Функциональные характеристики Серчинформ ДЛП

ВОЗМОЖНОСТИ СЕРЧИНФОРМ ДЛП

Серчинформ ДЛП предназначен для сбора и анализа информационных потоков в рамках локальной вычислительной сети. Сбор данных возможен двумя способами, в зависимости от используемого серверного компонента: EndpointController или NetworkController. Серверные компоненты представляют собой платформы, на которых работают модули перехвата данных. Каждый модуль перехвата выступает в роли анализатора трафика и контролирует свой канал передачи данных.

В данном документе подробно рассмотрены возможности модулей перехвата, входящих в состав серверных компонентов СЕРЧИНФОРМ ДЛП.

1 Возможности модулей перехвата EndpointController для Windows

В нижеследующей таблице приведены возможности EndpointController, использующего агентов, установленных на рабочие станции сети.

Модуль	Функциональность	Опции
KeyLogger	1. Перехват нажатых клавиш 2. Перехват функциональных клавиш 3. Перехват текста из буфера обмена	Фильтрация для Пользователей/Групп или процессов. Возможность исключить системные действия. Возможность исключить перехват паролей Блокировка нажатия PrintScreen Перехват только клавиш/буфера обмена/всего Настройка размера буфера обмена в КБ
CameraController	1. Создание снимков 2. Видеозапись 3. Подключение к камере в реальном времени	Возможность задать интервал создания снимков, опции видеозаписи, отдельные опции для выбранных приложений, пользователей, url, настройки сохранения снимка в указанном размере (в % от исходного).
Cloud & Sharepoint	1. Google Drive, Docs 2. OneDrive 3. SkyDrive 4. Office 365 5. DropBox 6. Evernote 7. Яндекс.Диск 8. Cloud.mail.ru 9. Amazon S3 10. iCloud 11. DropMeFiles 12. OwnCloud 13. Pcloud 14. OziBox 15. MediaFire 16. OpenDrive 17. 4shared 18. Box 19. Syncplicity 20. CloudMe 21. MiMedia 22. My-Files 23. Nextcloud	Нет

Модуль	Функциональность	Опции
	24. Seafile 25. SharePoint 26. Acronis File Advanced 27. TeamViewer 28. RealVNC 29. Radmin 30. LiteManager	
FTPController	Перехват файлов, передаваемых по протоколу FTP	Максимальный размер перехватываемого файла, интервал обновления, тайм-ауты последней активности
ProgramController	Перехват времени работы в приложениях и на веб-сайтах. Контроль времени, проведенного на веб-сайтах, поддерживается для следующих актуальных версий браузеров: ▪ Internet Explorer (с версии 8) ▪ Mozilla Firefox (с версии 50.1.0) ▪ Google Chrome (с версии 55.0.2883.87) ▪ Yandex Browser (16.11.0.2680) ▪ Opera (Presto) (36.0.2130.80) ▪ Opera (Chromium) ▪ Safari ▪ Tor Browser ▪ Netscape Navigator ▪ Амиго (с версии 54.0.2840.189) ▪ Спутник (с версии 2.1.1051.0) ▪ Flock (02.06.2001) ▪ Avant Browser ▪ Lunascape ▪ Maxthon ▪ SeaMonkey ▪ K-Meleon ▪ SlimBrowser ▪ Edge (с версии 38.14) ▪ Comodo Dragon (с версии 52.15.25.664) ▪ CoolNovo (2.0.9.20) ▪ Cốc Cốc (с версии 56.3.150) ▪ Titan Browser (с версии 33.0.1712.0 (235591) ▪ Uran (с версии 43.0.2357.134)	Фильтрация для Пользователей\Групп или процессов. Возможность исключить системные действия. Возможность отключить аудит активности на веб-сайтах.
PrintController	1. Перехват печати на локальных принтерах 2. Перехват печати на сетевых принтерах 3. Перехват печати на виртуальных принтерах	Опции качества (сжатия) для изображений Фильтрация по пользователям, процессам, описанию, принтеру и расположению. Возможность заблокировать Escape функции (управление принтером напрямую через escape команды).
HTTPController	1. Перехват POST-запросов 2. Перехват GET-запросов	Ограничение по минимальному размеру POST-запроса. Ограничение по перехватываемым узлам, IP-адресам, портам, типу (SSL/без SSL), процессам. Возможность добавить список сервисов анонимайзеров. Возможность блокировать SPDY и QUIC. Возможность исключать MIME типы (аудио, видео, картинки)

Модуль	Функциональность	Опции
		Перехват паролей, хранящихся в браузерах. Создание белых и черных списков для блокировки и/или разрешения посещения Интернет-ресурсов. Определение выводимого оповещения при блокировке доступа к запрещенному ресурсу.
MonitorController	1. Создание скриншотов 2. Видеозапись действий пользователя 3. Подключение к монитору пользователя в реальном времени.	Возможность задать интервал снятия скриншотов, принудительный скриншот при смене активного окна, снятие скриншота по нажатию клавиши PrintScreen, интервал снятия скриншотов для видеоконференций Skype, Lync и для URL, отдельные опции для выбранных приложений, пользователей, настройки цветности, настройки для нескольких мониторов, настройки сохранения снимка в указанном размере (в % от исходного). Возможность задать настройки цветности, исключения фона, настройки частоты кадров. Возможность задать расписание и режим работы (для всех или только для выбранных) Возможность задать настройки доступа к подключению по паролю или для указанных пользователей.
MicrophoneController	1. Запись с микрофона 2. Подключение к микрофону пользователя в реальном времени	Возможность задать настройки для профилей *В офисе/Вне офиса*: максимальная длительность файла, шумоподавление, запись без логина пользователя, автоматическое включение выключенного микрофона, качество записи, определение речи, перечень ПО. Возможность задать расписание записи. Возможность задать настройки доступа к подключению по паролю или для указанных пользователей. Распознавание аудио (перевод речи в текст)
MailController	Перехват следующих протоколов: ▪ IMAP ▪ MAPI ▪ POP3 ▪ SMTP ▪ NNTP ▪ WebMail в составе: – mail.ru – gmail.com – tut.by – yandex.ru – rambler.ru – outlook.com – office 365 – ukr.net – yahoo.com – qip.ru – Google Sync – и другие	<u>Общие настройки:</u> Фильтрация по отправителю, получателю, доменному пользователю, теме, протоколу, размеру, количеству получателей. Индивидуальные настройки для WebMail: возможность отключить/включить перехват входящей почты. Блокировка почты по контентным и\или контекстным критериям передаваемой по протоколам SMTP, MAPI, IMAP с помощью агента. Блокировка исходящей почты по контентным и\или контекстным критериям на почтовом сервере без необходимости установки агента.

Модуль	Функциональность	Опции
IMController	Перехват следующих протоколов: 1. ICQ 2. MMP (mail.ru агент) 3. XMPP (Jabber) 4. Gadu-Gadu 5. Lync (Skype for Business, Microsoft Teams) 6. Viber 7. Telegram 8. WhatsApp 9. Skype 10. HTTPIM в составе: – vk.com – ok.ru – facebook.com – mamba.ru – my.mail.ru – linkedin – Evernote – Google+ – Yammer – Fotostrana – Slack.com – Web-Skype – Web-Telegram – Web-WhatsApp – icq.com – Bitrix24 – Lotus Sametime – Rocket.chat – Mattermost – Imo.Im – Discord – Hipchat – и другие	Перехват списка контактов Перехват чатов, звонков, файлов, контактов, истории сообщений, настройки максимального размера файла, звука и длительности Распознавание аудио (перевод речи в текст) ▪ Skype – Перехват чатов, звонков, файлов, контактов, SMS, истории сообщений ▪ Lync – Перехват чатов, звонков, файлов, контактов ▪ Viber – Перехват чатов, звонков, файлов, контактов, истории сообщений ▪ Telegram – Перехват чатов, звонков, файлов, контактов ▪ WhatsApp – Перехват чатов ▪ Web-Skype – Перехват чатов, файлов ▪ Web-Telegram – Перехват чатов ▪ Web-WhatsApp – Перехват чатов
Индексация рабочих станций	Отслеживание появления, копирования, перемещения и удаления конфиденциальной информации на рабочих станциях.	Фильтрация по расположению, типам файлов. Возможность сохранять удаленные файлы с указанием периода хранения.
DeviceController	**A)** Доступны *Аудит* + *Запрет доступа*: 1. USB HID устройства (кроме клавиатур и мышей) 2. Принтеры (USB) 3. Bluetooth адаптеры (USB) 4. Сканеры (USB) 5. Токены 6. Сетевые адаптеры (USB) 7. Все устройства USB (кроме концентраторов) 8. COM порты 9. LPT порты 10. Bluetooth 11. Сетевые адаптеры 12. Принтеры 13. ИК порты 14. Медиа устройства 15. HID устройства (кроме клавиатур и мышей) 16. Клавиатура и мышь 17. FireWire 18. Смарт карты 19. КПК	Общие опции: ▪ Максимальный размер обрабатываемого файла ▪ Исключение системных пользователей ▪ Черные и белые списки по типу, устройству, производителю, серийному номеру, пользователю, компьютеру. ▪ Ограничение по объему записываемых данных. ▪ Блокировка записи по содержимому для USB-устройств хранения данных. ▪ Ограничения для LAN, позволяет управлять настройками сетевых устройств (кроме встроенных сетевых карт) при подключении LAN-кабеля. Опции для группы "**A**": ▪ Пользователи\Группы ▪ Компьютеры ▪ Полный доступ\Нет доступа

Модуль	Функциональность	Опции
	20. Ленточные накопители 21. Блокировка папок 22. Блокировка дисков 23. Процессы 24. Модемы (PPP соединение) 25. Wi-Fi **Б)** Доступны *Аудит* + *Запрет доступа* + *Теневое копирование*: 1. Устройства хранения USB 2. CD/DVD-ROM 3. Камеры/Сканеры 4. Floppy диски 5. SCSI 6. Сетевые папки 7. Буфер обмена 8. RDP (диски, буфер) 9. Переносимые устройства: ▪ Android ▪ Apple ▪ Blackberry ▪ Palm ▪ Windows Phone ▪ Все переносимые устройства	▪ Аудит Вкл\Выкл ▪ Исключение системных пользователей. Дополнительные опции для группы "**Б**": Опции, доступные для вышеописанных, а также: ▪ Теневое копирование по имени файла, типу файла, процессу, пользователю, компьютеру ▪ Доступ по имени файла, типу файла, процессу, пользователю, компьютеру. ▪ Теневое копирование **хранящейся** на устройстве информации.
Файловый аудит	Аудит любых событий файловой системы (создание, изменение, открытие, удаление и т.д.) для файлов или папок. Отслеживание появления, копирования, перемещения и удаления конфиденциальной информации на рабочих станциях, сканирование (как локальное, так и сетевое), классификация, теневое копирование и вычитка прав доступа файлов	Фильтрация для Пользователей/Групп или процессов/файлов. Возможность исключить системные действия. Аудит изменений прав доступа на файл/папку. Возможность исключить аудит временных файлов MS Office. Доступен следующий вид поиска: ▪ поиск по тексту (включая морфологию); ▪ поиск с использованием регулярных выражений; ▪ поиск по значениям атрибутов (имя файла, тип файла, размер, местоположение и т.д.). Доступна настройка по количеству хранения теневых копий версий документа.
Шифрование данных	Шифрование всех типов данных, записываемых на внешние устройства хранения USB с использованием уникального ключа (генерируется пользователем)	Доступно шифрование для выбранных пользователей или групп. Для зашифрованных файлов есть настойки доступа для: ▪ Всех пользователей, кроме указанных ▪ Только указанных пользователей. Файл возможно открыть только при наличии агента и разрешения на открытие. Настройки черного/белого списка так же могут относиться к шифрованию. Доступна настройки теневой копии, где будут фиксироваться ТОЛЬКО шифрованные файлы.

Модуль	Функциональность	Опции
SSL-уведомления	Уведомления о неудачных попытках агента внедриться в соединение[1]	Доступно автоматическое добавление таких соединений в исключения перехвата. Доступна фильтрация по времени, ПК, пользователю, процессу и типу.
Аудит технических данных	Аудит тех. данных с PC с агентами[2]: ▪ Установленное ПО ▪ Аппаратная конфигурация ▪ Активный пользователь ▪ Статус агента и ПК ▪ Свободное место на диске ▪ Последняя активность агента ▪ Аудит данных диспетчера задач	Нет опций

2 Возможности NetworkController

В нижеследующей таблице приведены возможности NetworkController при сетевом перехвате данных с использованием технологии SPAN (зеркальный перехват) или при интеграции с прокси-сервером.[3] Возможность блокировки работает только при интеграции с прокси сервером по ICAP.

Модуль	Где доступно	Функциональность	Опции
Cloud & Sharepoint	Полноценная работа, как правило, в ICAP (все соединения шифрованные). Либо использование схемы подмена сертификата + SPAN (например, с оборудованием PaloAlto)	Перехват следующих сервисов при работе через web-интерфейс (не используя приложение!): 1. Перехват сервиса Google Drive, Docs 2. Перехват сервиса OneDrive (Microsoft) 3. Перехват сервиса Office 365 (Office Online) 4. Перехват сервиса DropBox 5. Перехват сервиса Evernote 6. Перехват сервиса Яндекс.Диск 7. Перехват сервиса Cloud.mail.ru 8. Перехват сервиса OwnCloud 9. Перехват сервиса MediaFire 10. Перехват сервиса MyFiles.ru 11. Перехват SharePoint	Ограничение по портам. Фильтрация по хостам, отправителю, размеру и содержимому. Возможна блокировка по атрибутам [4]

[1] Данный отчет доступен только совместно с HTTPController.

[2] Доступно вне зависимости от используемых протоколов. Не требует лицензирования.

[3] Все соединения, проходящие с использованием SSL, возможно перехватить при интеграции с прокси-сервером, либо схема подмена сертификата + SPAN на специализированном оборудовании.

[4] Блокировка возможна только при схеме ICAP, блокировка не работает со SPAN!

Модуль	Где доступно	Функциональность	Опции
MailController	SPAN – доступно все. ICAP - только web mail.	Перехват следующих протоколов: ▪ IMAP ▪ MAPI (без шифрования) ▪ POP3 ▪ SMTP ▪ NNTP ▪ WebMail в составе: – mail.ru – gmail.com – tut.by – yandex.ru – rambler.ru – outlook.com – office 365 – ukr.net – yahoo.com – qip.ru – Google Sync – и другие	Общие настройки: Фильтрация по отправителю, получателю, доменному пользователю, теме, протоколу, размеру, порту, служебным полям. Индивидуальные настройки для WebMail: возможность отключить/включить перехват входящей почты. Возможна блокировка WebMail по атрибутам
HTTPController	И в SPAN, и в ICAP Для части прокси-серверов не работает перехват GET-запросов [5]	Перехват POST-запросов Перехват GET-запросов	Ограничение по минимальному размеру POST запроса. Ограничение по перехватываемым узлам, IP, портам, отправителю, размеру. Возможность добавить список сервисов анонимайзеров. Возможна блокировка по атрибутам
FTPController	И в SPAN, и в ICAP	Перехват файлов, передаваемых по протоколу FTP	Максимальный размер перехватываемого файла, интервал обновления, тайм-ауты последней активности
IMController	SPAN – доступно все. ICAP – только web IM.	Перехват следующих протоколов: ▪ ICQ ▪ MMP (mail.ru агент) ▪ XMPP(Jabber) ▪ HTTPIM в составе: – vk.com – ok.ru – facebook.com – mamba.ru – my.mail.ru – linkedin – Evernote – Google+ – Yammer – Fotostrana – Web-Skype – icq.com – Imo.Im – и другие	Ограничение по перехватываемым узлам, IP, портам, отправителю, размеру. Возможность добавить список сервисов анонимайзеров. Возможность перехвата любого перечисленного протокола с использованием HTTP туннелирования. Возможна блокировка Web IM по атрибутам

[5] Список прокси-серверов, работающих полноценно со входящим и исходящим трафиком: SQUID, BLUE COAT, MCAFEE, WEBSENSE (Forcepoint), ISA\TMG. Только исходящий трафик поддерживают прокси-серверы FortiGate и Check Point. Список прокси-серверов не является полным, он содержит лишь те прокси, которые тестировались компанией-разработчиком на предмет совместимости со своим решением.

Модуль	Где доступно	Функциональность	Опции
Телефония	Только SPAN	Перехват аудио звонков и текстовых сообщений телефонии SIP через стандарты: ▪ GSM ▪ A-Law ▪ u-Law ▪ G.722	Возможность ограничения по используемым портам, пользователям, компьютерам, IP адресам, MAC адресам.

3 Возможности интеграции NetworkController с почтовыми серверами, Lync (Skype for Business) и ISA\TMG

Модуль	Где доступно	Функциональность
Lync/Skype for Business	Перехват: ▪ Чаты Аудит: ▪ Звонки ▪ Файлы	В режиме интеграции полноценно перехватываются только сообщения. Переданные файлы и звонки будут зафиксированы в аудите, но их содержание останется недоступно. Для полноценной работы с файлами и звонками рекомендуется использовать платформу Endpoint
ISA/TMG	1. Перехват POST-запросов 2. Перехват GET-запросов	Решение полностью функционально в плане перехвата данных, но не способно производить блокировку – это связано с особенностями архитектуры TMG (данный прокси не поддерживает ICAP, именно поэтому у нас используется отдельный модуль интеграции)
Почтовые сервера	1. Вычитка корпоративных ящиков через механизм POP3 или IMAP. 2. Вычитка корпоративных почтовых ящиков через механизм EWS 3. Прослушивание SMTP	Данные методики интеграции не завязаны на конкретных производителях или версиях почтовых серверов (за исключением EWS) и являются крайне универсальными. Они могут быть использованы в Exchange, Lotus, Postfix и даже ряде публичных почтовых серверов.

4 Возможности модулей перехвата EndpointController для Linux [6]

Модуль	Функциональность	Опции
Cloud & Sharepoint	Перехват следующих сервисов при работе через web-интерфейс (не используя приложение!): ▪ Google Drive, Docs ▪ OneDrive ▪ SkyDrive ▪ Office 365 ▪ DropBox ▪ Evernote ▪ Яндекс.Диск ▪ Cloud.mail.ru ▪ Amazon S3 ▪ iCloud ▪ DropMeFiles ▪ OwnCloud ▪ Pcloud ▪ OziBox ▪ MediaFire ▪ OpenDrive ▪ 4shared ▪ Box ▪ Syncplicity ▪ CloudMe ▪ MiMedia ▪ My-Files ▪ Перехват SharePoint	Нет
FTPController	Перехват файлов, передаваемых по протоколу FTP	Максимальный размер перехватываемого файла, интервал обновления, тайм-ауты последней активности
HTTPController	1. Перехват POST-запросов 2. Перехват GET-запросов	Ограничение по минимальному размеру POST-запроса. Ограничение по перехватываемым узлам, IP-адресам, портам, типу (SSL/без SSL), процессам. Возможность добавить список сервисов анонимайзеров. Возможность блокировать SPDY и QUIC. Возможность исключать MIME типы (аудио, видео, картинки)

[6] Поддерживаются следующие операционные системы семейства Linux: Astra Linux (1.4 x64 «Смоленск» и «Орел», 1.6 x64 «Смоленск», 2.12 x64 «Орёл»), AltLinux (8 x32/x64 и 9 x32/x64), CentOS (7.3 x64, 7.6 x64), GosLinux (6.4 x64) ROSA Linux (6.8 x64), Ubuntu (16.04 x32/x64, 17.04 x32/x64, 18.04 x64).

Модуль	Функциональность	Опции
MailController	Перехват следующих протоколов: ▪ IMAP ▪ MAPI (без шифрования) ▪ POP3 ▪ SMTP ▪ NNTP ▪ Web Mail в составе: – mail.ru – gmail.com – tut.by – yandex.ru – rambler.ru – outlook.com – office 365 – ukr.net – yahoo.com – qip.ru – Google Sync – и другие	Общие настройки: Фильтрация по отправителю, получателю, доменному пользователю, теме, протоколу, размеру. Индивидуальные настройки для Web Mail: Возможность отключить/включить перехват входящей почты.
IMController	Перехват следующих протоколов: 1. ICQ 2. MMP (mail.ru агент) 3. XMPP (Jabber) 4. HTTP IM в составе: – vk.com – ok.ru – facebook.com – mamba.ru – my.mail.ru – linkedin – Evernote – Google+ – Yammer – Fotostrana – webim.ru – Slack.com – Web-Skype – icq.com – Bitrix24 – и другие	Перехват списка контактов
SSL-уведомления	Уведомления о неудачных попытках агента внедриться в соединение	Доступно автоматическое добавление таких соединений в исключения перехвата. Доступна фильтрация по времени, ПК, пользователю, процессу и типу.
DeviceController[7]	Доступны Аудит + Запрет доступа: 1. Устройства хранения USB 2. Сетевые папки 3. Модемы 4. Сетевые адаптеры, в том числе подключаемые по USB 5. Wi-Fi-адаптеры	Общие опции: ▪ Пользователи ▪ Компьютеры ▪ Аудит Вкл\Выкл ▪ Полный доступ\Нет доступа ▪ Черные и белые списки по типу, устройству, производителю, серийному номеру

[7] Возможность блокировки USB-устройств и сетевых ресурсов поддерживается только на следующих операционных системах семейства Linux: Astra Linux (1.6 x64 «Смоленск» и 2.12 x64 «Орёл»), AltLinux (8 x32/x64 и 9 x32/x64), CentOS (7.6 x64), Ubuntu (16.04 x32/x64, 17.04 x32/x64, 18.04 x64).

Модуль	Функциональность	Опции
MonitorController [8]	Создание скриншотов	Возможность задать интервал снятия скриншотов, принудительный скриншот при смене активного окна, снятие скриншота по нажатию клавиши PrintScreen, настройки цветности, настройки сохранения снимка в указанном размере (в % от исходного). Возможность задать расписание.
KeyLogger [9]	Перехват нажатых клавиш Перехват функциональных клавиш Перехват текста из буфера обмена	Фильтрация для Пользователей/Групп или процессов. Возможность исключить системные действия. Перехват только клавиш/буфера обмена/всего

[8] Поддерживается только на следующих операционных системах семейства Linux: AltLinux (8 x32/x64 и 9 x32/x64), CentOS (7.6 x64), Ubuntu (16.04 x32/x64, 18.04 x64)

[9] Поддерживается только на следующих операционных системах семейства Linux: AltLinux (8 x32/x64 и 9 x32/x64), CentOS (7.6 x64), Ubuntu (16.04 x32/x64, 18.04 x64)

5 Возможности блокировки в СЕРЧИНФОРМ ДЛП

Контур информационной безопасности не только проводит подробнейший аудит перемещаемой информации и создает теневые копии документов, но и позволяет блокировать передачу информации по широкому списку каналов коммуникации. Список каналов, которые возможно перехватывать и список каналов, которые можно блокировать, различаются, поэтому ниже приведен подробный список возможной блокировки данных, доступной в DLP.

Блокировка может работать на разных уровнях: при передаче информации по сети, на конечной рабочей станции и с использованием почтового сервера заказчика.

5.1 Блокировка на уровне агента

- Блокировка любых подключаемых устройств по их типу, серийному номеру и другим атрибутам. Например, блокировка COM, LPT портов, принтеров, сканеров и т.д. В первой таблице приведен полный список возможностей модуля DeviceController.
- Блокировка передачи на устройства хранения (USB, CD/DVD, SCSI и т.д.).
- Блокировка по объему записываемых данных на устройства хранения, переносные устройства и RDP-диски.
- Блокировка записи по содержимому для USB-устройств хранения.
- Блокировка запуска ПО, в том числе portable версий.
- Блокировка передачи при работе с удаленным рабочим столом (через подключаемые диски, сетевые папки и буфер обмена)
- Блокировка по типу подключаемого устройства (Android, Apple, Blackberry, Palm, Windows Phone и т.д.)
- Блокировка беспроводных сетей и интерфейсов (Wi-Fi и Bluetooth)
- Блокировка передачи на сетевые хранилища (SMB)
- Блокировка работы с локальными папками
- Блокировка работы с локальными дисками
- Блокировка посещения запрещенных ресурсов по HTTP(S)

5.2 Блокировка на уровне сети

Также доступна блокировка сетевого траффика HTTP(S) на основании передаваемого текста, выбранных пользователей, хостов, URI, POST, GET и множества других атрибутов. Такая блокировка, помимо запрета отправки указанного текста, позволяет реализовать безопасные схемы работы с веб-почтой, чатами, форумами, облачными хранилищами. Например, можно заблокировать отправку файлов из сети компании в облако (возможность скачивать остается), возможность сохранять черновики или вложения при работе с веб-почтой, возможность запретить любую загрузку в социальные сети (без блокировки остального функционала соц. сети) и многое другое.

Метод	Опции	Может содержать
Текст		
	Все слова	Текст или регулярное выражение
	Любое из слов	Текст или регулярное выражение
	Точное слово или фраза	Текст или регулярное выражение
	Ни одно из указанных слов	Текст или регулярное выражение
Дата		
	Равно	Дата\месяц\год
	Не равно	Дата\месяц\год
	В диапазоне	Диапазон дат\месяцев\лет
	Вне диапазона	Диапазон дат\месяцев\лет
Время		

Метод	Опции	Может содержать
	В диапазоне	Часы
	Вне диапазона	Часы
День недели		
	Равно	Дни недели
	Не равно	Дни недели
Пользователь		
	Равно	Пользователи
	Не равно	Пользователи
IP адрес		
	Локальный адрес	Адрес или диапазон
	Удаленный адрес	Адрес или диапазон
HTTP метод		
	GET	
	POST	
	CONNECT	
	PUT	
Web поле		
	URI	Содержит, отсутствует, присутствует, начинается на, заканчивается на, равно, не равно, в диапазоне, вне диапазона и т.д.
	HOST	Содержит, отсутствует, присутствует, начинается на, заканчивается на, равно, не равно, в диапазоне, вне диапазона и т.д.
	USER-AGENT	Содержит, отсутствует, присутствует, начинается на, заканчивается на, равно, не равно, в диапазоне, вне диапазона и т.д.
	Content-length	Содержит, отсутствует, присутствует, начинается на, заканчивается на, равно, не равно, в диапазоне, вне диапазона и т.д.

Данная опция доступна на сетевом уровне, возможна работа как с нешифрованным, так и с SSL траффиком. Блокировка может распространяться на ПК и любые другие сетевые устройства внутри компании, вне зависимости от подключения (Ethernet или Wi-Fi) для HTTP(S) или FTP(S) трафика.

Комбинируя эти правила можно создавать гибкие настройки блокировки сервисов, либо отдельных возможностей на этих сервисах. Например,

- правило (**Web поле = host** содержит **mail.ru**) И (**Web поле URI** содержит **attaches/add**) – заблокирует возможность сохранения или отправки вложений в почте mail.ru при работе через веб интерфейс;
- правило (**Web поле = host** содержит **vk.com**) И (**Web поле URI** содержит **act=do_add** ИЛИ **act=add_doc** ИЛИ **act=album_photo**) заблокирует возможность загрузки файлов на ресурс “В Контакте”;
- правило (**Web поле = URI** содержит **/objects**) И (**Web поле host** содержит **api.asm.skype.com**) И (**HTTP метод = PUT**) заблокирует возможность пересылки файлов через веб скайп.

5.3 Блокировка почты на уровне рабочей станции или почтового сервера (агент)

Доступна блокировка исходящей корпоративной почты по протоколам SMTP, MAPI и IMAP. Она реализована путем установки агента блокировки на конечный почтовый сервер (edge) или локальные ПК с последующей проверкой всей исходящей корреспонденции. Почта, нарушающая политики безопасности, будет остановлена до ее проверки вручную, после данной проверки письмо можно окончательно заблокировать либо же отправить конечному получателю.

Блокировка может быть:

- **контекстная** – по отправителю, получателю, типу файла (более 100 форматов), размеру, вложению и множеству других атрибутов;
- **контентная** – на основании наличия в передаваемых документах конфиденциальной информации. Например, цифровых отпечатков, фраз, синонимов, морфологических форм, регулярных выражений, зашифрованных вложений, изображений, визуально похожих на паспорта, кредитные карты, документы, содержащие печати организации или документы, являющиеся подделками и многое другое.

Также доступна блокировка посещения запрещенных ресурсов по протоколу HTTP(S).

5.4 Блокировка почты на уровне почтового сервера

Доступна блокировка исходящей корпоративной почты на уровне почтового сервере. Она реализована путем перенаправления исходящей почты на сервер EndpointController с последующей проверкой. Почта, нарушающая политики безопасности, будет остановлена до ее проверки вручную, после данной проверки письмо можно окончательно заблокировать либо же отправить конечному получателю.

Блокировка может быть:

- **контекстная** – по отправителю, получателю, типу файла (более 100 форматов), размеру, вложению и множеству других атрибутов;
- **контентная** – на основании наличия в передаваемых документах конфиденциальной информации. Например, фраз, синонимов, морфологических форм, регулярных выражений, зашифрованных вложений, изображений и многое другое.

6 Защита данных в покое (Data at Rest)

СЕРЧИНФОРМ ДЛП способен производить аудит и детектировать конфиденциальное содержание внутри файлов в следующих местах хранения данных:

- Локальные ПК на базе Windows;
- Перемещаемые профили пользователей (в Active Directory или Novel eDirectory);
- Сетевые папки операционных систем Windows, Linux, Unix, Mac;
- Корпоративные NAS (Synology, HP, QNAP и т.д.);
- Корпоративные хранилища SharePoint;
- Текстовые поля в популярных СУБД (MS SQL, MySQL, PostgreSQL, Oracle и т.д.);
- Базы данных веб-сайтов;
- Веб-почта;
- Облачные хранилища (Dropbox, Yandex.Disk, OneDrive и CMIS);
- Личные переносные устройства хранения (USB HDD, флешки) при подключении к корпоративному оборудованию;
- Личные мобильные устройства (телефоны, планшеты) при подключении к корпоративному оборудованию в режиме доступа к файловой системе.

Ниже приведен неполный список возможных форматов, с которыми может работать СЕРЧИНФОРМ ДЛП. В дополнение возможно создавать свои типы файлов и присваивать им парсеры (обрабатывать как бинарный, текст, xml и т.д.)

Категория	Расширения
Файлы MS Office	DOC, DOCX, DOT, XLS, XLSB, XLSX, XLSM, XLT, XLTX, XLTM, PPT, PPTX, RTF, POT, VSD, VST, VSDX[10], VSSX, VSTX, VSDM, VSSM, VSTM, VDW, VSS
Базы данных	MDB, ACCDB
Файлы Internet	HTM, HTML, SHTML, CSS, JS, MAFF
Электронные сообщения	MSG, EML, PST, OST
Программные файлы MS Windows	TXT, CSV, PDF, DJVU, XML, LST, CHM, BAT, LOG, INI, WRI, MHT, HLP, C2V, SVG, FB2, FR3
Архивы и сжатые файлы	7Z, ARJ, RAR, ZIP, JAR, TAR, ISO, GZ, GZIP, TGZ, TPZ, CAB, LZH, LHA, Z, TAZ, LZMA, BZ2, BZIP2, TBZ2, TBZ, HFS, 001
Файлы языков программирования	JAVA, PAS, DFM, DPR, BAS, CPP, HPP, C, C++, H, CS, SQL, JSP, ASP, ASPX, PHP, SH, WSDL, PY, PL, INC, VB, VBS, XLA, CMD
Файлы PowerBuilder	SRA, SRJ, SRW, SRU, SRM, SRS, SRF, SRD, SRQ, SRP
Аудио/видео файлы	MP3, AVI, WAV, WAVE, FLAC, Opus
Файлы OpenOffice	SXW, STW, ODT, ODS, SXC, OTT, OTS, FODT, ODP, STC, ODF, ODG

[10] Из документов формата VSDX извлекаются только внедренные OLE-объекты, внутренний текст таких документов не индексируется.

Категория	Расширения
Графические форматы	JPG, JPEG, TIF, TIFF, BMP, PNG, GIF
Старые текстовые форматы	LEX, ASC
Файлы CAD	DWG, DXF

7 Интеграция со СКУД

СЕРЧИНФОРМ ДЛП способен интегрироваться с системами СКУД для использования полученных от этих систем данных в построении отчетов по ProgramController.

Интеграция возможна со следующими СКУД:

- PERCo-S-20 версии 3.9.6.0
- Орион Про (необходимо наличие в его составе «Модуль интеграции Орион Про»).