LibraSoft

Программный комплекс
LibraDLP

24.02.2025

ОГЛАВЛЕНИЕ

ЗАЩИТА ИНФОРМАЦИИ: LIBRADLP

Каналы утечки информации и важность их контроля

Информация сегодня является одним из критически важных факторов успеха деятельности любой организации. Средняя стоимость одной утечки информации в мире составляет около 5,3 млн. долларов.

Как «утекает» информация? Существует множество каналов передачи данных: электронная почта, социальные сети, форумы, блоги, интернет-мессенджеры, внешние носители информации, принтеры, FTP-серверы, облачные хранилища и другие.

Если данные каналы передачи информации в вашей организации не контролируются, либо контролируется всего 1-2 канала, информация, критичная для Вашего бизнеса, может быть свободно передана конкурентам.

Современная система информационной безопасности должна позволять сотруднику использовать все каналы для передачи информации, а специалистам по информационной безопасности – перехватывать и анализировать информационные потоки, идущие по этим каналам. При этом реализация комплексной политики информационной безопасности невозможна при наличии хотя бы одного неконтролируемого службой безопасности канала потенциальных утечек.

LibraDLP – признанный лидер на рынке информационной безопасности Беларуси. Продукт используется во многих крупных организациях, работающих в самых разных отраслях – от банковского дела до машиностроения, и позволяет эффективно защищать бизнес от убытков, связанных с утечками информации.

Программное решение позволяет эффективно контролировать информационные потоки предприятия на всех уровнях: от компьютера отдельного пользователя до серверов локальной сети. Контролируются также все данные, уходящие в Интернет.

LibraDLP имеет модульную структуру, то есть заказчик может по своему выбору установить только необходимые ему модули. Контроль данных может осуществляться двумя способами: путём зеркалирования трафика и/или посредством агентов, устанавливаемых на рабочих станциях пользователей.

ПЕРЕХВАТ НА АГЕНТАХ

Сервер **EndpointController** позволяет перехватывать и останавливать трафик посредством установленных на рабочие станции агентов. Дополнительно позволяет контролировать сотрудника, находящегося в командировке за пределами корпоративной сети, ведь работник может свободно передать конфиденциальные данные с ноутбука третьим лицам.

Агенты EndpointController могут контролировать:

- **MailController** – входящую и исходящую электронную почту, как через почтовые клиенты, так и с доступом через веб-браузер (с возможностью блокировки передачи, в том числе по контентным и/или контекстным критериям);
- **IMController** – сообщения, файлы и звонки популярных мессенджеров (Skype, Lync, Teams, Viber, Telegram, WhatsApp, Zoom и др.), а также отслеживать общение в популярных социальных сетях (с возможностью блокировки передачи сообщений и файлов в социальные сети и посредством мессенджеров согласно их содержимому);
- **HTTPController** – информацию, передаваемую по протоколу HTTP(S) посредством POST- и GET-запросов (с возможностью блокировки передачи файлов через веб-браузер по контентным и/или контекстным критериям);
- **DeviceController** – информацию, записываемую на подключаемые внешние устройства (USB-flash, CD/DVD и пр.), с возможностью блокировки подключаемых устройств, блокировки записи данных на USB-устройства по их содержимому и/или объему, а также доступ к буферу обмена (в том числе по его содержимому);
- **FTPController** – информацию, передаваемую по протоколу FTP;
- **CloudController** – входящие и исходящие файлы облачных хранилищ данных и SharePoint (с возможностью блокировки передачи файлов из веб-браузера в облачные хранилища согласно их содержимому);
- **PrintController** – содержимое документов, отправленных на печать (с возможностью блокировки печати по контентным и/или контекстным критериям);
- **MonitorController** – информацию, отображаемую на мониторах пользователей, нажатия клавиш и содержимое буфера обмена, а также происходящее за компьютером посредством веб-камеры.
- **ProgramController** – активность пользователей в запускаемых ими приложениях и на посещаемых веб-сайтах.
- **FileController с функцией тегирования** – содержимое локальных и сетевых документов, которые соответствуют настроенным правилам сканирования, а также операции с этими файлами, установка меток как вручную, так и автоматически (с возможностью блокировки использования файлов, имеющих определенную метку).

Принцип работы

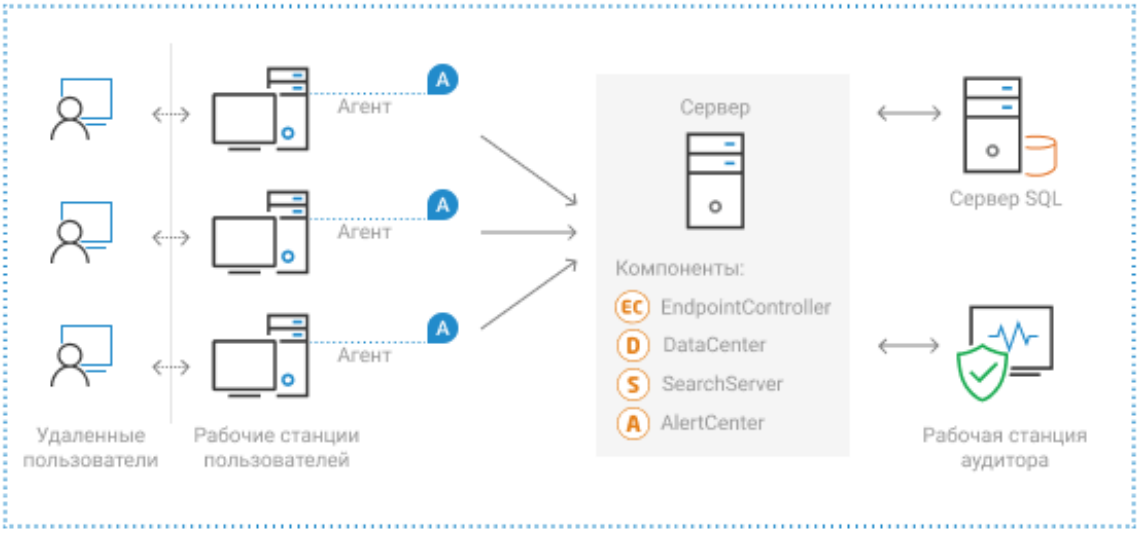
Агенты EndpointController производят перехват данных и (или) фиксирование операций с данными и направляют их серверу EndpointController.

Данные от агентов помещаются в базу данных под управлением СУБД MS SQL / PostgreSQL либо в файловое хранилище, которые индексируются при помощи сервера индексации SearchServer. Индекс – особая структура, необходимая для быстрого поиска по перехваченным документам. При помощи планировщика обновлений обеспечивается поддержание индекса в постоянно актуальном состоянии.

Для автоматизации проверок и уведомлений используется клиентское приложение AlertCenter, которое в соответствии с расписанием опрашивает подключенные индексы и базы данных по списку критериев поиска и оповещает аудиторов безопасности в случае обнаружения инцидентов.

Для просмотра документов, отвечающих поисковому запросу, используется клиентское приложение AnalyticConsole, позволяющее подключаться и производить поиск по любым индексам и базам данных модулей LibraDLP.

Контроль данных и действий пользователей с помощью агентов



- Большое количество подконтрольных каналов и устройств
- Возможность контроля сотрудников не только в офисе, но и за его пределами
- Перехват шифрованного трафика
- Сохранность информации при потере связи с сервером
- Скрытие службы агента для конечного пользователя
- Адаптация системы под компании с разветвленной филиальной сетью и с большим количествои ПК

СЕТЕВОЙ ПЕРЕХВАТ

Помимо перехвата на агентах, сервер EndpointController позволяет осуществлять перехват данных на сетевом уровне путем зеркалирования трафика. Таким образом, служба сетевого перехвата обрабатывает трафик, не влияя на работу корпоративной сети.

Перехватываются данные, пересылаемые пользователями по популярным сетевым протоколам и каналам (SMTP, POP3, HTTP(S), IMAP, MAPI, NNTP, XMPP, SIP, FTP) на уровне локальной сети.

Дополнительно к этому в состав EndpointController входит:

- модуль интеграции с почтовыми серверами, позволяющий копировать сообщения напрямую из корпоративного почтового сервера в отдельный ящик;
- модуль SMTP-интеграции, позволяющий получать пересылаемые контейнеры отчетов журнала.

Сетевой перехват включает в себя следующие модули:

- **MailController;**
- **IMController;**
- **HTTPController** (с возможностью блокировки посещаемых веб-ресурсов, загрузки данных и др. функциональных возможностей в соответствии с настроенными правилами);
- **FTPController;**
- **CloudController.**

Принцип работы

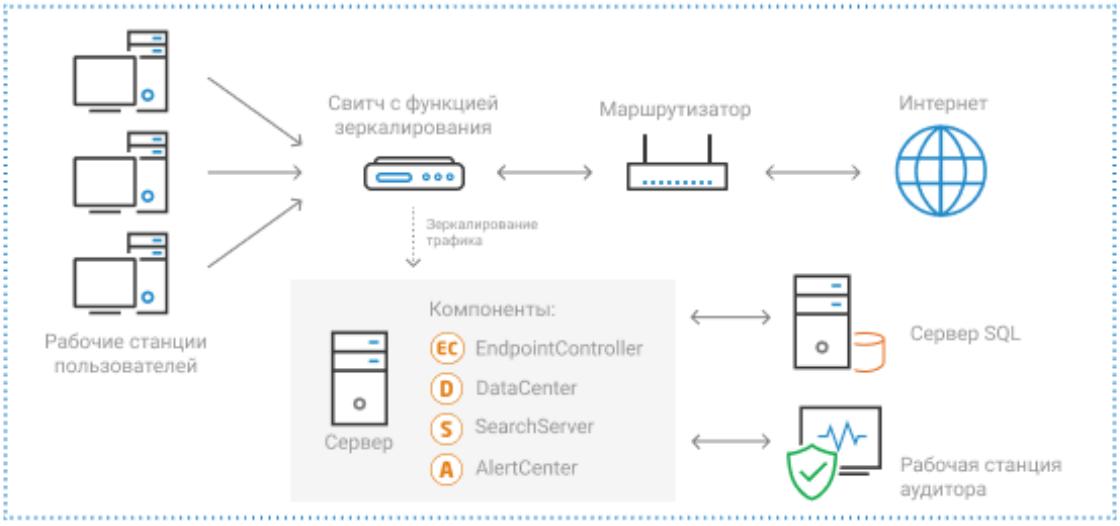
Перехват сетевого трафика производится на уровне сетевых протоколов (Mail, HTTP, IM, FTP, Cloud). Возможна фильтрация по доменному имени пользователя, имени компьютера, IP- и MAC-адресам.

Перехваченные данные помещаются в базы данных MS SQL / PostgreSQL либо в файловые хранилища, которые индексируются при помощи сервера индексации SearchServer. Индекс – особая структура, необходимая для быстрого поиска по перехваченным документам.

Приложение AlertCenter по расписанию сверяет данные в индексе на соответствие настроенным политикам безопасности, состоящим из поисковых запросов. Расписание проверок и список запросов настраиваются работниками службы информационной безопасности. В случае обнаружения совпадений AlertCenter оповещает об этом сотрудника службы безопасности.

Для просмотра документов, отвечающих поисковому запросу, используется клиентское приложение AnalyticConsole, позволяющее подключаться и производить поиск по любым индексам, имеющимся на сервере индексации.

Зеркалирование трафика, проходящего через сетевой шлюз



- Полная незаметность контроля
- Независимость от операционной системы и устройств передачи
- Отсутствие нагрузки на устройство сотрудника
- Возможность интеграции с серверами по ICAP для контроля шифрованного трафика и ограничения доступа пользователей к веб-ресурсам

ПЕРЕХВАТ НА АГЕНТАХ И СЕТЕВОЙ ПЕРЕХВАТ: ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ ОБОИХ МЕТОДОВ ПЕРЕХВАТА

Для комплексного контроля передаваемых данных целесообразно использовать одновременно и перехват на агентах, и сетевой перехват. Например, если агент сумел перехватить сообщения, не перехваченные на «зеркале», то, очевидно, имеет место шифрование трафика, которое может использоваться для передачи конфиденциальных данных за пределы организации. Когда же агент не перехватывает данные, появляющиеся на «зеркале», становится очевидным, что пользователь каким-то образом деактивировал агент, что также требует немедленного проведения расследования.

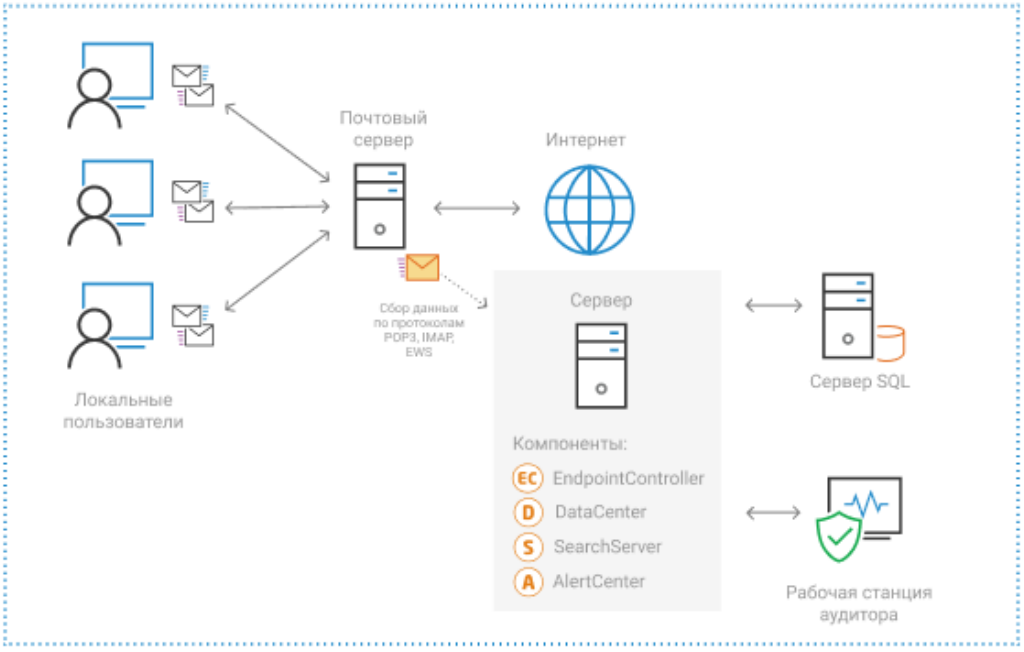
ИНТЕГРАЦИЯ С ПОЧТОВЫМИ СЕРВЕРАМИ

Производится в случае, если перехватываемые данные нужно получать напрямую с почтовых серверов, а не только путём сетевого перехвата.

В такой схеме EndpointController подключается к отдельно созданному на почтовом сервере ящику, принимает все поступившие сообщения и записывает их в свою базу данных. Теневая копия почтовых сообщений хранится и на почтовом сервере (временно), и в базе данных EndpointController.

Интеграция возможна с любыми серверами, поддерживающими данную схему работы (например, MS Exchange Office 365, Postfix, Lotus Domino и др.).

Сбор почтовых сообщений с почтового сервера



- Повышенная надежность и независимость от нагрузки на сеть
- Совместимость практически с любой версией большинства почтовых серверов
- Независимость от операционной системы и устройств передачи пользователя
- Независимость от протоколов отправки и получения писем пользователем
- Отсутствие нагрузки на устройство сотрудника
- Определение пользователей по их почтовым адресам
- Получение сообщений от почтового сервера в расшифрованном виде

SMTP-ИНТЕГРАЦИЯ

Исходя из необходимости соблюдения постоянно растущего количества регулятивных и нормативных требований, каждая организация должна хранить записи об обмене сообщениями при выполнении сотрудниками ежедневных деловых задач.

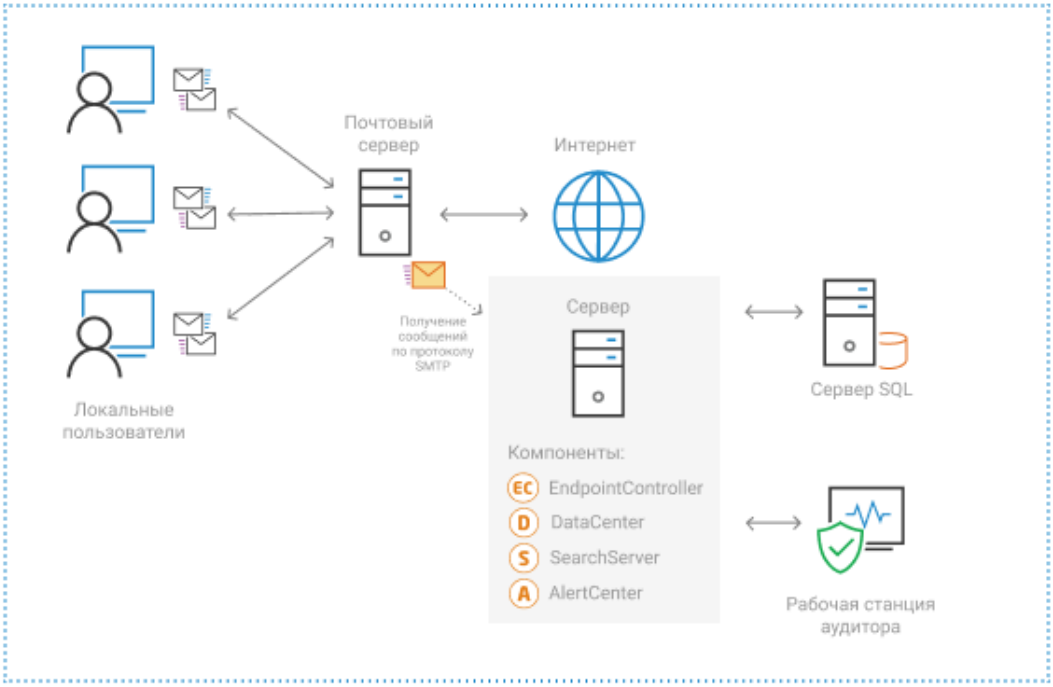
Функция *журналирования* почтового севера позволяет хранить копии сообщений в центральном почтовом ящике для различных целей, включая архивацию почты.

Для перехвата отчёты журнала помещаются в контейнеры. Далее трафик журналирования передается непосредственно на сервер EndpointController.

В данной схеме EndpointController выступает в роли SMTP-сервера: он получает контейнеры отчётов журнала, обрабатывает их и помещает в базу данных.

Интеграция возможна с любыми серверами, поддерживающими данную схему работы (например, MS Exchange, Postfix, CommuniGate Pro и др.).

Получение отчетов журнала в специальных контейнерах



- Высокая скорость получения писем
- Возможность обнаружения получателя скрытой копии
- Совместимость практически с любой версией большинства почтовых серверов
- Независимость от операционной системы и устройств передачи пользователя
- Отсутствие нагрузки на устройство сотрудника
- Независимость от протоколов отправки и получения писем пользователем
- Определение пользователей по их почтовым адресам
- Получение сообщений от почтового сервера в расшифрованном виде

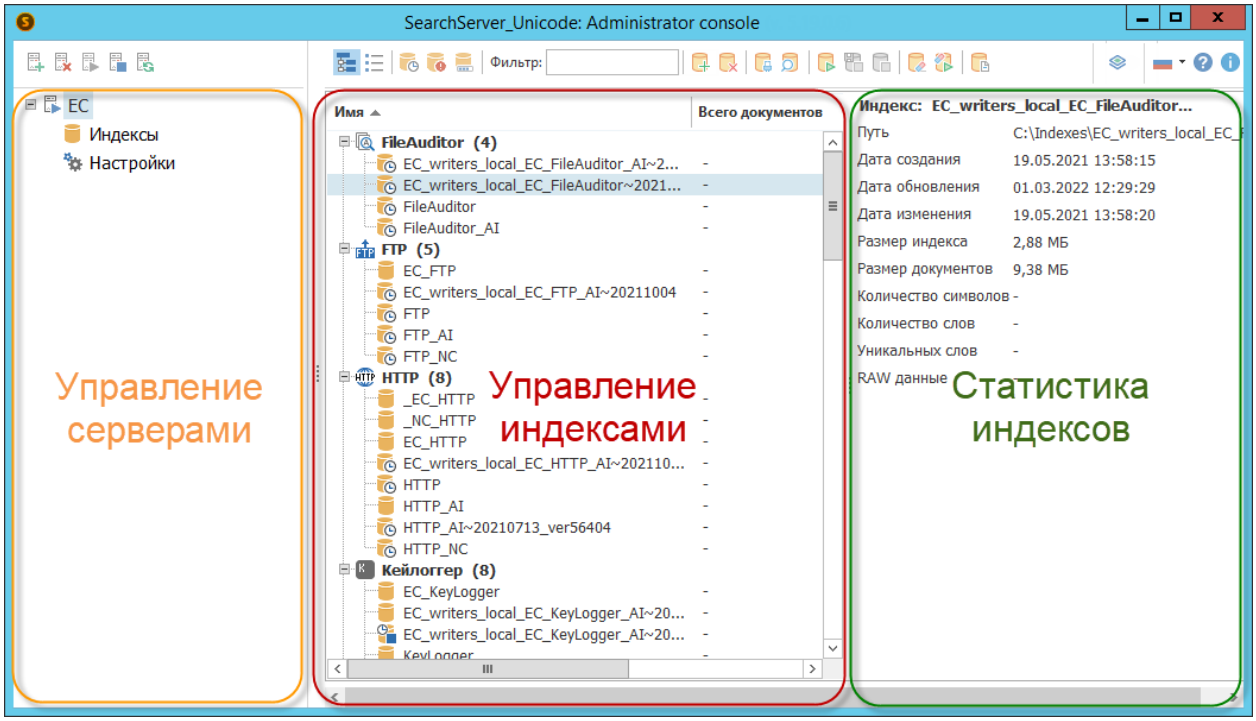
СЕРВЕР ИНДЕКСАЦИИ

SearchServer является неотъемлемым компонентом LibraDLP, который выполняет функции индексации и поиска документов. Результатом индексации является создание **индексов** – особой структуры данных, предназначенной для ускорения доступа к обработанной информации. Благодаря этому обеспечивается возможность поиска информации при высокой скорости обработки запросов.

Приложение SearchServer позволяет проводить индексирование более 140 типов файлов.

Богатство настроек позволяет получать индекс требуемой конфигурации. В процессе создания и работы с индексами SearchServer используется диалоговый режим настройки, в сложных случаях – с применением пошаговых мастеров.

Индексирование носит **инкрементальный** характер: при обновлении индекса обрабатываются только новые или измененные со времени последнего индексирования документы. Тем не менее, после изменения свойств индекса осуществляется полная переиндексация данных.



SearchServer может распознавать текст в документах индексируемых графических форматов: JPG, JPEG, TIF, TIFF, BMP, PNG, GIF и др. Для этого в приложение интегрирован OCR-модуль NicomSoft OCR.

Использование оригинальных поисковых технологий обеспечивает высокую скорость и точность поиска, при этом используются возможности морфологии и синонимии.

ALERTCENTER

AlertCenter – «мозговой центр» системы безопасности. Осуществляет автоматический мониторинг собранных модулями данных и, при наличии в этой информации определенных ключевых слов, фраз или фрагментов текста, указывающих на инцидент информационной безопасности, немедленно оповещает об этом аудиторов.

В клиентской консоли AlertCenter настраиваются политики безопасности, применяемые к собранным данным.

Для идентификации конфиденциальной информации в AlertCenter могут быть использованы следующие методы:

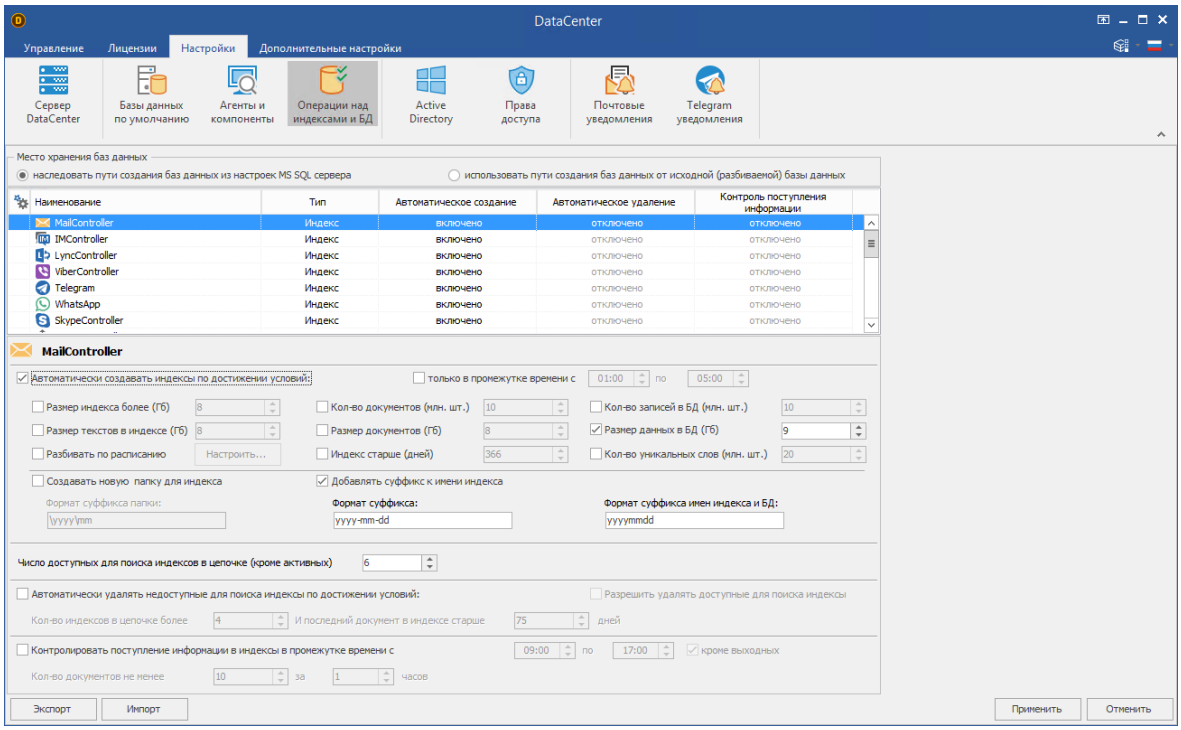
- Поиск по ключевым словам и фразам с учетом морфологии, синонимов, расстояния между словами фразы, с учетом положения фразы в тексте документа, а также по комбинациям фраз;
- Поиск по номеру телефона;
- Поиск по заполненным формам, позволяющий отыскать такие шаблонные документы, как анкета, резюме и др.;
- Поиск с использованием целого текста или текстового фрагмента в качестве запроса (поиск похожих);
- Поиск по словарю – вид поиска, при котором все документы в индексе проверяются на наличие в них содержимого из указанного тематического словаря;
- Запросы с цифровыми отпечатками – сравнение всех перехваченных документов с набором контрольных документов;
- Поиск по атрибутам сообщений и файлов: дата, размер, тип документа, пользователь домена, адреса электронной почты и другие формальные признаки документов;
- Поиск по базам данных;
- Поиск документов, защищенных паролем;
- Сложные запросы – комбинирование нескольких простых запросов при помощи логических операторов;
- Запросы с регулярными выражениями – поиск информации не по точному значению, а по ее форме: последовательности и типе символов;
- Статистические запросы по количественным показателям (числу отправленных писем / распечатанных страниц / сообщений в Skype, Lync, Viber, IM и пр.);
- Поиск по цепочкам событий или событиям с определенной продолжительностью (попытка подбора учетной записи, создание временной учетной записи, временное включение учетной записи и др.);
- Использование синонимических рядов;
- Распознавание текста графических документов;
- Поиск документов с умышленно измененным расширением.

DATACENTER

DataCenter входит в состав LibraDLP и предназначен для автоматизированного и ручного управления различными аспектами работы DLP-системы.

Основные возможности DataCenter:

- распределение лицензий модулей LibraDLP и контроль их срока действия;
- отслеживание состояния служб LibraDLP, их опциональный запуск либо перезапуск;
- контроль наличия свободного дискового пространства для индексов и баз данных модулей LibraDLP, а также поступление в них перехваченной информации;
- выполнение автоматических действий по созданию, переносу, архивированию, удалению индексов и баз по достижении заданных условий;
- настройка формирования отчетов и данных для отображения в веб-интерфейсе;
- настройках серверных частей AAServer, AlertCenter, ReportCenter, WebAnalytic;
- синхронизация LibraDLP с доменами Active Directory, FreeIPA, ALD Pro;
- разграничение и контроль прав доступа аудиторов службы безопасности к информации определенных пользователей;
- журналирование действий аудиторов в консолях модулей LibraDLP;
- оповещение о различных событиях или неудовлетворительных условиях для работы LibraDLP;
- архивирование/перенос баз данных протоколов перехвата и архивирование баз данных компонентов LibraDLP.
- управление настройками возможно как из консольного приложения, так и через веб-браузер.

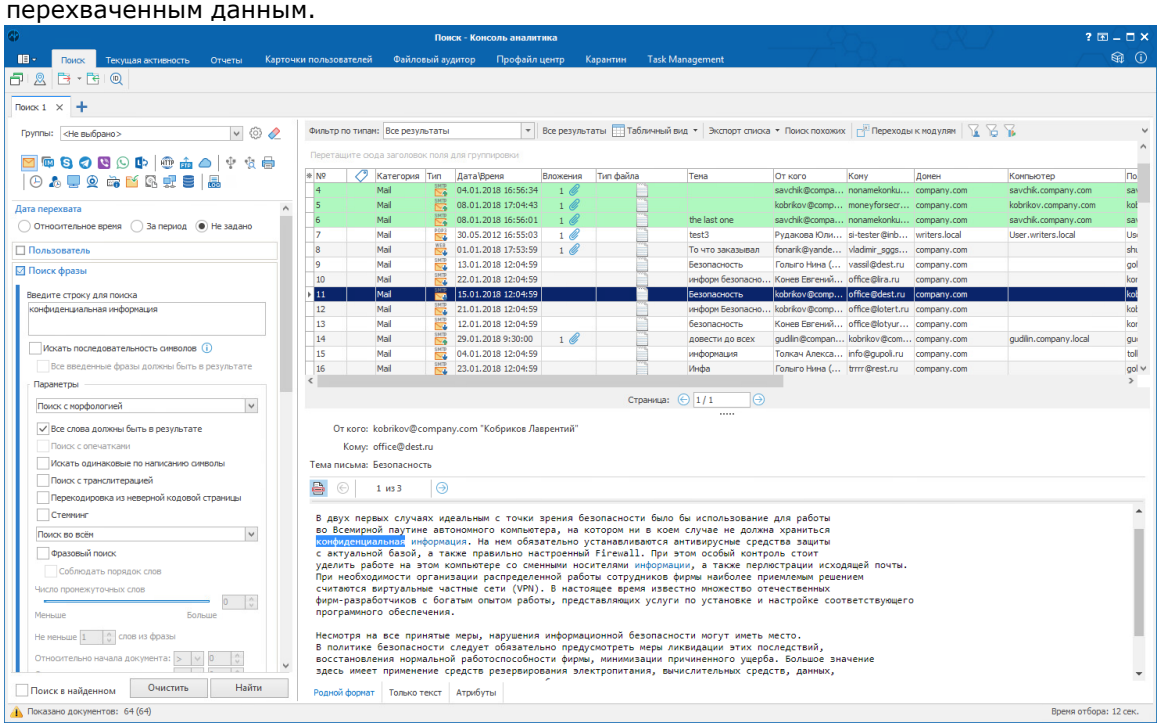


ANALYTICCONSOLE

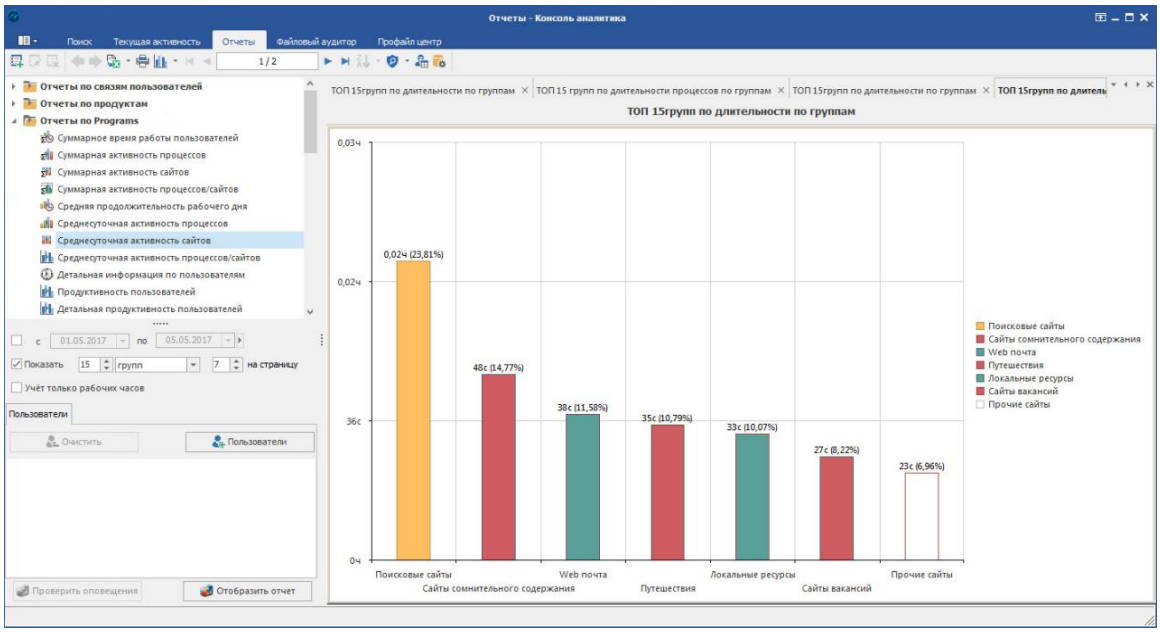
AnalyticConsole – клиентское приложение для поиска по перехваченным и собранным DLP-системой данным, просмотра отчетов, контроля активности сотрудников, просмотра их местоположения, работы с личными карточками и психологическими профилями пользователей, письмами карантина и контролируемыми файлами организации, а также для упрощения работы с задачами информационной безопасности.

Функциональные возможности приложения сосредоточены на следующих вкладках:

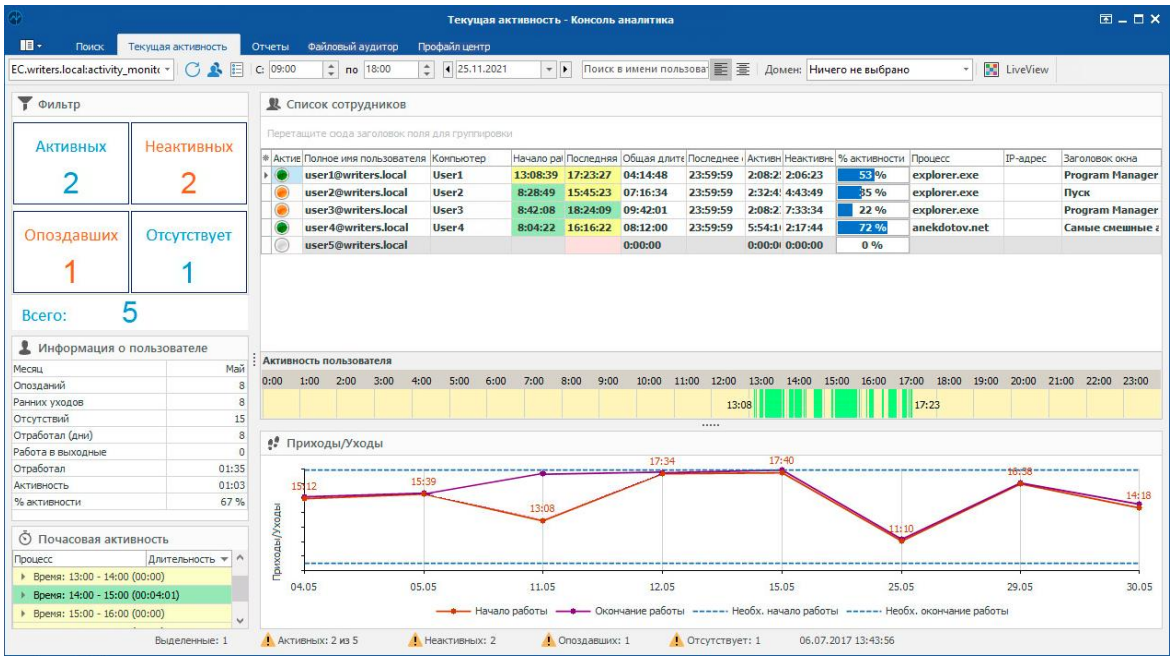
- Вкладка **Поиск** предназначена для мониторинга трафика различных каналов передачи данных (HTTP, Skype, почтовой переписки и др.), а также осуществления поиска по перехваченным данным.



- Вкладка **Отчеты** позволяет формировать статистику по активности пользователей, фактам нарушения политик информационной безопасности и нерациональном использовании сотрудниками рабочего времени, представляя статистические данные в виде отчетов.

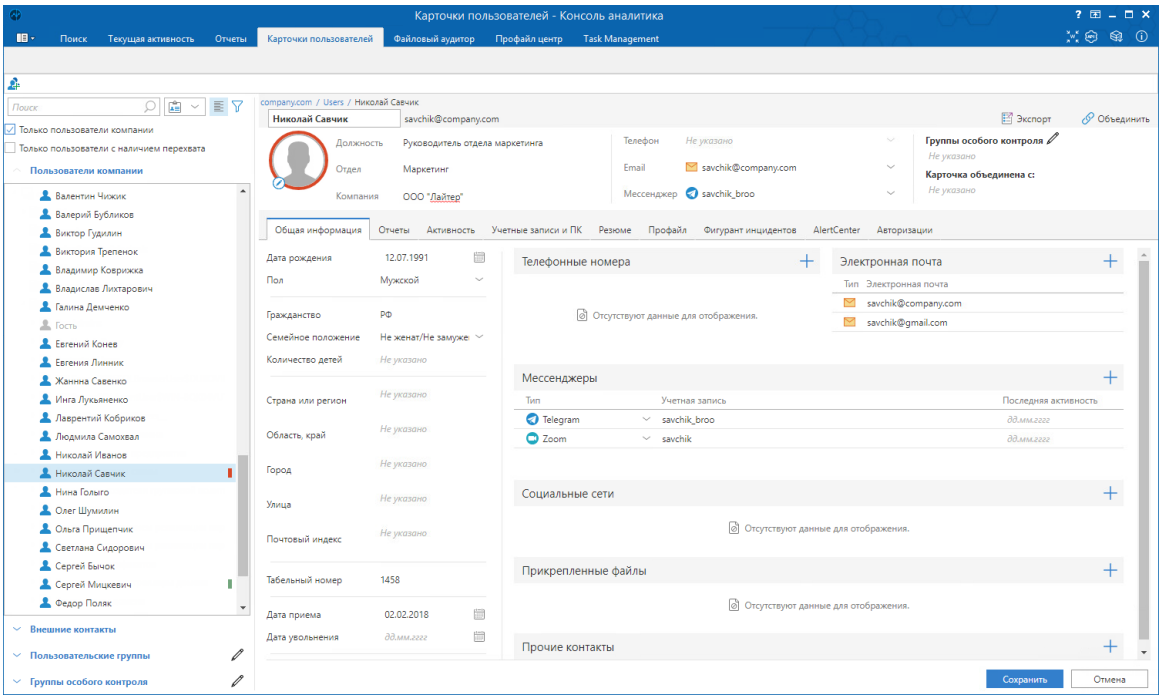


- Вкладка **Текущая активность** предназначена для мониторинга активности сотрудников в режиме реального времени.

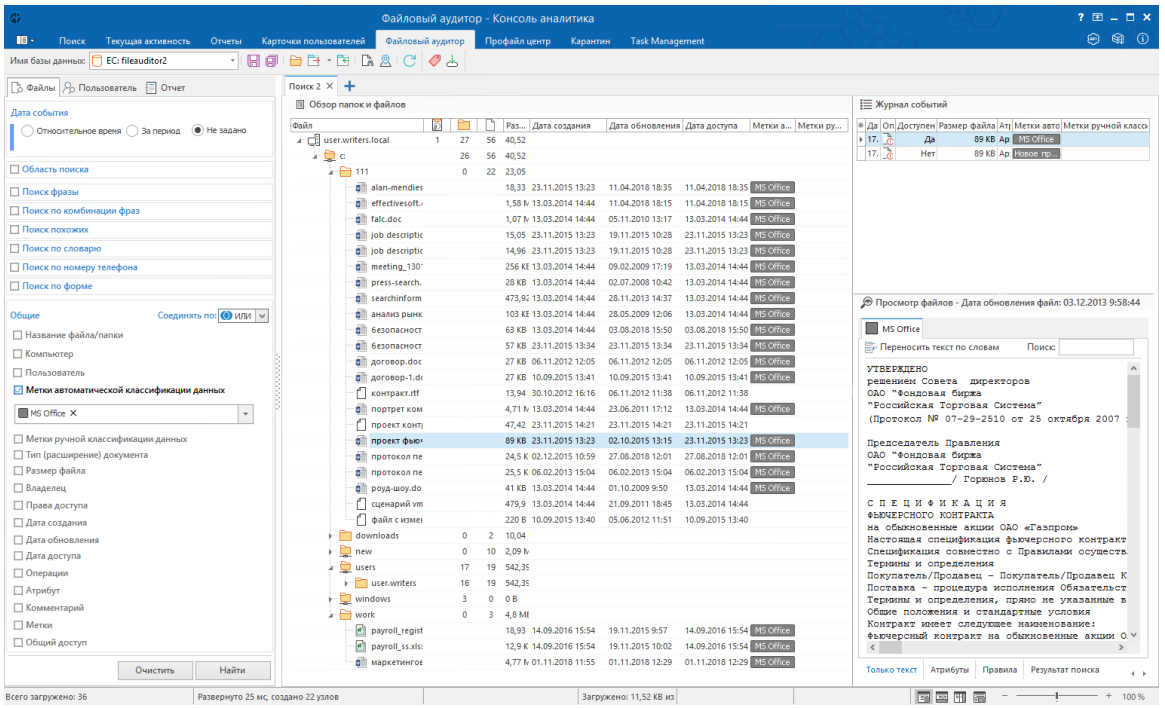


Для оперативного контроля за происходящим на рабочих мониторах пользователей предусмотрен специальный режим **LiveView**, позволяющий аудитору осуществлять просмотр до 16 мониторов в режиме реального времени. Также доступно прослушивание речи сотрудников в режиме реального времени с помощью режима **LiveSound** и просмотр происходящего за компьютером с помощью режима **LiveCam**.

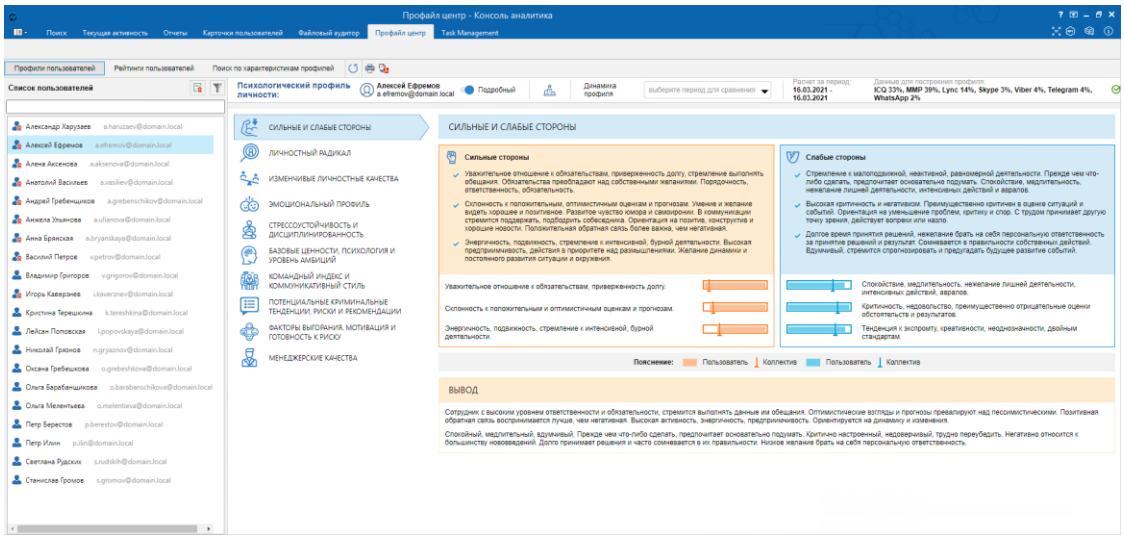
- Вкладка **Карточки пользователей** позволяет просматривать и редактировать карточки пользователей, содержащие используемые сотрудниками учетные записи Active Directory, их служебные и контактные данные (e-mail адреса, учетные записи Skype, ICQ, MSN и других мессенджеров, социальных сетей), резюме, информацию о последней активности и причастности к задачам **Task Management**.



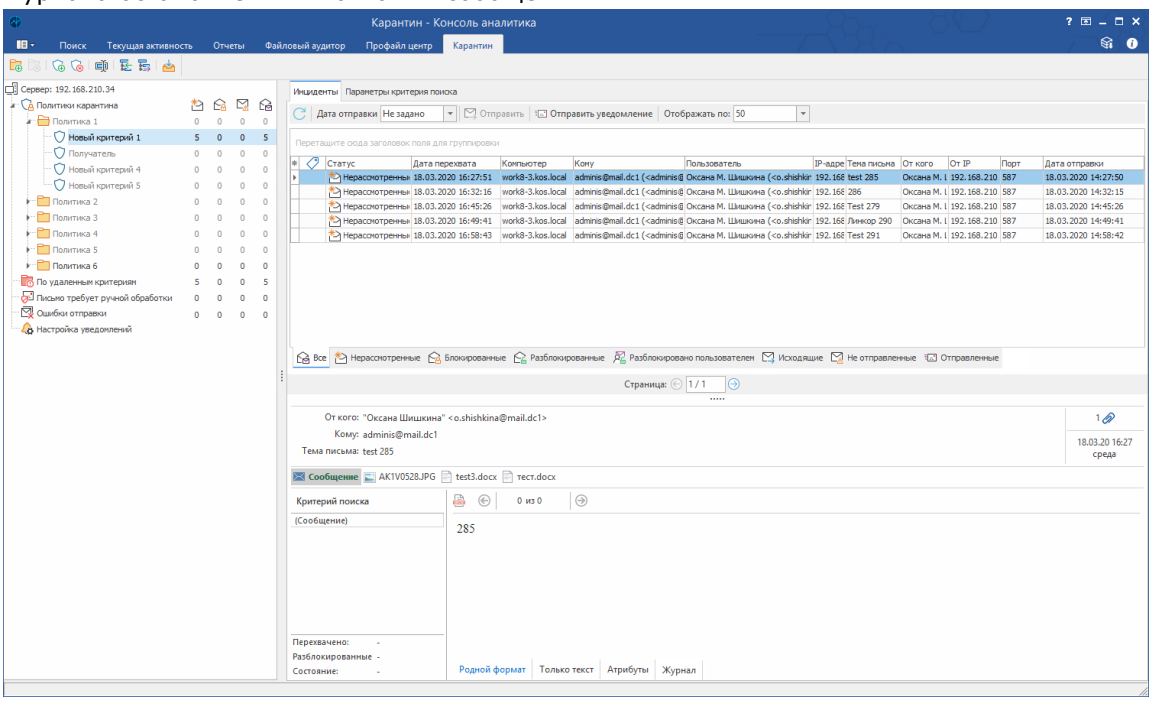
- Вкладка **Файловый аудитор** предназначена для просмотра файлов, контролируемых продуктом «FileController с функцией тегирования».



- Вкладка **Профайл центр** позволяет работать с психологическими профилями сотрудников, подготовленных продуктом LibraDLP ProfileCenter.

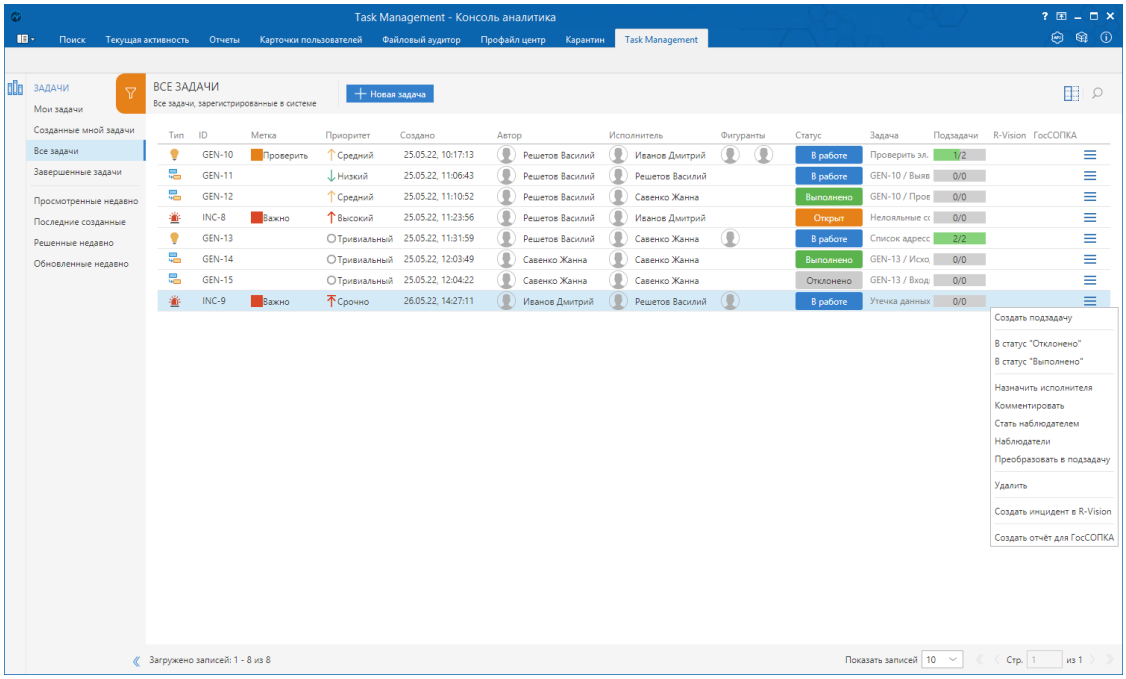


- Вкладка **Карантин** предназначена для управления политиками карантина и просмотра журнала остановленных почтовых сообщений.

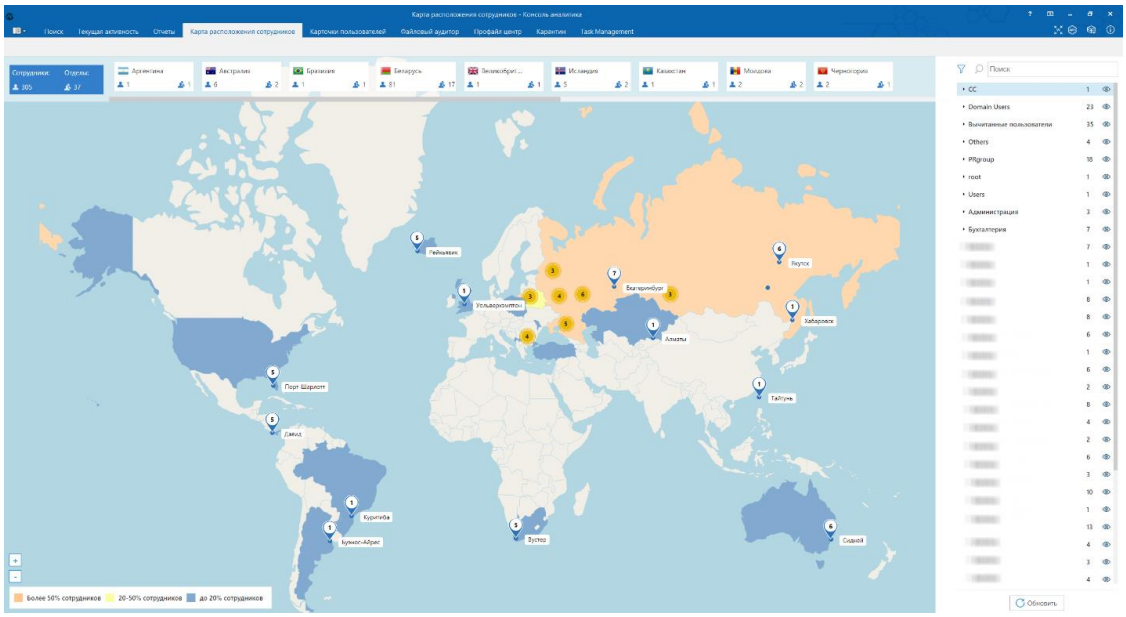


- Вкладка **Task Management** предназначена для помощи аудиторам в расследовании инцидентов безопасности. Вкладка предоставляет пользователям возможность создавать задачи, прикреплять к ним инциденты и фигурантов инцидентов, назначать аудитора,

ответственного за выполнение задачи, передавать сведения о задаче в **R-Vision** и **ГосСОПКА**.



- Вкладка **Карта расположения сотрудников** отображает в интерактивном виде карту с информацией о местонахождении рабочих станций с установленными агентами.



АНАЛИТИЧЕСКИЕ ВОЗМОЖНОСТИ

Наиболее важным компонентом любой DLP-системы является аналитический модуль. Совместное использование всех видов поиска позволяет максимально эффективно защищать конфиденциальные данные в корпоративной сети и сократить трудозатраты на их анализ. Поисковые механизмы, встроенные в LibraDLP, позволяют эффективно работать со всеми видами конфиденциальной информации, содержащейся в перехваченных данных.

Поддерживаются следующие виды поиска:

1. **Поиск по словам с учетом морфологии и синонимов.** Простейший вид поиска, позволяющий находить документы, содержащие заданные слова, их различные формы и синонимы, вне зависимости от того, в каком месте документа они находятся.

2. **Поиск по фразам с учетом порядка слов и расстояния между ними.** С помощью данного вида поиска можно анализировать документ не по отдельным словам, а по словосочетаниям (например, фамилии и имени) или устоявшимся определениям.

3. **Поиск по словарю** позволяет отыскать документы, относящиеся к определенной тематике. В редактор параметров поиска вводится некоторое количество слов, относящихся к заданной теме (например, теме наркомании, алкоголизма, денежных долгов и т.д.). Словарь может быть создан вручную либо импортирован из текстового файла.

4. **Поиск по форме** позволяет отыскать такие шаблонные документы, как анкета, резюме и др. документы, в которых значения полей удовлетворяют заданным.

5. **Поиск по номеру телефона** предназначен для обнаружения документов, содержащих телефонные номера. Поиск может осуществляться как по частично, так и целиком указанному номеру, а также с учетом выбранного шаблона.

6. **Поиск по атрибутам.** Использование этого вида поиска позволяет искать документы по их признакам (формату, имени отправителя или получателя и др.). Также можно отслеживать активность отдельных доменных пользователей, IP-адреса, определенные адреса электронной почты, документы и т.д.

7. **Поиск по регулярным выражениям.** Такой поиск позволяет отследить последовательности символов, характерные для различных форм персональных данных: содержащихся в финансовых документах, структурированных записях баз данных и т.п. С его помощью система оперативно реагирует на попытку отправки записи с такими персональными данными, как фамилия человека, день его рождения, номера кредитных карт, телефонов и т.д.

8. **Поиск по цифровым отпечаткам.** Этот вид поиска предполагает выявление группы конфиденциальных документов и снятие с них цифровых «отпечатков», по которым в дальнейшем и будет осуществляться поиск. С помощью данного метода можно быстро отследить в информационных потоках файлы, содержащие большие фрагменты текста из документов, относящихся к конфиденциальным.

9. **Запатентованный алгоритм «Поиск похожих», разработанный нашей компанией.** Интеллектуальные возможности данного типа поиска позволяют отслеживать отсылку конфиденциальных документов даже в том случае, если они были предварительно отредактированы. В качестве поискового запроса используются как фрагменты документов, так и документы целиком. В результате поиска выявляются документы, содержащие не только весь поисковый запрос, но и файлы, похожие на него по смыслу. Данный алгоритм позволяет существенно сократить временные затраты на анализ информации, значительно упрощая работу специалиста по безопасности.

10. **Комплексные поисковые запросы**. Сложные запросы могут включать в себя два и более простых запросов, объединенных с помощью логических операторов AND, OR, NOT. С их помощью можно решать нестандартные поисковые задачи, выбирая именно те данные, которые нужны в данный момент специалисту по информационной безопасности.

Идентификация сотрудников

Интеграция с доменной системой Windows дает возможность:

- **Достоверно** идентифицировать пользователя, отправившего документ по e-mail, Skype, посредством IM-клиента, оставившего его на форуме или в блоге, распечатавшего на принтере или передавшего по протоколу FTP, даже если сотрудник воспользовался для этого почтовым ящиком на бесплатном сервере, подписался чужим именем или вошел в сеть с чужого компьютера.
- **Легко** идентифицировать интересующего Вас сотрудника по его доменному имени даже в том случае, если сотрудник использует псевдоним.

Распознавание ухищрений инсайдеров

Зачастую недобросовестные сотрудники, пытаясь обмануть службу безопасности, изменяют расширение передаваемого документа либо запаковывают данные в запароленный архив.

LibraDLP позволяет:

- распознавать текст в графических файлах и осуществлять поиск по ним;
- обнаружить передачу защищенных паролем архивов по всем каналам возможной утечки информации;
- выявлять пересылку файлов с умышленно измененным типом документа.

Перехват информации с ноутбуков

В современном мире портативных компьютеров сотрудники нередко берут с собой домой или в командировку рабочие ноутбуки, инсайдеры же передают с них конфиденциальные данные третьим лицам.

Вот почему нужно осуществлять **полный контроль информации**, отсылаемой с ноутбука, даже если сотрудник находится вне корпоративной сети.

Как только устройство снова подключается к корпоративной сети, все отправленные данные незаметно передаются на сервер системы для анализа отделом информационной безопасности.

Контроль действий сотрудников

Исследования показывают, что типичный офисный сотрудник использует от 30 до 70% рабочего времени в личных целях. Игры, чаты и социальные сети отнимают львиную долю оплаченного работодателем времени, снижают эффективность работы персонала и понижают конкурентоспособность компании.

Контроль соблюдения сотрудниками **трудового распорядка**, их активности в течение рабочего дня, а также анализ их работы в запускаемых приложениях позволяют не только решить вопросы безопасности и дисциплины, но и стимулируют сотрудников эффективно использовать рабочее время в целях организации.

Профилирование сотрудников

Профайлинг успешно применяется в работе служб безопасности, в ходе служебных расследований, аналитических экспертиз, кадровой работы. Используя профилирование, можно не применять такие затратные меры, как испытательный срок, снизить количество внутрикорпоративных штрафов. Можно не только лучше понять самого сотрудника, но и найти к нему необходимый подход. Также возможно заранее подобрать сплоченный коллектив, ведь профилирование личности позволяет определить возможные особенности коллективных межличностных отношений.

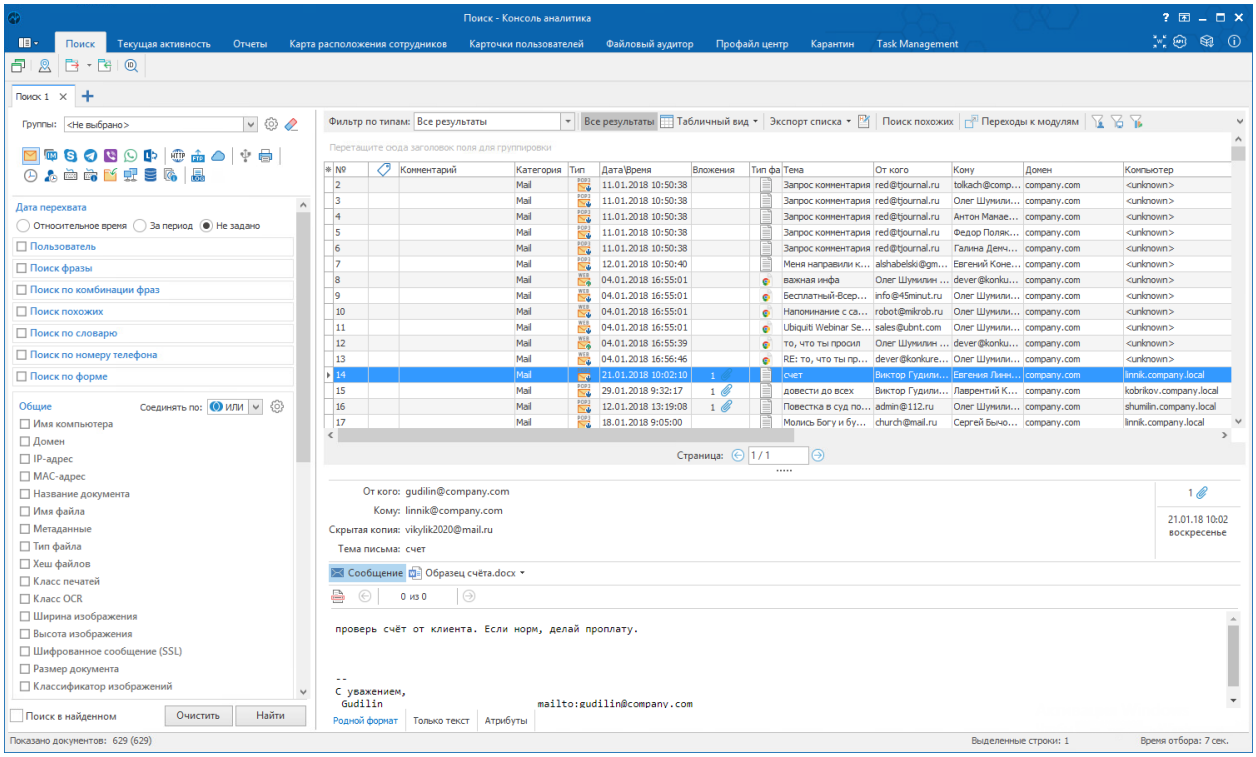
СРЕДСТВА КОНТРОЛЯ ИНФОРМАЦИОННЫХ ПОТОКОВ

Архитектура

Все модули системы имеют клиент-серверную структуру.

Под серверной частью подразумеваются службы перехвата EndpointController, под клиентской – клиентские приложения, предназначенные для поиска и просмотра перехваченных данных в целях проведения служебных расследований (AlertCenter, AnalyticConsole), а также веб-интерфейс, обеспечивающий те же функции через интернет-браузер.

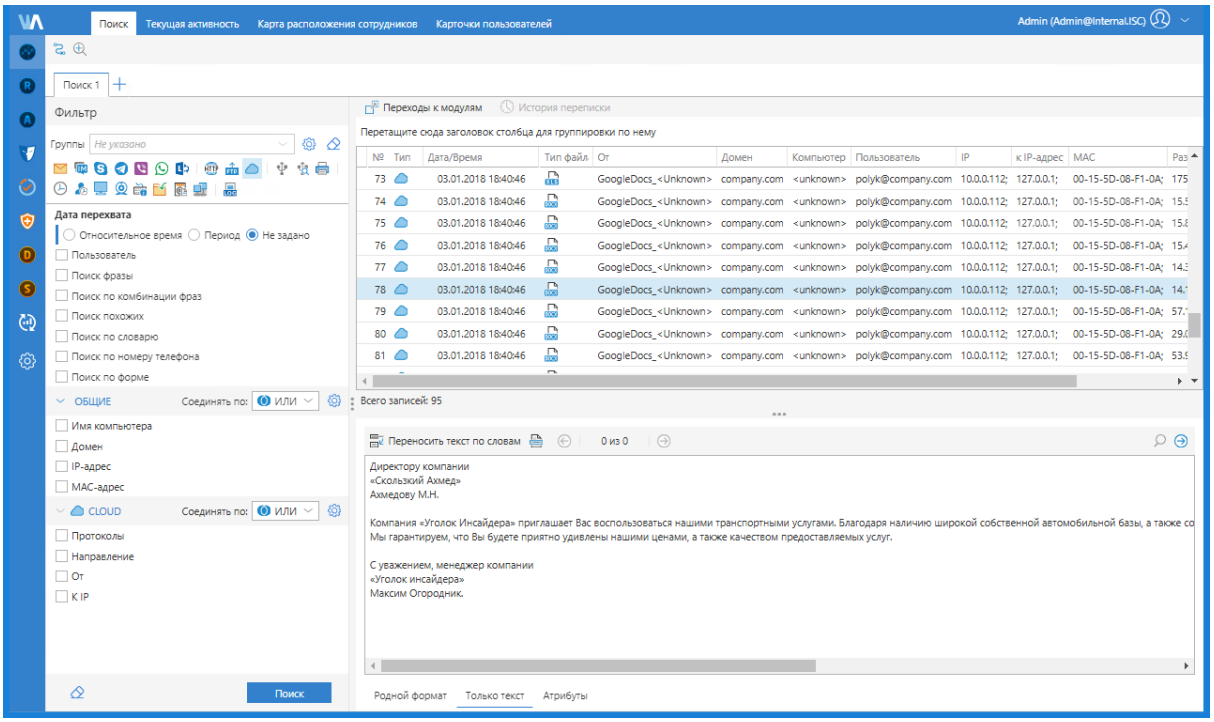
Использование единого поискового и аналитического движка позволяет в полной мере использовать богатые поисковые возможности вне зависимости от выбранного инструмента: клиентское приложение либо веб-интерфейс.



РАБОТА ЧЕРЕЗ БРАУЗЕР

DLP-система предоставляет возможность работать с перехваченными данными через сеть Интернет, используя системный веб-интерфейс WebAnalytic. В связи с этим пользователю не обязательно находиться внутри корпоративной сети.

Например, аналитик безопасности хочет просмотреть перехваченных данные, но сам находится вне офиса. В этом и других случаях просмотр данных удобно осуществлять через WebAnalytic. Понадобится лишь браузер[1] и любое портативное устройство (например, планшет).



Для использования WebAnalytic не требуется дополнительного программного обеспечения (клиентских частей, компонентов, библиотек). При работе с WebAnalytic, как и при работе с остальными приложениями LibraDLP, доступно разграничение прав доступа к информации.

Таким образом, WebAnalytic позволяет предоставить доступ к информации различным категориям пользователей: системным администраторам, HR, руководителям отделов и подразделений и т.д.

Кроме поисковых возможностей в веб-интерфейсе доступны следующие функции LibraDLP:

- Работа с отчетами, политиками и инцидентами безопасности;
- Работа с письмами карантина;
- Просмотр онлайн-активности и местоположения сотрудников, их карточек и психологических профилей;
- Работа с задачами Task Management;
- Управление индексами и серверами индексации;
- Выдача, управление лицензиями, управление настройками индексов, БД и компонентов LibraDLP.

[1] Поддерживается работа в следующих браузерах: Google Chrome, Safari, Mozilla Firefox, Opera, Яндекс.Браузер, Microsoft Edge.

MAILCONTROLLER

Утечку информации в глобальную сеть Интернет посредством электронных писем сложно контролировать. Этим активно пользуются инсайдеры, и огромная доля конфиденциальной информации утекает именно по электронной почте. Найти же что-то нужное в огромном количестве электронных сообщений, принятых и отправленных в небольшой компании даже за один день, очень сложно.

Программный модуль MailController предназначен для перехвата почтового трафика на уровне рабочих станций и сетевых протоколов, индексирования полученных сообщений и осуществления поиска по ним. Это позволяет отследить утечку конфиденциальной информации.

Содержимое всех перехваченных писем (включая присоединенные файлы) индексируется и помещается в хранилище. Создается своеобразный архив всей почтовой базы предприятия. И в случае, если корпоративный почтовый сервер выйдет из строя (что несомненно является неприятным происшествием, влекущим огромные временные, а иногда и финансовые затраты на восстановление), то данные, перехваченные компонентом MailController, будут являться своеобразной резервной копией всей почтовой базы предприятия.

Контролируемые протоколы:

- **SMTP** (исходящая почта через почтовый клиент);
- **POP3** (входящая почта через почтовый клиент);
- **IMAP** (в том числе *IMAP Compressed*);
- **MAPI** (в том числе *RPC over HTTP*);
- **NNTP**;
- **HTTP(S)** (исходящая и входящая почта Exchange Web Services, Kerio Outlook Connect, Outlook Web App и Outlook Web App light, Zimbra Web Client, исходящая и входящая почта с веб-сервисов yandex.ru, tut.by, qip.ru, gmail.com, outlook.com, mail.ru, rambler.ru, office 365, ukr.net, yahoo.com, Google Sync, World Client).

Возможна интеграция с:

- почтовыми серверами **MS Exchange, Lotus Domino** и др., а при интеграции с **MS Outlook** 2010+ возможен перехват исходящих писем и их черновиков.
- любыми прокси-серверами, работающими по протоколу **ICAP**.

Доступна блокировка:

- исходящих сообщений почты на уровне сервера по настроенным политикам карантина. Заблокированные сообщения могут быть разблокированы аудитором или непосредственным руководителем и отправлены после рассмотрения;
- почтовых сообщений и вложенных файлов, отправляемых посредством веб-браузера, в соответствии с контентными и/или контекстными критериями.

IMCONTROLLER

Программы для мгновенного обмена сообщениями давно перестали быть средством развлечения и стали полноценным инструментом для ведения деловых переговоров и передачи ценной информации. С другой стороны, посредством таких программ можно легко передавать конфиденциальную информацию сторонним людям.

Программный модуль IMController предназначен для перехвата сообщений, файлов и голосовых сеансов связи популярных интернет-мессенджеров.

Программа сохраняет всю переписку в базу данных, по которой впоследствии можно производить поиск, используя поисковые возможности программы AnalyticConsole (морфология, тематические словари, поиск похожих и т.д.).

Поиск может быть ограничен различными критериями, например, перепиской двух конкретных сотрудников за определенный период времени.

В дополнение к отслеживанию утечек данных, можно контролировать ведение переговоров и целесообразность использования рабочего времени.

Контролируемые протоколы:

- **XMPP** (Jabber);
- **HTTP IM** (Facebook, Мой Мир@Mail.Ru, ВКонтакте, Одноклассники.ru, Linkedin и другие).

Контролируемые приложения:

- **Microsoft Lync 2013 / Skype for Business 2015, 2019 / MS Teams;**
- **Viber (Desktop);**
- **Telegram;**
- **WhatsApp;**
- **Skype;**
- **Zoom;**
- **Line;**
- **Lync;**
- **True Conf;**
- **Slack;**
- **и др.**

Возможна:

- блокировка по контентным и/или контекстным критериям сообщений и файлов, отправляемых посредством мессенджеров (подробный перечень мессенджеров представлен в документе «Возможности LibraDLP».
- блокировка доступа к ресурсу Web-Telegram.

HTTPCONTROLLER

Социальные сети и блоги стремительно развиваются в последние годы. С одной стороны, они помогают поиску необходимых кадровых ресурсов, изучению потенциальных партнеров по бизнесу и набору персонала. Это помогает организациям критически и по-новому взглянуть на себя. С другой стороны, использование новых способов коммуникации приводит к росту уязвимости утечки информации. Сотрудники могут использовать социальные сети, блоги, чаты для незаконных действий, способных причинить урон репутации и финансовой деятельности компании.

Программный модуль HTTPController предназначен для перехвата сообщений, передаваемых по HTTP-протоколу, индексирования перехваченных сообщений и полнотекстового поиска по ним. Модуль позволяет отслеживать сообщения, передаваемые через интернет-форумы, блоги, соцсети, чаты в браузере.

Контролируется передача данных по протоколу HTTP(S) с использованием методов POST:

- Блоги;
- Интернет-форумы;
- Формы обратной связи;
- Веб-чаты;
- Социальные сети (Facebook, ВКонтакте, Одноклассники.ru, Мой Мир@Mail.ru, Linkedin);

Также перехватываются GET-запросы поисковых систем.

Возможна блокировка:

- доступа к запрещенным веб-ресурсам в соответствии с настроенными правилами;
- передачи посредством веб-браузера файлов, соответствующих контентным и/или контекстным критериям;
- передачи сообщений и файлов по протоколу HTTP в социальных сетях;
- расширений браузеров (аддонов/плагинов/дополнений и т.п.).

DEVICECONTROLLER

Одним из самых простых способов хищения информации является переписывание данных из локальной сети предприятия на внешние устройства. Это могут быть как CD-/DVD-диски, так и устройства, подключаемые через порты USB.

Блокировка съемных носителей информации в качестве меры защиты от утечек неблаготворно влияет на сотрудников, а иногда и вовсе препятствует надлежащему выполнению ими своих рабочих обязанностей. Современная система безопасности должна предполагать блокировку каналов коммуникации лишь в исключительных случаях. В штатных условиях все каналы должны быть открыты сотрудникам для передачи информации, но при этом информационные потоки должны подвергаться мониторингу и анализу.

DeviceController – программный модуль, перехватывающий информацию, передаваемую пользователем на внешние устройства, а также отслеживающий сам факт подключения такого рода устройств. Перехваченная информация помещается в хранилище, откуда спустя некоторое время она становится доступной для быстрого поиска.

В дополнение к этому, DeviceController позволяет ограничить доступ к различным типам внешних устройств, будь то сканеры, модемы, принтеры или планшеты.

Дополнительные возможности:

- Частичная и полная блокировка доступа к устройствам хранения данных, когда данные разрешается использовать для чтения с одновременным запретом всех других операций (запись, создание, копирование, переименование).
- Использование списков исключений для устройств.
- Теневое копирование данных, имеющихся на подключаемых устройствах.
- Ограничение доступа к папкам и дискам.
- Ограничение объема данных, которые могут быть записаны сотрудником на USB-устройства хранения данных.
- Формирование запроса на получение доступа а также получение уведомлений о блокировке доступа к файлам, устройствам, процессам, через специальный интерфейс на PC сотрудника.

Блокировка:

- записи на USB-устройства хранения данных определенного содержимого;
- помещения в буфер обмена и вставки из него определенного содержимого, в том числе и для RDP-сессий;
- операций ‘Drag and Drop’ при копировании файлов на внешние устройства;
- работы USB-устройств с файловыми системами, не поддерживающими метаданные. Но с возможностью разрешения чтения данных с таких устройств.

FTPCONTROLLER

FTPController производит мониторинг документов, загруженных или переданных как по обычному FTP-соединению, так и переданных по зашифрованному SSL-соединению.

Блокировка передачи файлов по контентным и/или контекстным критериям.

Наиболее часто FTP (File Transfer Protocol – протокол передачи данных) используется для решения таких задач, как загрузка программного обеспечения, размещение материалов на сайтах, передача документов на файл-серверы.

Средства работы с FTP-серверами широко распространены и доступны каждому, в том числе инсайдерам и недобросовестным работникам.

Модуль FTPController предназначен для контроля входящего и исходящего FTP-трафика на уровне рабочих станций. Отправленные и загруженные файлы перехватываются, записываются в файловое хранилище, их содержимое индексируется и становится доступным для полнотекстового поиска.

PRINTCONTROLLER

Используя принтер, установленный на рабочем месте, или даже сетевой принтер, находящийся в общем доступе, любой сотрудник может распечатать и вынести за пределы компании конфиденциальные данные. Также случаются ситуации, когда недобросовестный сотрудник часто использует принтер для личных нужд, не имеющих ничего общего с рабочим процессом.

PrintController предназначен для контроля содержимого документов, отправленных пользователем на печать как посредством сетевых, так и локальных принтеров.

Отслеживая документы, напечатанные на принтере, можно не только предотвращать попытки хищения информации, но также и оценивать степень целевого использования принтера каждым сотрудником.

Образы и тексты распечатанных документов (при необходимости также и оригиналы файлов, отправленных на печать) помещаются в базу данных, индексируются и становятся доступными для просмотра и анализа. Модуль позволяет проследить «историю» документов: кто распечатал, когда, какое количество страниц.

Также при анализе распечатанных документов можно использовать OCR-модуль, так как часть данных выводится на печать в графическом формате.

Возможна блокировка печати документов согласно:

- содержимому отправляемого на печать документа;
- имени принтера / процесса / пользователя / компьютера.

Возможна блокировка Escape функции (управление принтером напрямую через Escape-команды).

Возможность включить поддержку виртуальных приложений App-V.

Блокировка печати или ограничение количества распечатываемых страниц по контентным и/или контекстным критериям. Блокировка печати файлов с тегами классификации.

MonitorController (включая KeyLogger и CameraController)

Подключение офисных компьютеров к глобальной информационной сети может работать как на благо, так и во вред компании. Наличие неограниченного доступа в Интернет может вызывать у сотрудников соблазн погружаться в просмотр новостного, коммерческого или развлекательного контента в ущерб выполнению непосредственных производственных задач.

MonitorController предназначен для перехвата информации, отображаемой на мониторах пользователей. Решение поставляется совместно с программным модулем KeyLogger, который позволяет перехватывать данные, вводимые пользователем с клавиатуры и помещаемые в буфер обмена.

Принцип работы состоит в периодическом перехвате содержимого пользовательских экранов, нажатий клавиш в различных приложениях, содержимого буфера обмена и сохранении полученных данных в базе данных. Функциональность MonitorController обеспечивает также одновременный просмотр активности экрана одного или нескольких пользователей в настоящем времени.

С целью идентификации сотрудников, которые создают скриншоты или ведут видеозапись экрана, можно включить наложение водяного знака на экран и их отображение на созданных снимках и видеозаписях.

При наличии подключенной к компьютеру **веб-камеры** можно **идентифицировать авторизовавшегося** в системе **пользователя** и **обнаруживать сьёмку экрана на телефон**.

Для просмотра происходящего на рабочем месте в реальном времени предусмотрен специальный режим LiveCam.

Модуль может быть установлен на любую рабочую станцию. Перехват происходит незаметно для пользователя.

Отслеживание состояния экранов и перехват нажатия клавиш пользователей происходит и при работе в терминальных сессиях (подключение по RDP-соединению).

Снятие скриншотов и запись видео может осуществляться по настроенным условиям, таким как:

- авторизация пользователя ОС;
- смена активного окна;
- открытие определённых сайтов или процессов;
- ввод ключевых слов пользователями и др.

CloudController

Сегодняшняя популярность облачных сервисов легко объясняется стремительным ростом информационных технологий и увеличением скоростей Интернета. Данные, хранящиеся в облачных хранилищах, доступны для пользователей из любой точки мира и любого устройства, подключенного к сети Интернет.

Достоинства таких сервисов налицо, и руководители организаций с легкостью могут представить, сколько денег можно сэкономить на оснащении сотрудников рабочими компьютерами, покупке лицензионных программных продуктов и оплате труда IT-специалистов.

Тем не менее, при использовании облачных хранилищ Ваша информация хранится непосредственно не у Вас, а на удаленном компьютере. И хотя все сервисы заботятся о сохранении и нераспространении данных своих клиентов, защиту от утечки информации, осуществленную руками собственных сотрудников, никто не гарантирует.

CloudController предназначен для контроля входящих и исходящих данных облачных сервисов:

- 4shared
- Acronis File Advanced
- ADrive
- Amazon S3
- ASUS WebStorage
- Box
- Cloudian S3 storage
- CloudMe
- Disk Bitrix 24
- disk-o.cloud
- DropBox
- DropMeFiles
- Evernote
- Google Docs, Drive, Colab
- Hightail
- iCloud
- Inbox.com
- MediaFire
- MiMedia
- My-Files
- Nextcloud
- Office 365
- OneDrive
- OpenDrive
- OwnCloud
- OziBox
- Pcloud
- Seafile
- SharePoint
- SkyDrive
- SpiderOak
- SugarSync
- Syncplicity
- Userscloud
- Wondershare Document Cloud
- Облако Mail.ru
- СберДиск и Яндекс.Диск
- Контур.Диадок

Контроль файлов, передаваемые в программах удаленного доступа (TeamViewer, RealVNC, Radmin, LiteManager, AnyDesk, Ассистент).

Блокировка передачи файлов и сообщений по контентным и/или контекстным критериям.

PROGRAMCONTROLLER

Трудно представить руководителя, которого бы не интересовало, каким образом сотрудники используют корпоративные вычислительные средства в рамках выполнения ими своих служебных обязанностей. Например, какую долю времени сотрудник уделяет выполнению своих должностных обязанностей, с какой целью и в каком объеме он пользуется сервисами сети Интернет, какую информацию передает по электронной почте, какую информацию и с какой целью набирает в текстовом редакторе.

ProgramController предназначен для ведения учета активности пользователей в запускаемых ими приложениях и на посещаемых веб-ресурсах на протяжении рабочего дня. Перехваченная активность сохраняется в базу данных, после чего с помощью клиентского приложения к ней можно применять атрибутный поиск и просматривать.

- Агент может быть установлен на любую рабочую станцию. Мониторинг активности происходит незаметно для пользователя.
- Предусмотрена возможность мониторинга отдельных процессов и веб-ресурсов.
- Возможен поиск перехваченных данных за определенный период времени применительно к аданным пользователям, компьютерам, MAC- и IP-адресам, именам запущенных процессов и продолжительности работы в них.
- Присутствует возможность выявлять симулированную деятельность пользователей, например, с помощью программ автокликеров или зажатия клавиш на клавиатуре.
- Просмотр информации о рабочем времени, собственной активности через специальный интерфейс на PC сотрудника.

FileController с функцией тегирования

FileController с функцией тегирования позволяет вычислять конфиденциальную информацию на рабочих станциях сети, в сетевых папках или на серверах, используя настройки правил сканирования для выбранных ресурсов. Функции программного продукта реализуются с помощью агента и/или с помощью серверной службы анализа данных.

FileController с функцией тегирования обеспечивает:

Локальное сканирование файлов посредством агента DLP-системы.

Сетевое сканирование без установки агента DLP-системы по протоколам:

- SMB (NFS);
- FTP(S);
- SSH (SFTP);
- WebDAV (DAV(S), HTTP(S));
- Microsoft 365.

Сканирование содержимого электронных писем на серверах Microsoft **Exchange**.

Аудит операций с файлами с использованием функций агента, а также с использованием функции чтения журналов событий Windows и/или NetApp.

Получение информации об изменениях на контроллере домена через журнал безопасности **Active Directory**.

Классификация, **теневое копирование и вычитка прав доступа** к файлам и папкам.

Установка меток классификации файлов как в автоматическом, так и в ручном режиме из контекстного меню Проводника, приложений MS Office, AutoCAD, MS Outlook.

Управление правами на операции с метками ручной классификации.

Отслеживание операций с файлами (появления, копирования, перемещения и удаления конфиденциальной информации на рабочих станциях).

Архивирование критичных документов позволяет создавать теневые копии критичных файлов, найденных на рабочих станциях, серверах или в сетевых папках, сохраняет историю их редакций. Архив уязвимых данных помогает в расследованиях инцидентов и гарантирует восстановление потерянной информации.

Продукт позволяет производить мониторинг следующих операций с файлами:

- создание;
- чтение;
- перемещение;
- переименование;
- запись;
- удаление;
- выполнение;
- копирование;
- запрет доступа;
- изменение прав доступа;
- изменение расширения.

Блокировка:

- передачи, печати файлов с метками автоматической или ручной классификации данных;
- использования USB-устройств с файловыми системами, не поддерживающими метаданные.

ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ ПРОДУКТОВ LIBRADLP

Программный комплекс LibraDLP разработан с учётом специфики работы крупных компаний и обладает рядом достоинств:

- **Простота внедрения.** Программный комплекс LibraDLP можно проинсталлировать всего за несколько часов силами собственных IT-специалистов. При этом нет необходимости предоставлять внутренние документы сотрудникам ООО «Либрасофт». Внедрение комплекса не влияет на функционирование существующих внутри компании информационных систем.
- **Комплексность решения** позволяет контролировать все каналы утечки информации, а многокомпонентная структура позволяет выбрать только необходимые модули.
- **Полный контроль информации, передаваемой через Skype** (голосовые, текстовые, SMS-сообщения и файлы).
- **Контроль ноутбуков** позволяет выявить утечку информации через ноутбуки, используемые сотрудниками вне корпоративной сети (например, дома или в командировках).
- **Полная интеграция с доменной структурой Windows** позволяет однозначно установить отправителя данных независимо от используемых им электронного почтового ящика, номера ICQ, аккаунта Skype.
- **Мощный аналитический модуль** позволяет быстро и гибко настроить систему оповещения, не привлекая сторонних специалистов. При этом для эффективной защиты конфиденциальных данных необходимы минимальные трудозатраты на анализ информационных потоков.
- Благодаря **запатентованному алгоритму «Поиск похожих»**, позволяющему находить документы, похожие на оригинал не только технически, достигается существенная экономия времени, необходимого на анализ перехваченной информации.
- **Отслеживание и визуализация связей между сотрудниками.** Можно автоматически выявлять и анализировать связи сотрудников друг с другом и с внешними адресатами для удобной работы и проведения внутренних расследований.
- **Разграничение прав доступа к информации** дает возможность настройки прав доступа к перехваченной информации.
- **Контроль содержимого рабочих станций и общедоступных сетевых ресурсов** позволяет отслеживать появление конфиденциальной информации в местах, для этого не предназначенных.
- **Создание архива перехваченной информации** позволяет проводить полноценные служебные расследования, существенно упрощая восстановление последовательности событий инцидента.
- **Собственный отдел внедрения и учебный центр.** Богатый опыт работы с более чем 1700 различными компаниями позволяет оперативно создавать уникальные наборы политик безопасности, ориентированные непосредственно на деятельность организации.

Наши клиенты

Среди заказчиков «Либрасофт» — белорусские, иностранные и совместные предприятия, организации и учреждения:

- Финансовые организации;
- Промышленные предприятия;
- Учреждения образования;
- IT и телеком-компании;
- Оборонные предприятия;
- Ритейл-компании;
- Организации сферы гостеприимства;
- Учреждения здравоохранения;
- Предприятия нефтегазового сектора;
- Органы государственной власти и управления.

Наши контакты

Беларусь, Минск

220040 пер. М. Богдановича, д. 1, эт. 2, каб. 3

Телефон: +375 (17) 227-56-80
E-mail: official@librasoft.by
Сайт: www.librasoft.by