Техническое задание на систему DLP

* 1. Общие требования к системе
* Система должна быть построена по модульному принципу с использованием следующих подсистем:
* сервер перехвата и управления конфигурациями
* сервер журналирования
* сервер поиска и управления средствами контентного анализа
* прокси-сервер
* агентский модуль, устанавливаемый на АРМ пользователей
* консоль управления
* модуль OCR распознавания
* система должна обеспечить механизмы для масштабирования и наращивания контура подключаемых рабочих АРМ пользователей
* система должна иметь единую для всех подсистем консоль управления настройками и конфигурациями
* система должна предоставлять удобный визуально-ориентированный интерфейс управления для использования основных функций системы и ее настройки без необходимости использования языков программирования и вызова внешних скриптов
* система должна автоматически обнаруживать, классифицировать и определять принадлежность перехваченных данных к конфиденциальной информации
* система должна иметь возможность управления настройками методов контентного анализа, алгоритмов классификации и анализа конфиденциальной информации (словари, шаблоны, базы цифровых отпечатков и таблицы замен) с использованием единого для всех подсистем сервера поиска
* система должна иметь возможность задавать правила контентного анализа и обработки перехваченных данных через интерфейс консоли управления (без программирования и использования внешних скриптов)
* система должна иметь русскоязычный интерфейс управления
* система должна иметь возможность разграничения доступа различных категорий пользователей и администраторов к средствам управления системой и контроля информационных потоков
* система должна иметь возможность разграничения доступа различных категорий пользователей к средствам управления системой контроля информационных потоков;
* система должна иметь возможность разделения прав между несколькими офицерами безопасности, с сохранением функций по администрированию системы, но с разделением прав просмотра с возможностью перекрестного контроля
* в системе в консоли управления должна быть реализована сквозная авторизация пользователей, использующая учетные записи пользователей из каталога Active Directory
* система должна обеспечивать поддержку анализа русского и английского языков
* система должна иметь собственный прокси-сервер для контроля доступа пользователей к ресурсам в Интернет
* система должна полноценно функционировать на серверах под управлением ОС: Microsoft Windows Server 2003 SP2/2008 SP2/2008R2/2012 (версии для x86 и x64)
* клиентские модули системы должны работать на следующих операционных системах: MS Windows XP SP3, Vista, Windows 7/8/8.1, MS Windows Server 2003/2008/2008R2/2012 (версии для x86 и x64)
* система должна обеспечивать работу с СУБД Microsoft SQL Server (не ниже 2005) и Oracle Database (не ниже 10g версии)
* система должна обеспечивать возможность работы в сетях как с доменной структурой (Active Directory), так и без неё
* в системе должен быть организован информационный обмен между компонентами системы на основе стандартных унифицированных протоколов семейства TCP/IP
* система должна обеспечивать развертывание и управление агентами системы как напрямую через консоль, так и через групповые политики домена Microsoft Active Directory.
	1. Требования к подсистеме поиска и классификации конфиденциальной информации
* Система должна извлекать текстовую составляющую для контентного анализа из файлов следующих форматов: HTML, MHT, CHM, XML, PDF, TXT, DOC, DOCX, RTF, PPT, PPTX, XLS, XLSX, EML, MPP, MSG, ODB, ODF, ODG, ODP, ODS, ODT, PST, TNEF, WPS, WRI, CDW, FRW, M3D;
* система должна извлекать файлы для контентного анализа из архивов следующих форматов: 7z, ARC, ARJ, bzip2, CAB, dmg (Apple Disk Image), gzip, ISO, RAR, RPM, tar, ZIP;
* система должна анализировать текстовую составляющую (производить контентный анализ) с помощью следующих встроенных методов анализа:
* анализ текста по словарю, содержащего группы слов, объединенные по какому-либо признаку (категории);
* анализ текста с использованием метода «Поиск похожего»;
* морфологический анализ, с возможностью поиска слов, употребляемых в тексте в различных грамматических формах;
* возможность анализа с использованием шаблонов, построенных на основе регулярных выражений и спецсимволов подстановки (\*, ?, ^, !, #, @ и др.)
* возможность использовать технологию спецсимволов при вводе слов при формировании словарей (\*, ?, ^, !, #, @ и др.);
* возможность использовать поиска словоформ методом стемминга;
* возможность производить анализ с использованием транслитерации, т.е. поиск возможного преобразование кириллицы в буквы латинского алфавита по заранее сформированным правилам преобразований;
* возможность использовать метод таблиц замен по заранее настроенным правилам проверки возможных вариантов замен;
* возможность использовать метода Байеса для определения вероятности принадлежности текста к определенной категории;
* возможность использовать метод опорных векторов для определения вероятности принадлежности текста к определенной категории;
* возможность использовать метод цифровых отпечатков;
* возможность использовать метод графических отпечатков для данных, хранящихся в виде растровых изображений;
* возможность использовать метод анализа с учетом ошибок и подстановок для обнаружения текста, подвергшегося непреднамеренному искажению;
* возможность использовать метод поиска слов с учетом звучания на русском или английском языках, подвергшихся намеренному или случайному искажению;
* возможность использовать метод поиск синонимов;
* возможность осуществлять поиск текстовых данных в сетевых папках и базах данных локальной сети;
* возможность использовать метод цифровых отпечатков таблиц базы данных.
	1. Требования к подсистеме контроля почты и веб трафика
* Система должна иметь возможность работать в гибридном режиме: осуществлять перехват почтового и интернет трафика с центрального шлюза прокси-сервера (и почтового сервера), а также перехватывать трафик с агентов на АРМ пользователей
* система должна иметь возможность осуществлять контроль протоколов ICQ, Mail.Ru Агент, Jabber, Yahoo! Messenger, MS Office Communicator как в режиме фильтрации, так и в режиме зеркалирования с использованием функций шлюзового и агентского перехвата
* система должна иметь возможность осуществлять контроль протоколов FTP, IMAP, SMTP, POP3, MAPI в режиме зеркалирования с использованием функций шлюзового и агентского перехвата
* система должна иметь возможность осуществлять контроль протоколов HTTP/HTTPS как в режиме фильтрации, так и в режиме зеркалирования с использованием функций шлюзового и агентского перехвата
* система должна иметь возможность проверки передаваемого почтового трафика по протоколам SMTP, ESMTP, SMTPS, POP3, MAPI, IMAP
* система должна иметь возможность контроля входящего и исходящего трафика, передаваемых по протоколу SMTP, электронных писем (и вложений в них) от Microsoft Exchange Server, IBM Lotus Domino, Kerio MailServer, CommunigatePro, Sendmail, Postfix и других почтовых SMTP серверов
* система должна иметь возможность контроля внутренней почты пользователей Microsoft Exchange 2007/2010/2013, пересылаемой между пользователями и не выходящей за пределы внутреннего почтового домена
* система должна иметь возможность установки агента системы для сбора внутреннего почтового трафика пользователей непосредственно на сервер с развернутым транспортным агентом Microsoft Exchange 2007/2010/2013
* система должна иметь возможность производить автоматическую остановку и отправку подозрительных писем для ручной проверки в системный «карантин»
* система должна позволять настраивать для перехваченного трафика проверочные условия, которые последовательно проверяют, соответствует ли фильтруемое сообщение заданным критериям
* система должна поддерживать отбор по следующим условиям:
* наличие зашифрованных файлов-вложений (RAR, ZIP, DOC, DOCX, XLS, XLSX, PDF, ODB, ODF, ODG) методами шифрования, используемых в соответствующей программе
* поиск текста в сообщениях и файлах-вложениях по правилам: содержит, не содержит, совпадает, начинается, заканчивается (с учетом регистра)
* поиск текстовых фрагментов по словарям терминов
* проверка полей сообщения: отправитель (FROM), получатель (TO), копия (CC), скрытая копия (BCC), обратный адрес (Reply to) на совпадение вхождения текстовых срок, имен пользователей и или групп домена, а так же групп рассылок MS Exchange
* проверка формальных признаков и атрибутов сообщений с возможностью произвольно группировать условия по правилам «и», «или», «нет»
* наличие файлов-вложений определенных типов: аудиофайлы, исполняемые файлы, файлы неизвестных типов, файлы с видео, файлы с графикой, файлы с зашифрованной информацией, файлы с текстом, файлы-архивы
* система должна поддерживать следующие автоматически выполняемые действия над сообщениями:
* вставлять текст заданного содержания в начало или конец сообщения
* доставлять сообщения адресату
* заменять значения полей (копия (CC), обратный адрес (Reply to), отправитель, получатель, скрытая копия (BCC), тема сообщения) сообщения текстом заданного содержания
* осуществлять доставку уведомления заданного содержания об обрабатываемом сообщении на указанный адрес пользователя или администратора
* осуществлять изоляцию сообщения в карантин
* осуществлять сохранение сообщений в архив
* осуществлять удаление вложения
* система должна иметь возможность при конструировании политик задавать произвольное необходимое соответствие «Проверочное условие» - «Действия» из перечисленных выше условий и действий для выполнения автоматического системного действия над перехваченным почтовым сообщением, подпавшего под соответствующее условие отбора
* система должна иметь возможность при задании соответствия «Проверочное условие» - «Действия» использовать графический визуально-ориентированный конструктор создания политик
* система должна иметь единый раздел в консоли администрирования, где отображаются все существующие активные и не активные политики, отображающие краткую сводку по проверочным условиям и связанным с ними действиями системы
* система должна иметь возможность в консоль управления при работе с архивом и карантином выполнять оператору следующие действия над перехваченными сообщениями: доставить получателю, переслать на заданный адрес, удалить из архива, очистить, пометить как прочтенное, пометить как непрочтенное, установить метку
* система должна иметь возможность проверки трафика, пересылаемого по протоколам HTTP, HTTPS, FTP, FTPS, FTP-over-HTTP
* система должна иметь возможность производить инспекцию данных, передаваемых с использованием зашифрованных протоколов SSL
* система должна иметь возможность осуществлять сбор и расшифровку HTTPS трафика при помощи агентов системы, установленных локально на АРМ пользователя
* система должна иметь возможность контролировать и предотвращать утечку данных через все сетевые интерфейсы АРМ пользователя с установленным агентом
* система должны иметь возможность зеркалировать и фильтровать трафик для протоколов HTTP/HTTPS, ICQ, Mail.Ru Агент, XMPP (Jabber), Yahoo! Messenger, MS Office Communicator, а также производить зеркалирование трафика для протоколов FTP, IMAP, SMTP, POP3, Skype, MAPI с использованием агентов на АРМ пользователя
* система должна иметь возможность задавать список приложений, интернет-трафик которых контролирует агентом системы на АРМ и список приложений, интернет-трафик которых игнорируется
* система должна иметь возможность устанавливать соединение между агентами и центральным сервером конфигураций для передачи данных по заранее предопределенному порту и с заданным периодом переподключения для последующего обмена
* система должна иметь возможность задавать различные режим работы агента на АРМ в зависимости от настроек сетевого подключения и доступности домена: компьютер подключен к корпоративной локальной сети и домен доступен, домен доступен через корпоративное VPN соединение, домен не доступен по сети и компьютер работает автономно
* система должна иметь агентский модуль контроля приложения Skype, устанавливаемого на АРМ пользователя, с возможностью: журналировать передаваемые текстовые сообщения, файлы и звуковой трафик, осуществлять запрет передачи файлов, осуществлять при необходимости запрет запуска клиента Skype, а также иметь режим защиты от закрытия агента пользователем, обладающим правами администратора
* система должна иметь возможность перехватывать трафик Microsoft Lync: мгновенные сообщения, уведомления об отправке файлов, уведомления об открытии доступа к удаленному рабочему столу
* система должна иметь режим контроля HTTP/HTTPS веб-сервисов, с возможностью перехватывать весь трафик контролируемого веб-сервиса, в том числе служебные сообщения, которыми обмениваются веб-браузер и сервис
* система должна иметь возможность контроля служб: ICQ, Mail.Ru Агент, Jabber, Yahoo! Messenger, MS Office Communicator, Skype, Viber
* система должна иметь возможность контроля следующих HTTP(S) почтовых сервисов: Mail.ru, Yandex.ru, Qip.ru, Rambler.ru, Hotmail.com, Gmail.com, Yahoo.com, Outlook Web App
* система должна иметь возможность контроля облачных HTTP(S) сервисов и файл хостингов: Google Docs, Office 365, Яндекс диск, Google диск, Dropbox, Облако Mail.Ru, Microsoft OneDrive
* система должна иметь возможность контроля поисковых запросов: Google, Bing, Yandex, Rambler, Yahoo!
* система должна иметь возможность контроля следующих HTTP(S) сервисов социальных сетей: Facebook.com, Odnoklassniki.ru, VKontakte.ru, Livejournal.com, Blogger.com, Loveplanet.ru, LinkedIn.com, Twitter.com, MySpace.com
* система должна иметь возможность контроля сервисов поиска работы: superjob.ru, hh.ru, rabota.ru, job.ru, zarplata.ru, career.ru, vacansia.ru, rosrabota.ru, mnl.ru, vakant.ru, job.ws, job-mo.ru
* система должна иметь возможность контроля HTTP(S) сервисов web-служб отправки сообщений SMS/MMS: Megafon, Beeline, [MTS](http://mts), TELE2, Skylink
* система должна иметь возможность контроля и перехват трафика на фото- и видеохостинги: Picasa, Panoramio, YouTube
* система должна иметь возможность выбора режима перехвата сообщений индивидуально для каждого перехватываемого веб-сервиса без необходимости администратору системы вносить изменения на уровне скриптов и программного кода текущих настроек системы
* система должна иметь возможность идентифицировать доменное имя пользователя, принимающего/ передающего интернет-трафик
* система должна иметь возможность при анализе выделять текст из файлов вложений различных типов: с текстовой составляющей (в том числе скомбинированных с другими файлами) и растровой графики
* система должна иметь возможность при анализе обрабатывать файлы (DOC, DOCX, XLS, XLSX, PDF, RAR, 7z, содержащими файлы с текстовой составляющей) комбинированные по методу склейки путем бинарного копирования объектов
* система должна иметь возможность при анализе обрабатывать документы MS Office с текстовым документом (DOC, DOCX, XLS, XSLX, PPT, PPTX, PDF, TXT, HTML, XML), вложенным с использованием команды «Вставка — Объект».
	1. Требования к подсистеме контроля АРМ пользователей
* Система должна иметь возможность разграничения доступа к внешним устройствам на основе политик доступа, определяющих связь устройства с правилами доступа к нему, в том числе и по серийному номеру устройства, производителю, пользователю, местонахождению компьютера, дате и времени
* система должна иметь возможность разграничения операций с файлами на основе политик доступа, регламентирующих разрешенные операции с файлами на USB-носителях и использование функции печати документов
* система должна иметь возможность осуществлять контроль доступа по содержимому файла и выполнять контентный анализ текста, содержащегося в файле, по результатам которого происходит разрешение или запрет чтения, записи или печати согласно соответствующей политике
* система должна иметь возможность использования контентного анализа для обнаружения конфиденциальной информации с использованием методов: морфологического анализа, стемминга, спецсимволов и транслитерации, анализа по цифровым отпечаткам, поиска по словарям или по заранее установленным шаблонам
* система должна иметь возможность применения политик доступа на основе местоположения (домен доступен, домен не доступен), расписания и срока действия
* система должна иметь возможность применения политик доступа (как к отдельному физическому устройству (порты COM и LPT, контроллеры SCSI, сетевые устройства, жесткие диски) или принтеру, так и к группе устройств, имеющих определенные характеристики:
* типы устройств (накопители с интерфейсом USB, брелки флэш-памяти, МР3-плееры, фотокамеры)
* отдельные характеристики USB-устройств (класс, интерфейс, подкласс, протокол, идентификатор производителя, идентификатор продукта, название производителя, название продукта, серийный номер устройства)
* классы физических устройств
* система должна иметь возможность контроля использования USB, WiFi, CD-DVD-ROM, Bluetooth, PCMCIA
* система должна иметь возможность контролировать доступ в интернет вне сети организации, разрешая доступ только по разрешенным VPN-каналам
* система должна иметь возможность контроля локальных, сетевых и виртуальных принтеров
* система должна иметь возможность автоматически выполнять теневое копирование файлов при следующих операциях, выполняемых на АРМ пользователя: записи на CD/DVD, печати, операций с использованием буфера обмена, запись файлов на RDP-диски
* система должна иметь возможность ведения локального хранилища при осуществлении операций теневого копирования файлов
* локальное хранилище должно быть защищено от изменений и перезаписи файлов, запись в папку должен производить только агентский модуль системы
* система должна иметь возможность выполнять операцию шифрования файлов при записи на внешнее USB- устройство
* система должна иметь возможность при выполнении операцию шифрования файлов при записи на внешнее USB-устройство определять критерии применения операции шифрования: для каких политик выполнять шифрование файлов
* расшифровывание ранее зашифрованных файлов должно выполняться только на АРМ с установленным клиентским модулем и загруженными актуальными версиями ключей шифрования
* хранение ключей шифрования должно выполняться на специальном защищенном сервере конфигураций
* ключи шифрования должны загружается на клиентский модуль на АРМ при старте ОС
* клиентский модуль должен сохранять ключ шифрования в защищенном локальном хранилище, для выполнения операции шифрования даже при временной недоступности сервера конфигураций
* система должна иметь возможность автоматически генерировать новые ключи шифрования с заданной периодичностью, при этом на сервере конфигураций должны храниться ранее использованные ключи шифрования для того, чтобы можно было открыть зашифрованные ими файлы
* система должна иметь возможность блокирования записи и печати файла по типу (аудио-файлы, исполняемые файлы, файлы с видео, файлы с графикой, файлы с зашифрованной информацией, файлы-архивы) и содержанию
* система должна иметь возможность блокировки записи зашифрованных файлов
* система должна иметь возможность распространять политики контроля доступа и операций с файлами на АРМ пользователей по сети
* система должна иметь возможность производить регулярные запросы и обмен данными между агентом на АРМ пользователя и сервером поиска для загрузки и обновления локальных конфигураций и настроек средств контентного анализа
* система должна иметь возможность работы системы обнаружения при работе АРМ вне корпоративной сети
* клиентский модуль должен обеспечивать информирование пользователя через системный трей OC о режиме работы и формировать список, в котором перечислены все доступные устройства и политики их использования
* система должна предоставлять возможность пользователю создать запрос Администратору системы на получение доступа к устройству
* система должна предоставлять возможность предоставлять удаленному пользователю доступ к локальному устройству, используя только телефонную связь с администратором системы
* система должна иметь возможность доставки служебных уведомлений оператору системы и Администратору
* система должна иметь функционал снятия снимков экрана с рабочих станций выбранных пользователей в любой момент времени и с заданной периодичностью в форматах: PNG и JPG с заданными настройками цветности, GIF
* при наличии на компьютере нескольких активных сессий (терминальный сервер), снимки экранов должны создаваться с каждой пользовательской сессии
* при наличии нескольких мониторов при снятии снимков должен создаваться один графический файл, содержащий снимки всех рабочих столов пользователя.
	1. Требования к подсистеме поиска несанкционированных копий файлов
* Система должна иметь возможность осуществлять поиск несанкционированных копии конфиденциальной информации на АРМ пользователей, ноутбуках и серверах, с установленным агентским модулем системы
* возможность осуществлять поиск конфиденциальных документов в корпоративных файловых хранилищах, на которых установлен агентский модуль системы
* система должна иметь возможность осуществлять поиск в режиме реального времени: сканирование проводится всякий раз, как только на локальном жестком диске изменяется какой-либо файл
* система должна иметь возможность осуществлять поиск в режиме сканирования по расписанию: агент системы в заданный момент времени начинает поиск изменившихся с момента последнего сканирования файлов
* система должна иметь возможность при обнаружении инцидентного файла агентским модулем выполнять следующие действия: осуществлять запись в журнале событий, выполнять теневое копирование обнаруженного файла в указанное хранилище, оповещать пользователя
* система должна иметь возможность проведения операций теневого копирования файлов в выбранное хранилище на сетевой папке или сервере баз данных
* система должна иметь возможность, в случае недоступности файла или сетевой папки, повторять регулярные попытки чтения до тех пор, пока файл или папка станут доступными
* система должна иметь возможность выводить на экран АРМ пользователя всплывающее предупреждение об обнаружении инцидентного файла, а также окно с перечислением всех случаев нарушения файловых политик
* система должна иметь возможность с помощью настроек скрыть ярлык модуля из области уведомлений ОС (системный трей)
* система должна иметь возможность осуществлять пользователем просмотр списка инцидентных файлов с описанием примененной политики, даты обнаружения файлов и пути к ним в случае доступного ярлыка программы в области уведомлений ОС (системный трей)
* система должна иметь возможность осуществлять агентским модулем регулярные обращения по расписанию к серверу конфигураций для обновления конфигурации политик
* система должна иметь возможность осуществлять централизованную перенастройку агентских модулей для получения обновлений конфигурации от альтернативного сервера
* система должна иметь возможность осуществлять обновление клиентских модулей с использованием групповых политик
* система должна иметь возможность осуществлять проверку на наличие зашифрованных файлов форматов: DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, ODB, ODF, ODG, ODP, ODS, ODT, RAR, ZIP, 7Z, PST
* система должна иметь возможность осуществлять агентом в режиме ведения журнала записи о появлении инцидентных файлов и сохранять текстовую составляющую этих файлов на сервере в соответствии с настройками журналирования инцидентов
* агент должен иметь возможность рассчитывать для проверяемого файла цифровой отпечаток и передавать его серверу поиска вместе со списком категорий, на соответствие которым необходимо проверить отпечаток
* сервер поиска должен иметь возможность выполнить сравнение присланного отпечатка с отпечатками, хранящимися в базе данных, а затем возвращает агенту информацию о найденных совпадениях
* поиск конфиденциальных данных в сетевых папках, базах данных и на серверах SharePoint.
	1. Требования к подсистеме прокси-контроля пользователей Интернет
* Прокси-сервер должен поддерживать работу с протоколами HTTP/HTTPS и SOCKS и обрабатывать приходящие на соответствующие порты запросы
* система должна обеспечивать выполнение HTTP/HTTPS-запросов и их журналирование
* система должна иметь возможность передавать трафик для анализа на сервер перехвата и поддерживать совместную работу как в режиме зеркалирования (журналирования), так и в режиме фильтрации (блокировки)
* система должна обеспечивать задаваемый перечень хостов, доступ на которые разрешается без прокси контроля
* система должна иметь возможность поддерживать авторизацию пользователей по логин/паролю передаваемых как в зашифрованном, так и не зашифрованном виде, расположенных в сетях с доступным контроллером домена (NTLM, Kerberos) или без него
* система должна иметь возможность использовать обновляемый и разделенный на категории список доменных имен интернет-сайтов
* система должна иметь возможность задавать формат и состав журналируемых данных о перехваченном запросе
* система должна иметь возможность задавать правила доступа пользователей к ресурсам сети Интернет на основе разрешающих правил с возможностью производить: SSL-инспекцию трафика, разрешение/запрет доступа, журналирование запроса, передачу данных на сервер анализа
* система должна иметь возможность задавать произвольное количество правил доступа с возможностью выставлять их внутренний приоритет исполнения
* система должна иметь возможность использовать при задании правил заранее подготовленные списки доменных имен адресатов в виде текстовых файлах.
	1. Требования к подсистеме OCR распознавания графических файлов
* Система должна иметь возможность выделять текст на русском и английском языке из графических файлов с помощью технологии OCR (оптического распознавания символов) компании Abbyy
* система должна иметь возможность подключения и встраивания в систему свободно распространяемого OCR модуля Tesseract для распознавания графических файлов
* система должна иметь возможность проводить распознавание текста с помощью агента на АРМ с локально установленным модулем OCR Tesseract
* система должна иметь возможность выделять текст из изображения документа, содержащего графические элементы, произвольно скомбинированные с текстом
* система должна иметь возможность использовать OCR для автоматической генерации словарей терминов на базе сканированных оригиналов документов
* система должна иметь возможность использовать OCR для автоматической генерации базы данных цифровых отпечатков документов.
	1. Требования к подсистеме ведения архива
* Система должна иметь архив, содержащий полную копию перехваченной информации в оригинальном формате и с оригинальной кодировкой
* система должна иметь возможность помещать в архив копии анализируемых почтовых сообщений, теневые копии документов и данных, передаваемых по всем контролируемым каналам
* карточка события или инцидента должна содержать следующие информационные поля: время, размер, тип, пользователь, отправитель, получатель, тема сообщения, вложение, текст сообщения, текст во вложениях, присвоенные системой атрибуты, количество вложений, хост отправителя, канал, направление передачи, оригинал сообщения в формате MIME без вложений, вложения в сообщение в формате MIME.
* карточка события или инцидента должна содержать записи о проведенных системой автоматических проверках перехваченного сообщения и полученных результатах: результаты проверок по настроенным в системе условиям отбора трафика, результаты автоматически выполняемых действий, связанных с выполнением условий отбора трафика, итоговое заключение по выполненным в отношении данного события действиям
* система должна иметь возможность проводить ретроспективный анализа перехваченной ранее информации, с возможностью изменения правил проверки.
* система должна иметь возможность отображения истории сообщений с возможностью группировки переписки между любыми выбранными пользователями (режим «беседа»)
* система должна иметь возможность осуществлять поиск сообщений по свойствам (дате, отправителю, наличию в теме или тексте сообщения определенных символьных строк)
* система должна иметь возможность осуществлять поиск сообщений с использованием заранее настроенных фильтров (с использованием спецсимволов \* и ?)
* система должна иметь возможность осуществлять поиск сообщений с использованием составных условий, позволяющих искать сообщения по любому сочетанию («и», «или», «не») значений полей и признаков (дате, отправителю, IP-адресу компьютера и проч.) и наличию в тексте символьных строк
* система должна иметь возможность хранения архива в СУБД Microsoft SQL Server (не ниже 2005) и Oracle Database (не ниже 10g версии).
	1. Требования к подсистеме журналирования событий
* В системе должен быть унифицированный журнал событий
* в системе при чтении, записи или печати файлов или документов, подпадающих под действие политики безопасности должна быть возможность выполнять операции журналирования и теневого копирования
* при использовании политики контроля файлов должны журналироваться только те операции, которые подпадают под действие политики: если файл не содержит искомый текст, действия журналирования не должны производиться
* при использовании функции журналирования в политиках доступа к устройству должно выполняется журналирование всех файловых операций
* система должна иметь возможность просмотра инцидентного файла из журнала событий с использованием прямой гиперссылки в формате UNC.
	1. Требования к подсистеме мониторинга событий
* Настройка параметров мониторинга в системе должна производится как для отдельного компьютера, так и для группы либо домена в целом
* функция мониторинга должна позволять детально анализировать, какие именно изменения произведены, а также обнаруживать отличия конфигурации удаленного компьютера с распространяемой
* мониторинг компьютеров должен осуществляется в фоновом режиме, независимо от запущенной консоли управления и сеанса пользователя
* модуль мониторинга должен производит опрос клиентских модулей на АРМ пользователей и отображать статус опрашиваемых компьютеров
* при мониторинге должны отслеживаться следующие ситуации: изменена конфигурация клиентского модуля, изменена конфигурация обработки уведомлений клиентского модуля, изменены настройки безопасности клиентского модуля, нарушена целостность клиентского модуля, компьютер выключен или не доступен по сети, соединение с компьютером восстановлено, служба или клиентский модуль не отвечает
* система должна иметь возможность экспортировать результаты мониторинга в файл формата XML для создания отчетов и анализа возникавших ситуаций.
	1. Требования к подсистеме графических отчетов
* Система должна иметь подсистему отчетности в виде графических отчетов и сводных таблиц
* система должна иметь возможность разделения прав доступа к отчетам
* система должна иметь возможность выставлять метки на выбранные сообщения и инциденты
* система должна иметь возможность генерировать выбранные отчеты по расписанию
* система должна иметь возможность рассылки сгенерированных отчетов по расписанию на почтовые адреса выбранных пользователей в виде прикрепленного архива
* система должна иметь возможность создания табличных отчетов с использованием встроенного визуально-ориентированного конструктора
* система должна иметь возможность при создании нового табличного отчета задавать следующие основные параметры: выводимые колонки с атрибутами, интервал времени, правила группировки выводимых записей, условия отбора и фильтры, права доступа
* система должна иметь возможность при создании нового табличного отчета задавать условия отбора записей в виде проверок соответствующих атрибутов по задаваемому значению по правилам: содержит, не содержит, начинается, заканчивается, равно, не равно, не определен
* система должна иметь возможность комбинировать условия отбора по правилам «и», «или», «нет»
* система должна иметь возможность генерировать настраиваемые пользователем отчеты с возможностью выбора анализируемых параметров и выводом результатов в виде визуальных диаграмм (вертикальные столбчатые, горизонтальные столбчатые, графики, круговые) по выбранным параметрам
* система должна иметь возможность при выводе числовых показателей, имеющих большой разброс с отличаем на несколько порядков для разных элементов представлять в виде диаграммы с логарифмической шкалой по осям (натуральный или десятичный логарифм).
	1. Требования к функционалу консоли управления и администрирования
* Система должна иметь возможность назначения конфигурации агентским модулям с использованием в консоли визуального дерева подключенных АРМ пользователей
* система должна иметь возможность назначать конфигурации как отдельному компьютеру в дереве, так и группе компьютеров
* система должна иметь возможность использовать режим наследования конфигураций между различными иерархичными группами компьютеров для облегчения процедуры распространения необходимой конфигурации
* система должна иметь возможность настройки отображения защищаемых компьютеров в консоли управления конфигурациями с использованием средств группировки: по версии, по дате синхронизации, по виду наследования, по наличию шифрования, по наличию назначенной компьютеру конфигурацией на сервере, по вхождению в домен
* система должна иметь возможность использовать механизм drag-n-drop (перетаскивание) для перемещения объектов-компьютеров между различными отображаемыми категориями, списками и узлами в консоли администратора.