Описание - Кибер Протего

Архитектура и системные требования

1. Программный комплекс предотвращения утечек данных Кибер Протего (далее **программный комплекс**) имеет иерархическую структуру и состоит из следующих компонентов:
    - Агент предотвращения утечек данных (далее **агент DLP**);
    - Агент обнаружения хранимых данных (далее **агент Discovery**);
    - **Консоли управления**;
    - **Сервер управления**;
    - **Content Security Server,** служащий хостом:
        - Серверу индексирования журналов событийного протоколирования и теневых копий и полнотекстового поиска (далее **Сервер поиска**);
        - Серверу обнаружения хранимых данных (далее **сервер Discovery**).
2. Компоненты Кибер Протего могут быть установлены в среды, отвечающие следующим требованиям:
    1. **Агент DLP**
        - Операционная система
            - Microsoft Windows
                - 7/8/8.1/10, Server 2008/2008 R2, Server 2012/2012 R2, Server 2016 или Server 2019;
                - Допускаются 32- и 64-разрядные версии операционной системы.
            - Mac OS
                - 10.15 (Catalina) или 11.2.3 (Big Sur).
        - Память (ОЗУ) минимум 512 МБ
        - Свободное место на жестком диске минимум 400 МБ
        - Процессор минимум Intel Pentium 4
        - Поддерживаемые средства виртуализации
            - Microsoft Remote Desktop Services (RDS), Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View, VMware Workstation, VMware Player, Oracle VM VirtualBox и Windows Virtual PC.
    2. **Агент Discovery**
        - Операционная система
            - Microsoft Windows
                - 7/8/8.1/10, Server 2008/2008 R2, Server 2012/2012 R2, Server 2016 или Server 2019.
        - Допускаются 32- и 64-разрядные версии операционной системы.Память (ОЗУ) минимум 512 МБ
        - Свободное место на жестком диске минимум 200 МБ
        - Процессор минимум Intel Pentium 4
    3. **Консоли управления**
        - Операционная система
            - Microsoft Windows
                - 7/8/8.1/10, Server 2008/2008 R2, Server 2012/2012 R2, Server 2016 или Server 2019;
                - Допускаются 32- и 64-разрядные версии операционной системы

- Память (ОЗУ) минимум 512 МБ
- Свободное место на жестком диске минимум 1 ГБ
- Процессор минимум Intel Pentium 4

4. **Сервер управления**
   - Операционная система
     - Microsoft Windows
       - Server 2008/2008 R2, Server 2012/2012 R2, Server 2016 или Server 2019;
       - Допускаются 32- и 64-разрядные версии операционной системы.
   - Память (ОЗУ)
     - Минимум 1 ГБ
     - Рекомендуется 8 ГБ
   - Свободное место на жестком диске
     - Минимум 1 ГБ
     - Рекомендуется 800 ГБ (в случае локального сервера базы данных)
   - Процессор
     - Минимум Intel Pentium 4
     - Рекомендуется 2x Intel Xeon Quad Core 2,33 ГГц
   - Сервер базы данных
     - Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017 или 2019, любой выпуск, в том числе SQL Server Express;
     - PostgreSQL версии 9.5 (9.5.19 или выше), 9.6 (9.6.15 или выше), 10 (10.10 или выше), 11 (11.5 или выше) или 12 (12.0 или выше).
     - PostgreSQL ODBC Driver версии 9.6.500 или выше. Предпочтительной является новейшая версия драйвера.
5. **Content Security Server (Сервер поиска, сервер Discovery)**
   - Операционная система
     - Microsoft Windows
       - Server 2008/2008 R2, Server 2012/2012 R2, Server 2016 или Server 2019.
       - Допускаются 32- и 64-разрядные версии операционной системы.
     - Память (ОЗУ)
       - Минимум 1 ГБ
       - Рекомендуется 8 ГБ
     - Свободное место на жестком диске
       - Минимум 1 ГБ
       - Рекомендуется 800 ГБ (в случае локального сервера базы данных)
     - Процессор
       - Минимум Intel Pentium 4
       - Рекомендуется 2x Intel Xeon Quad Core 2,33 ГГц
     - Сервер базы данных
       - Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017 или 2019, любой выпуск, в том числе SQL Server Express.

Функциональные возможности и

особенности программного комплекса

1. Программный комплекс удовлетворяет требованиям масштабируемости, не усложняя процесс наращивания компонентов программного комплекса, поддерживает использование в многосегментных и многодоменных конфигурациях (пользователи/группы из нескольких доменов).
2. Программный комплекс обеспечивает возможность предоставления пользователям управляемого доступа к устройствам и/или группам устройств, каналам сетевых коммуникаций (сетевым протоколам и сервисам) на глобальном уровне, отражая политику безопасности Заказчика, с применением различных методов контекстного анализа и анализа содержимого (контентной фильтрации), реализуемых программным комплексом в режиме реального времени.
3. Программный комплекс обеспечивает возможность обнаружения файлов с заданным содержимым на рабочих станциях, общих сетевых ресурсах и системах хранения данных с последующим применением к таким файлам опциональных действий, включая удаление контейнера при обнаружении таких данных внутри контейнера или архива, изменение прав доступа, тревожное оповещение администратора, оповещение локального пользователя, шифрование с использованием встроенных механизмов ОС.
4. Программный комплекс обеспечивает централизованное управление клиентскими модулями и применяемыми DLP-политиками. При этом для пользователей обеспечивается предоставление полномочий на основании доменных учетных записей членства в и групп, равно как и локальных учетных записей и групп. Изменение полномочий для пользователей при изменении членства в доменных группах не требует перезагрузки АРМ или изменения и распространения DLP-политик программного комплекса.
5. Конфигурационная информация, используемая агентами DLP программного комплекса, хранится локально и недоступна для модификации конечными пользователями; предоставляемые пользователям полномочия и заданные ограничения действуют всегда, независимо от подключения АРМ к локальной сети организации.
6. Программный комплекс обеспечивает возможность назначения различных наборов DLP-политик для следующих состояний работы агента DLP:
    - Online (ПК пользователя подключен к корпоративной сети, доступны контроллер домена или Сервер(ы) управления));
    - Offline (ПК пользователя отключен от корпоративной сети, контроллер домена или Сервер(ы) управления недоступны)).
7. Программный комплекс поддерживает получение данных о пользователях и группах пользователей из службы каталога Microsoft Active Directory или иных каталогов LDAP, а также опциональную возможность распространения агентов DLP и политик программного комплекса через механизмы групповых политик контроллера домена.
8. Программный комплекс поддерживает интеграцию с любыми системами класса SIEM или иными решениями, обеспечивающими ручную или автоматизированную обработку событий и инцидентов, регистрируемых программным комплексом. Для передачи данных в интегрируемые системы используются стандартные протоколы SMTP, SNMP, SYSLOG.
9. **Серверы программного комплекса обеспечивают:**
    1. Взаимодействие агентов DLP и централизованного архива событий;
    2. Распространение политик и пользовательских полномочий на агенты DLP и Discovery;
    3. Протоколирование действий администраторов программного комплекса;
    4. Поддержку ролевой модели управления серверами;
    5. Поддержку архитектуры «master-slave» для связанных баз данных с возможностью

консолидации распределенного архива из удаленных (подчиненных) серверов программного комплекса в единый централизованный архив;
6. Централизованный сбор с агентов DLP и хранение событий и файлов, переданных в режиме теневого копирования, а также видеозаписей экрана, записи нажатий клавиш и сведений о запущенных процессах;
7. Возможность формирования статистических и графических отчетов по данным журналов, хранимым в централизованном архиве событий программного комплекса, с возможностью просмотра в консоли управления и экспорта в форматах, пригодных для обработки офисным программным обеспечением;
8. Возможность формирования досье (карточки) пользователя, включающего выдачу аналитики отклонений его поведения от нормы и поведения группы, к которой он принадлежит, используя данные из журналов событий, хранимых в централизованном архиве;
9. Автоматизированный мониторинг статуса и целостности политик безопасности на контролируемых АРМ, включая возможность автоматического восстановления целостности политик безопасности при выявлении отклонений применяемых политик от эталонных;
10. Сервер Discovery обеспечивает удаленное автоматизированное сканирование и обнаружение хранимых данных на АРМ и в сетевых хранилищах, установку и удаление клиентских модулей для агентского сканирования и обнаружения хранимых данных на контролируемые АРМ;
11. Сервер поиска обеспечивает возможность ручного и автоматизированного полнотекстового поиска по централизованным базам данных теневого копирования и событийного протоколирования, включая возможность синонимического поиска, наличие языка поисковых запросов, а также функцию распознавания текста в графике.

10. **Консоли управления программным комплексом обеспечивают выполнение следующих задач:**
    1. Управление правами доступа пользователей к портам ввода/вывода, периферийным устройствам и носителям информации, к каналам сетевых коммуникаций;
    2. Управление политиками протоколирования, теневого копирования, видеозаписи экрана, записи нажатий клавиш и сведений о запущенных процессах, и тревожных оповещений для контролируемых каналов и устройств;
    3. Управление правилами и параметрами контентной фильтрации;
    4. Управление политиками сканирования и обнаружения хранимых данных;
    5. Управление параметрами функционирования агентов и серверов программного комплекса;
    6. Просмотр списков и/или содержимого файлов, полученных в режиме теневого копирования;
    7. Просмотр видеозаписей экрана, записей нажатий клавиш и сведений о запущенных процессах, полученных в режиме мониторинга активности пользователей;
    8. Просмотр журналов и отчетов;
    9. Просмотр агрегированной статистической информации по пользователям в виде досье (карточек) пользователя;
    10. Управление и доступ к результатам полнотекстового поиска по архиву данных событий и теневого копирования;
    11. Возможность централизованного управления и администрирования агентов посредством полной интеграции в корпоративную службу каталогов Active Directory.
    12. Управление компонентами программного комплекса и политиками

авторизованными администраторами в ролевой модели.

11. **Агенты DLP программного комплекса обеспечивают:**
    1. Принудительное назначение прав доступа к устройствам и каналам сетевых коммуникаций любому пользователю или группе пользователей (политики per user/group) в соответствии с заданными политиками;
    2. Возможность обновления или изменения применяемых политик на отключенных от корпоративной сети (недоступных для консоли управления в режиме онлайн) АРМ с использованием цифровой подписи;
    3. Возможность информирования пользователей о предоставлении или запрещении доступа в соответствии с заданными политиками;
    4. Предоставление пользователям доступа только к авторизированным устройствам, только к авторизованным каналам сетевых коммуникаций (Белые списки);
    5. Автоматическое принятие решения в режиме реального времени на основании результатов анализа содержимого передаваемых (печатаемых или сохраняемых) файлов и данных:
        - блокирование доступа к портам ввода/вывода и каналам сетевых коммуникаций при отсутствии соответствующих прав, при наличии запрещающих политик доступа, при детектировании недопустимого для передачи (печати, сохранения на внешнее устройство) содержимого файлов и данных (исполнение запрещающих DLP-политик);
        - предоставление (разрешение) доступа к портам ввода/вывода и каналам сетевых коммуникаций при детектировании допустимого для передачи (печати, сохранения на внешнее устройство) содержимого файлов и данных, даже если отсутствуют соответствующие права на доступ (исполнение разрешающих DLP-политик);
        - избирательное создание теневых копий передаваемых (печатаемых, сохраняемых) файлов и данных на основании результатов анализа содержимого передаваемых (печатаемых или сохраняемых) файлов и данных, с выполнением контентного анализа в момент передачи данных либо в асинхронном режиме без вмешательства в процесс передачи данных;
    6. Регистрацию событий, связанных с доступом пользователей к каналам сетевых коммуникаций и локальным устройствам, а именно попыткам (успешным и не успешным) передачи, печати и сохранения файлов и данных, включая, но не ограничиваясь, следующими данными: идентификатор пользователя, время события, документ, вызвавший срабатывание политики, политика, вызвавшая срабатывание, содержимое данных (текстовые данные, файл);
    7. Создание и промежуточное хранение теневых копий файлов и данных, передаваемых, сохраняемых и печатаемых пользователями;
    8. Создание и промежуточное хранение данных мониторинга активности пользователя (видеозаписей экрана, записи нажатий клавиш и сведений о запущенных процессах);
    9. Избирательное создание видеозаписей экрана, записи нажатий клавиш и сведений о запущенных процессах по наступлении заданных системных событий (вход в систему, работа процесса, обнаружение подключений VPN, LAN, WLAN, подключение периферийных устройств);
    10. Избирательное создание видеозаписей экрана, записи нажатий клавиш и сведений о запущенных процессах по при срабатывании DLP-политик, включая основанные на анализе содержимого при детектировании заданного содержимого в передаваемых, сохраняемых, печатаемых данных, независимо от наличия подключения АРМ к корпоративной сети/серверам.
    11. Извлечение текста из графических изображений с помощью встроенного модуля

оптического распознавания символов OCR, не требующего отдельного лицензирования или выделения отдельного сервера;
    12. Детектирование реального типа файла вне зависимости от расширения с возможностью применения избирательных политик на основании типа файла;
    13. Сканирование и обнаружение хранимых данных на контролируемом АРМ, функции устранения выявленных нарушений политики безопасного хранения данных;
    14. Возможность автоматического переключения между различными наборами DLP-политик в зависимости от наличия подключения к корпоративной сети или серверам;
    15. Невозможность изменения конечными пользователями разрешений и полномочий;
    16. Защиту от удаления программного обеспечения агента DLP с правами привилегированной учетной записи, а также проверку целостности кода исполняемого агента при загрузке и проведение действий по предотвращению бесконтрольного использования компьютера пользователем в том случае, если получен отрицательный результат;
    17. Оповещение пользователя о выполнении им несанкционированных действий;
    18. Тревожное оповещение администратора (офицера безопасности) о выполнении пользователем несанкционированных действий.
12. Агенты DLP применяют DLP-политики, заданные как для контроля периферийных устройств, так и каналов сетевых коммуникаций независимо от способа подключения контролируемого компьютера к сети Интернет или доступности корпоративной локальной сети. Это относится ко всем характеристическим опциям DLP-политик, включая функции контроля доступа, протоколирования, теневого копирования, видеозаписи экрана, записи последовательности нажатий клавиш, записи сведений о запущенных процессах, создания тревожных оповещений, анализа содержимого передаваемых (сохраняемых, печатаемых) файлов и данных, извлечения текста из графических изображений.
13. Программный комплекс обеспечивает возможность оперативного распространения политик на все или отдельно указанные АРМ (клиентские модули). Изменения в политиках вступают в действие немедленно, без необходимости перезагрузки или перерегистрации агентов DLP.
14. Программный комплекс предоставляет возможность централизованной установки агентов DLP и Discovery на АРМ конечных пользователей и передачи политик безопасности на них различными способами – как посредством Сервера или Консолей управления, так и сторонними средствами (через системы управления конфигурациями АРМ, групповые политики домена и другие). Обеспечивается возможность формирования предконфигурированных инсталляционных пакетов формата msi. Предоставляется возможность локальной установки и настройки клиентских модулей на АРМ конечных пользователей.
15. Программный комплекс обеспечивает регистрацию всех изменений конфигурации, вносимых администраторами программного комплекса, а также всех действий конечных пользователей на хостах агентов DLP.
16. Агенты DLP штатно функционируют на компьютерах под управлением актуальных версий ОС Windows, как 32-х, так и 64-битной разрядности.
17. Контроль периферийных устройств и интерфейсов поддерживается для всех операционных систем Windows, начиная с Windows 7, как 32-х, так и 64-битной разрядности, а также на компьютерах под управлением Mac OS.
18. Функции контроля периферийных устройств и интерфейсов включают:
    1. Контроль локальных устройств: Floppy, CD-ROM/DVD/BD, адаптеры Wi-Fi и Bluetooth, принтеры (локальные, сетевые и виртуальные), любые съемные носители данных

(внешние устройства хранения данных), жесткие диски, ленточные накопители, MTP-устройства, системный буфер обмена данными, устройства класса Terminal Service Devices;
2. Контроль на уровне интерфейса для USB, FireWire, Infrared, последовательный и параллельный порты;
3. Контроль устройств хранения данных, сетевых ресурсов, USB-устройств, принтеров, буфера обмена данными, последовательных портов, перенаправленных в терминальную сессию по протоколам RDP, ICA, PCoIP, HTML5/WebSockets с использованием сред виртуализации и терминального доступа MS RDP/RDS/ MS RemoteFX, Citrix XenApp, Citrix XenDesktop, Citrix XenServer, VMware View, Windows Virtual PC, Oracle VM VirtualBox;
4. Расширенный контроль протоколов синхронизации мобильных устройств (Apple iPhone/iPod touch/iPad, BlackBerry, Windows Mobile, Palm OS) с рабочими станциями с точностью до отдельных объектов в протоколах синхронизации;
5. Ведение перечня разрешенных внешних устройств хранения данных (Белый список) с идентификацией и контролем устройств по производителю, модели, уникальному серийному номеру устройства;
6. Возможность предоставления пользователям доступа к неавторизированным устройствам на указанный промежуток времени или до извлечения путем обмена кодами между администратором и пользователем, без подключения администратора к контролируемому АРМ;
7. Возможность задавать специальные политики безопасности, обеспечивающие принудительное шифрование (или запрет шифрования) съемных носителей с использованием криптографических продуктов сторонних производителей, включая встроенные средства шифрования в ОС (Windows BitLocker To Go, Apple OS X FileVault);
8. Контроль буфера обмена, включая:
9. Контроль операций обмена данными между приложениями;
10. Раздельный контроль типов данных: файлы, текстовые данные, графические данные, аудио данные, неопределенные данные;
11. Контроль операций обмена данными между гостевой и родительской ОС;
12. Контроль снимков экрана (для приложений и клавиши PrintScreen).

19. Контроль процессов печати, использования буфера обмена и записи данных на внешние устройства хранения данных осуществляется избирательно (по пользователям или группам пользователей) в реальном времени, на основании анализа параметров окружения (контекста) и/или результатов анализа содержимого (контента) файлов и данных, используемых в указанных процессах, и включает возможности:
    1. предоставления или блокировки доступа,
    2. журналирования событий,
    3. создания теневых копий передаваемых файлов и данных,
    4. видеозаписи экрана,
    5. записи нажатий клавиш,
    6. записи сведений о запущенных процессах,
    7. отправки тревожных оповещений в реальном времени.
20. Функции контроля сетевых протоколов и web-сервисов включают:
    1. Контроль доступа пользователей к каналам сетевых коммуникаций, включая стандартные почтовые протоколы (MAPI, SMTP, SMTP over SSL, IBM/Lotus Notes, Outlook Web Access и другие), сетевые протоколы HTTP, HTTPS, FTP, FTP over HTTP, SFTP, Telnet, Torrent, Tor, почтовые веб-сервисы и их мобильные версии (Почта Mail.Ru, Рамблер-Почта, Яндекс.Почта, Gmail, AOL Mail, Hotmail/Outlook.com, Outlook Web App/Access (OWA) и др.), социальные сети и их мобильные версии (Facebook,

Twitter, Google+, LinkedIn, ВКонтакте, Одноклассники и др.), сетевые сервисы файлового обмена и синхронизации (Яндекс.Диск, Облако Mail.Ru, Google Drive, Dropbox, OneDrive и др.), службы мгновенных сообщений (Skype, Telegram, Агент Mail.Ru, Zoom, Viber, Jabber, ICQ, IRC, WhatsApp, др.), звонки и частные беседы Skype, сервисы веб-поиска (Google, Яндекс, Bing, и др.), сервисы поиска работы (hh.ru, Яндекс.Работа, Rabota.ru, SuperJob.ru, Авито и др.), внутрисетевые файловые ресурсы (SMB) и др.

2. Для электронной почты, веб-почты и служб мгновенных сообщений реализован раздельный контроль сообщений и вложений.
3. Для сетевых сервисов, основанных на протоколе HTTP/HTTPS, а именно почтовые веб-сервисы и их мобильные версии, социальные сети и их мобильные версии, сетевые сервисы файлового обмена и синхронизации, службы мгновенных сообщений, сервисы веб-поиска, сервисы поиска работы политики контроля задаваются независимо от политик контроля для протокола HTTP/HTTPS.
4. Возможность назначения белых списков для сетевых протоколов, позволяющих задавать исключения на основании таких признаков, как IP-адреса, имена хостов, используемые порты, идентификаторы отправителей и получателей и др.
5. Возможность блокировки сетевых сервисов.

21. Контроль каналов сетевых коммуникаций осуществляется избирательно по пользователям или группам пользователей в реальном времени, на основании анализа параметров окружения (контекста) и/или результатов анализа содержимого (контента) файлов и данных (включая почтовые сообщения, переписку и др.) и включает возможности:
    1. предоставления или блокировки доступа,
    2. журналирования событий,
    3. создания теневых копий передаваемых файлов и данных,
    4. видеозаписи экрана,
    5. записи нажатий клавиш.
    6. записи сведений о запущенных процессах,
    7. отправки тревожных оповещений в реальном времени.
22. Осуществление функций контроля для каналов сетевых коммуникаций выполняется независимо от способа подключения контролируемого компьютера к сети Интернет или доступности корпоративной локальной сети.
23. Функции контентного анализа и фильтрации включают:
    1. контентную фильтрацию данных, отправляемых на печать, копируемых на съемные устройства хранения данных, передаваемых в/из буфера обмена данными, а также устройств и буфера обмена, перенаправленных в терминальные сессии;
    2. извлечение и фильтрацию содержимого (контента) данных из файлов и объектов, передаваемых в службах мгновенных сообщений, веб-формах, социальных сетях, электронной почте и сервисах веб-почты, в облачных файловых хранилищах и корпоративных сетевых хранилищах по протоколу SMB и т.д., в реальном времени, вне зависимости от наличия подключения контролируемого АРМ к корпоративной сети или корпоративным серверам;
    3. возможность использования результатов контентного анализа данных для избирательного предоставления доступа (блокировки или разрешения) к каналу печати, каналам сетевых коммуникаций, устройствам хранения данных;
    4. анализ и фильтрацию данных по ключевым словам с применением морфологического анализа (для русского, английского, и других языков) по целым словам или частичному совпадению, с поддержкой транслитерации для русского языка;

5. анализ и фильтрацию данных по шаблонам на базе регулярных выражений с числовыми и булевыми порогами срабатывания;
6. анализ и фильтрацию данных по встроенным комплексным шаблонам регулярных выражений (номера кредитных карт, адреса, паспортные данные и т.д.);
7. анализ и фильтрацию данных текстовых и бинарных данных с использованием технологии цифровых отпечатков, с поддержкой автоматической классификации образцов данных с учетом заданных уровней важности или секретности;
8. анализ и фильтрацию данных по расширенным свойствам документов и файлов (имя, размер, наличие парольной защиты, наличие текста, дата и время последнего изменения, титул, тема, метки и категории документа, комментарии и авторы, и др.);
9. возможность создания сложносоставных правил контентного анализа и фильтрации с использованием логических функций для их объединения;
10. оптическое распознавание символов (OCR) для русского, английского и других языков;
11. В комплекте поставки присутствуют встроенные отраслевые терминологические словари, доступные для самостоятельной модификации Заказчиком, равно как и возможность создания новых словарей.

24. Осуществление функций анализа содержимого выполняется независимо от способа подключения контролируемого компьютера к сети Интернет или доступности корпоративной локальной сети.
25. Функции контроля хранимых данных агентами и сервером Discovery включают:
    1. Автоматизированное (по расписанию) или принудительное сканирование файловых систем на АРМ пользователей, доступных пользователям сетевых хранилищ, локальных папок синхронизации облачных сервисов файлового обмена, систем хранения данных в целях выявления (обнаружения) информации (файлов), хранимых с нарушением корпоративной политики безопасного хранения данных, с последующим выполнением действий, направленных на устранение нарушений политики хранения данных;
    2. Возможность автоматического выполнения превентивных действий с обнаруженными файлами, содержащими конфиденциальную информацию, для предотвращения потенциальной утечки данных (оповещение пользователя и администратора, изменение прав доступа к обнаруженным файлам, шифрование обнаруженных файлов, удаление обнаруженных файлов);
    3. Генерацию отчета о результатах выполнения задач сканирования и обнаружения;
    4. Возможность выполнения функций сканирования и обнаружения в агентском (с установкой клиентского модуля с ограниченной функциональностью или использованием полнофункционального клиентского модуля) или удаленном (без использования клиентских модулей) режиме, путем удаленного сканирования АРМ и сетевых ресурсов непосредственно с сервера Discovery.
26. Функции полнотекстового поиска (анализа архива) Сервером поиска включают:
    1. Индексирование, выполняемое для различных форматов файлов, включая документы Microsoft Office, Adobe PDF, AutoCAD, OpenOffice, Lotus 1-2-3, WordPerfect, WordStar, Quattro Pro, архивы и репозитории электронной почты, CSV, DBF, XML, Unicode, др., в том числе вложенных в архивы различных форматов, а также для теневых копий заданий на печать в форматах PCL, Postscript и др.
    2. Индексирование и поиск, выполняемые для отдельных слов и комбинаций слов, фраз, регулярных выражений, специальных символов, численных диапазонов, полей документов, записей журналов аудита, среди журналов событийного протоколирования и теневого копирования, централизованно хранимых на серверах баз данных, используемых программным комплексом;

3. Морфологический поиск и фильтрацию «стоп-слов» для русского, английского и других языков;
4. Синонимический поиск текста для английского и русского языков;
5. Оптическое распознавание символов (OCR) в целях извлечения текста из графических файлов для его дальнейшего индексирования, без дополнительного лицензирования встроенного модуля OCR;
6. Сортировку результатов поиска: комбинация слов и фраз по логике «И», релевантность, весовые коэффициенты терминов и полей документов;
7. Возможность запуска поисковых запросов вручную или по расписанию с автоматической отправкой результатов поиска по электронной почте, в том числе с поддержкой инкрементального поиска (выявления отличий от предыдущего результата аналогичного поиска).

27. Функции просмотра журналов и построения отчетов Сервером управления включают:
    1. Формирование статистических и графических отчетов на основе набора встроенных шаблонов отчётов и выбранных администратором параметров, на базе данных из журналов, хранимых на Сервере управления, с автоматической отправкой сгенерированных отчетов по электронной почте; поддерживается экспорт построенных отчетов в форматы PDF, HTML и RTF;
    2. Возможность построения интерактивного отчета для визуального анализа внутренних и внешних связей пользователей;
    3. Возможность просмотра агрегированной аналитической информации по пользователям в формате досье (карточек) пользователя, построенных с использованием данных из журналов событий, хранимых на Сервере управления;
    4. Формирование отчетов по применяемым политикам;
    5. Просмотр журналов событийного протоколирования, теневого копирования, видеозаписей экрана, записи нажатий клавиш и сведений о запущенных процессах, в консоли Системы, с возможностью фильтрации по всем атрибутам событий, с возможностью экспорта полученного списка событий для последующей обработки;
    6. Просмотр файлов теневых копий, видеозаписей экрана, последовательности нажатий клавиш в консоли Системы или внешним программным обеспечением.

Дополнительные особенности

1. Программный комплекс имеет подтвержденный опыт успешной эксплуатации в России и других странах;
2. Производительность агентов программного комплекса ограничена только аппаратной производительностью контролируемых АРМ;
3. У программного комплекса отсутствуют недокументированные функции, т.е. реализованные в ней возможности и особенности, не отраженные в прилагаемой документации.

Описание Технической поддержки

1. ПО сопровождается подпиской на техническую поддержку на период от одного года
2. Контакт со службой технической поддержки посредством телефона, электронной почты.

3. Техническая поддержка доступна на русском языке в рабочие часы, в будни.
4. Обозначение критичности проблемы при создании заявке в службе технической поддержке.
5. В критичных случаях при обращении в службу технической поддержки первая реакция инженера следует в течение нескольких часов.
6. Подписка на техническую поддержку в период своего действия гарантирует бесплатные обновления продукта, в том числе переход на новую версию продукта.