Оглавление

[1. Описание DLP системы 3](#_Toc93913377)

[2. Централизованный перехват данных 3](#_Toc93913378)

[3. Перехват электронной почты, переданной через почтовые сервера 3](#_Toc93913379)

[4. Перехват HTTP-трафика, переданного через прокси-сервер 4](#_Toc93913380)

[5. Перехвата данных с помощью агента 4](#_Toc93913381)

[5.1. Администрирование 4](#_Toc93913382)

[5.2. Контролируемые каналы передачи данных 5](#_Toc93913383)

[5.2.1. Модуль контроля HTTP трафика 5](#_Toc93913384)

[5.2.2. Модуль контроля FTP трафика 6](#_Toc93913385)

[5.2.3. Модуль контроля почты 6](#_Toc93913386)

[5.2.4. Модуль контроля переписки в мессенджерах 7](#_Toc93913387)

[5.2.5. Модуль контроля печати 8](#_Toc93913388)

[5.2.6. Модуль контроля внешних устройств и накопителей 8](#_Toc93913389)

[5.2.7. Модуль контроля облачных хранилищ 9](#_Toc93913390)

[5.2.8. Модуль контроля сетевых ресурсов 10](#_Toc93913391)

[5.2.9. Модуль блокировки передачи данных 10](#_Toc93913392)

[5.2.10. Модуль снимков экрана 11](#_Toc93913393)

[5.2.11. Модуль видеомониторинга 12](#_Toc93913394)

[5.2.12. Модуль аудиомониторинга 12](#_Toc93913395)

[5.2.13. Модуль мониторинга пользовательской активности 12](#_Toc93913396)

[5.2.14. Модуль браузер активности 13](#_Toc93913397)

[5.2.15. Модуль контроля буфера обмена 13](#_Toc93913398)

[5.2.16. Модуль контроля ввода с клавиатуры 14](#_Toc93913399)

[5.2.17. Модуль индексации рабочих станций 14](#_Toc93913400)

[6. Модуль хранения и обработки данных 14](#_Toc93913401)

[7. Анализ данных 17](#_Toc93913402)

[8. Распознавание изображений 21](#_Toc93913403)

[9. Распознавание речи 21](#_Toc93913404)

[10. Управление контролируемыми пользователями 22](#_Toc93913405)

[11. Мониторинг работоспособности системы 23](#_Toc93913406)

[12. Поиск информации 23](#_Toc93913407)

[13. Отчетность 23](#_Toc93913408)

[14. Модуль политик безопасности 27](#_Toc93913409)

[15. Модуль расследования инцидентов 29](#_Toc93913410)

[16. Анализ рисков 30](#_Toc93913411)

[17. Прочие требования 30](#_Toc93913412)

[18. Масштабируемость системы 30](#_Toc93913413)

[19. Ориентация работы всех компонентов системы на многопоточность 31](#_Toc93913414)

[20. Удобство администрирования 31](#_Toc93913415)

# Описание DLP системы

Комплексный программный продукт предназначен для обеспечения внутрикорпоративной информационной безопасности посредством перехвата и анализа сетевого трафика, данных, переданных на внешние устройства, локальные сетевые ресурсы, облачные хранилища, локальные и сетевые принтеры. Система осуществляет контроль и анализ активности пользователя на компьютере (нажатия клавиш клавиатуры, содержимое буфера обмена и т.п.) и поддерживает возможность мониторинга аудиопотоков со звуковых устройств и видео с рабочих столов и веб-камер компьютеров, а также контроль изменений файловых систем компьютеров в режиме реального времени. Данное решение позволяет контролировать утечку и нежелательное распространение конфиденциальной информации через Интернет, перехватывая входящие и исходящие сообщения электронной почты, переписку в программах мгновенных сообщений, переданные документы, файлы, веб-страницы и т.д. В системе поддерживаются функции блокирования исходящего сетевого трафика, переданного по HTTP, SMTP, MAPI и их шифрованным аналогам, блокировка документов отправляемых на печать, а также возможность контроля доступа и использования внешних устройств, облачных хранилищ, локальных сетевых ресурсов и приложений.

# Централизованный перехват данных

Трафик контролируемой локальной сети с помощью управляемого коммутатора зеркалируется на специально выделенный сервер, на котором установлен компонент системы «Сервер перехвата». «Сервер перехвата» получает данные с заданного сетевого адаптера и обеспечивает следующие возможности:

* централизованный перехват данных, отправляемых по протоколам, не использующим шифрование (FTP, HTTP, IMAP, POP3, SMTP, MAPI, MRA (Mail.Ru Агент), OSCAR (AIM, ICQ), XMPP (Jabber), YMSG (Y!M) посредством зеркалирования трафика;
* фильтрация перехватываемых данных, отправляемых по протоколу HTTP по MIME типу, и по набору атрибутов (IP-адрес, порт, HTTP-метод, web-поле и др.), в том числе с использованием сложных условий («И», «Или», «Не»);
* настройка исключений из перехвата по IP-адресам (отдельным и диапазону) и отдельным МАС-адресам, протоколам, учетным записям и адресам электронной почты, учетным записям систем мгновенного обмена сообщениями;

# Перехват электронной почты, переданной через почтовые сервера

Перехват почты, отправляемой через почтовые сервера, развернутые на базе Microsoft Exchange Server, IBM Lotus Domino, Sendmail, hMailServer и другого программного обеспечения, может осуществляться путем интеграции с почтовыми серверами по протоколам POP3, IMAP, SMTP, а также при помощи коннектора MS Exchange. Модуль обеспечивает следующие возможности:

* перехват всех почтовых сообщений и вложений, переданных и полученных с помощью почтовых серверов;
* настройка исключений контролируемых сообщений по почтовым адресам, с возможностью использования символов подстановки для настройки исключений;
* импорт и экспорт настроенных фильтров;
* настройка интервалов выгрузки почты при интеграции по протоколам POP3, IMAP, SMTP;
* использование шифрованного соединения для выгрузки почтовых сообщений с почтовых серверов.

# Перехват HTTP-трафика, переданного через прокси-сервер

Перехват данных, переданных по протоколам HTTP и HTTPS через прокси-сервер, выполняется путем интеграции с прокси-сервером по ICAP-протоколу. При этом обеспечиваются следующие возможности:

* перехват данных, отправляемых по протоколу HTTP(S);
* фильтрация данных, перехватываемых по протоколу HTTP(S) по набору атрибутов (IP-адрес, порт, HTTP-метод, web-поле и др.), в том числе с использованием сложных условий («И», «Или», «Не»);
* фильтрация данных, перехватываемых по протоколу HTTP(S) по IP-адресу, в том числе по диапазону адресов, с возможностью настройки белого и черного списка исключений;
* блокирования передачи исходящих сообщений по протоколу HTTP(S), содержащих определенную информацию на основании контентного и атрибутивного анализа передаваемых данных с возможностью настройки сообщения, отображаемого при блокировке;
* настройка очереди отправки данных в модуль хранения и обработки данных по максимальному размеру передаваемых элементов, максимальному числу элементов в очереди, максимальному общему размеру очереди с возможностью хранения очереди как на диске, так и в оперативной памяти;
* отображение статистики по работе модуля в реальном времени;
* импорт и экспорт правил фильтрации и блокировки.

# Перехвата данных с помощью агента

# Администрирование

Агент контроля рабочих станций - независимый программный модуль, который устанавливается на рабочие станции в сети. Централизованная установка и управление работой агентов в системе осуществляется путем соответствующих настроек Сервера контроля агентов. Сервер контроля агентов располагает следующими возможностями управления работой агентов:

* централизованная установка агентов через Консоль администратора, с возможностью установки только на конкретные рабочие станции с использованием фильтрации по имени компьютера и объектам Active Directory и возможностью настройки прав доступа, на все рабочие станции в Active Directory;
* установка агентов при помощи групповых политик;
* создание дистрибутива агентов для последующей установки вручную;
* автоматическое обновление агентов, с возможностью исключения отдельных рабочих станций из обновления;
* защита агентов от удаления;
* защита процесса агента, файлов агента и данных агента в реестре от изменения пользователем;
* скрытие процесса и сервиса, а также файлов и папок агента на компьютере пользователя;
* настраиваемые уведомления при блокировке действий пользователя;
* настройка очереди отправки данных в модуль хранения и обработки данных по максимальному размеру передаваемых элементов, максимальному числу элементов в очереди, максимальному общему размеру очереди с возможностью хранения очереди как на диске, так и в оперативной памяти;
* логирование событий агента с возможностью настройки нескольких режимов детализации: стандартный, расширенный, и возможностью полного отключения логирования;
* общая статистика всех принятых и отправленных данных от агентов;
* детализированная статистика по состоянию и активности агента с возможностями просмотра общей информации об имени компьютера, устройствах и операционной системе компьютера, детальной информацией о данных перехваченных пользователей компьютера, лога действий с компьютером и др.;
* агент поддерживает работу в автономном режиме, в случае отсутствия соединения между компонентами системы или с внешними сетями, при этом перехваченные данные хранятся в локальном хранилище с возможностями ограничения размера локального хранилища и срока хранения данных в нем;
* оптимизация нагрузки на сетевые ресурсы путем настройки расписания и скорости передачи данных агентами.

## Контролируемые каналы передачи данных

Агентский модуль выполняет перехват трафика, в том числе шифрованного, и данных, переданных по использующим шифрование протоколам, а также фиксирует активность пользователя на контролируемой рабочей станции. К общим возможностям настройки контролируемых каналов передачи данных относятся:

* индивидуальные профили настроек работы агентов как для отдельных учетных записей пользователей, компьютеров и групп Active Directory (включая домены, контейнеры и организационные единицы), так и для отдельных компьютеров, находящихся вне доменной группы Active Directory.;
* активация профиля настроек агента по следующим условиям: недоступность сервера в течении некоторого времени, активное vpn-подключение, пользовательское условие, задаваемое при помощи Lua-скрипта;
* выбор одного из режима перехвата трафика: весь трафик, только шифрованный трафик, только нешифрованный трафик;
* использование при перехвате шифрованного трафика как пользовательского SSL-сертификата в качестве корневого, так и автоматическая генерация агентом корневого SSL-сертификата;
* исключение как отдельных локальных пользователей, так и отдельных пользователей из Active Directory из процесса мониторинга;
* исключение серверов из перехвата сетевого трафика;
* исключение отдельных процессов их перехвата сетевого траффика;
* исключение отдельных IP-адресов и диапазонов из перехвата сетевого траффика.

## 5.2.1. Модуль контроля HTTP трафика

Система позволяет контролировать входящую и исходящую информацию, передаваемую по протоколу HTTP и шифрованному аналогу HTTPS и располагает следующим функционалом:

* возможность создания и гибкой настройки фильтров по параметрам HTTP-запроса для исключения из перехвата определенной исходящей и входящей информации по ряду предустановленных правил и правил, созданных пользователе;
* возможность настройки фильтрации перехвата данных по MIME-типам по ряду предустановленных правил и правил, созданных пользователе;
* возможность перехвата, блокирования и фильтрации GET/POST/PUT запросов при выборе HTTP-методов контроля переданных данных;
* перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы;
* перехват и анализ поисковых запросов пользователя;
* сохранение адресов всех страниц, посещенных пользователем;
* перехват входящих и исходящих данных веб-коммуникаций (переписки в чатах, публикация статусов, комментарии) на веб-ресурсах: Facebook, Twitter, ВКонтакте, Одноклассники;
* перехват входящих и исходящих электронных писем и вложений, переданных либо полученных через почтовые веб-сервисы (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex и т.д.);
* перехват сообщений и файлов, переданных в веб-клиентах мессенджеров: Skype, Telegram, Discord, Microsoft Teams, Slack, также перехват сообщений, переданных в веб-клиентах мессенджеров: WhatsApp, ICQ, Google Hangouts;
* автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
* возможность поиска по тексту и атрибутам сообщений и файлов, переданных по протоколу HTTP(S);
* возможность блокирования посещений веб-ресурсов, исходящих сообщений и файлов, по контенту, по набору атрибутов, а также по хеш-сумме отправляемых файлов;
* возможность настройки пользовательского сообщения про блокировки HTTP(S) трафика.

## 5.2.2. Модуль контроля FTP трафика

Система позволяет контролировать входящие и исходящие файлы, передаваемые по протоколу FTP и шифрованному аналогу, и располагает следующим функционалом:

* Перехват исходящих и входящих файлов, переданных по FTP-соединению, а также переданных по зашифрованному SSL-соединению;
* возможность настройки ограничения по размеру перехватываемых файлов;
* автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
* возможность поиска по тексту и атрибутам файлов, переданных по протоколу FTP(S), в том числе с применением шаблонов.

## 5.2.3. Модуль контроля почты

Система позволяет контролировать входящую и исходящую почту, а также вложения и располагает следующим функционалом:

* перехват почтовых сообщений, передаваемых по протоколам IMAP, POP3, SMTP, MAPI, а также по их шифрованным аналогам;
* настройка исключений из перехвата почты определенных контактов;
* перехват агентами почтовых сообщений, переданных посредством почтовых программ с поддержкой стандарта защищённой электронной почты S/MIME, при этом обеспечивается автоматическая расшифровка содержимого письма;
* перехват почтовых сообщений путем интеграции с Microsoft Outlook;
* перехват и анализ почтовых сообщений, отправленных либо полученных при помощи почтовых веб-сервисов по протоколу HTTP(S) (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex и т.д.);
* перехват и анализ файлов-вложений почтовых сообщений;
* автоматическое обнаружение почтовых сообщений и почтовых вложений, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
* блокировка агентским модулем исходящих почтовых сообщений по протоколу SMTP(S), HTTP(S), MAPI на основании заданных политик безопасности с использованием контентного и атрибутивного анализа сообщений, в том числе по дополнительным атрибутам и произвольным полям заголовка письма, а также по хеш-суммам отправляемых файлов;
* возможность сохранения электронных писем в HTML-формате и в формате, совместимом с Microsoft Outlook;
* возможность поиска по тексту и атрибутам почтовых сообщений и файлов, в том числе с применением шаблонов.

## 5.2.4. Модуль контроля переписки в мессенджерах

Система позволяет контролировать переписку пользователей, отправляемые файлы и разговоры в программах многозвенного обмена и располагает следующим функционалом:

* Перехват текстовых сообщений в мессенджерах Viber, Telegram (включая веб-версию), WhatsApp (включая веб-версию), Skype (включая веб-версию), Microsoft Lync, Microsoft Teams (включая веб-версию), Discord (включая веб-версию), Hangouts, Slack (включая веб-версию), Агент Mail.ru, ICQ10, ICQ, а также в мессенджерах использующих протоколы SIP, OSCAR, XMPP (включая XMPP по HTTP), YMSG.
* Перехват файлов, передаваемых в мессенджерах Viber, Telegram, WhatsApp, Skype (включая веб-версию), Microsoft Lync, Microsoft Teams (включая веб-версию), Discord (включая веб-версию), Slack (включая веб-версию).
* Перехват голосовых разговоров, осуществляемых через Skype (в том числе звонки Skype-to-Skype, Skype-to-phone), а также через Microsoft Lync, Viber и по протоколу SIP с сохранением разговоров в файлы формата MP3;
* возможность распознавания и перевода в текстовый формат голосовых разговоров (коммуникаций) Microsoft Lync, Skype, Viber и SIP;
* возможность воспроизведения сохраненных разговоров Microsoft Lync, Skype, Viber и SIP;
* перехват голосовых сообщений Telegram;
* возможность ограничения перехвата по отдельным учетным записям пользователей;
* автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
* возможность осуществления поиска по тексту и атрибутам сообщений и файлов, переданных черезмессенджеры, в том числе с применением шаблонов.
* перехват сообщений и файлов, переданных в веб-клиентах мессенджеров: Skype, Telegram, Discord, Microsoft Teams, Slack, также перехват сообщений, переданных в веб-клиентах мессенджеров: WhatsApp, ICQ, Google Hangouts;
* Добавлена возможность перехвата голосовых разговоров в программе Zoom.
* Добавлена возможность контроля переписок и постов в новой версии социальной сети Facebook.
* Добавлена возможность контроля переписок, электронной почты и файлов в CMS Bitrix24.
* Добавлена возможность контроля переписок и постов в социальной сети LinkedIn.
* Добавлена возможность контроля переписок в социальной сети Instagram.
* Добавлена возможность перехвата голосовых разговоров в мессенджере Telegram.
* Добавлена возможность перехвата голосовых сообщений и файлов в web- и dekstop-версиях мессенджера WhatsApp.

## 5.2.5. Модуль контроля печати

Система контролирует печать документов отправляемых на сетевые, локальные и виртуальные принтеры, и располагает следующим функционалом:

* перехват отправляемых на печать документов агентами, установленными на рабочих станциях пользователей;
* возможность перехвата документов, отправляемых на сетевые, виртуальные и локальные принтеры (в том числе подключенные к COM-, LPT-портам);
* возможность перехвата печати в XPS-формат;
* возможность настройки исключений из перехвата по отдельным принтерам;
* возможность ограничения перехвата печати по количеству страниц и по размеру документа;
* возможность исключения процессов для модуля перехвата печати на принтерах.
* извлечение и анализ текста отправленных на печать документов;
* автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
* возможность блокировки печати по названию документа. текстовому содержимому документа и по названию принтера;
* возможность поиска по тексту и атрибутам отправленных на печать файлов, в том числе с применением шаблонов;
* сохранение в PDF- и XPS-формате.
* возможность блокировки документов, отправляемых на печать как по набору атрибутов, так и по содержимому документа, отправляемого на печать.

## 5.2.6. Модуль контроля внешних устройств и накопителей

Система позволяет контролировать использование накопителей и устройств пользователями, и располагает следующим функционалом:

* Теневое копирование файлов, отправляемых на внешние накопители (съемные жесткие диски, флеш-накопители, карты памяти, съемные накопители, CD/DVD и флоппи-диски и т.д.);
* аудит событий копирования файлов на внешние накопители (съемные жесткие диски, флеш-накопители, карты памяти, съемные накопители, CD/DVD и флоппи-диски и т.д.), фиксируется имя файла, пользователь, дата, время и данные устройства;
* возможность настройки исключений из теневого копирования и аудита по размеру и расширению файлов;
* возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
* возможность настройки размера хранилища для теневых копий на контролируемых компьютерах;
* возможность блокирования записи файлов на съёмные носители по содержимому передаваемой информации и другим атрибутам.
* возможность настройки исключений из теневого копирования и аудита для определенных внешних накопителей информации (по типам устройств, идентификаторам, производителям, названиям, серийным номерам);
* контроль доступа к внешним накопителям информации, с возможностью запрета на использование устройств с определенными параметрами (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства и др.);
* управление правами записи на внешние накопители с возможностью запрета записи на определенные устройства (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства), а также запрета записи файлов с определенным расширением;
* возможность контроля копирования информации на внешние накопители как в локальных, так и терминальных пользовательских сессиях;
* исключение отдельных процессов из процедуры контроля, аудита теневого копирования.
* контроль доступа и аудит использования внешних устройств любого типа из списка поддерживаемых (USB Bus Devices (hubs and host controllers), CD\DVD, Audio, Network Adapters,Serial and parallel ports, SCSI and RAID controllers, Floppy drives, Cameras and scanners, Windows Portable Devices (WPD), Universal cameras), подключаемых к рабочей станции, с фильтрацией по набору параметров (название устройства, идентификатор устройства, идентификатор производителя, идентификатор продукта, производитель, серийный номер, тип устройства);
* добавление в фильтр исключений устройств, подключенных на контролируемых рабочих станциях;
* автоматическое обнаружение случаев использования внешних устройств с указанными параметрами (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
* автоматическое обнаружение случаев передачи на внешние накопители файлов в целом и, в частности, содержащих определенную информацию (на основании заданных политик безопасности), с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
* возможность поиска по тексту и атрибутам отправленных на внешние накопители файлов, в том числе с применением шаблонов.

## 5.2.7. Модуль контроля облачных хранилищ

Система обеспечивает следующие возможности по контролю облачных хранилищ (iCloud, Dropbox, Google Drive, OneDrive, Диск-О (в т.ч. Облако Mail.ru), Яндекс.Диск):

* аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, имя пользователя, дата, время и имя облачного сервиса хранения;
* теневое копирование файлов, отправляемых в облачные хранилища пользователем либо процессом;
* настройка аудита и теневого копирования только исходящих, только входящих, либо всех файлов;
* возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
* возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
* контроль доступа к отдельным облачным хранилищам с возможностью запрета доступа для определенных пользователей;
* контроль доступа к отдельным облачным хранилищам с возможностью настройки режима «только чтение» для определенных пользователей;
* управление правами передачи данных в облачные хранилища с возможностью запрета отправки файлов определенных форматов;
* возможность настройки исключений из аудита, теневого копирования и контроля доступа по расширениям файлов;
* автоматическое обнаружение переданных в облачные хранилища файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
* аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, имя пользователя, дата, время и имя облачного сервиса хранения;
* возможность поиска по тексту и атрибутам отправленных файлов, в том числе с применением шаблонов.

## 5.2.8. Модуль контроля сетевых ресурсов

Система позволяет контролировать использование пользователями сетевых ресурсов, и располагает следующим функционалом:

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

## 5.2.9. Модуль блокировки передачи данных

Система обеспечивает оперативное реагирование на случаи нарушения политик безопасности организации, путем блокировки чувствительных данных, отправляемых по протоколам HTTP, MAPI, SMTP, а также на печать, в режиме реального времени. Система располагает следующими возможностями:

* блокировка данных, передаваемых по протоколу HTTP, на основании анализа содержимого (контентный анализ) с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др. При этом обеспечивается возможность блокировать по содержимому такие операции как отправка сообщений и файлов в почтовых веб сервисах и социальных сетях, поиск информации в интернете, и многие другие;
* блокировка данных, передаваемых по протоколу HTTP, на основании анализа атрибутов (контекстный анализ) с использованием таких атрибутов как: IP-адрес, порт, факт использования шифрованного соединения, HTTP-метод, параметры web-поля, атрибуты файла и др.
* блокировка файлов, передаваемых по протоколу HTTP, на основании хеш суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы;
* блокировка почты, отправляемой по протоколу SMTP, на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.;
* блокировка почты, отправляемой по протоколу SMTP, на основании анализа атрибутов (контекстный анализ) письма и вложений с использованием таких атрибутов как: IP-адрес, порт, отправитель, получатель, атрибуты файла и др.
* блокировка вложений, передаваемых по протоколу SMTP, на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы;
* блокировка почты, отправляемой по протоколу MAPI, на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.;
* блокировка почты, отправляемой по протоколу MAPI, на основании анализа атрибутов (контекстный анализ) письма и вложений с использованием таких атрибутов как: IP-адрес, порт, отправитель, получатель, атрибуты файла и др.
* блокировка вложений, передаваемых по протоколу MAPI, на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы;
* блокировка документов, отправляемых на печать, на основании анализа содержимого (контентный анализ) документа с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.;
* блокировка документов, отправляемых на печать, на основании анализа атрибутов (контекстный анализ) печати с использованием таких атрибутов как: компьютер, домен, пользователь, время, день недели и др.
* возможность уведомления конечного пользователя при блокировке, с настраиваемым текстом уведомления;
* возможность уведомления офицера безопасности о блокировке печати;
* возможность поиска по атрибутам заблокированной информации.

## 5.2.10. Модуль снимков экрана

Система позволяет контролировать активность рабочего стола пользователя при помощи снятия снимков экрана, и располагает следующими возможностями:

* возможность снятия скриншотов с заданным интервалом с точностью до секунды;
* возможность снятия скриншотов при смене активного окна;
* возможность снятия скриншотов при смене вкладки браузера;
* возможность снятия скриншотов при запуске процесса;
* возможность снятия скриншотов при срабатывании правила блокировки;
* возможность снятия скриншотов при нажатии клавиши Print Screen;
* возможность отключения снятия скриншотов при простое рабочей станции.
* возможность настройки качества скриншотов, в том числе сохранения в черно-белом формате;
* возможность настройки размера скриншотов (в процентах от оригинала);
* возможность настройки формата скриншотов (JPEG, PNG);
* сохранение специальной отметки в случае невозможности снятия скриншота (сессия пользователя отключена, заблокирована и т.п.);
* возможность отключения снятия скриншотов при посещении заданных сайтов в браузере;
* возможность снятия скриншотов только для заданных активных процессов;
* возможность экспорта скриншотов во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к просмотру перехваченных данных через веб-браузер;
* возможность сохранения скриншотов отдельного пользователя за день (или за выбранный временной интервал) в виде набора графических файлов, либо объединенных в один PDF- или видеофайл.

## 5.2.11. Модуль видеомониторинга

Система позволяет контролировать активность пользователя при помощи снятия видео рабочего стола, а также видео с вебкамеры, и располагает следующими возможностями:

* подключение к монитору компьютера пользователя и просмотр видео рабочего стола в режиме реального времени;
* мониторинг рабочих столов нескольких пользователей одновременно;
* возможность вывода окна просмотра на отдельный экран;
* автоматическая запись видеоизображения рабочего стола и видео с подключенной веб-камеры по расписанию;
* запись видео рабочего стола вручную;
* возможность настройки качества записи;
* возможность как записи видео в цветном, так и в черно-белом формате;
* возможность сохранения записей нескольких пользователей одновременно;
* возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

## 5.2.12. Модуль аудиомониторинга

Система позволяет контролировать активность пользователя при помощи записи аудио с микрофона и аудио, поступающего на динамики рабочей станции, и располагает следующими возможностями:

* подключение к микрофонам контролируемых рабочих станций с возможностью прослушивания аудиопотока в режиме реального времени;
* прослушивание микрофонов нескольких пользователей одновременно;
* автоматическая запись поступающего с микрофона аудиопотока и системных звуков компьютера по расписанию;
* запись вручную;
* возможность сохранения записей нескольких пользователей одновременно;
* возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

## 5.2.13. Модуль мониторинга пользовательской активности

Система позволяет контролировать активность пользователя на рабочем месте, и располагает следующими возможностями:

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

## 5.2.14. Модуль браузер активности

Модуль браузер активности позволяет вести комплексую статистику по активности контролируемых пользователях в следующих браузерах: Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Tor, Yandex браузер, Rambler, Amigo, Chromium, Microsoft Edge. Модуль располагает следующими возможностями:

* контроль времени посещения веб-сайтов с помощью браузера, при этом учитывается только время работы на активной вкладке, фиксируются переходы между страницами веб-сайтов и ведется комплексная статистика времени, проведенного на различных веб-ресурсах;
* возможность настройки исключения отдельных сайтов из процесса мониторинга браузер активности;
* возможность сохранения различных типов отчетов о браузер-активности (рейтинг посещенных сайтов за день, хронология событий) за выбранный временной интервал для отдельного пользователя или для нескольких пользователей в виде PDF-файла.
* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности пользователя в браузере (например, «Время пребывания пользователя на определенном сайте через браузер превысило 1 час за день» и т.д.);

## 5.2.15. Модуль контроля буфера обмена

Система позволяет контролировать использование пользователями буфера обмена, и располагает следующими возможностями:

* теневое копирование помещаемой в буфер обмена текстовой информации с фиксацией приложения, из которого данная информация была помещена в буфер обмена, и времени события;
* аудит файлов, помещаемых в буфер обмена;
* теневое копирование графического содержимого помещаемого в буфер обмена;
* теневое копирование файлов помещаемых в буфер обмена;
* возможность ограничения максимального объема данных, перехватываемых из буфера обмена;
* возможность исключения отдельных процессов из мониторинга буфера обмена;
* автоматическое обнаружение определенной информации (на основании заданных политик безопасности), помещаемой в буфер обмена, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
* возможность блокирования как копирования, так и вставки файлов по содержимому, в соответствии с настроенными правилами безопасности.
* возможность поиска по тексту, помещаемому пользователями в буфер обмена, в том числе с применением шаблонов.

## 5.2.16. Модуль контроля ввода с клавиатуры

Система позволяет контролировать ввод пользователя с клавиатуры, и располагает следующими возможностями:

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

## 5.2.17. Модуль индексации рабочих станций

Система позволяет контролировать файлы, хранящиеся в файловой системе рабочей станции, и располагает следующими возможностями:

* автоматическое сканирование файловых систем контролируемых рабочих станций на предмет наличия документов, которые носят статус конфиденциальных либо представляют интерес в рамках обеспечения информационной безопасности;
* формирование банков конфиденциальных документов, поиск которых должен выполняться во время сканирования;
* возможность автоматического импорта в банк конфиденциальных документов подготовленных хеш-функций из файлов txt- и csv-формата;
* возможность выбора рабочих станций и пользователей, чьи файловые системы будут контролироваться;
* гибкая настройка правил выбора файлов и папок, подлежащих автоматической проверке;
* исключение из сканирования файлов настраиваемого размера;
* возможность выполнения проверок файловой системы по расписанию;
* возможность создавать индивидуальные политики контроля за содержимым файловых систем для отдельных пользователей и рабочих станций, в том числе с применением шаблонов;
* возможность поиска документов в файловых системах контролируемых рабочих станций по атрибутам файлов и значениям их хеш-функций.

# Модуль хранения и обработки данных

За хранение и обработку данных отвечает Центральный сервер. Настройки сервера позволяют подключать хранилища информации под управлением ряда СУБД, управлять данным в территориально распределенных организациях при помощи репликации данных, создавать правила сохранения данных определенных типов в заданные хранилища и формировать группы ротации баз данных. Хранение и обработка данных характеризуется следующим функционалом:

* возможность хранения всех собираемых системой данных в СУБД Microsoft SQL Server, Oracle, PostgreSQL версии 9.3 и выше, MySQL версии 5.7.09 и выше, SQLite (на выбор);
* встроенная СУБД SQLite в комплекте поставки;
* хранение всех перехватываемых данных вне зависимости от срабатывания политик безопасности;
* поддержка работы с базами данных, расположенных на разных серверах;
* возможность сохранения файлов на диск сервера, а не в базу, с возможностью исключения из сохранения на диск файлов малого размера, при этом в базу данных помещаются относительные пути к файлам;
* возможность отключения распознавания изображений, печатей и речи для отдельных баз данных;
* возможность настройки длительности хранения информации в базе данных в группе ротации, в том числе установки различной длительности хранения для различных типов данных (например, хранить почтовую переписку за последние 60 дней, а переписку через мессенджеры – за последние 30 дней);
* возможность отключения базы данных вручную через Консоль администратора, при этом содержимое базы данных сохраняется;
* возможность очистки содержимого базы данных вручную через Консоль администратора;
* возможность архивирования баз данных с последующим подключением к системе для осуществления ретроспективного поиска в них критичной информации;
* возможность выборочного удаления пользователем перехваченной информации;
* возможность объединять одиночные базы данных в группы, поддерживающие кольцевую ротацию баз, при этом поисковые операции выполняются по всем базам данных в группе, а запись данных происходит только в активную;
* возможность настройки нескольких условий ротации баз данных: общий объем данных, размер базы данных, размер поисковых индексов, размер файлов на диске, временной интервал, количество записей, при этом запуск процесса ротации может быть настроен на определенный временной промежуток;
* возможность настроить выполнение скриптов до начала процесса ротации, после завершения ротации, и при ошибке ротации, при этом поддерживаются выполнение cmd, PowerShell, Script Host, Python скриптов;
* возможность балансировки нагрузки по двум и более группам баз данных либо базам данных согласно алгоритму "round robin": все поступающие в систему данные записываются в базы данных поочерёдно;
* поддержка режима параллельной обработки данных, перехваченных по различным каналам передачи информации, что позволяет повысить производительность системы при выполнении операций обновления, удаления и поиска данных;
* возможность настройки резервного хранилища агентского модуля в части ограничения размера и максимального периода хранения информации;
* возможность настройки правил записи данных в базы данных и группы ротации для регуляции, в какое хранилище записывать информацию в зависимости от часового пояса данных, типа данных, источника данных, вхождения пользователя или компьютера в домен или любой AD-контейнер по его имени, SID или GUID, IP-адреса и другой атрибутной информации;
* возможность автоматической репликации поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера в территориально распределённых организационных структурах;
* защита от некорректной настройки репликации, когда данные возвращаются на реплицирующий сервер и далее реплицируются повторно;
* возможность перенаправления поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;
* возможность настройки расписания для репликации данных;
* возможность хранения очереди репликации данных на диске для обеспечения сохранности и целостности реплицируемых данных в случае отказа системы;
* при переполнении очереди репликации сервер блокирует прием новых данных;
* возможность пропуска репликации при переполнении очереди;
* отображение статистики репликации данных;
* возможность хранения на диске очереди данных, поступающих от агентов, что повышает их сохранность по сравнению с хранением в оперативной памяти;
* возможность выбора режима очистки и обновления поисковых индексов (ручной и автоматический режимы);
* возможность индексации содержимого заголовков перехватываемых писем, при этом поддерживается фильтрация полей заголовков писем, значения которых будут индексироваться
* настройка максимальной скорости передачи перехваченных данных от агента на сервер;
* возможность осуществления асинхронного поиска по перехваченным данным (при проведении параллельного поиска по нескольким каналам передачи информации, отображение результатов выполняется по мере их получения);
* просмотр комплексной статистики по хранящимся и индексируемым данным в базах данных и группах ротации.

Система индексирует файлы следующих форматов:

* Adobe Acrobat (\*.pdf)
* Ami Pro (\*.sam)
* Ansi Text (\*.txt)
* ASCII Text
* ASF (метаданные) (\*.asf)
* CSV (Comma-separated values) (\*.csv)
* DBF (\*.dbf)
* DjVu
* DWG
* DXF
* EBCDIC
* EML files (электронные письма, сохраненные Outlook Express) (\*.eml)
* Enhanced Metafile Format (\*.emf)
* Eudora MBX файлы сообщений (\*.mbx)
* Flash (\*.swf)
* GZIP (\*.gz)
* HTML (\*.htm, \*.html)
* JPEG (метаданные) (\*.jpg)
* Lotus 1-2-3 (\*.wk?, \*.123)
* MBOX архивы электронных писем (включая Thunderbird) (\*.mbx)
* MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (\*.mht)
* Microsoft Access (\*.mdb)
* Microsoft Access 2007 (\*.accdb)
* Microsoft Document Imaging (\*.mdi)
* Microsoft Excel (\*.xls)
* Microsoft Excel 2003 XML (\*.xml)
* Microsoft Excel 2007 (\*.xlsx)
* Microsoft Open XML Paper Specification (\*.oxps)
* Microsoft Outlook (OST)
* Microsoft Outlook Express 5 и 6: базы сообщений (\*.dbx)
* Microsoft PowerPoint (\*.ppt)
* Microsoft Rich Text Format (\*.rtf)
* Microsoft Searchable Tiff (\*.tiff)
* Microsoft Word 2003 XML (\*.xml)
* Microsoft Word 2007 (\*.docx)
* Microsoft Word for DOS (\*.doc)
* Microsoft Word for Windows (\*.doc)
* Microsoft Works (\*.wks)
* MIME-сообщения
* MP3 (метаданные) (\*.mp3)
* MSG files (электронные письма, сохраненные Outlook) (\*.msg)
* Multimate Advantage II (\*.dox)
* Multimate version 4 (\*.doc)
* OpenOffice версий 1, 2 и 3: документы, электронные таблицы и презентации (\*.sxc, \*.sxd, \*.sxi, \*.sxw, \*.sxg, \*.stc, \*.sti, \*.stw, \*.stm, \*.odt, \*.ott, \*.odg, \*.otg, \*.odp, \*.otp, \*.ods, \*.ots, \*.odf) (включая OASIS Open Document Format для офисных приложений)
* OST (внутренний формат Microsoft Outlook)
* Quattro Pro (\*.wb1, \*.wb2, \*.wb3, \*.qpw)
* TAR (\*.tar)
* TIFF (\*.tif)
* TNEF (winmail.dat)
* Treepad HJT (\*.hjt)
* Unicode (UCS16, порядок байтов Mac или Windows, или UTF-8)
* Windows Metafile Format (\*.wmf)
* WMA видео (метаданные) (\*.wma)
* WMV видео (метаданные) (\*.wmv)
* WordPerfect (5.0 и выше) (\*.wpd, \*.wpf)
* WordPerfect 4.2 (\*.wpd, \*.wpf)
* WordStar 2000
* WordStar версий 1, 2, 3, 4, 5, 6 (\*.ws)
* Write (\*.wri)
* XBase (включая FoxPro, dBase и другие совместимые с XBase форматы) (\*.dbf)
* XML Paper Specification (\*.xps)
* XSL
* XyWrite
* ZIP (\*.zip)

# Анализ данных

Система располагает широким спектром возможностей анализа перехваченных данных: контентный анализ, атрибутивный анализ, статистический анализ, событийный анализ, поведенческий анализ, распознавание речи, распознавание изображений.

Контентный анализ:

* поиск по словам и словосочетаниям с учетом морфологии, с возможностью отключения;
* поиск по словам и словосочетаниям с учетом расстояния между словами;
* поиск по словам и словосочетаниям с учетом порядка слов;
* поиск по словам и словосочетаниям с учетом транслитерации кириллических символов латинскими,
* поиск по словам и словосочетаниям с возможностью нечеткого поиска, для поиска ключевых слов, в том числе написанных с ошибками и опечатками;
* технология поиска регулярных выражений, используемая для обнаружения фиксированных последовательностей символов, например, номеров паспортов, номеров банковских карт и т.п.;
* возможность использования предустановленных регулярных выражений и создания пользовательских;
* поиск по тематическим словарям с учетом морфологии (возможность отключения) и поддержкой масок и регулярных выражений в словарях, с возможностью настройки порога срабатывания (например, при обнаружении любых 3 из 10 слов или выражений, содержащихся в словаре);
* возможность использования предустановленных словарей и создания пользовательских;
* технология поиска по цифровым отпечатки документов с возможностью указания процента совпадения;
* создание цифровых отпечатков документов или папок с документами для последующего обнаружения в перехваченных данных похожих документов – с возможностью указания процента совпадения);
* создание цифровых отпечатков CSV-файлов, с выбором полей со значимой информацией для добавления в банк данных;
* создание цифровых отпечатков баз данных, при помощи настройки подключения системы к базе данных, для создания цифровых отпечатков определенных полей выбранных таблиц с целью последующего обнаружения утечки информации из этой базы данных (например, при одновременном обнаружении персональных данных из связки полей «ФИО + паспортные данные»);
* создание и обновление цифровых отпечатков баз данных осуществляется без промежуточных действий, таких как выгрузка базы данных в файл-источник цифрового отпечатка. При внесении изменений в базу данных система автоматически обновляет соответствующие цифровые отпечатки.

**Атрибутивный анализ:**

* анализ атрибутов документов, таких как «имя документа», «адрес получателя электронной почты», «пользователь», «учетная запись IM-клиента», «дата», «время», «день недели», «размер», «тип данных», «компьютер», «домен», «IP-адрес» и др.;
* анализ атрибутов документа по статусам, таким как пересылка документа по защищенному протоколу, шифрованного или защищенного документа, поврежденных данных, отправка вызвавших блокирование данных либо переданных в индивидуальном порядке данных и др.;
* анализ атрибутов процессов, таких как: имя исполняющего файла, полный путь к файлу, заголовок окна процесса и др.;
* анализ атрибутов перехваченной почты, таких как: отправитель, получатель, число получатель, заголовка письма и др;
* анализ атрибутов перехваченной переписки в мессенджерах, таких как: локальный идентификатор пользователя, удаленный идентификатор пользователя, число сообщений, тип данных, и др;
* анализ атрибутов контролируемых устройств, таких как: название устройства, производитель, тип устройства, идентификатор производителя, идентификатор продукта, тип устройства, серийный номер и др;
* анализ атрибутов печати, таких как: тип документа, название принтера, число распечатанных страниц и др;

**Распознавание изображений:**

* система обеспечивает возможность извлечения текстовой информации из файлов графических форматов (BMP, JPEG, PNG, TIFF, GIF и другие), а также из файлов формата PDF, DjVu, OXPS путем оптического распознавания символов (OCR);
* к извлеченному тексту могут быть применены все соответствующие инструменты контекстного и атрибутивного анализа;

**Распознавание печатей:**

* система обеспечивает возможность обнаружения печатей на изображениях по заданным эталонам;
* к обнаруженным печатям могут быть применены все соответствующие инструменты атрибутивного анализа;

**Распознавание речи:**

* система обеспечивает возможность извлечения текстового содержимого из аудиофайлов разговоров перехваченных в мессенджерах Skype, Microsoft Lync,Viber, а также в программах IP-телефонии использующих протокол SIP;
* к извлеченному тексту могут быть применены все соответствующие инструменты контекстного и атрибутивного анализа;

**Статистический анализ:**

* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по отправленным/полученным пользователем электронным письмам (например, «пользователь получил более 10 писем за час» или «пользователь отправил менее 20 писем за день» и т.д.);
* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по отправленным/полученным пользователем файлам (например, «пользователь получил более 10 файлов за час» или «пользователь отправил более 20 файлов за день» и т.д.);
* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по голосовым переговорам в IM-клиентах (например, «время голосовых переговоров пользователя в IM-клиентах за день превысило 1 час» или «пользователь совершил более 10 звонков за день» и т.д.);
* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по переписке пользователя в IM-клиентах (например, «пользователь провел более 10 сессий переписки за день» или «пользователь отправил более 100 сообщений за день» и т.д.);
* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по посещенным пользователем URL (например, «пользователь посетил более 100 URL за день», «пользователь посетил более 1000 URL за неделю» и т.д.);
* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по поисковым запросам пользователя (например, «пользователь отправил более 100 поисковых запросов в период с 13:00 до 15:00» и т.д.);
* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по данным, отправленным пользователем на печать (например, «пользователь распечатал более 10 документов за день» или «пользователь распечатал более 1000 страниц за неделю» и т.д.);
* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности/простоя ПК (например, «ПК бездействовал в течение более 3 часов за день», «начало активности ПК зафиксировано позже 10:30» и т.д.);
* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени работы пользователя с определенными приложениями (например, «пользователь работал в Microsoft Word в течение более 5 часов за день» или «пользователь работал в приложении “Пасьянс Косынка” в течение более 70% рабочего времени» и т.д.);
* возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности пользователя в браузере (например, «Время пребывания пользователя на определенном сайте через браузер превысило 1 час за день» и т.д.);

**Событийный анализ**

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

**Поведенческий анализ:**

* система позволяет формировать модели поведения сотрудников и задавать им соответствующий уровень риска;
* система позволяет информировать специалистов отдела безопасности об уровне риска и об инцидентах политик безопасности, которые вызвали изменения уровня риска;
* система позволяет офицеру безопасности исследовать аномалии в поведении сотрудников в режиме реального времени.

**Категории приложений:**

* система относит приложения, используемые контролируемыми пользователями к категориям в соответствии с настройками системы.
* категориззация приложений осуществляется с учетом следующих атрибутов приложений: хеш сумма исполняемого файла, имя исполняемого файла, имя продукта, описание приложения, версия приложения, имя компании разработчика приложения.
* Категоризация осуществляется с учетом следущих видов хеш-сумм исполняемых файлов: MD-5, SHA-1, SHA-256, CRC-32.

**Категории сайтов:**

* система относит сайты, посещенные пользователями к категориям в соответствии с настройками системы.
* категориззация сайтов осуществляется с учетом доменой части и пути в адресе перехваченного сайта.

**Продуктивность сайтов и приложений:**

* система позволяет оценивать продуктивность использования рабочего времени сотрудниками, которое они проводят на сайтах и при работе в приложениях.
* система позволяет устанавливать один из доступных классов продуктивности: продуктивно, непродуктивно, нейтрально.

# Распознавание изображений

Система позволяет осуществлять анализ текстового содержимого графических данных при помощи технологии OCR:

* система обеспечивает возможность извлечения текстовой информации из файлов графических форматов (BMP, JPEG, PNG, TIFF, GIF и другие), а также из файлов формата PDF, DjVu, OXPS путем оптического распознавания символов (OCR);
* система обеспечивает возможность обнаружения печатей на изображениях по заданным эталонам;
* по извлеченному тексту может быть произведен поиск с использованием инструментов контекстного и атрибутивного анализа;
* по обнаруженным печатям может быть произведен поиск с использованием инструментов атрибутивного анализа;
* пользователю на выбор доступны два средства распознавания Nicomsoft OCR и ABBYY FineReader;
* настройка очереди распознавания изображений по максимальному числу элементов в очереди, максимальному общему размеру очереди;
* поддержка много поточного распознавания печатей и текста из изображений;
* возможность настройки максимального времени распознавания одного документа;
* возможность настройки области распознавания в много страничных документах.

# Распознавание речи

Система позволяет осуществлять анализ текстовое содержимое перехваченных аудиоразговоров:

* система обеспечивает возможность извлечения текстового содержимого из аудиофайлов разговоров перехваченных в мессенджерах Skype, Microsoft Lync,Viber, а также в программах IP-телефонии использующих протокол SIP;
* пользователю на выбор доступны четыре средства распознавания одно встроенное: Sphinx, и три облачных: Wit.ai, Yandex SpeechKit, Goolge Clooud Speech-to-text.
* по извлеченному тексту может быть произведен поиск с использованием инструментов контекстного и атрибутивного анализа;
* настройка очереди распознавания изображений по максимальному числу элементов в очереди, максимальному общему размеру очереди;
* поддержка много поточного распознавания речи изображений;
* возможность настройки максимального времени распознавания одного документа;

# Управление контролируемыми пользователями

* создание внутренних карточек пользователей, содержащих всю идентификационную информацию контролируемых пользователей;
* возможность создания пользовательских карточек без выделения лицензий на соответствующих пользователей, например, создание карточки для внешнего пользователя с целью отслеживания его общения с внутренними абонентами; в случае увольнения сотрудника – возможность сохранения карточки пользователя для контроля его последующего общения с сотрудниками компании;
* отсутствие ограничений по количеству профилей пользователей в базе программы;
* возможность привязки к пользовательской карточке общей информации о пользователе: ФИО, организация, подразделение, должность, телефоны, адрес и др.,
* возможность автоматической привязки данных пользователя, из Active Directory (адреса электронной почты, названия организации, подразделения и должности пользователя, описания и фотографии пользователя);
* возможность аутентификации пользователей, работающих с системой, на основании внутренних учетных записей (с запросом имени и пароля пользователя при входе в систему);
* политика сложности и срока действия паролей в режиме внутренней аутентификации;
* возможность двухфакторной аутентификации пользователя при сохранении изменений серверных компонентов;
* возможность аутентификации пользователей, работающих с системой, на основании их учетных записей Windows;
* возможность автоматической привязки идентификационных данных пользователя (используемые идентификаторы Slack, номера ICQ, учетные записи Google Hangouts, Skype, Telegram, Viber, WhatsApp, Yahoo, ID социальных веб-сетей, SIP, адреса электронной почты, включая учетные записи XMPP и Microsoft Lync, а также IP-адреса и фотографии), к профилю пользователя для последующей идентификации;
* возможность разграничения прав доступа как к отдельным компонентам системы, так и к перехваченным данным отдельных пользователь для различных групп с назначением ролей (например, «системный администратор»- доступ только к изменению технических параметров системы – без доступа к просмотру перехваченной информации; «руководитель подразделения»– доступ только к просмотру информации об активности определенных сотрудников – без доступа к просмотру информации об инцидентах или об активности других сотрудников; «офицер безопасности»– доступ только к политикам безопасности и инцидентам – без доступа к просмотру информации об активности сотрудников, и т.п.) с использованием системы аутентификации пользователей;
* возможность интеграции с Active Directory с указанием доменов (объектов доменов) и контроллеров доменов, с которыми будет выполняться синхронизация;
* синхронизация пользователей Active Directory c возможность. автоматического создания и удаления карточек пользователей, при добавлении и удалении записей в Active Directory, с автоматическим создание карточек при обнаружении ранее неизвестной пользовательской информации;
* автоматическая синхронизация изменений идентификационных данных пользователей в Active Directory с данным в карточках пользователей возможностью настройки расписания синхронизации и синхронизируемых данных;
* ведение журнала действий и авторизации пользователей, работающих с системой.

# Мониторинг работоспособности системы

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

* ведение журнала событий серверных компонентов системы;
* просмотр журнала, а также детальной информации и рекомендаций по каждому событию в консоли администратора;
* фильтрация событий в журнале по дате, уровню события (информация, предупреждение, ошибка), серверному компоненту, источнику событий;
* выбор определенных серверов источников событий для ведения мониторинга;
* автоматическая очистка журнала по сроку хранения собтыий и их уровню;
* возможность экспорта и печати списка событий;
* автоматическое уведомление администратора системы о новых событиях серверных компонентов по почте;
* настройка правил отправки уведомлений по почте (выбор адресата, серверного компонента, уровня события или конкретных событий).

# Поиск информации

Инструменты поиска информации позволяют создавать поисковые запросы высокой детализации. Система предлагает два режима поиска поиск информации и комбинированный поиск. Поиск информации предназначен для оперативного поиска информации с использованием наиболее популярных инструментов. Комбинированный поиск предназначен для детального поиска по перехваченным данным с использованием всех доступных инструментов поиска. Система предоставляет следующие возможности:

* поиск информации по перехваченным данным с использованием всех доступных инструментов анализа: контентный анализ, атрибутивный анализ, поиск по распознанным изображениям, печатям, распознанной речи, событийный анализ и др.;
* поиск информации и по группам Active Directory;
* поиск по цифровым отпечаткам с возможностью настройки порога срабатывания;
* поиск по словарям, с возможностью учета порога срабатывания и морфологии;
* поиск по хеш-суммам, с возможностью поиска по преднастроенным банкам хеш-сумм;
* комбинирование нескольких простых запросов при помощи логических операторов «И», «ИЛИ», «НЕ», с возможностью объединения поисковых запросов в группы;
* использование шаблонов поиска – набора поисковых условий, которые можно использовать в других поисковых запросах комбинированного поиска;
* добавление условия комбинированного поиска в избранное, для дальнейшей работы;
* импорт и экспорт условий поиска.

# Отчетность

Все перехваченные данные представляются в форме отчетов следующих видов:

**Отчет «Активность пользователей»:**

1. Вкладка «Дневная активность» наглядно представляет инциденты пользователя на временной сетке с шагом в 1 час, в том числе:

* информация о количестве отправленных и полученных писем;
* информация о количестве сессий переписки пользователя в IM-клиентах с указанием длительности и количества сообщений в каждой сессии переписки;
* информация о количестве файлов, полученных и отправленных пользователем по электронной почте, через IM-клиенты, по протоколам HTTP(S) и FTP(S), скопированных на внешние устройства, сетевые ресурсы, в облачные хранилища или распечатанных на локальных/сетевых принтерах;
* информация о количестве посещенных URL и отправленных поисковых запросов;
* информация о количестве сделанных системой снимков экрана рабочего стола пользователя;
* информация о времени работы/простоя компьютера пользователя, детальная статистика активности приложений и данные о процентном соотношении времени работы в различных приложениях;
* информация о количестве документов, помещенных в буфер обмена;
* информация о посещении веб-сайтов с помощью веб-браузера с предоставлением комплексной и детальной статистики времени, проведенного на различных веб-ресурсах;
* информация о количестве символов, введенных пользователем с клавиатуры.
* вкладка динамическая и интерактивная. Переход по ссылкам приводит непосредственно к просмотру содержимого перехваченных документов либо веб-ссылок;
* обеспечивается возможность сохранения активности пользователя во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступа к перехваченным данным в веб-браузере. В расширенных настройках сохранения выбираются форматы внутреннего хранения разных типов документов, что влияет на их отображение в ассоциированных просмотрщиках.

1. Вкладка «Статистика по активности» представляет данные, собранные по определенному пользователю за конкретный интервал времени:

* в виде графиков по отдельным типам информации (график по отправленным/полученным письмам, по количеству сессий/сообщений переписок в IM-клиентах, по количеству полученных и отправленных файлов, количеству посещенных URL и веб-запросов);
* графики по типам информации являются интерактивными и динамическими, что позволяет осуществлять переход по ссылкам (точкам на графике) непосредственно к просмотру содержимого перехваченных документов;
* сохранение статистики во внешний файл формата PDF или XPS.

1. Вкладка «Взаимосвязи» отображает с кем пользователь обменивался какой-либо информацией в течение выбранного интервала времени:

* отображение в виде графа или таблицы взаимосвязи пользователя на основании собранной по нему информации для наглядного представления круга абонентов (как внутренних, так и внешних), с которыми данный пользователь общался;
* поддержка группировки контактов пользователя по принадлежности к установленным и не распознанным контактам.
* просмотр взаимосвязей внешнего абонента с пользователями сети организации после предварительного создания карточки внешнего пользователя.
* выбор масштаба отображения отчета при просмотре в клиентской консоли (с указанием % размера от оригинала).
* возможность интерактивного перехода от просмотра схемы взаимосвязей к содержимому документов (письма, переписки, файлы и т.д.), которыми пользователь обменивался с конкретным абонентом.
* поддержка сохранения отчета о взаимосвязях в виде графа во внешний файл формата PNG.

**Отчет по пользователям:**

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

1. статистика перехвата данных, в том числе

* количество переданной и полученной пользователем информации по всем каналам передачи, включая почту и мессенджеры;
* количество посещенных сайтов и поисковых запросов;
* количество файлов, переданных/принятых по FTP;
* количество распечатанных документов и страниц;
* количество операций копирования в буфер обмена;
* количество снятых скриншотов;
* количество файлов, переданных на внешние накопители/сетевые ресурсы/облачные хранилища;
* количество нажатых клавиш клавиатуры;

1. информация об активности пользователя за компьютером, в том числе

* общее время активной работы пользователя за ПК;
* среднесуточное время активной работы пользователя за ПК;
* общее время простоя ПК;
* среднесуточное время простоя ПК;
* общее время присутствия сотрудника на работе;
* среднесуточное время присутствия сотрудника на работе;
* среднее время начала работы;
* среднее время окончания работы;
* общее количество рабочих дней;
* календарь учета рабочих дней сотрудника с указанием времени начала/окончания работы, времени активности/простоя компьютера за каждый день (с цветовым выделением фактов раннего начала работы, начала работы с опозданием, раннего окончания работы, окончания работы с задержкой);
* гистограмму по времени активности/простоя компьютера пользователя за каждый день;

1. информация об активности приложений на компьютере пользователя, в том числе

* процентное соотношение времени работы в различных приложениях (с построением круговой диаграммы);
* полный список запускавшихся приложений с указанием абсолютного времени работы в каждом из них;

1. информация о браузер-активности, в том числе

* рейтинг посещенных веб-ресурсов;
* хронология активности в веб-браузере.

1. информация о количестве зафиксированных инцидентов безопасности, инициированных пользователем, и соответствующих им правилах с различной степенью детализации.
2. информация о количестве расследуемых дел, в которые вовлечен пользователь, в том числе

* открытых;
* закрытых.

Возможность пакетного сохранения и рассылки отчетов для групп пользователей с предварительной настройкой единой формы отчета. При этом допускается как отправка одним файлом по всем пользователям, так и создание отдельного файла для каждого пользователя.

**ТОП-отчет по пользователям**

Возможность построения рейтинговых интерактивных отчетов по контролируемым каналам передачи данных и статистическим показателям за все время наблюдения или за выбранный интервал времени с указанием числа пользователей:

* возможность создания ТОП-отчета для сотрудников, входящих в группы пользователей системы либо в группы пользователей Active Directory.
* возможность настройки рейтинга по более чем 40 показателям, с отчетами вида «ТОП-10 пользователей по количеству исходящих писем» или «ТОП-20 пользователей по количеству распечатанных страниц» и т.д.
* возможность построения отчетов по количеству инцидентов безопасности за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, активность которых привела к срабатыванию правил безопасности большее количество раз;
* возможность учета как общего суммарного, так и среднесуточного значения соответствующих параметров при составлении таких отчетов (например, отчет вида «ТОП-10 пользователей по среднесуточному количеству посещенных сайтов»).

**Отчет по политикам безопасности**

Возможность построения сводных интерактивных отчетов о статистике срабатывания правил безопасности, заданных в модуле Политики безопасности:

* просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям;
* детализация отчета по дням, месяцам, за произвольный временной промежуток с просмотром итогового количества срабатываний по каждому правилу в отдельности и суммарного количества по всем существующим правилам безопасности.

**Сводный отчет по пользователям**

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

* возможность выбора показателей активности, по которым будет построен отчет;
* просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям;
* детализация отчета по дням, месяцам, за произвольный временной промежуток и просмотр сводной статистики по выбранным статистическим показателей.

**Отчет табель рабочего времени**

Отчет регистрирующий использование рабочего времени сотрудниками, с регистрацией времени прихода и ухода с работы, активного времени работы, времени присутствия сотрудников на рабочем месте.

**Отчет по активности приложений**

Комплексный отчет об использовании приложений сотрудниками. Учитывается только время работы в активных приложениях.

**Отчет по браузер активности**

Комплексный отчет об использовании рабочего времени на сайтах. Учитывается только время работы на сайтах в активной вкладке браузера.

**Конструктор отчетов**

Инструмент создания отчетов с пользовательскими настройками.

# Модуль политик безопасности

Политики безопасности предназначены для настройки системы оповещения уполномоченных лиц о случаях нарушения правил безопасности. Перехваченные данные анализируются в автоматическом режиме на основании заданного списка правил безопасности. При работе с политиками безопасности пользователю доступен следующий функционал:

* настройка правил безопасности при помощи поисковых условий с использованием всех доступных инструментов анализа: контентный анализ, атрибутивный анализ, поиск по распознанным изображениям, печатям, распознанной речи, событийный анализ и др.;
* комбинирование нескольких простых запросов при помощи логических операторов «И», «ИЛИ», «НЕ», с возможностью объединения поисковых запросов в группы;
* поиск информации по группам Active Directory;
* использование шаблонов поиска – набора поисковых условий, которые можно использовать при формировании других правил безопасности;
* правила безопасности по цифровым отпечаткам с возможностью настройки порога срабатывания;
* правила безопасности по словарям, с возможностью учета порога срабатывания и морфологии;
* поиск по хеш-суммам, с возможностью поиска по преднастроенным банкам хеш-сумм;
* статистические правила безопасности, контролирующие превышение количественные показатели активности пользователя, например, количество электронных писем, переписок в мессенджерах, посещенных сайтов, отправленных запросов, распечатанных файлов и страниц, а также вычислять периоды активности пользователей и приложений, и др.;
* добавление, исключение групп Active Directory, к которым могут быть применены политики безопасности;
* добавление, исключение, редактирование категорий и уровня риска инцидентов сервера безопасности для автоматического расчёта показателей уровней риска пользователей и поведенческого анализа;
* возможность выполнения скриптов при срабатывании или ошибке срабатывания правила безопасности;
* возможность отправки данных о инцидентах в сторонние системы;
* автоматическая доставка уведомлений по электронной почте ответственному лицу в случае срабатывания политики безопасности (выявления инцидента);
* уведомление содержит общую информацию об инциденте (название политики безопасности, пользователь, допустивший нарушение, тип перехваченных данных, дата/время инцидента и др.), а также ссылку на открытие соответствующего инцидента в пользовательской консоли либо вложения с документами, вызвавшими срабатывание политики безопасности;
* возможность настройки периодичности отправки уведомлений на электронную почту (немедленная отправка уведомления по выявлению инцидента либо накопление и порционная отправка уведомлений с заданной периодичностью – раз в час, раз в сутки и т.д.);
* возможность просмотра всех инцидентов по выбранной политике безопасности в клиентской консоли с возможностью выделения просмотренных, непросмотренных инцидентов для каждого офицера безопасности, работающего с системой;
* при просмотре информации об инциденте в клиентской консоли доступна следующая информация: пользователь, допустивший нарушение, дата и время инцидента, показатель присвоенного уровня риска, тип документа, вызвавшего срабатывание политики безопасности (электронное письмо, файл, отправленный на печать и т.д.), содержание документа (электронного письма, переписки в IM-клиенте, файла и т.д.), вызвавшего срабатывание политики безопасности, а также другая дополнительная информация.
* возможность назначения статуса для инцидента (инцидент не расследован, расследование инцидента отложено, инцидент расследован, важный инцидент, неважный инцидент, ложное срабатывание);
* возможность гибкого выборочного просмотра инцидентов по политике безопасности (например, показать только новые или непросмотренные инциденты; показать только последние 100 инцидентов; показать инциденты за ближайший месяц, но не более 20 последних; показать инциденты, имеющие статус «Важный» и зарегистрированные в течение последней недели и т.д.);
* возможность полного или выборочного удаления записей об инцидентах по политике безопасности (например, удалить все инциденты старше 10 дней; удалить последние N инцидентов; удалить все инциденты, имеющие статус «Расследован»; удалить инциденты по данным, удаленным из БД, и т.д.);
* возможность сортировки списка инцидентов по различным параметрам (по релевантности, по дате/времени, по локальному/удаленному пользователю, по типу/размеру перехваченных данных, по статусу инцидента и т.д.);
* возможность фильтрации списка инцидентов по различным параметрам: по статусам (например, отобразить только важные), по типам данных (например, отобразить только инциденты, вызванные пересылкой информации по почтовым протоколам), по состоянию (например, отобразить только непросмотренные) – и по комбинациям этих параметров;
* возможность экспорта списка инцидентов в файл форматов CSV, MS Excel, PDF, XML (при этом сохраняется следующая информация об инцидентах – тип перехваченных данных, локальный/удаленный пользователь, дата/время перехвата, размер, статус инцидента, прочая информация);
* возможность экспорта перехваченных данных, вызвавших срабатывание политики безопасности, в файлы соответствующих форматов;
* ведение журнала (лога) действий офицера безопасности с возможностью экспорта событий журнала;
* в журнале событий регистрируется следующая информация создание, дублирования, редактирование, удаление правила безопасности, просмотр и удаление инцидента, изменения статусов инцидента и др.

# Модуль расследования инцидентов

Модуль расследований позволяет организовать работу с документацией в рамках расследований инцидентов безопасности. Модуль Расследования предоставляет следующие возможности:

1. сбор доказательств по инцидентам безопасности при помощи создания дела, которое включает в себя:

* название и описание;
* дата создания дела;
* информацию об инциденте;
* перечень вовлеченных лиц и их реквизиты;
* перечень проводимых проведенных мероприятий по расследованию инцидента и их результаты;
* выводы по результатам расследований;
* материалы расследований: документы и события, перехваченные системой, внешние документы, загруженные в дело;
* реквизиты внутренних документов: тип данных, локальный пользователь, удаленный пользователь, дата перехвата, размер документа;
* материалы расследований – внешние документы;
* возможность присоединения документов к делу из других модулей системы.

1. аудита результатов перехвата обеспечивают функции:

* просмотр содержания документов в расширенном виде напрямую из дела;
* фильтрацию документов при просмотре в деле;
* представление включенных в дело документов в режимах просмотра карточки, список;
* возможность экспорта дела в форматы \*.pdf, \*.xps.
* возможность распечатки дела на принтере.

1. контроль за внесением изменений в дело при помощи журнала событий, включающего в себя информацию о всех вносимых правках:

* имя пользователя, который совершил операцию в деле;
* совершенное действие;
* дату и время совершенного действия;
* прочую дополнительную информацию, которая может быть полезна для контроля за ведением дела.

1. в целях упрощения работы лиц, ведущих расследование, система обеспечивает:

* ведение списка дел;
* возможность сортировки дел в группы;
* возможность создания групп и подгрупп с количество уровней иерархии не менее 20;
* возможность переноса дел из группы в группу простым перетаскиванием «мышкой»;
* возможность переноса подгрупп из группы в группу простым перетаскиванием «мышкой»;
* возможность удаления дел и групп;
* возможность исправления дел;
* возможность просмотра: всех дел, только открытых дел, только закрытых дел;
* возможность глубокой пользовательской настройки просмотра дел: всех дел за определенный период; дел, открытых в определенный период; дел, закрытых в определенный период;
* возможность закрепления и открепления поля списка дел;
* возможность переноса поля списка дел к любой стороне окна программы.

# Анализ рисков

Анализ рисков – это контрольно-аналитическая система, позволяющая отслеживать аномальные и потенциально опасные для организации изменения в поведении сотрудников, которая позволяет:

* формировать модели поведения сотрудников и задавать им соответствующий уровень риска;
* информировать специалистов отдела безопасности об уровне риска, поведении сотрудников и об инцидентах правил безопасности, которые вызвали изменения уровня риска;
* отслеживать изменения в поведении сотрудников в режиме реального времени при помощи количественных показателей и графиков;
* просматривать изменения уровня риска как для непросмотренных событий, так и для всех событий;
* сохранять, отправлять на печать табличный отчет по уровню риска пользователей;
* гибкая фильтрация отчета по уровням риска по дате, избранным пользователям, категории риска, уровням критичности, факта наличия риска у пользователей, текстовая фильтрация;
* графическое представление уровня риска пользователей, с возможностью отображения линейного графика либо гистограммы;
* наличие предустановленных поведенческих моделей (категорий риска), готовых к использованию.

# Прочие требования

# Масштабируемость системы

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

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

# Ориентация работы всех компонентов системы на многопоточность

Система обеспечивает полную поддержку распределения нагрузки в многоядерных и многопроцессорных системах.

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

Возможность распознавания одновременно нескольких разговоров документов при использовании модуля распознавания речи.

# Удобство администрирования

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

Система обеспечивает возможность шифрования трафика между консолями администратора и пользователя и сервером.

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

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

Существует возможность отключения автоматического управления системным брандмауэром.

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

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

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