотвращает возможность встраивания в него стороннего или вредоносного кода.Система не должна ухудшать основные функциональные характеристики ИС (надежность, быстродействие, возможность изменения конфигурации, удобство использования).Система должна обладать характеристиками масштабирования и отказоустойчивости.Система должна обеспечить интеграцию в существующую у заказчика вычислительную сеть без изменения топологии сети.Система должна обеспечивать полноценный контроль пользователей, работающих на терминальных серверах.Все функции Системы должны выполняться в рамках единого решения, единой СУБД для перехваченных данных, вердиктов и работать в рамках одной линейки ОС. Исключением служат сторонние сервисы, с которыми Система имеет возможность интеграции.1.2. Требования к структуре и функционированию СистемыСтруктурно Система должна включать следующие компоненты:- сервер индексации;- сервер сетевого перехвата и/или сервер перехвата на рабочих станциях;- сервер хранилища данных;- модуль администрирования;- модуль принятия решений.В состав Системы должны входить следующие основные функции (которые могут быть представлены в Системы в качестве функциональных (логических) модулей):- функциональный модуль контроля почтового трафика;- функциональный модуль контроля сервисов обмена мгновенными сообщениями;- функциональный модуль контроля FTP-соединений;- функциональный модуль контроля HTTP-трафика;- функциональный модуль контроля трафика Skype;- функциональный модуль контроля печати;- функциональный модуль контроля съёмных устройств;- функциональный модуль контроля файловой системы;-функциональный модуль контроля событий на мониторах и действий сотрудников;- функциональный модуль контроля разговоров сотрудников;-функциональный модуль контроля активности пользователей и приложений;- функциональный модуль контроля данных, вводимых с клавиатуры;- функциональный модуль контроля облачных хранилищ данных;- функциональный модуль индексации;- функциональный модуль индексации файлов рабочих станций;- функциональный модуль хранения данных;- функциональный модуль принятия решений;- функциональный модуль контентного анализа;- функциональный модуль администрирования.Модуль контроля почтового трафика должен обеспечивать контроль сообщений электронной почты (протоколы SMTP/ESMTP, POP3, IMAP, MAPI, веб-почта), также иметь подключаемую функцию автоматической остановки отправки сообщения в случае возникновения инцидента на конечных станциях или почтовом сервере.Модуль контроля сервисов обмена мгновенными сообщениями должен обеспечивать перехват сообщений и файлов, переданных при помощи популярных интернет-мессенджеров, а также чаты, звонки и файлы коммуникационных клиентов Microsoft Lync, Viber Desktop, WhatsApp Desktop и Telegram Desktop.Модуль контроля FTP-соединений должен обеспечивать контроль входящего и исходящего FTP-трафика. В схеме 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, также иметь подключаемую функцию автоматической остановки траффика в случае возникновения инцидента.Модуль контроля Skype должен обеспечивать контроль сеансов текстовой и голосовой связи, файлов и SMS-сообщений, переданных посредством Skype.Модуль контроля печати должен обеспечивать контроль документов, отправленных на печать при помощи сетевых или локальных принтеров.Модуль контроля 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, возможность вести видеозапись действий, создание снимков и записи видео посредством веб-камеры, а также предоставлять возможность просмотра содержимого мониторов и действий пользователей за рабочей станцией в режиме реального времени.Модуль контроля разговоров сотрудников должен обеспечивать аудиозапись разговоров с помощью любого подключенного к рабочей станции микрофона. Контроль сотрудников должен вестись не только внутри офиса, но и когда те находятся в командировках с корпоративными ноутбуками.Модуль контроля активности пользователей и приложений должен обеспечивать мониторинг активности пользователей и запускаемых ими процессов в течение рабочего дня.Модуль контроля данных, вводимых с клавиатуры должен осуществлять логирование нажатий клавиш в любых приложениях (в том числе нажатия системных клавиш и их сочетаний).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 контроля файловой системы должен обеспечивать аудит всех файловых операций.Модуль индексации должен обеспечивать индексирование документов, перехваченных модулями контроля, для быстрого поиска по ним в дальнейшем.Модуль индексации файлов рабочих станций сети должен обеспечивать контроль всех документов, располагающихся на рабочих станциях локальной сети.Модуль хранения должен обеспечивать запись всех почтовых сообщений, сообщений интернет-мессенджеров, HTTP-запросов, мгновенных сообщений, звонков и файлов Skype, Viber, Lync и Telegram, отправленных на печать документов, записанных на съемные носители файлов, перехваченных посредством микрофона разговоров, данных об активности процессов и данных, вводимых с клавиатуры, перехваченных снимков экрана, снимков с веб-камер в базы данных.Модуль принятия решений должен предоставлять возможности для автоматического вынесения вердикта по перехваченному объекту – нарушает или не нарушает он существующие правила. А в случае с перехватом объекта по протоколу SMTP, IMAP или MAPI выносить вердикт о внесении или не внесении письма в карантин и остановки отправки сообщения (до расследования события сотрудником, ответственным за информационную безопасность).Модуль администрирования должен обеспечивать управление настройками конфигурации Системы и обеспечивать 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 верной работоспособности всех компонентов системы и автоматическое уведомление администратора в случае нештатных ситуаций.Модуль контентного анализа должен предоставлять возможности:- проведения ретроспективного анализа перехваченной 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.1.3. Требования к способам и средствам связи для информационного обменаВнедряемая Система должна функционировать в составе информационно-вычислительной сети заказчика.Система должна корректно работать в сетях доменного типа.Система должна поддерживать виртуальную инфраструктуру (VMware ESX/ESXi).Для информационного обмена между компонентами системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP и интерфейсы (Ethernet/ Fast Ethernet /Gigabit Ethernet).Для информационного обмена между Системой и корпоративной почтовой системой должен использоваться протокол SMTP.Должна использоваться единая точка съема почтового и HTTP-трафика.1.4. Требования к характеристикам взаимосвязейПредусмотреть взаимодействие доменов и поддоменов, как связанных, так и не связанных отношениями доверия.Предусмотреть взаимодействие корпоративных почтовых серверов заказчика с Системой через механизмы ретрансляции почтового трафика SMTP-relay.Предусмотреть 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).1.5. Требования к режимам функционирования СистемОсновной режим функционирования Системы – автоматизированный, под управлением администратора.Система должна обеспечивать возможность работы в следующих режимах:- штатный режим (непрерывная круглосуточная работа);- сервисный режим (для проведения обслуживания, реконфигурации и модернизации компонент);- автономный режим (в случае отсутствия связи между компонентами системы или с внешними сетями, для доступа к конфигурационной и архивной информации).1.6. Требования по диагностированию СистемыСистема 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.1.7. Перспективы развития и модернизации СистемыСистема должна быть реализована как открытая система и допускать наращивание производительности за счет улучшения характеристик технических средств.Система должна обеспечивать возможность модернизации путем замены технического и/или программного обеспечения.1.8. Требования к характеристикам, при которых сохраняется целевое назначение СистемыСистема должна обеспечивать штатное функционирование в случае одновременной работы всех пользователей заказчика на объекте автоматизации.Целевое назначение Системы должно сохраняться на протяжении всего срока эксплуатации системы.1.9. Требования к надежностиНа всех серверах Системы должно быть предусмотрено наличие массива RAID1 (зеркалирование).Должна быть обеспечена непрерывность бизнес-процессов заказчика в случае отказов Системы.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 (предпочтительно) в срок не более 6 часов.В случае возникновения сбоя технического или программного обеспечения Системы должна быть обеспечена возможность восстановления ее данных и настроек. Процедуры восстановления работоспособности Системы должны быть описаны и задокументированы в соответствующей эксплуатационной документации на Систему.**2.** **Общие требования к функциям (задачам)**2.1. Требования к модулю контроля почтовых сообщенийМодуль должен предоставлять возможности для контроля сообщений и вложений, переданных 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 исходящего SMTP и HTTP-трафика, а также блокировки исходящих электронных сообщений, передаваемых с помощью почтового клиента Outlook по протоколам IMAP и MAPI.Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, адресов отправителя и получателей, темы письма и др.Модуль должен обеспечивать помещение перехваченных документов в базу данных.Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса модулю контентного анализа и модулю принятия решений для вынесения вердикта.Модуль должен предоставлять средства интеграции с прокси-серверами по протоколу ICAP.Модуль должен обеспечивать интеграцию как с аппаратными, так и с программными прокси-серверами для перехвата HTTPS-траффика (MS ISA/TMG, Squid и др.). Модуль должен предоставлять средства интеграции с корпоративными почтовыми серверами (Lotus Domino, Microsoft Exchange и др.). Модуль должен обеспечивать SMTP-интеграцию с корпоративными почтовыми серверами, поддерживающими функцию журналирования.2.2. Требования к модулю контроля сервисов обмена мгновенными сообщениямиМодуль должен обеспечивать перехват входящих/исходящих сообщений и файлов, переданных пользователями по протоколам OSCAR (ICQ/QIP), XMPP (Jabber, Google Hangouts), MMP (Агент Mail.ru), SIP (X-Lite и др.), YAHOO (Yahoo! Messenger), Gadu-Gadu, входящих и исходящих сообщения по протоколу HTTP в социальных сетях (Facebook, LinkedIn, ВКонтакте, Moй Мир@Mail.ru, Одноклассники.ru, Google+, Мамба.ru и прочее) и сообщений веб-версии Skype (web.skype.com), Telegram (web.telegram.org), входящих и исходящих сообщений, переданных при помощи WhatsApp, в том числе веб-версии (web.whatsapp.com), сообщения ресурса slack.com.Модуль должен обеспечивать перехват входящих/исходящих сообщений, звонков и файлов коммуникационных программ-клиентов Microsoft Lync, Viber и Telegram.Модуль должен обеспечивать перехват 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.Модуль должен обеспечивать помещение перехваченных документов в базу данных.Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса подсистеме анализа и принятия решений для вынесения вердикта.2.3. Требования к модулю контроля FTP-соединенийМодуль должен обеспечивать перехват документов, загруженных или переданных по FTP-соединению, 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 базу данных.Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса подсистеме анализа и принятия решений для вынесения вердикта.2.4. Требования к модулю контроля HTTP-трафикаМодуль должен предоставлять возможности для контроля POST-запросов (сообщений и файлов).Модуль должен поддерживать перехват HTTP-запросов, поступающих от ICAP-сервера.Модуль должен поддерживать фильтрацию запросов, генерируемых всеми современными браузерами, в том числе Internet Explorer 6+; Mozilla Firefox 2+; Opera 8+; Google Chrome 8+.Модуль должен поддерживать перехват 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.Модуль должен обеспечивать помещение перехваченных документов в базу данных.Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса подсистеме анализа и принятия решений для вынесения вердикта.2.5. Требования к модулю контроля SkypeМодуль должен осуществлять перехват сеансов текстовой и голосовой связи (в том числе, звонки на телефонные номера и звуковые дорожки сеансов видеосвязи), файлов и SMS-сообщений, переданных при помощи Skype.Модуль должен осуществлять перехват как входящего, так и исходящего трафика.Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, логинов Skype, количества сообщений и др.Модуль должен обеспечивать помещение перехваченных документов в базу данных.Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса подсистеме анализа и принятия решений для вынесения вердикта.2.6. Требования к модулю контроля печатиМодуль должен осуществлять перехват документов, отправленных на печать при помощи локальных и сетевых принтеров.Модуль должен осуществлять перехват 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 сетевого перехвата отдельных принтеров.Модуль должен поддерживать возможность исключения из сетевого перехвата отдельных документов по их именам.Модуль должен позволять блокировку Escape-функций для PostScript/PCL принтеров, при активации которых перехват распечатанных документов невозможен.Модуль должен обеспечивать помещение перехваченных графических и текстовых представлений документов в базу данных.Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса подсистеме анализа и принятия решений для вынесения вердикта.2.7. Требования к модулю контроля съёмных устройствМодуль должен предоставлять возможности контроля доступа пользователя к внешним устройствам (СD-/DVD-приводы, съемные накопители USB и FireWire, USB-устройства, Wi-Fi и Bluetooth) и портам (USB, FireWire, COM, LPT, IRDA + IDE/SATA, Serial Port, Parallel Port, PCI, PCMCIA, SCSI и прочее). 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 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 ограничивать теневое копирование, исходя из формальных признаков файлов (доменное имя, формат).Модуль должен предоставлять возможность блокировки запуска определенных процессов на компьютере пользователя.Модуль должен предоставлять возможность контроля и блокировки буфера обмена на компьютере пользователя.Модуль должен предоставлять возможность блокировки доступа пользователей к определенным папкам и/или всем 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 предоставлять возможность шифрования данных, записываемых на USB- устройства. Настройки шифрования должны позволять задать правила, в которых можно выбрать пользователей/группу пользователей, записываемые данные которых будут зашифрованы, а также пользователей/группу пользователей, доступ к зашифрованным данным для которых будет разрешен либо заблокирован.Модуль должен обеспечивать присваивание перехваченным файлам атрибутов: доменных учетных записей, имен файлов, серийных номеров устройств и др.Модуль должен обеспечивать помещение перехваченных документов в базу данных.Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса модулям контентного анализа и принятия решений для вынесения вердикта.2.8. Требования к модулю контроля файловой системыМодуль должен протоколировать файлы, статически хранящиеся, создаваемые, изменяемые на рабочих станциях пользователей. Модуль должен обеспечивать возможность выборки протоколируемых ресурсов (рабочие станции, файл-серверы, отдельные жесткие диски и папки).Модуль должен обеспечивать регистрацию следующих событий с файлами: создание, чтение, запись, удаление, переименование, выполнение, изменение расширения, перемещение, копирование, запрет доступа, изменение прав доступа.Модуль должен обеспечивать помещение перехваченной информации в базу данных.Модуль должен обеспечивать присваивание зафиксированным операциям с файлами следующих атрибутов: доменных учетных записей, вид произведенной над файлом операции, имя и тип файла, путь к файлу и др.Модуль не должен хранить копии файлов для случая, если те будут перемещены или удалены. Он производит только регистрацию произошедших событий.Модуль должен предоставлять возможность исключения из аудита системных пользователей.Модуль должен предоставлять возможность указания перечня процессов и файлов (в том числе системных и временных), которые будут исключены из аудита или наоборот – включены в него.Модуль должен предоставлять возможность передать запротоколированную информацию модулю контентного анализа.2.9. Требования к модулю контроля событий на мониторах и действий сотрудниковМодуль 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 позволять скорректировать расписание снятия скриншотов при посещении определенных (настроенных заранее) интернет-узлов, звонке или активации видеоконференции Skype, отсутствии активности от клавиатуры и мыши, нажатии клавиши «PrintScreen».Модуль должен обеспечивать видеозапись происходящего на экранах мониторов согласно настроенному расписанию или событиям.Модуль должен обеспечивать создание снимков посредством любой 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 обеспечивать создание видеозаписи посредством веб-камеры согласно настроенному расписанию или событиям.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 в режиме реального времени.Модуль должен обеспечивать помещение перехваченных документов в базу данных.Модуль должен предоставлять возможность экспорта перехваченных снимков экрана и видеозаписей в отдельную папку.2.10. Требования к модулю контроля разговоров сотрудниковМодуль должен обеспечивать аудиозапись происходящих событий как внутри офиса, так и за его пределами, с помощью любого подключенного микрофона (в гарнитуре, ноутбуке, веб-камере и пр.). 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, а также возможность настройки качества записываемого звукового файла.Модуль должен обеспечивать помещение записанных звуковых файлов в базу данных.Модуль должен предоставлять возможность поиска перехваченных звуковых файлов за указанный период времени применительно к заданным пользователям, компьютерам, IP-/MAC-адресам, продолжительности записи. Модуль должен предоставлять возможность экспорта перехваченных разговоров в отдельную папку.2.11. Требования к модулю контроля активности пользователей и приложенийМодуль должен обеспечивать контроль активности сотрудников в запускаемых ими приложениях или на сайтах.Модуль должен обеспечивать подсчет реального времени работы сотрудника за компьютером. Модуль должен обеспечивать помещение данных об активности пользователей и приложений в базу данных.Модуль должен предоставлять возможность поиска перехваченных данных за указанный период времени применительно к заданным пользователям, компьютерам, IP-/MAC-адресам, продолжительности активности пользователя/процесса, имени активного процесса. Модуль должен обеспечивать использование перехваченных данных для генерации отчетов и оповещений.Модуль должен иметь подключаемую возможность автоматической категоризации любых посещенных сайтов на тематические группы, используя локальный или сторонний классификатор сайтов.2.12. Требования к модулю контроля данных, вводимых с клавиатурыМодуль должен обеспечивать перехват нажатий клавиш в любых запущенных приложениях, включая нажатия системных клавиш и их сочетаний.Модуль должен обеспечивать перехват текстовой информации, помещенной пользователем в буфер обмена. Модуль должен обеспечивать возможность блокировки нажатий клавиши «PrintScreen».Модуль должен предоставлять возможность задать правила логирования нажатий клавиш относительно доменных пользователей либо процессов. Модуль должен обеспечивать помещение перехваченной информации в базу данных.Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса модулю анализа и принятия решений для вынесения вердикта. 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.2.13. Требования к модулю контроля облачных хранилищ данныхМодуль должен предоставлять возможности для контроля входящих и исходящих данных облачных сервисов Evernote, Skydrive, Office 365, Google Drive, Dropbox, YandexDisk, MailRuCloud, SharePoint, ICloud, DropMeFiles, Amazon S3, OwnCloud, Pcloud, OziBox, MediaFire, OpenDrive, 4shared, Box, Syncplicity, CloudMe, MiMedia, My-Files.Модуль должен обеспечивать перехват файлов, передаваемых в программах удаленного доступа TeamViewer, RealVNC, Radmin, LiteManager.Модуль должен обеспечивать присваивание перехваченным документам атрибутов: доменных учетных записей, имени файла, IP-адресов и др.Модуль должен обеспечивать помещение перехваченных документов в базу данных.Модуль должен поддерживать возможность индексирования перехваченных данных модулем индексации файлов, а также передачу индекса модулю анализа и принятия решений для вынесения вердикта.2.14. Требования к модулю индексацииМодуль должен обеспечивать индексирование баз данных Системы и сторонних баз данных.Модуль должен обеспечивать подключение внешних источников данных для индексации.Модуль должен обеспечивать индексирование документов SharePoint и облачных хранилищ Яндекс.Диск, Dropbox и CMIS.2.15. Требования к модулю индексации файлов рабочих станцийМодуль должен обеспечивать отслеживание изменений файлов и высокую частоту переиндексации информации (отслеживание и переиндексацию только новых и измененных файлов). Модуль должен обеспечивать возможность сохранения теневой копии данных, в случае, если те умышленно удалены пользователем.2.16. Требования к модулю хранения данныхМодуль должен обеспечивать архивирование следующих данных:- почтовых сообщений и вложенных в них файлов;- сообщений и файлов IM-клиентов;- сообщений, звонков и файлов коммуникационных программ-клиентов Microsoft Lync, Viber и Telegram;- сообщений WhatsApp;- HTTP-запросов (сообщения и файлы);- сеансов текстовой и голосовой связи, файлов и SMS-сообщений, переданных или полученных по Skype;- графических представлений и текста отправленных на печать документов;- журнала аудита внешних устройств, где фиксируются данные об операциях, выполняемых на подключаемых внешних устройствах;- информации, содержащей перехваченные нажатия клавиш, и текстовую информацию, помещенную в буфер обмена;- аудиозаписей перехваченных разговоров пользователей;- зафиксированных операций с файлами;- входящих и исходящих данных облачных сервисов;- данных об активности пользователей и приложений;- перехваченных снимков в графическом формате.Для архивирования перехваченных данных, система должна использовать базы данных. Модуль должен архивировать все перехваченные объекты, а не только те, по которым зафиксированы инциденты.2.17. Требования к модулю принятия решенийМодуль должен использовать два пользовательских приложения: консоль сервера для задания настроек и клиентскую консоль для управления политиками безопасности, инцидентами и карантином.Модуль должен выносить единый вердикт (инцидент / не инцидент) для каждого перехваченного объекта.Модуль должен предоставлять возможности для ведения журнала инцидентов с возможностью рубрикации по каналам передачи данных, протоколам, пользователям, правилам проверки. Модуль должен предоставлять возможность уведомления ответственных лиц об инцидентах по электронной почте. Модуль должен предоставлять возможность блокировки (помещения в карантин) трафика электронной почты, передаваемого по протоколу SMTP, а также исходящей почты, передаваемой посредством клиента Outlook по протоколам IMAP и MAPI, до принятия вердикта ответственным лицом.Модуль должен 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 файлов и 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).Модуль должен предоставлять возможности для изменения существующих и применения новых правил автоматического вынесения вердикта. Модуль должен предоставлять возможность выполнения ретроспективного контроля перехваченных документов с учетом обновленных правил проверки. Модуль должен предусматривать возможность объединения политик безопасности (правил проверки) в группы.Модуль должен предоставлять возможность задания для каждой группы политик безопасности индивидуальных настроек: перечня индексов, по которым будет проводиться опрос, расписания проверки, списка получателей оповещений об инцидентах, списка исключений.Модуль должен предоставлять возможности для использования «белых списков» (списки пользователей, документы которых исключены из проверок) и «черных списков» (списки пользователей, только по документам, которых будет проводиться проверка). Модуль должен предоставлять возможность экспорта/импорта структуры настроек (политик безопасности, критериев поиска, списков исключений и др.).Модуль должен 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.Модуль должен предоставлять возможности протоколирования выявленных инцидентов. Модуль должен поддерживать возможность категоризации инцидентов с помощью цветовых меток. Модуль должен поддержать возможность экспорта данных об инцидентах и событиях посредством syslog.Модуль должен предоставлять возможность подбора паролей для перехваченных архивов, защищенных паролем. Модуль должен 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.Модуль должен 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 и смыслу 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 (включая вложенные файлы), с возможностью указания порога срабатывания;- по значениям атрибутов баз данных (как общих атрибутов, так и уникальных для отдельных продуктов);- по количественным показателям статистических запросов (числу отправленных писем/распечатанных страниц/сообщений в Skype, Lync, Viber, IM и пр.);- возможность сузить результаты поиска путем дополнительного поискового запроса (фильтры по найденному).Модуль должен предусматривать наличие в дистрибутиве нескольких словарей.Модуль должен 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.Модуль должен предоставлять возможности для просмотра детальной информации по каждому инциденту.2.18. Требования к модулю администрированияМодуль должен предоставлять возможность контроля работоспособности Системы.Модуль должен обеспечивать возможность управления службами модулей Системы.Модуль должен предоставлять возможность управления всеми индексами и базами данных модулей контроля информации.Модуль должен предоставлять возможность мониторинга дискового пространства на серверах Системы.Модуль должен предоставлять возможность автоматического оповещения о важных событиях.Модуль должен обеспечивать возможность синхронизации с одним или более доменом Active Directory.Модуль должен обеспечивать возможность работы с пользователями рабочих групп.Модуль должен предоставлять возможность разграничения прав доступа сотрудников службы безопасности к функционалу консолей подсистем и к данным по тем или иным пользователям, группам пользователей, компьютерам и источникам данных. Под данными подразумеваются зафиксированные модулем принятия решений инциденты, сообщения, попавшие в карантин модуля принятия решений, а также содержимое документов при просмотре в модуле контекстного анализа.Модуль должен предоставлять возможность указания настроек для подключения к базам данных, которые можно впоследствии использовать по умолчанию.Модуль должен обеспечивать возможность управления настройками модуля сбора статистики и предоставления отчетов, а также обеспечивать возможность настройки просмотра отчетов посредством веб-интерфейса.2.19. Требования к модулю контентного анализаМодуль контентного анализа должен быть ориентирован на работу с индексами и базами данных модулей контроля информации.Модуль должен предоставлять возможность выполнять ретроспективный анализ всех перехваченных или запротоколированных объектов:- поиск по ключевым словам и фразам в базах перехваченных документов;- выборка перехваченных данных по дате, доменному имени, адресам и хостам электронной почты, псевдонимам Skype, 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.Модуль должен 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. Модуль должен предоставлять возможность просмотра контентного маршрута перехваченного документа.Модуль должен предоставлять возможности экспорта выборки перехваченных данных (полного списка или набора файлов с оглавлением).Модуль должен 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 Skype, ICQ, и других IM-клиентов), а также информацию по связям текущего пользователя за указанный период времени.Модуль должен предоставлять возможность просмотра информации по активности сотрудников в режиме реального времени с возможностью фильтрации по категориям активности пользователя.Модуль должен 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.Модуль должен предоставлять предусматривать быстрое выполнение генерации отчетов по имеющимся базовым шаблонам (более 30), а также предусматривать возможность добавления пользовательских шаблоны.Модуль должен поддерживать предоставление отчетов в табличном, диаграммном, в виде временного графика, а также в виде графа связей.Модуль должен производить сбор статистики и генерацию отчетов по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности.Модуль должен 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. Модуль должен генерировать краткие и детальные отчеты по продуктивности работы пользователей за выбранный период времени.Модуль должен обеспечивать возможность интеграции с системой контроля и управления доступом (СКУД) и использовать полученные данные при построении отчетов.Модуль должен 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.Модуль должен генерировать отчеты по устройствам: перечень установленного оборудования на компьютерах пользователей и отчет по изменениям в устройствах (комплектующих) компьютеров.Модуль должен генерировать системные отчеты, отображающие:- операции с агентами/протоколами, совершенные любым либо указанным пользователем;- список компьютеров, выполнивших вход в домен, но не проявлявших активность;- список компьютеров с нерабочими агентами;- список компьютеров без агентов;- список компьютеров, выполнивших вход в домен, но не имеющих установленного агента;- информацию о количестве сообщений по выбранным компьютерам за заданный промежуток времени.Модуль должен предоставлять возможность быстрого перехода к поиску и просмотру найденных документов.Модуль должен предоставлять возможность переходов по связанным отчетам.Модуль должен 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.Модуль должен обеспечивать получение наглядного представления об адресах, с которых выбранный пользователь отправлял либо на которые получал сообщения.Модуль должен предусматривать возможность конвертации сгенерированных отчетов в PDF-файл, равно как и вывод их на печать.Ввод в действие программного обеспечения системы предотвращения утечек конфиденциальной информации должен включать обследование информационной системы и подготовку к вводу Системы в действие, а также установку и настройку Системы. |
| 2.3. Требования к безопасности Системы | Передаваемые права на использование Системы не должны являться предметом залога, ареста, или иного обременения, а также предметом иска со стороны третьих лиц. Система должна быть разработана в соответствии с требованиями нормативных документов, перечисленных в пункте 2.1 настоящего технического задания.Предоставляемый гарантийный срок обслуживания Системы должен соответствовать гарантийным срокам правообладателя, поставляемой Системы, но не менее 12 месяцев с момента подписания акта приема-передачи прав на использование Системы. |
| 2.4. Требования к качеству Системы | Поставляемая лицензионная Система является новой и ранее не использовавшейся, по своему качеству и комплектности соответствует стандартам, всем параметрам, а также требованиям, предъявляемым к Системе подобного рода. Система должна соответствовать лицензии правообладателя. |
| 2.5. Сведения о возможности предоставить эквивалентную Систему. Параметры эквивалентности | Допускается поставка эквивалентной Системы, соответствующей параметрам, установленным в пункте 2.2 настоящего технического задания, при условии сохранения всех функциональных требований и условий, а также иных технических характеристик, предъявляемых к Системе. |
| 2.6. Иные требования связанные с определением соответствия поставляемой Системе, потребностям заказчика | Сведения о программном обеспечении, на которое передается право использования, должны быть включены в единый реестр российских программ для электронных, вычислительных машин и баз данных, созданный в соответствии со статьей 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации». |
| **3. Требования к результатам** |
| Права на Систему должны быть переданы в полном объеме, в установленный срок и соответствовать предъявляемым в соответствии с документацией и договором требованиям. |