**Техническое задание:**

# DLP-система для Windows

# Falcongaze SecureTower

**Техническое задание**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Наименование** | **Кол-во, шт** | **Обоснование количества** | **Что подразумевает позиция** |
| **1** | Лицензия на программное обеспечение «FalconGaze  SecureTower», перехват агентами (контроль: MAIL; WEB;  IM; FTP; USB; Printers; Desktop activity), на 1100 пользователей**, сроком на 1 год** | **1** | 1 Лицензия распространяется на 1100 пользователи (все сотрудники ГК Мрия)  Количество указано с учетом возможного расширения.  Распространяется на все ПК и ноутбуки с операционной системой Windows. | DLP-система — система, которая предотвращает утечку конфиденциальной информации из внутренней сети компании. |

\*Срок действия лицензий составляет 1 год

Полное наименование системы: Data leak prevention — система «FalconGaze SecureTower»

Сокращенное наименование системы: «FalconGaze»

Заказчик: Наименование организации заказчика – ООО «Гарант СВ» (далее – Заказчик).

Плановые сроки начала и окончания работы:

плановый срок начала работ – с даты заключения договора;s

плановый срок окончания работ – 1 год с даты заключения договора.

Требования к функциональным возможностям системы предотвращения утечек данных и мониторингу сетевой активности пользователей (DLP)

Термины и сокращения

- Аппаратно-программный комплекс – совокупность программного обеспечения и технических средств, совместно применяемых для решения задач определенного типа;

- Заявка – запрос Заказчика на предоставление услуг;

- ИБ – информационная безопасность;

- Инцидент ИБ – отдельно или серийно возникающие сбой в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;

- ИС – информационная система;

- Объект информатизации – электронные информационные ресурсы, программное обеспечение и информационно-коммуникационная инфраструктура;

- ОЗУ – оперативное запоминающее устройство;

- ОС – операционная система;

- ПО – программное обеспечение;

- AD – LDAP-совместимая реализация службы каталогов (англ. Active Directory);

- LDAP – облегчённый протокол доступа к каталогам (англ. Lightweight Directory Access Protocol);

- SOC – оперативный центр информационной безопасности (англ. Security Operation Center).

Цели услуги:

1) соответствие требования законодательства в области информационной безопасности;

2) повышение общего уровня защищенности информационных активов Заказчика;

3) снижение количества и уровня рисков, экономических потерь, обусловленных угрозами и инцидентами ИБ;

4) повышение уровня зрелости процессов ИБ за счет предоставления услуги;

5) автоматизация процесса управления ИБ;

6) соответствие требованиям законодательства Республики Казахстан в области информационной безопасности и СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования».

1. Требования к перехвату 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, должен осуществляться путем интеграции с почтовыми серверами по протоколам POP3, IMAP, SMTP, а также при помощи коннектора MS Exchange. Модуль должен обеспечивать следующие возможности:

1) перехват всех почтовых сообщений и вложений, переданных и полученных с помощью почтовых серверов;

2) настройка исключений контролируемых сообщений по почтовым адресам, с возможностью использования символов подстановки для настройки исключений;

3) импорт и экспорт настроенных фильтров;

4) настройка интервалов выгрузки почты при интеграции по протоколам POP3, IMAP.

5) использование шифрованного соединения для выгрузки почтовых сообщений с почтовых серверов.

2. Требования к перехвату данных с помощью локального средства (агента контроля рабочей станции).

2.1. Общие требования:

Агент контроля рабочих станций - независимый программный модуль, который устанавливается на рабочие станции в сети. Централизованная установка и управление работой агентов в системе должно осуществляться путем соответствующих настроек, которые должны позволять производить следующие возможности управления работой агентов:

1) централизованная установка агентов, 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;

2) установка агентов при помощи групповых политик Windows;

3) создание дистрибутива агентов для последующей установки вручную (с сохранением в файле дистрибутива ранее выполненных настроек для агента);

4) автоматическое обновление агентов, с возможностью исключения отдельных рабочих станций из обновления;

5) отслеживание состояния агентов и, в случае отсутствия, сбоя или принудительного отключения агентов пользователем какой-либо конечной станции, автоматическая повторная установка агентов на соответствующей станции.

6) защита агентов от удаления;

7) защита процесса агента, файлов агента и данных агента в реестре от изменения пользователем;

8) скрытие процесса и сервиса, а также файлов и папок агента на компьютере пользователя;

9) настраиваемые уведомления при блокировке действий пользователя;

10) 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;

11) логирование событий агента с возможностью настройки нескольких режимов детализации: стандартный, расширенный, и возможностью полного отключения логирования;

12) общая статистика всех принятых и отправленных данных от агентов;

13) 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.;

14) поддержание работы в автономном режиме, в случае отсутствия соединения между компонентами системы или с внешними сетями, перехваченные данные должны хранятся в локальном хранилище с возможностями ограничения размера локального хранилища и срока хранения данных в нем;

15) возможность ограничения предельного размера локального хранилища как в Мб, так и в процентах от свободного места на диске

16) возможность настройки в интерфейсе интервала подключения агентов к серверам агентов: задание временного интервала, а также подключение по достижению заданного объема полученных данных

17) оптимизация нагрузки на сетевые ресурсы путем настройки расписания и ограничения максимальной скорости передачи данных агентами.

Способ передачи данных с агентов на сервер должен соответствовать следующим требованиям:

1) для оптимизации нагрузки на сеть передача данных от агентов на центральный сервер должна происходит через промежуточные серверы агентов.

2) возможность установки нескольких серверов агентов для балансировки нагрузки на сеть

3) возможность использования защищенного протокола сетевого взаимодействия между агентами и серверами агентов

4) возможность выбора способа защиты трафика между агентами и серверами агентов (шифрование трафика либо цифровая подпись)

5) протокол сетевого взаимодействия между агентами и серверами агентов должен поддерживать сжатие трафика

2.2. Требования к контролируемым агентами каналам передачи данных:

Агентский модуль должен выполнять перехват трафика, в том числе шифрованного, и данных, переданных по использующим шифрование протоколам, а также фиксировать активность пользователя на контролируемой рабочей станции. Возможности настройки контролируемых каналов передачи данных должны включать:

1) 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;

2) активация профиля настроек агента по следующим условиям: недоступность сервера в течении некоторого времени, активное vpn-подключение, пользовательское условие, задаваемое при помощи Lua-скрипта;

3) выбор одного из режима перехвата трафика: весь трафик, только шифрованный трафик, только нешифрованный трафик;

4) использование при перехвате шифрованного трафика как пользовательского SSL-сертификата в качестве корневого, так и автоматическая генерация агентом корневого SSL-сертификата;

5) исключение как отдельных локальных пользователей, так и отдельных пользователей из Active Directory из процесса мониторинга;

6) исключение серверов из перехвата сетевого трафика;

7) исключение отдельных процессов их перехвата сетевого траффика;

8) исключение отдельных IP-адресов и диапазонов из перехвата сетевого траффика.

2.3. Требования к функциональным возможностям Windows-агента

2.3.1 Требования к контролю агентом HTTP/HTTPS трафика:

Система должна позволять контролировать входящую и исходящую информацию, передаваемую по протоколу HTTP и шифрованному аналогу HTTPS и располагать следующим функционалом:

1) 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;

2) возможность настройки фильтрации перехвата данных по MIME-типам по ряду предустановленных правил и правил, созданных пользователе;

3) возможность перехвата, блокирования и фильтрации GET/POST/PUT запросов при выборе HTTP-методов контроля переданных данных;

4) перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы;

5) перехват и анализ поисковых запросов пользователя;

6) сохранение адресов всех страниц, посещенных пользователем;

7) перехват входящих и исходящих данных веб-коммуникаций (переписки в чатах, публикация статусов, комментарии) на веб-ресурсах: Facebook, Twitter, ВКонтакте, Одноклассники;

8) перехват входящих и исходящих электронных писем и вложений, переданных либо полученных через почтовые веб-сервисы (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex, Zimbra и т.д.);

9) перехват сообщений и файлов, переданных в веб-клиентах мессенджеров: Skype, Telegram, Discord, Microsoft Teams, Slack, RocketChat, а также перехват сообщений, переданных в веб-клиентах мессенджеров: WhatsApp, ICQ, Google Hangouts;

10) 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;

11) возможность поиска по тексту и атрибутам сообщений и файлов, переданных по протоколу HTTP(S);

12) возможность блокирования посещений веб-ресурсов, исходящих сообщений и файлов, по контенту, по набору атрибутов, а также по хеш-сумме отправляемых файлов;

13) возможность настройки пользовательского сообщения про блокировки HTTP(S) трафика.

2.3.2 Требования к контролю агентом FTP/FTPS трафика:

Система должна позволять контролировать входящие и исходящие файлы, передаваемые по протоколу FTP и шифрованному аналогу, и располагать следующим функционалом:

1) Перехват исходящих и входящих файлов, переданных по FTP-соединению, а также переданных по зашифрованному SSL-соединению;

2) возможность настройки ограничения по размеру перехватываемых файлов;

3) автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

4) возможность поиска по тексту и атрибутам файлов, переданных по протоколу FTP(S), в том числе с применением шаблонов.

2.3.3 Требования к контролю агентом почтового трафика:

Система должна позволять контролировать входящую и исходящую почту, а также вложения и располагать следующим функционалом:

1) перехват почтовых сообщений, передаваемых по протоколам IMAP, POP3, SMTP, MAPI, а также по их шифрованным аналогам;

2) настройка исключений из перехвата почты определенных контактов;

3) перехват агентами почтовых сообщений, переданных посредством почтовых программ с поддержкой стандарта защищённой электронной почты S/MIME, при этом обеспечивается автоматическая расшифровка содержимого письма;

4) перехват почтовых сообщений путем интеграции с Microsoft Outlook;

5) перехват и анализ почтовых сообщений, отправленных либо полученных при помощи почтовых веб-сервисов по протоколу HTTP(S) (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex, Zimbra и т.д.);

6) перехват и анализ файлов-вложений почтовых сообщений;

7) 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;

8) 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;

9) возможность сохранения электронных писем в HTML-формате и в формате, совместимом с Microsoft Outlook;

10) возможность поиска по тексту и атрибутам почтовых сообщений и файлов, в том числе с применением шаблонов.

2.3.4 Требования к контролю переписки в мессенджерах:

Система должна позволять контролировать переписку пользователей, отправляемые файлы и разговоры в программах многозвенного обмена и располагать следующим функционалом:

1) 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, RocketChat, а также в мессенджерах, использующих протоколы SIP, OSCAR, XMPP (включая XMPP по HTTP), YMSG.

2) Перехват файлов, передаваемых в мессенджерах Viber, Telegram, WhatsApp, Skype (включая веб-версию), Microsoft Lync, RocketChat, Microsoft Teams (включая веб-версию), Discord (включая веб-версию), Slack (включая веб-версию).

3) Перехват голосовых разговоров, осуществляемых через Skype (в том числе звонки Skype-to-Skype, Skype-to-phone), а также через Microsoft Lync, Viber, Zoom, Telegram, WhatsApp и по протоколу SIP с сохранением разговоров в файлы формата MP3;

4) возможность распознавания и перевода в текстовый формат голосовых разговоров (коммуникаций) Microsoft Lync, Skype, Viber, Zoom, Telegram, WhatsApp и SIP;

5) возможность воспроизведения сохраненных разговоров Microsoft Lync, Skype, Viber и SIP;

6) перехват голосовых сообщений Telegram;

7) возможность ограничения перехвата по отдельным учетным записям пользователей;

8) 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;

9) возможность осуществления поиска по тексту и атрибутам сообщений и файлов, переданных через мессенджеры, в том числе с применением шаблонов.

10) 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;

11) контроль переписок и постов в Facebook, LinkedIn.

12) контроль переписок в Instagram.

13) контроль переписок, электронной почты и файлов в CMS Bitrix24.

14) перехват голосовых сообщений и файлов в web- и dekstop-версиях мессенджера WhatsApp.

2.3.5 Требования к контролю печати:

Система должна контролировать печать документов, отправляемых на сетевые, локальные и виртуальные принтеры, и располагать следующим функционалом:

1) перехват отправляемых на печать документов агентами, установленными на рабочих станциях пользователей;

2) возможность перехвата документов, отправляемых на сетевые, виртуальные и локальные принтеры (в том числе подключенные к COM-, LPT-портам);

3) возможность перехвата печати в XPS-формат;

4) возможность настройки исключений из перехвата по отдельным принтерам;

5) возможность ограничения перехвата печати по количеству страниц и по размеру документа;

6) возможность исключения процессов для модуля перехвата печати на принтерах.

7) извлечение и анализ текста отправленных на печать документов;

8) автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

9) возможность блокировки печати по названию документа. текстовому содержимому документа и по названию принтера;

10) возможность поиска по тексту и атрибутам отправленных на печать файлов, в том числе с применением шаблонов;

11) сохранение в PDF- и XPS-формате.

12) возможность блокировки документов, отправляемых на печать как по набору атрибутов, так и по содержимому документа, отправляемого на печать.

2.3.6 Требования к контролю внешних устройств и накопителей:

Система должна позволять контролировать использование накопителей и устройств пользователями, и располагать следующим функционалом:

1) Теневое копирование файлов, отправляемых на внешние накопители (съемные жесткие диски, флеш-накопители, карты памяти, съемные накопители, CD/DVD и флоппи-диски и т.д.);

2) 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;

3) возможность настройки исключений из теневого копирования и аудита по размеру и расширению файлов;

4) возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);

5) сохранение теневых копий файлов, записанных на внешние накопители, локально на контролируемых компьютерах перед отправкой данных на сервер;

6) возможность настройки размера хранилища для теневых копий на контролируемых компьютерах;

7) возможность блокирования записи файлов на съёмные носители по содержимому передаваемой информации и другим атрибутам.

8) возможность настройки исключений из теневого копирования и аудита для определенных внешних накопителей информации (по типам устройств, идентификаторам, производителям, названиям, серийным номерам);

9) 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.);

10) 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;

11) возможность контроля копирования информации на внешние накопители как в локальных, так и терминальных пользовательских сессиях;

12) исключение отдельных процессов из процедуры контроля, аудита теневого копирования.

13) 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);

14) добавление в фильтр исключений устройств, подключенных на контролируемых рабочих станциях;

15) 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;

16) 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;

17) возможность поиска по тексту и атрибутам отправленных на внешние накопители файлов, в том числе с применением шаблонов.

2.3.7 Требования к контролю облачных хранилищ:

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

1) аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, имя пользователя, дата, время и имя облачного сервиса хранения;

2) теневое копирование файлов, отправляемых в облачные хранилища пользователем либо процессом;

3) настройка аудита и теневого копирования только исходящих, только входящих, либо всех файлов;

4) возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);

5) сохранение теневых копий файлов, записанных в облачное хранилище, локально на контролируемых компьютерах перед отправкой на сервер;

6) возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;

7) контроль доступа к отдельным облачным хранилищам с возможностью запрета доступа для определенных пользователей;

8) контроль доступа к отдельным облачным хранилищам с возможностью настройки режима «только чтение» для определенных пользователей;

9) управление правами передачи данных в облачные хранилища с возможностью запрета отправки файлов определенных форматов;

10) возможность настройки исключений из аудита, теневого копирования и контроля доступа по расширениям файлов;

11) 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;

12) аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, имя пользователя, дата, время и имя облачного сервиса хранения;

13) возможность поиска по тексту и атрибутам отправленных файлов, в том числе с применением шаблонов.

2.3.8 Требования к контролю сетевых ресурсов:

Система должна позволять контролировать использование пользователями сетевых ресурсов, и располагать следующим функционалом:

1) аудит событий копирования файлов на локальные сетевые ресурсы: фиксируется имя файла, пользователь, дата, время и сетевой путь к ресурсу;

2) теневое копирование файлов, отправляемых на сетевые ресурсы;

3) возможность настройки исключений из аудита и теневого копирования по расширениям файлов;

4) возможность настройки исключений из аудита и теневого перехвата определенных сетевых ресурсов;

5) возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);

6) сохранение теневых копий файлов, записанных на сетевые ресурсы, локально на контролируемых компьютерах перед отправкой на сервер;

7) возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;

8) возможность теневого копирования файлов, передаваемых на сетевые ресурсы терминальных серверов;

9) контроль доступа к сетевым ресурсам с возможностью запрета доступа на определенные сетевые ресурсы;

10) управление правами записи на сетевые ресурсы с возможностью запрета записи определенных форматов файлов;

11) исключение отдельных процессов из процедуры контроля, аудита теневого копирования;

12) 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;

13) возможность поиска по тексту и атрибутам отправленных на сетевые ресурсы файлов, в том числе с применением шаблонов.

2.3.9 Требования к блокировке передачи данных:

Система должна обеспечивать 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 должна располагать следующими возможностями:

1) 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, количество вхождений фразы в документ 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;

2) 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.

3) 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;

4) возможность добавления в банк хеш-сумм всех файлов, расположенных в определеной папке, а также только файлов определенного расширения из указанной папки.

5) 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.;

6) 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.

7) 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;

8) 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.;

9) 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.

10) 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;

11) 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.;

12) 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.

13) возможность уведомления конечного пользователя при блокировке, с настраиваемым текстом уведомления;

14) возможность уведомления офицера безопасности о блокировке печати;

15) возможность поиска по атрибутам заблокированной информации.

2.3.10 Требования к функции снимков экрана:

Система должна позволять контролировать активность рабочего стола пользователя при помощи снятия снимков экрана, и располагать следующими возможностями:

1) возможность снятия скриншотов с заданным интервалом с точностью до секунды;

2) возможность снятия скриншотов при смене активного окна;

3) возможность снятия скриншотов при смене вкладки браузера;

4) возможность снятия скриншотов при запуске процесса;

5) возможность снятия скриншотов при срабатывании правила блокировки;

6) возможность снятия скриншотов при нажатии клавиши Print Screen;

7) возможность отключения снятия скриншотов при простое рабочей станции.

8) возможность настройки качества скриншотов, в том числе сохранения в черно-белом формате;

9) возможность настройки размера скриншотов (в процентах от оригинала);

10) возможность настройки формата скриншотов (JPEG, PNG);

11) сохранение специальной отметки в случае невозможности снятия скриншота (сессия пользователя отключена, заблокирована и т.п.);

12) возможность отключения снятия скриншотов при посещении заданных сайтов в браузере;

13) возможность снятия скриншотов только для заданных активных процессов;

14) возможность экспорта скриншотов во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к просмотру перехваченных данных через веб-браузер;

15) возможность сохранения скриншотов отдельного пользователя за день (или за выбранный временной интервал) в виде набора графических файлов, либо объединенных в один PDF- или видеофайл.

2.3.11 Требования к функции видеомониторинга:

Система должна позволять контролировать активность пользователя при помощи снятия видео рабочего стола, а также видео с веб-камеры, и располагать следующими возможностями:

1) подключение к монитору компьютера пользователя и просмотр видео рабочего стола в режиме реального времени;

2) мониторинг рабочих столов нескольких пользователей одновременно;

3) возможность вывода окна просмотра на отдельный экран;

4) автоматическая запись видеоизображения рабочего стола и видео с подключенной веб-камеры по расписанию;

5) запись видео рабочего стола вручную;

6) возможность настройки качества записи;

7) возможность как записи видео в цветном, так и в черно-белом формате;

8) возможность сохранения записей нескольких пользователей одновременно;

9) возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

2.3.12 Требования к функции аудиомониторинга:

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

1) подключение к микрофонам контролируемых рабочих станций с возможностью прослушивания аудиопотока в режиме реального времени;

2) прослушивание микрофонов нескольких пользователей одновременно;

3) автоматическая запись поступающего с микрофона аудиопотока и системных звуков компьютера по расписанию;

4) запись вручную;

5) возможность сохранения записей нескольких пользователей одновременно;

6) возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

2.3.13 Требования к мониторингу пользовательской активности:

Система должна позволять контролировать активность пользователя на рабочем месте и располагать следующими возможностями:

1) ведение статистики по активному времени работы и простоя (отсутствия действий пользователя) с возможностью настройки периода отсутствия активности до начала простоя;

2) ведение статистики по времени работы пользователя в приложениях с представлением собранной информации, при этом учитывается время, а время работы пользователя в активном окне;

3) исключение отдельных процессов из мониторинга;

4) 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;

5) возможность блокировки запуска отдельных приложений;

6) возможность сохранения отдельных отчетов по активности (активность пользователя за ПК, активность приложений, хронология событий) за выбранный временной интервал для отдельного пользователя или нескольких пользователей.

2.3.14 Требования к мониторингу браузер активности:

Мониторинг браузер активности должен позволять вести комплексную статистику по активности контролируемых пользователей в следующих браузерах: Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Tor, Yandex браузер, Rambler, Amigo, Chromium, Microsoft Edge и располагать следующими возможностями:

1) 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;

2) возможность настройки исключения отдельных сайтов из процесса мониторинга браузер активности;

3) 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.

4) 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.);

2.3.15 Требования к контролю буфера обмена:

Система должна позволять контролировать использование пользователями буфера обмена, и располагать следующими возможностями:

1) теневое копирование помещаемой в буфер обмена текстовой информации с фиксацией приложения, из которого данная информация была помещена в буфер обмена, и времени события;

2) аудит файлов, помещаемых в буфер обмена;

3) теневое копирование графического содержимого помещаемого в буфер обмена;

4) теневое копирование файлов, помещаемых в буфер обмена;

5) возможность ограничения максимального объема данных, перехватываемых из буфера обмена;

6) возможность исключения отдельных процессов из мониторинга буфера обмена либо мониторинг только определенных процессов;

7) возможность исключения отдельных файлов из мониторинга буфера обмена либо мониторинг только определенных файлов;

8) 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;

9) возможность блокирования как копирования, так и вставки файлов по содержимому, в соответствии с настроенными правилами безопасности.

10) возможность поиска по тексту, помещаемому пользователями в буфер обмена, в том числе с применением шаблонов.

11) возможность настройки обнаружения отдельно информации, скопированной в буфер обмена, и информации, вставляемой из буфера обмена;

12) возможность настройки обнаружения в буфере обмена только файлов, только текста либо только изображений.

2.3.16 Требования к контролю ввода с клавиатуры:

Система должна позволять контролировать ввод пользователя с клавиатуры, и располагать следующими возможностями:

1) 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.);

2) возможность исключения перехвата клавиатуры в заданных приложениях либо осуществление перехвата только в определенных приложениях;

3) возможность исключения перехвата клавиатуры по адресу активной страницы в браузере либо осуществление перехвата только на определенной активной странице в браузере;

4) 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;

5) возможность поиска по тексту, вводимому пользователями с клавиатуры, в том числе с применением шаблонов.

2.3.17 Требования к контролю файловой системы:

Система должна позволять контролировать файлы, хранящиеся в файловой системе рабочей станции и располагать следующими возможностями:

1) автоматическое сканирование файловых систем контролируемых рабочих станций на предмет наличия документов, которые носят статус конфиденциальных либо представляют интерес в рамках обеспечения информационной безопасности;

2) формирование банков конфиденциальных документов, поиск которых должен выполняться во время сканирования;

3) возможность автоматического импорта в банк конфиденциальных документов подготовленных хеш-функций из файлов txt- и csv-формата;

4) возможность выбора рабочих станций и пользователей, чьи файловые системы будут контролироваться;

5) гибкая настройка правил выбора файлов и папок, подлежащих автоматической проверке;

6) исключение из сканирования файлов настраиваемого размера;

7) возможность выполнения проверок файловой системы по расписанию;

8) возможность создавать индивидуальные политики контроля за содержимым файловых систем для отдельных пользователей и рабочих станций, в том числе с применением шаблонов;

9) возможность поиска документов в файловых системах контролируемых рабочих станций по атрибутам файлов и значениям их хеш-функций.

2.3.18 Требования к аудиту файловых операций:

Система должна позволять выполнять аудит операций с файлами и папками. При этом должно отслеживаться следующие операции с файлами:

1) создание

2) чтение

3) запись

4) удаление

5) переименование

6) открытие

7) изменение прав доступа

Система должна отслеживать следующие операции с папками:

1) создание

2) удаление

3) переименование

4) открытие

5) изменение прав доступа

Также должны быть предусмотрены дополнительный возможности:

1) исключение из аудита определенных файлов, папок и процессов, либо ведение аудита только определенных файлов, папок и процессов;

2) возможность экспорта списка исключений для аудита в формат XML, а также импорта списка.

2.4. Требования к функциональным возможностям Linux-агента:

Система должна поддерживать следующие дистрибутивы Linux: Ubuntu 20.04, Debian 11, Fedora 33, Rosa R12 и Astra 2.12

2.4.1 Требования к контролю агентом HTTP/HTTPS трафика:

Система должна перехватывать HTTP- иS)- запросы

2.4.2 Требования к контролю агентом FTP трафика:

Система должна позволять контролировать входящие и исходящие файлы, передаваемые по протоколу FTP и шифрованному аналогу, и располагать 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; (не до конца уверен, что это работает)

• возможность поиска по тексту и атрибутам файлов, переданных по протоколу FTP(S), в том числе с применением шаблонов.

2.4.3 Требования к контролю агентом почтового трафика:

Система должна позволять контролировать входящую и исходящую почту, а также вложения и располагать следующим функционалом:

• перехват почтовых сообщений, передаваемых по протоколам IMAP, POP3, SMTP, а также по их шифрованным аналогам;

• настройка исключений из перехвата почты определенных контактов;

• перехват 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;

• возможность поиска по тексту и атрибутам почтовых сообщений и файлов, в том числе с применением шаблонов.

2.4.5 Требования к контролю внешних устройств и накопителей:

Система должна позволять контролировать использование USB-накопителей и USB-устройств пользователями, и располагать следующим функционалом:

• контроль доступа к внешним USB-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.);

• контроль доступа и аудит использования внешних USB-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;

2.4.6 Требования к функции снимков экрана:

Система должна позволять контролировать активность рабочего стола пользователя при помощи снятия снимков экрана, и располагать следующими возможностями:

• возможность снятия скриншотов с заданным интервалом с точностью до секунды;

• возможность снятия скриншотов при нажатии клавиши Print Screen;

• 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);

2.4.7 Требования к контролю ввода с клавиатуры:

Система должна позволять контролировать ввод пользователя с клавиатуры, и располагать 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 либо осуществление перехвата только в определенных приложениях;

• 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.

3. Требования к хранению и обработке данных:

Настройки должны позволять подключать хранилища информации под управлением ряда СУБД, управлять данными 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 должна обладать следующим функционалом:

1) 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);

2) встроенная СУБД SQLite в комплекте поставки;

3) хранение всех перехватываемых данных вне зависимости от срабатывания политик безопасности;

4) поддержка работы с базами данных, расположенных на разных серверах;

5) 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;

6) возможность включения/отключения распознавания изображений, печатей и речи для отдельных баз данных;

7) возможность настройки длительности хранения информации в базе данных в группе ротации,

8) возможность отключения базы данных вручную через Консоль администратора, при этом содержимое базы данных сохраняется;

9) возможность очистки содержимого базы данных вручную через Консоль администратора;

10) возможность архивирования баз данных с последующим подключением к системе для осуществления ретроспективного поиска в них критичной информации;

11) возможность выборочного удаления пользователем перехваченной информации;

12) 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;

13) 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;

14) 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;

15) 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;

16) поддержка режима параллельной обработки данных, перехваченных по различным каналам передачи информации, что позволяет повысить производительность системы при выполнении операций обновления, удаления и поиска данных;

17) 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;

18) возможность автоматической репликации поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера в территориально распределённых организационных структурах;

19) защита от некорректной настройки репликации, когда данные возвращаются на реплицирующий сервер и далее реплицируются повторно;

20) возможность перенаправления поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;

21) возможность настройки расписания для репликации данных;

22) возможность хранения очереди репликации данных на диске для обеспечения сохранности и целостности реплицируемых данных в случае отказа системы;

23) при переполнении очереди репликации сервер блокирует прием новых данных;

24) возможность пропуска репликации при переполнении очереди;

25) отображение статистики репликации данных;

26) возможность хранения на диске очереди данных, поступающих от агентов, что повышает их сохранность по сравнению с хранением в оперативной памяти;

27) возможность выбора режима очистки и обновления поисковых индексов (ручной и автоматический режимы);

28) возможность индексации содержимого заголовков перехватываемых писем, при этом поддерживается фильтрация полей заголовков писем, значения которых будут индексироваться

29) возможность осуществления асинхронного поиска по перехваченным данным (при проведении параллельного поиска по нескольким каналам передачи информации, отображение результатов выполняется по мере их получения);

30) просмотр комплексной статистики по хранящимся и индексируемым данным в базах данных и группах ротации.

Система должна индексировать файлы следующих форматов:

1) Adobe Acrobat (\*.pdf)

2) Ami Pro (\*.sam)

3) Ansi Text (\*.txt)

4) ASCII Text

5) ASF (метаданные) (\*.asf)

6) CSV (Comma-separated values) (\*.csv)

7) DBF (\*.dbf)

8) DjVu

9) DWG

10) DXF

11) EBCDIC

12) EML files (электронные письма, сохраненные Outlook Express) (\*.eml)

13) Enhanced Metafile Format (\*.emf)

14) Eudora MBX файлы сообщений (\*.mbx)

15) Flash (\*.swf)

16) GZIP (\*.gz)

17) HTML (\*.htm, \*.html)

18) JPEG (метаданные) (\*.jpg)

19) Lotus 1-2-3 (\*.wk?, \*.123)

20) MBOX архивы электронных писем (включая Thunderbird) (\*.mbx)

21) MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (\*.mht)

22) Microsoft Access (\*.mdb)

23) Microsoft Access 2007 (\*.accdb)

24) Microsoft Document Imaging (\*.mdi)

25) Microsoft Excel (\*.xls)

26) Microsoft Excel 2003 XML (\*.xml)

27) Microsoft Excel 2007 (\*.xlsx)

28) Microsoft Open XML Paper Specification (\*.oxps)

29) Microsoft Outlook (OST)

30) Microsoft Outlook Express 5 и 6: базы сообщений (\*.dbx)

31) Microsoft PowerPoint (\*.ppt)

32) Microsoft Rich Text Format (\*.rtf)

33) Microsoft Searchable Tiff (\*.tiff)

34) Microsoft Word 2003 XML (\*.xml)

35) Microsoft Word 2007 (\*.docx)

36) Microsoft Word for DOS (\*.doc)

37) Microsoft Word for Windows (\*.doc)

38) Microsoft Works (\*.wks)

39) MIME-сообщения

40) MP3 (метаданные) (\*.mp3)

41) MSG files (электронные письма, сохраненные Outlook) (\*.msg)

42) Multimate Advantage II (\*.dox)

43) Multimate version 4 (\*.doc)

44) 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)

45) OST (внутренний формат Microsoft Outlook)

46) Quattro Pro (\*.wb1, \*.wb2, \*.wb3, \*.qpw)

47) TAR (\*.tar)

48) TIFF (\*.tif)

49) TNEF (winmail.dat)

50) Treepad HJT (\*.hjt)

51) Unicode (UCS16, порядок байтов Mac или Windows, или UTF-8)

52) Windows Metafile Format (\*.wmf)

53) WMA видео (метаданные) (\*.wma)

54) WMV видео (метаданные) (\*.wmv)

55) WordPerfect (5.0 и выше) (\*.wpd, \*.wpf)

56) WordPerfect 4.2 (\*.wpd, \*.wpf)

57) WordStar 2000

58) WordStar версий 1, 2, 3, 4, 5, 6 (\*.ws)

59) Write (\*.wri)

60) XBase (включая FoxPro, dBase и другие совместимые с XBase форматы) (\*.dbf)

61) XML Paper Specification (\*.xps)

62) XSL

63) XyWrite

64) ZIP (\*.zip)

4. Требования к анализу данных.

Система должна располагать широким спектром возможностей анализа перехваченных данных:

1) контентный анализ;

2) атрибутивный анализ;

3) распознавание изображений;

4) распознавание печатей;

5) распознавание речи;

6) статистический анализ;

7) событийный анализ;

8) поведенческий анализ;

9) Категоризация приложений;

10) Категоризация веб-сайтов;

11) Учет продуктивности веб-сайтов и приложений.

4.1. Контентный анализ:

Контентный анализ данных должен включать в себя:

1) поиск по словам и словосочетаниям с учетом морфологии, с возможностью отключения;

2) поиск по словам и словосочетаниям с учетом расстояния между словами;

3) поиск по словам и словосочетаниям с учетом порядка слов;

4) поиск по словам и словосочетаниям с учетом транслитерации кириллических символов латинскими,

5) поиск по словам и словосочетаниям с возможностью нечеткого поиска, для поиска ключевых слов, в том числе написанных с ошибками и опечатками;

6) технология поиска регулярных выражений, используемая для обнаружения фиксированных последовательностей символов, например, номеров паспортов, номеров банковских карт и т.п.;

7) возможность использования предустановленных регулярных выражений и создания пользовательских;

8) 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);

9) создание цифровых отпечатков документов или папок с документами для последующего обнаружения в перехваченных данных похожих документов – с возможностью указания процента соответствия перехваченного документа оригиналу);

10) возможность использования предустановленных словарей и создания пользовательских;

11) технология поиска по цифровым отпечаткам документов с возможностью указания процента соответствия перехваченного документа оригиналу;

12) синхронизация банка цифровых отпечатков с папками, в которых располагаются документы, с возможностью настройки интервала обновления

13) создание цифровых отпечатков CSV-файлов, с выбором полей со значимой информацией для добавления в банк данных;

14) 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»);

15) 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.

4.2. Атрибутивный анализ:

Атрибутивный анализ данных должен включать в себя:

1) 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.;

2) 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.;

3) анализ атрибутов процессов, таких как: имя исполняющего файла, полный путь к файлу, заголовок окна процесса и др.;

4) анализ атрибутов перехваченной почты, таких как: отправитель, получатель, число получатель, заголовка письма и др;

5) анализ атрибутов перехваченной переписки в мессенджерах, таких как: локальный идентификатор пользователя, удаленный идентификатор пользователя, число сообщений, тип данных, и др;

6) анализ атрибутов контролируемых устройств, таких как: название устройства, производитель, тип устройства, идентификатор производителя, идентификатор продукта, тип устройства, серийный номер и др;

7) анализ атрибутов печати, таких как: тип документа, название принтера, число распечатанных страниц и др;

4.3. Распознавание изображений:

Система должна обеспечивать 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 должна быть возможность применять все соответствующие инструменты контекстного и атрибутивного анализа.

4.4. Распознавание печатей:

Система должна обеспечивать возможность обнаружения печатей на изображениях по заданным эталонам.

К обнаруженным печатям должна быть возможность применять все соответствующие инструменты атрибутивного анализа.

4.5. Распознавание речи:

Система должна обеспечивать возможность извлечения текстового содержимого из аудиофайлов разговоров, перехваченных в мессенджерах Skype, MS Lync, Viber, Zoom, MS Teams, Telegram, WhatsApp, а также в программах IP-телефонии, использующей протокол SIP.

К извлеченному тексту должна быть возможность применять все соответствующие инструменты контекстного и атрибутивного анализа.

4.6. Статистический анализ:

Должна быть предусмотрена возможность настройки автоматических уведомлений о достижении определенных показателей в течение определенного времени (час, день, неделя, произвольный интервал):

1) количество отправленных/полученных пользователем электронным письмам

2) количество переписок/сообщений пользователя

3) количество/время звонков пользователя 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.);

4) количество посещенных веб-страниц;

5) количество отправленных веб-запросов;

6) количество распечатанных страниц/документов на принтерах;

7) количество отправленных/полученных файлов

8) продолжительность работы в браузерах, том числе на определенных сайтах (например, «Время пребывания пользователя на определенном сайте через браузер превысило 1 час за день» и т.д.);

9) продолжительность работы в приложениях, в т.ч. в определенных приложениях (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.);

10) продолжительность активной работы/бездействия ПК, в том числе в процентах от общего времени (например, «ПК бездействовал в течение более 3 часов за день», «начало активности ПК зафиксировано позже 10:30» и т.д.);

Должна быть предусмотрена возможность настройки автоматических уведомлений об отклонении от нормы начала/окончания рабочего, от нормы продолжительности активной работы за ПК «продолжительность рабочего дня».

4.7. Событийный анализ:

Событийный анализ должен обладать следующими возможностями:

1) регистрация запуска, завершения работы пользователем определенного приложения;

2) обнаружение пересылки зашифрованного вложения (например, защищенный паролем документ MS Office или архив);

3) копирование файлов с контролируемых компьютеров на внешние накопители, облачные хранилища и сетевые диски с определенными параметрами;

4) подключение и использования на контролируемых рабочих станциях устройств с определенными параметрами;

5) посещение определенных web-ресурсов;

6) блокирование пересылки данных по протоколам SMTP, HTTP, MAPI, отправки документов на печать, в том числе по дополнительным атрибутам;

7) обнаружение конфиденциальных файлов на компьютерных дисках пользователей;

8) выявление 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).

4.8. Поведенческий анализ:

Поведенческий анализ должен обладать следующими возможностями:

1) формирование модели поведения сотрудников и присвоение им соответствующего уровня риска;

2) информирование специалистов отдела безопасности об уровне риска и об инцидентах политик безопасности, которые вызвали изменения уровня риска;

3) предоставлять офицеру безопасности возможность исследовать аномалии в поведении сотрудников в режиме реального времени.

4.9. Категоризация приложений:

1) система должна автоматически относить приложения, используемые контролируемыми пользователями, к категориям в соответствии с настройками системы;

2) категоризация приложений должна осуществляться с учетом следующих атрибутов приложений: хеш-сумма исполняемого файла, имя исполняемого файла, имя продукта, описание приложения, версия приложения, имя компании разработчика приложения;

3) категоризация должна осуществляться с учетом следующих видов хеш-сумм исполняемых файлов: MD-5, SHA-1, SHA-256, CRC-32;

4) с системой должен поставляться набор системных категорий (должен содержать не менее 4000 приложений), а также предоставляться возможность создавать пользовательские категории;

5) должен быть предусмотрен приоритет пользовательских категорий приложений над системными;

6) должна быть предоставлена возможность отключения системных категорий приложений.

6.10. Категоризация веб-сайтов:

1) система должна автоматически относить сайты, посещенные контролируемыми пользователями, к категориям в соответствии с настройками системы;

2) категоризация сайтов должна осуществляться с учетом доменной части и пути в адресе перехваченного сайта;

3) с системой должен поставляться набор системных категорий (должен содержать не менее 20000 веб-сайтов), а также предоставлять возможность создавать пользовательские категории;

4) должен быть предусмотрен приоритет пользовательских категорий веб-сайтов над системными;

5) должна быть предоставлена возможность отключения системных категорий веб-сайтов.

6.11. Продуктивность веб-сайтов и приложений:

1) система должна позволять оценивать продуктивность использования рабочего времени сотрудниками, которое они проводят на веб-сайтах и при работе в приложениях;

2) система должна позволять устанавливать для каждого веб-сайта/приложения один из доступных классов продуктивности: продуктивно, непродуктивно, нейтрально.

3) в ситуации, когда пользователь находится в нескольких группах с разными настройками продуктивности приоритет продуктивности сайтов и приложений для этого пользователя следующий: продуктивно – непродуктивно - нейтрально

5. Требования к распознаванию изображений:

Система должна иметь несколько встроенных средств распознавания изображений (не менее 2-х): Nicomsoft, Tesseract.

Cистема должна иметь возможность интеграции со средством распознавания изображений ABBYY FineReader.

Система должна иметь модуль предварительного анализа схожести изображений с документами, который позволяет снизить нагрузку на сервер распознавания, отправляя на распознавание только файлы, похожие на документы.

Система позволяет настраивать в интерфейсе минимальный порог схожести изображения с документом, до достижения которого, документы не отправляются на сервер распознавания.

Система должна позволять осуществлять анализ текстового содержимого графических данных при помощи технологии OCR и обладать следующими возможностями:

1) 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);

2) возможность обнаружения печатей на изображениях по заданным эталонам;

3) возможность произведения по извлеченному тексту поиска с использованием инструментов контекстного и атрибутивного анализа;

4) возможность произведения по обнаруженным печатям поиска с использованием инструментов атрибутивного анализа;

5) возможность настройки очереди распознавания изображений по максимальному числу элементов в очереди, максимальному общему размеру очереди;

6) поддержка многопоточного распознавания печатей и текста из изображений, с возможностью выбора числа потоков для обработки печатей и числа потоков для обработки текста;

7) возможность настройки максимального времени распознавания одного документа;

8) возможность настройки области (количество первых страниц) распознавания в многостраничных документах.

9) отображение статистики по загрузке процессора, использованию оперативной памяти, по общему количеству обработанных документов, количеству документов в обработке, документов в очереди, количеству распознанных с ошибками документов

10) для распознавания файлов с дефектами изображений должна быть предусмотрена возможность тонкой настройки средств распознавания (загрузка изображений в 8-битном и 24-битном режимах, возможность автоматического применения бинаризации в зависимости от степени повреждения документа, тонкие настройки бинаризации, в т.ч. выбор порога бинаризации, настройки фильтрации дефектов).

6. Требования к распознаванию речи:

Система должна позволять осуществлять анализ текстового содержимого перехваченных аудиоразговоров и обладать следующими возможностями:

1) возможность извлечения текстового содержимого из аудиофайлов разговоров перехваченных в мессенджерах Skype, MS Lync, Viber, Zoom, MS Teams, Telegram, WhatsApp а также в программах IP-телефонии использующих протокол SIP;

2) Наличие встроенного средства распознавания речи Sphinx)

3) возможность выбора средства распознавания между Sphinx, Wit.ai, Yandex SpeechKit, Goolge Clooud Speech-to-text.

4) Возможность произведения по извлеченному тексту поиска с использованием инструментов контекстного и атрибутивного анализа;

5) поддержка многопоточного распознавания речи, с возможностью выбора числа потоков;

6) возможность настройки максимального времени распознавания одного документа;

7) отображение статистики по загрузке процессора, использованию оперативной памяти, по общему количеству обработанных документов, количеству документов в обработке, документов в очереди, количеству распознанных с ошибками документов.

7. Требования к управлению контролируемых пользователей:

Управление контролируемыми пользователями должно предусматривать:

1) создание внутренних карточек пользователей, содержащих всю идентификационную информацию контролируемых пользователей;

2) 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;

3) отсутствие ограничений по количеству профилей пользователей в базе программы;

4) возможность привязки к пользовательской карточке общей информации о пользователе: ФИО, организация, подразделение, должность, телефоны, адрес и др.,

5) возможность автоматической привязки к карточке данных пользователя из Active Directory (адреса электронной почты, названия организации, подразделения и должности пользователя, описания и фотографии пользователя);

6) возможность отображения в карточке пользователя информации из произвольных полей соответствующего пользователя Active Directory

7) возможность аутентификации пользователей, работающих с системой, на основании внутренних учетных записей (с запросом имени и пароля пользователя при входе в систему);

8) 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;

9) возможность выбора типов контактной информации, которая будет автоматически привязываться к карточке пользователя

10) возможность исключения определенных пользователей из процесса автоматической привязки контактной информации

11) возможность исключения определенной информации (IP-адрес, адрес электронной почты, имя компьютера, учетные записи Skype, ICQ, Viber, Telegram, WhatsApp, MS Exchange, ID социальной сети) из процесса автоматической привязки контактной информации

12) 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;

13) возможность интеграции с Active Directory с указанием доменов (объектов доменов) и контроллеров доменов, с которыми будет выполняться синхронизация;

14) синхронизацию 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;

15) автоматическую синхронизацию изменений идентификационных данных пользователей в Active Directory с данным в карточках пользователей возможностью настройки расписания синхронизации и синхронизируемых данных;

16) ведение журнала действий и авторизации пользователей, работающих с системой.

8. Требования к мониторингу работоспособности системы:

Мониторинг работоспособности должен позволять контролировать состояние системы в режиме реального времени. При этом обеспечивать следующие возможности:

1) панель мониторинга работоспособности системы, на которой представлена основная информация о работе всех основных компонентов системы, а также использовании ресурсов оборудования

2) ведение журнала событий серверных компонентов системы;

3) просмотр журнала, а также детальной информации и рекомендаций по каждому событию в консоли администратора;

4) фильтрация событий в журнале по дате, уровню события (информация, предупреждение, ошибка), серверному компоненту, источнику событий;

5) выбор определенных серверов источников событий для ведения мониторинга;

6) автоматическая очистка журнала по сроку хранения событий и их уровню;

7) возможность экспорта журнала событий в форматах PDF, XPS, CSV, XLS, XLSX, HTML, RTF, TXT

8) возможность печати журнала событий;

9) автоматическое уведомление администратора системы о новых событиях серверных компонентов по почте;

10) настройка правил отправки уведомлений по почте (выбор адресата, серверного компонента, уровня события или конкретных событий).

9. Требования к поиску информации:

Инструменты поиска информации должны позволять создавать поисковые запросы высокой детализации. Система должна предоставлять следующие возможности:

1) 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.;

2) поиск информации и по группам Active Directory;

3) поиск информации по категориям сайтов и приложений

4) поиск по цифровым отпечаткам с возможностью настройки порога срабатывания;

5) поиск по словарям, с возможностью учета порога срабатывания и морфологии;

6) поиск по хеш-суммам, с возможностью поиска по преднастроенным банкам хеш-сумм;

7) комбинирование нескольких простых поисковых условий при помощи логических операторов «И», «ИЛИ», «НЕ», с возможностью объединения поисковых условий в группы;

8) создание и использование шаблонов поиска – набора поисковых условий, которые можно использовать в других поисковых запросах комбинированного поиска;

9) добавление условия поиска в избранное, для дальнейшей работы;

10) импорт и экспорт условий поиска;

11) ограничение количества отображаемых результатов поиска.

10. Требования к отчетности:

Модуль отчетности системы должен обладать следующими возможностями:

1) построение отчетов по данным произвольно выбранных пользователей, групп пользователей либо групп Active Directory;

2) построение отчета как за весь период, так и за определенный интервал;

3) наличие мастера создания отчетов с кратким описанием возможностей отчета;

4) наличие предустановленных отчетов;

5) создание групп и подгрупп с количество уровней иерархии не менее 20;

6) перенос отчетов из группы в группу простым перетаскиванием «мышью»;

7) перенос подгрупп из группы в группу простым перетаскиванием «мышью»;

8) настройка прав доступа к различным типам отчетов

9) настройка расписания формирования отчетов, а также выбор почтовых адресов для рассылки

Все перехваченные данные должны представляться в форме отчетов следующих видов:

1) отчет «Активность пользователей»;

2) отчет по пользователям;

3) ТОП-отчет по пользователям;

4) отчет по политикам безопасности;

5) сводный отчет по пользователям;

6) отчет табель рабочего времени;

7) отчет по активности приложений;

8) отчет по браузер-активности.

9) отчет об общей активности пользователя

10.1. Требования к отчету «активность пользователей»:

«Активность пользователя» должна наглядно представлять активность пользователя на временной сетке с шагом в 1 час и содержать следующие данные и возможности:

1) информация о количестве отправленных и полученных писем;

2) информация о количестве сессий переписки пользователя в IM-клиентах с указанием длительности и количества сообщений в каждой сессии переписки;

3) 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;

4) информация о количестве посещенных URL и отправленных поисковых запросов;

5) информация о количестве сделанных системой снимков экрана рабочего стола пользователя;

6) информация о времени работы/простоя компьютера пользователя, детальная статистика активности приложений и данные о процентном соотношении времени работы в различных приложениях;

7) информация о количестве документов, помещенных в буфер обмена;

8) информация о посещении веб-сайтов с помощью веб-браузера с предоставлением комплексной и детальной статистики времени, проведенного на различных веб-ресурсах;

9) информация о количестве символов, введенных пользователем с клавиатуры;

10) информация должна быть динамическая и интерактивная. Переход по ссылкам должен приводить непосредственно к просмотру содержимого перехваченных документов либо веб-ссылок;

11) должна обеспечиваться 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 должна быть возможность выбора форматов внутреннего хранения разных типов документов и влиять на их отображение в ассоциированных просмотрщиках.

12) должна быть предусмотрена возможность представления информации 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);

13) графики по типам информации должны быть интерактивными и динамическими, для обеспечения перехода по ссылкам (точкам на графике) непосредственно к просмотру содержимого перехваченных документов;

14) сохранение статистики во внешний файл формата PDF или XPS;

15) 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;

16) возможность построения графа взаимосвязей с учетом промежуточных связей (количество промежуточных взаимосвязей до 5)

17) поддержка группировки контактов пользователя по принадлежности к установленным и не распознанным контактам.

18) просмотр взаимосвязей внешнего абонента с пользователями сети организации после предварительного создания карточки внешнего пользователя.

19) выбор масштаба отображения отчета при просмотре в клиентской консоли (с указанием % размера от оригинала).

20) возможность интерактивного перехода от просмотра схемы взаимосвязей к содержимому документов (письма, переписки, файлы и т.д.), которыми пользователь обменивался с конкретным абонентом.

21) поддержка сохранения отчета о взаимосвязях в виде графа во внешний файл формата PNG.

10.2. Требования к отчету по пользователям:

Отчет по пользователям должен предоставлять возможность построения сводного интерактивного отчета как по определенному пользователю, так и по нескольким пользователям, групп пользователей либо групп Active Directory за все время наблюдения или за выбранный интервал времени.

Отчет должен включать в себя следующую информацию:

Статистика перехвата данных, в том числе:

1) количество переданной и полученной пользователем информации по всем каналам передачи, включая почту и мессенджеры;

2) количество посещенных сайтов и поисковых запросов;

3) количество файлов, переданных/принятых по FTP;

4) количество распечатанных документов и страниц;

5) количество операций копирования в буфер обмена;

6) количество снятых скриншотов;

7) количество файлов, переданных на внешние накопители/сетевые ресурсы/облачные хранилища;

8) количество нажатых клавиш клавиатуры;

Информация об активности пользователя за компьютером, в том числе:

1) общее время активной работы пользователя за ПК;

2) среднесуточное время активной работы пользователя за ПК;

3) общее время простоя ПК;

4) среднесуточное время простоя ПК;

5) общее время присутствия сотрудника на работе;

6) среднесуточное время присутствия сотрудника на работе;

7) среднее время начала работы;

8) среднее время окончания работы;

9) общее количество рабочих дней;

10) 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);

11) гистограмму по времени активности/простоя компьютера пользователя за каждый день;

Информация об активности приложений на компьютере пользователя, в том числе:

1) процентное соотношение времени работы в различных приложениях (с построением круговой диаграммы);

2) полный список запускавшихся приложений с указанием абсолютного времени работы в каждом из них;

Информация о браузер-активности, в том числе:

1) рейтинг посещенных веб-ресурсов;

2) хронология активности в веб-браузере.

Информация о количестве зафиксированных инцидентов безопасности, инициированных пользователем, и соответствующих им правилах с различной степенью детализации.

Информация о количестве расследуемых дел, в которые вовлечен пользователь, в том числе:

1) открытых;

2) закрытых.

Должна быть предусмотрена возможность пакетного сохранения и настройки расписания рассылки отчетов для нескольких пользователей с предварительной настройкой единой формы отчета. При этом должна допускаться как отправка одним файлом по всем пользователям, так и создание отдельного файла для каждого пользователя.

10.3. Требования к ТОП-отчету по пользователям:

Должна быть предоставлена 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, в том числе:

1) возможность создания ТОП-отчета для произвольно выбранных пользователей, групп пользователей либо групп Active Directory;

2) возможность настройки количества пользователей в ТОП-отчете («ТОП-10», «ТОП-20» и т.д.) ;

3) возможность построения топ-отчетов за все время наблюдения или за выбранный интервал времени ;

4) 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»).

Должна быть предусмотрена возможность настройки рейтинга по различным показателям, в том числе:

1) количество входящих/исходящих писем, общее количество писем;

2) количество входящих/исходящих сообщений в мессенджерах, общее количество сообщений, количество переписок;

3) количество/время аудио-разговоров в Skype, Lync, Viber, Telegram, MS Teams, Zoom;

4) количество/время аудио-разговоров IP-телефонии;

5) количество посещенных веб-страниц;

6) количество поисковых запросов;

7) количество писем/публикаций в web-коммуникациях;

8) количество/размер файлов, записанных на USB-накопитель, сетевые ресурсы, облачные хранилища;

9) количество отправленных/принятых файлов, общее количество файлов по протоколу FTP, размер отправленных/принятых файлов, общий размер всех файлов по протоколу FTP;

10) количество распечатанных страниц/документов;

11) количество операций копирования текста в буфер обмена;

12) количество нажатых клавиш;

13) количество инцидентов безопасности;

14) количество дел с участием пользователя;

15) время активной работы/простоя ПК;

16) среднее время начала/окончания работы, время нахождения на работе.

10.4. Требования к отчету по нарушениям:

Должна быть предусмотрена возможность построения сводных интерактивных отчетов о статистике срабатывания правил безопасности, в том числе:

1) просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям;

2) детализация отчета по дням, неделям, месяцам, по пользователям

3) построение отчета за произвольный временной промежуток с просмотром итогового количества срабатываний и суммарного риска по каждому правилу в отдельности, а также суммарного количества срабатываний и суммарного риска по всем существующим правилам безопасности.

10.5 Требования к сводному отчету по пользователям:

Должна быть предусмотрена возможность построения сводных интерактивных отчетов о статистических показателях сетевой и локальной активности выбранных пользователей, в том числе:

1) возможность выбора показателей активности, по которым будет построен отчет;

2) просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям;

3) детализация отчета по дням, месяцам, за произвольный временной промежуток и просмотр сводной статистики по выбранным статистическим показателей.

Отчет должен предусматривать построение по следующим показателям активности:

1) количество входящих/исходящих писем, общее количество писем;

2) количество входящих/исходящих сообщений в мессенджерах, общее количество сообщений, количество переписок;

3) количество/время аудио-разговоров в Skype, Lync, Viber, Telegram, MS Teams, Zoom;

4) количество/время аудио-разговоров IP-телефонии;

5) количество посещенных веб-страниц;

6) количество поисковых запросов;

7) количество писем/публикаций в web-коммуникациях;

8) количество/размер файлов, записанных на USB-накопитель, сетевые ресурсы, облачные хранилища;

9) количество отправленных/принятых файлов, общее количество файлов по протоколу FTP, размер отправленных/принятых файлов, общий размер всех файлов по протоколу FTP;

10) количество распечатанных страниц/документов;

11) количество операций копирования текста в буфер обмена;

12) количество нажатых клавиш;

13) количество инцидентов безопасности;

14) количество дел с участием пользователя;

15) время активной работы/простоя ПК;

16) среднее время начала/окончания работы, время нахождения на работе.

10.6 Требования к отчету «табель рабочего времени»:

Отчет должен регистрировать использование рабочего времени сотрудниками, с регистрацией времени прихода и ухода с работы, активного времени работы, времени присутствия сотрудников на рабочем месте, а также иметь следующие возможности:

1) возможность задания графика рабочего времени и выделения отклонения от рабочего графика;

2) возможность задать норму активной работы пользователя и выделять отклонения от нее;

3) возможность исключать из учета определенный временной промежуток (например, время обеда);

4) возможность построения отчета за текущий календарный месяц, а также за указанный месяц.

10.7 Требования к отчету по активности приложений:

Отчет должен содержать информацию об использовании приложений сотрудниками и учитывать только время работы в активных приложениях, а также иметь следующие возможности:

1) возможность построения отчетов по приложениям либо по категориям/продуктивности приложений с учетом данных категоризатора приложений;

2) представление отчета на выбор в виде гистограммы, линейчатой либо круговой диаграммы, в виде таблицы;

3) возможность настройки отчета по активности работы в определенных приложениях, либо исключения определенных приложений из отчета;

4) возможность построения отчета в разрезе наиболее активных пользователей с указанием их количества.

10.8 Требования к отчету по браузер-активности:

Отчет должен содержать информацию об использовании рабочего времени на сайтах и учитывать только время работы на сайтах в активной вкладке браузера а также иметь следующие возможности:

1) возможность построения отчетов по веб-сайтам либо по категориям/продуктивности веб-сайтов с учетом данных категоризатора веб-сайтов;

2) представление отчета на выбор в виде гистограммы, линейчатой либо круговой диаграммы, в виде таблицы;

3) возможность настройки отчета только по определнным веб-сайтам, либо исключения определенных веб-сайтов из отчета;

4) возможность построения отчета в разрезе наиболее активных пользователей с указанием их количества.

10.9 Требования к отчету по общей активности:

Отчет должен содержать информацию об использовании рабочего времени на сайтах и учитывать только время работы на сайтах в активной вкладке браузера а также иметь следующие возможности:

1) возможность построения отчетов по приложениям и веб-сайтам либо по категориям/продуктивности веб-сайтов с учетом данных категоризатора веб-сайтов и приложений;

2) представление отчета на выбор в виде гистограммы, линейчатой либо круговой диаграммы, в виде таблицы;

3) возможность настройки отчета только по определнным веб-сайтам и приложениям, либо исключения определенных веб-сайтов и приложений из отчета;

4) возможность построения отчета в разрезе наиболее активных пользователей с указанием их количества.

11. Требования к формированию правил/политик безопасности:

Система должна обладать функционалом, предназначеным для настройки системы оповещения уполномоченных лиц о случаях нарушения правил безопасности. Перехваченные данные должны анализироваться в автоматическом режиме на основании заданного списка правил безопасности. При работе с политиками безопасности пользователю должен быть доступен следующий функционал:

1) 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.;

2) комбинирование нескольких простых поисковых условий при помощи логических операторов «И», «ИЛИ», «НЕ», с возможностью объединения поисковых условий в группы;

3) правила безопасности по группам Active Directory;

4) правила безопасности по категориям сайтов и приложений;

5) создание политик безопасности с использованием шаблонов поиска – набора поисковых условий, которые можно использовать при формировании других правил безопасности;

6) правила безопасности по цифровым отпечаткам с возможностью настройки порога срабатывания;

7) правила безопасности по словарям, с возможностью учета порога срабатывания и морфологии;

8) правила безопасности по хеш-суммам, с возможностью поиска по преднастроенным банкам хеш-сумм;

9) 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.;

10) наличие предустановленных правил безопасности;

11) возможность создания групп и подгрупп с количество уровней иерархии не менее 20;

12) возможность отключения правила безопасности

13) фильтр включенных/выключенных правил безопасности

14) возможность переноса политик безопасности из группы в группу простым перетаскиванием «мышью»;

15) возможность переноса подгрупп из группы в группу простым перетаскиванием «мышью»;

16) добавление, исключение групп Active Directory, к которым могут быть применены политики безопасности;

17) добавление, исключение, редактирование категорий инцидентов сервера безопасности

18) задание и редактирование уровня риска инцидентов сервера безопасности

19) автоматический расчёт показателей уровней риска пользователей и поведенческого анализ на основании уровней риска инцидентов;

20) возможность выполнения скриптов при срабатывании или ошибке срабатывания правила безопасности;

21) возможность отправки данных о инцидентах в сторонние системы;

22) автоматическая доставка уведомлений по электронной почте ответственному лицу в случае срабатывания политики безопасности (выявления инцидента);

23) инцидент содержит общую информацию (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;

24) 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.);

25) возможность просмотра всех инцидентов по выбранной политике безопасности в клиентской консоли с возможностью выделения просмотренных, непросмотренных инцидентов для каждого офицера безопасности, работающего с системой;

26) 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.

27) возможность назначения статуса для инцидента (инцидент не расследован, расследование инцидента отложено, инцидент расследован, важный инцидент, неважный инцидент, ложное срабатывание);

28) возможность присвоения цветовой категории инциденту

29) возможность добавления комментария к инциденту

30) возможность гибкого выборочного просмотра инцидентов по политике безопасности (например, показать только новые или не просмотренные 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.);

31) 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.);

32) 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.);

33) 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 не просмотренные) – и по комбинациям этих параметров;

34) 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);

35) возможность экспорта перехваченных данных, вызвавших срабатывание политики безопасности, в файлы соответствующих форматов;

36) ведение журнала (лога) действий офицера безопасности с возможностью экспорта событий журнала;

37) в журнале событий регистрируется следующая информация создание, дублирования, редактирование, удаление правила безопасности, просмотр и удаление инцидента, изменения статусов инцидента и др.

12. Требования к функционалу расследования нарушений:

Система должна обладать функционалом, позволяющим организовать работу с документацией в рамках расследований инцидентов безопасности и обладать следующими возможностями:

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;

2) аудит результатов перехвата, обеспечивающий 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.

3) 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, в том числе просмотр дела;

 дату и время совершенного действия;

 прочую дополнительную информацию, которая может быть полезна для контроля за ведением дела.

4) в целях упрощения работы лиц, ведущих расследование, система должна обеспечивать:

 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 «мышью»;

 возможность переноса подгрупп из группы в группу простым перетаскиванием «мышью»;

 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 левой либо правой стороне окна программы.

13. Требования к функционалу анализа рисков:

Система должна предусматривать контрольно-аналитические механизмы, позволяющие отслеживать аномальные и потенциально опасные для организации изменения в поведении сотрудников, которые позволяют:

1) формировать модели поведения сотрудников и задавать им соответствующий уровень риска;

2) информировать специалистов отдела безопасности об уровне риска, поведении сотрудников и об инцидентах правил безопасности, которые вызвали изменения уровня риска;

3) отслеживать изменения в поведении сотрудников в режиме реального времени при помощи количественных показателей и графиков;

4) просматривать изменения уровня риска как для непросмотренных событий, так и для всех событий;

5) сохранять, отправлять на печать табличный отчет по уровню риска пользователей;

Также должны быть предусмотрено:

1) гибкая фильтрация отчета по уровням риска по дате, избранным пользователям, категории риска, уровням критичности, факта наличия риска у пользователей, текстовая фильтрация;

2) графическое представление уровня риска пользователей, с возможностью отображения линейного графика либо гистограммы;

3) наличие предустановленных поведенческих моделей (категорий риска), готовых к использованию.

14. Требования к масштабированию системы:

1) Все компоненты должны иметь возможность устанавливаться на один сервер или разнесены по разным, чтобы обеспечить нужную масштабируемость при одновременном контроле большого количества сотрудников;

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

3) возможность установки нескольких серверов перехвата данных– для распараллеливания перехвата нескольких контролируемых каналов выхода в интернет;

4) возможность установки нескольких серверов контроля агентов– для контроля разных сегментов сети или разных групп компьютеров;

5) возможность установки нескольких промежуточных серверов агентов для балансировки нагрузки на сеть.

6) возможность организации кластера для горизонтального масштабирования больших нагрузок по множеству серверов;

7) возможность установки нескольких серверов индексирования– для оптимизации и распределения нагрузки на сервер и базу данных;

8) возможность работы с несколькими почтовыми серверами (MS Exchange, IBM Lotus Domino и др.) одновременно.

Система должна обеспечивать полную поддержку распределения нагрузки в многоядерных и многопроцессорных системах.

15. Требования к администрированию системы:

Система должна предусматривать следующие возможности:

1) централизованное управление всеми компонентами системы из двух консолей: единая консоль администратора и единая консоль пользователя (сотрудника службы ИБ);

2) обеспечивать возможность шифрования трафика между консолями и сервером;

3) централизованное подключение и настройка хранилищ информации для всех серверных компонентов системы;

4) возможность отключения автоматического управления системным брандмауэром;

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

6) возможность настройки автоматического запуска программ и скриптов при срабатывании правил безопасности;

7) обеспечивать наблюдение за состоянием всех серверных компонентов и сервисов системы в режиме реального времени, с выводом основной статистики по каждому из них, а также управление запуском серверных компонентов и сервисов из системы;

8) поддерживать параллельную работу нескольких пользователей в консоли администратора;

9) возможность авторизации серверов системы на в автоматическом и ручном режиме;

10) возможность замены логотипа системы в экспортируемых документах на пользовательский логотип.

11) возможность перевода часового пояса для улучшения качества просмотра данных полученных из других часовых поясов

16. Требования к авторизации пользователей:

Система должна предоставлять несколько вариантов авторизации

1) на основании учетных записей Windows;

2) на основании внутренней системы аутентификации.

Система должна обладать следующими возможностями:

1) возможность ограничения срока действия пароля (в днях), по истечении которого доступ к системе будет закрыт;

2) возможность блокировки пользователя после 3-х неудачных попыток входа;

3) возможность сохранения информации обо всех попытках авторизации в журнале;

4) возможность задания дополнительного пароля для изменения настроек консоли Администратора;

5) возможность автоматического выхода из консолей при превышении заданного времени простоя;

6) возможность автоматического выхода из консоли по истечении заданной продолжительности сеанса.

17. Требования к политике лицензирования ПО:

Схема лицензирования должна определяться выбором количества подконтрольных рабочих мест, способов перехвата, а также возможностью помодульной поставки в случае использования агентского типа перехвата:

1) Контроль MAIL: SMTP(S); POP3(S); MAPI, IMAP;

2) Контроль WEB: HTTP(S) (сообщения в форумах и социальных сетях, посещенные сайты, отправленные файлы), web-коммуникации (Gmail.com, Mail.ru, Rambler.ru, Yahoo.ru, Yandex.ru);

3) Контроль мессенджеров: возможность перехвата и архивирования вложенных файлов, текстовых и голосовых данных в SIP, Skype, Telegram, Viber; перехват голосовых и текстовых сообщений в Microsoft Lync; возможность перехвата текстовых данных и вложенных файлов в Slack, перехват текстовых сообщений в AIM, Google Hangouts, Google Talk, ICQ, Mail.Ru Агент, Miranda, PSI, WhatsApp, Windows Messenger, Yahoo! Messenger, и др., в том числе использующих шифрование;

4) Контроль внешних устройств: внешние накопители информации; локальные и сетевые принтеры; мобильные телефоны, подключаемые в качестве накопителя; файлы, пересылаемые на сетевые ресурсы;

5) Контроль устройств печати;

6) Контроль FTP(S);

7) Контроль активности персонала: формирование скриншотов; функционал кейлогера; перехват содержимого буфера обмена; контроль запуска и времени использования любых приложений; контроль рабочего времени и простоя компьютера; контроль времени, проведенного на каждом из сайтов; мониторинг и запись аудио с микрофонов, системных звуков, видео с рабочих столов и веб-камер;

8) Индексация рабочих станций: контроль файловых систем, в ходе которого выполняется поиск на рабочих станциях или серверах файлов, представляющих интерес в рамках обеспечения информационной безопасности.

9) Аудит операций с файлами и папками

Система должна лицензироваться в соответствии с количеством серверных компонентов, входящих в комплект поставки и, в зависимости от схемы лицензирования, в соответствии с количеством одновременно контролируемых пользователей, IP-адресов или email-адресов.

В случае использования перехвата агентами, либо перехвата через ICAP-сервер, то лицензия должна распространяться на количество одновременно контролируемых пользователей. При этом должна отсутствовать жесткая привязка лицензии к конкретным рабочим станциям или пользователям. Количество приобретенных лицензий должно определяться только количеством одновременно контролируемых пользователей, при этом сам список контролируемых пользователей должен быстро и гибко изменяться в случае необходимости (например, при наличии 100 пользователей в сети и только 50 лицензий – возможность контролировать попеременно то первых, то вторых 50 пользователей, при этом должна быть предусмотрена возможность переназначения лицензионных слотов не чаще 1 раза в сутки).

Если схема перехвата предусматривает контроль сторонних почтовых серверов, то должно лицензироваться количество почтовых учетных записей, контролируемых сервером обработки почты.

В процессе своего функционирования система не должна оказывать негативного влияния на функционирование прикладных ИС Заказчика.