Контур информационной безопасности

SEARCHINFORM

СОДЕРЖАНИЕ

Защита информации: «Контур информационной безопасности»

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 (Facebook, Одноклассники, ВКонтакте и др.), форумы, блоги, службы мгновенного обмена сообщениями (ICQ, MSN, Google Hangouts, Mail.ru Агент, Windows Live, X-Lite и пр.), внешние носители информации, мобильные устройства, принтеры, FTP-серверы, и, что сейчас особенно актуально, Skype.

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.

«Контур информационной безопасности Серчинформ» – признанный лидер на рынках информационной безопасности России и стран СНГ. 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.

Контур имеет модульную структуру, то есть заказчик может по своему выбору установить только часть компонентов. Все компоненты можно причислить к двум большим группам: суть работы первой платформы – SearchInform NetworkController – в зеркалировании трафика, вторая же – SearchInform EndpointController – задействует агентов, установленных на рабочих станциях пользователей.

SEARCHINFORM NETWORKCONTROLLER

SearchInform NetworkController – платформа для перехвата данных на уровне зеркалируемого трафика. Таким образом, NetworkController обрабатывает трафик, не влияя на работу корпоративной сети.

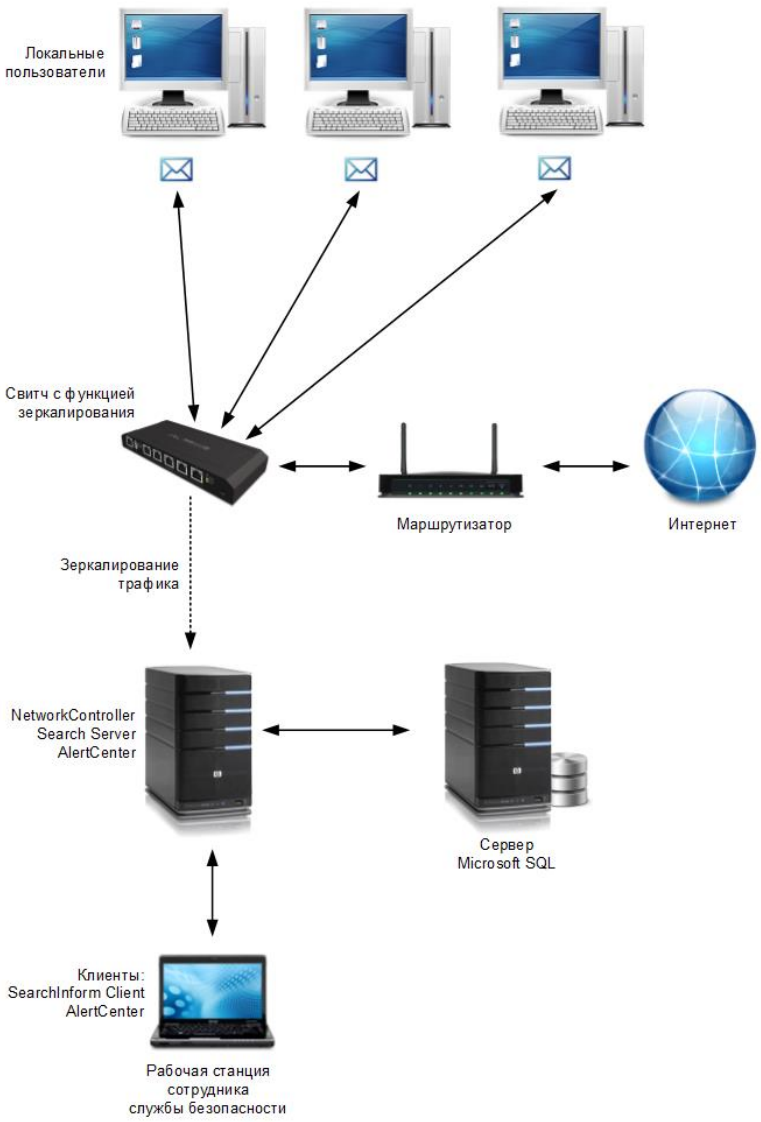
Перехватываются данные, пересылаемые пользователями по популярным сетевым протоколам и каналам (SMTP, POP3, HTTP(S), IMAP, MAPI, NNTP, ICQ, XMPP, MMP, MSN, SIP, YAHOO, FTP) на уровне локальной сети.

Дополнительно к этому, в состав NetworkController входит:

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

Платформа включает в себя следующие продукты:

- **SearchInform MailController**;
- **SearchInform IMController**;
- **SearchInform HTTPController**;
- **SearchInform FTPController**;
- **SearchInform 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 сообщения помещаются в базу данных SQL, которая индексируется при помощи компонента Search Server. Индекс – особая структура, необходимая для быстрого поиска по перехваченным документам.

При помощи приложения SearchInform AlertCenter данные индекса с заданным интервалом проверяются на соответствие заранее настроенным политикам безопасности, состоящим из поисковых запросов. Расписание проверок и список запросов настраиваются работниками службы безопасности организации. В случае обнаружения совпадений SearchInform AlertCenter немедленно оповещает об этом сотрудника службы безопасности.

SEARCHINFORM ENDPOINTCONTROLLER

SearchInform EndpointController – платформа для перехвата и остановки трафика через агенты. Дополнительно позволяет контролировать сотрудника, находящегося в командировке за пределами корпоративной сети, ведь работник может свободно передать конфиденциальные данные с ноутбука третьим лицам.

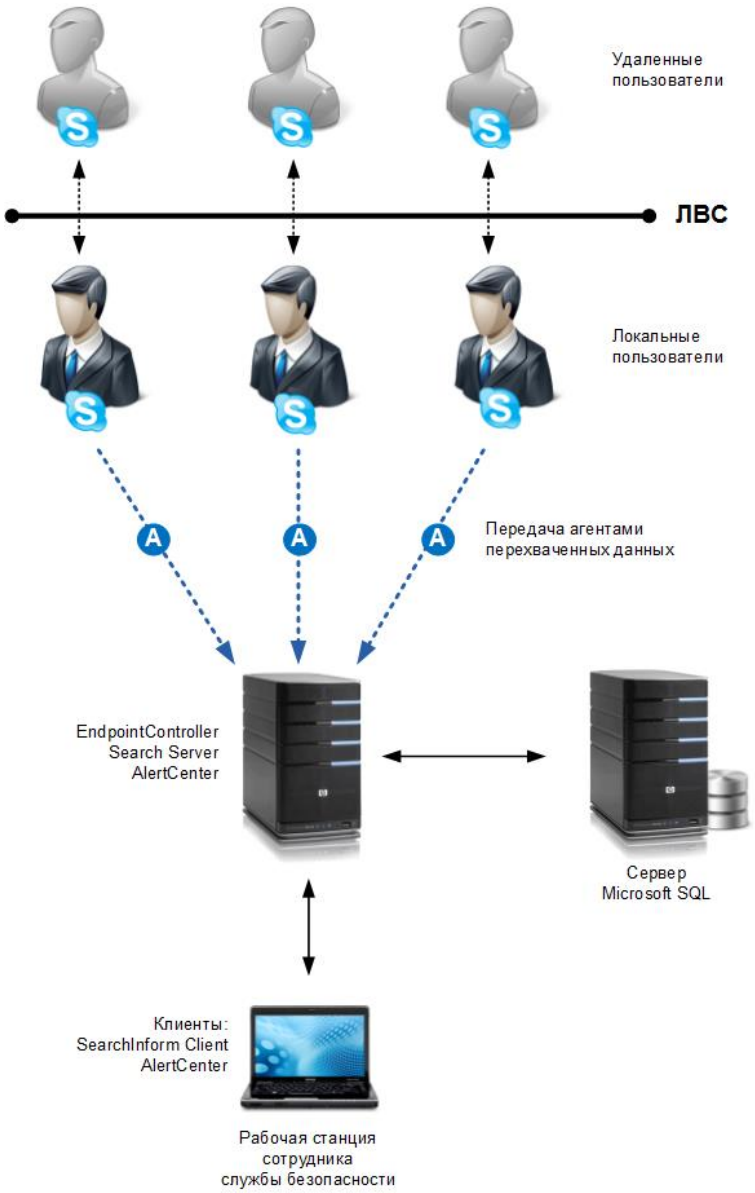
Агенты SearchInform EndpointController позволяют перехватывать:

- **SearchInform MailController** – входящую и исходящую (с возможностью блокировки) электронную почту, как через почтовые клиенты, так и с доступом через браузер;
- **SearchInform IMController** – сообщения популярных мессенджеров, а также отслеживать общение в популярных социальных сетях;
- **SearchInform SkypeController** – голосовые и текстовые сообщения, а также файлы и SMS, передаваемые через Skype;
- **SearchInform DeviceController** – информацию, записываемую на подключаемые внешние устройства (USB-flash, CD/DVD и пр.);
- **SearchInform FTPController** – информацию, передаваемую по протоколу FTP;
- **SearchInform CloudController** – входящие и исходящие файлы облачных хранилищ данных и SharePoint;
- **SearchInform PrintController** – содержимое документов, отправленных на печать;
- **SearchInform MicrophoneController** – разговоры сотрудников внутри офиса или за его пределами.

А также контролировать и отслеживать:

- **SearchInform FileController** – операции с файлами, хранящимися на серверах и в общих сетевых папках.
- **SearchInform MonitorController** – информацию, отображаемую на мониторах пользователей, нажатия клавиш и содержимое буфера обмена.
- **SearchInform ProgramController** – активность пользователей в запускаемых ими приложениях и на посещаемых веб-сайтах.

Принцип работы



Агенты SearchInform Endpoint-Controller производят теневое копирование отправленных на печать документов, перего-воров в Skype; информации, записываемой на сменные носители, передаваемой по протоколу FTP и отображаемой на мониторах пользователей; отслеживают операции с файлами и направляют полученные данные серверу SearchInform EndpointController.

Сервер помещает перехва-ченные данные в базу под управлением СУБД Microsoft SQL Server.

Для быстрого поиска по базе и просмотра документов база индексируется компонентом Search Server. При помощи планировщика обновлений обеспечивается поддержание индекса в постоянно актуальном состоянии. В случае обнаружения фактов нарушения политик безопас-ности организации, Search-Inform AlertCenter немедленно оповещает об этом сотрудника службы безопасности.

NetworkController и EndpointController: преимущества использования обеих платформ

Для комплексного контроля передаваемых данных целесообразно использовать одновременно и SearchInform NetworkController, и SearchInform EndpointController. 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 проведения немедленного расследования.

Сервер индексации рабочих станций

Search Server индексирует новые и измененные файлы, благодаря чему их содержимое становится доступным для полнотекстового поиска. Данная функция позволяет отследить наличие конфиденциальной информации на компьютерах пользователей.

На компьютеры устанавливаются программы-агенты, которые позволяют проиндексировать всю информацию с заданных компьютеров в локальной сети предприятия. Агенты протоколируют изменения существующих файлов и создание новых файлов на рабочих станциях пользователей.

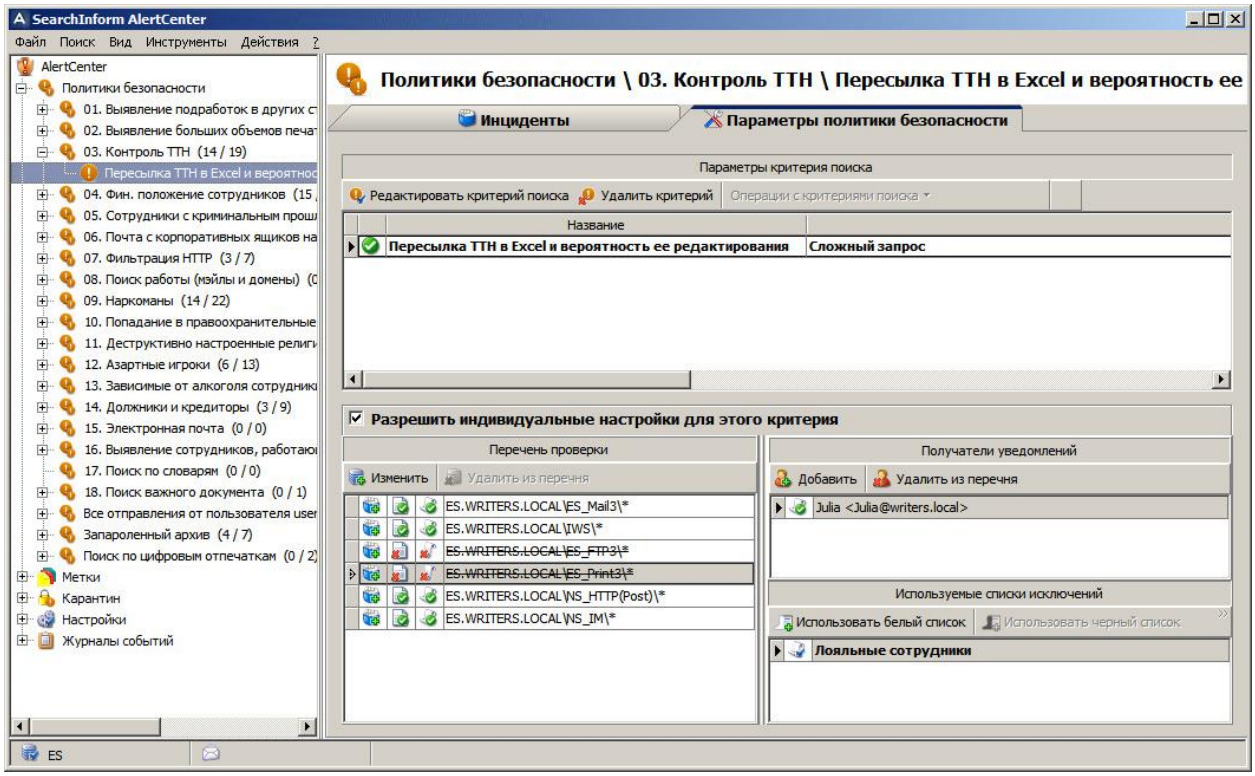
В режиме реального времени анализируется информация в созданных, измененных, перемещенных и удаленных файлах на пользовательских компьютерах.

Приложение Search Server поддерживает индексирование более 100 типов файлов.

SEARCHINFORM ALERTCENTER

SearchInform AlertCenter – «мозговой центр» системы безопасности. Опрашивает все модули и, при наличии в перехваченной информации определенных ключевых слов, фраз или фрагментов текста, немедленно оповещает об этом офицеров безопасности.

В клиентской консоли AlertCenter создаются политики информационной безопасности, применяемые к перехваченным данным.



Для идентификации конфиденциальной информации в AlertCenter можно использовать следующие методы:

- Поиск по ключевым словам и фразам с учетом морфологии, синонимов и расстояния между словами фразы;
- 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;

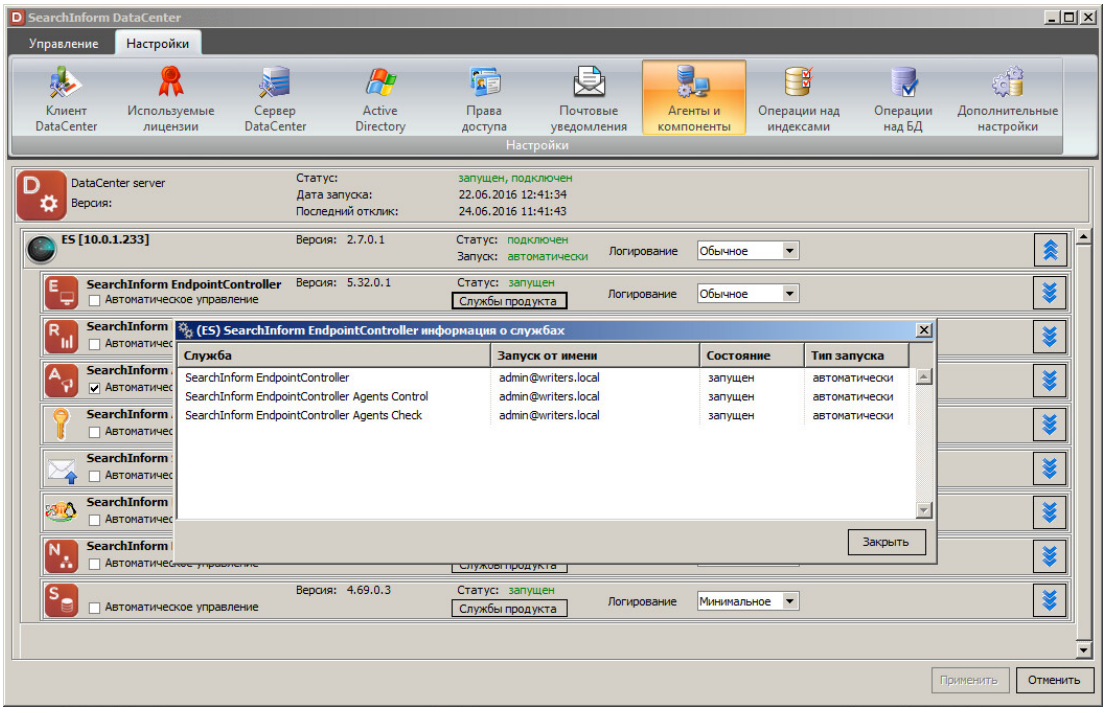
- Запросы с цифровыми отпечатками – сравнение всех перехваченных документов с набором контрольных документов;
- Поиск по атрибутам сообщений и файлов: дата, размер, тип документа, пользователь домена, адреса электронной почты и другие формальные признаки документов;
- Поиск по базам данных;
- Поиск документов, защищенных паролем;
- Сложные запросы – комбинирование нескольких простых запросов при помощи логических операторов;
- Запросы с регулярными выражениями – поиск информации не по точному значению, а по форме данных (последовательность и тип 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.

SEARCHINFORM DATACENTER

Продукт **SearchInform DataCenter** входит в состав «Контура информационной безопасности Серчинформ» (КИБ) и предназначен для автоматизированного и ручного управления различными аспектами работы КИБ.

Основные возможности DataCenter:

- отслеживает состояние служб КИБ;
- контролирует наличие свободного дискового пространства для индексов и баз данных компонентов КИБ, а также поступление в них перехваченной информации;
- выполняет автоматические действия по созданию новых индексов и баз, настройку перехвата на них, а также автоматическое удаление недоступных для поиска индексов и БД по достижении заданных условий;
- производит синхронизацию КИБ с Active Directory;
- позволяет разграничить права доступа сотрудников службы безопасности к информации определенных пользователей;
- в зависимости от настроек, извещает пользователя о различных событиях или неудовлетворительных условиях для работы КИБ.



SEARCHINFORM REPORTCENTER

Продукт **SearchInform ReportCenter** предназначен для сбора статистики по активности пользователей и инцидентам, связанным с нарушениями политик информационной безопасности, и представления ее в виде отчетов.

Основные возможности ReportCenter:

- генерация отчетов по имеющимся шаблонам;
- наличие библиотеки базовых шаблонов;
- возможность добавлять пользовательские шаблоны;
- переключение между различными формами отчетов;
- переход по связанным отчетам одним щелчком;
- генерирование и рассылка оповещений по активности пользователей, запускаемых ими процессов и/или посещаемых веб-сайтах.

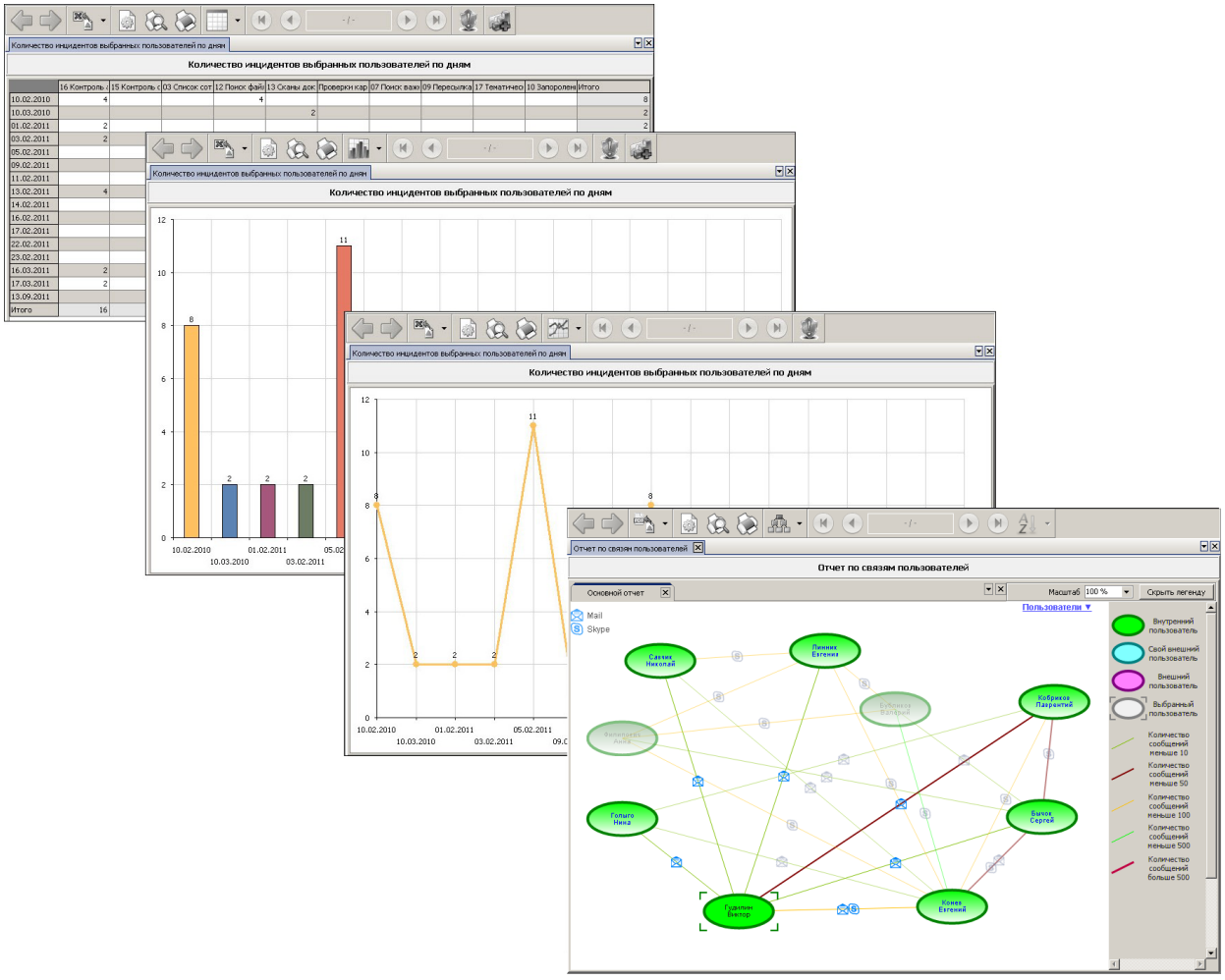
В приложении предусмотрена возможность формирования разнообразных отчетов, позволяющих составить представление о рациональности использования рабочего времени тем или иным пользователем, а также соблюдении им политик безопасности организации, например:

- «топ» по числу перехваченных файлов и сообщений;
- «топ» пользователей по числу инцидентов;
- распределение инцидентов по группам пользователей и ассоциированным политикам безопасности;
- визуализация связей сотрудников с их адресатами;
- средняя продолжительность рабочего дня и суммарное время работы сотрудников;
- среднесуточная и суммарная активность запускаемых пользователями процессов;
- среднесуточная и суммарная активность на посещаемых пользователями веб-сайтах;
- детальная информация по работе пользователей;
- оповещения по активности пользователей и процессов/сайтов;
- журнал рабочего времени пользователей;
- отчет по нарушениям рабочего режима;

- отчет по установленному и измененному на компьютерах пользователей оборудованию;
- список установленного на рабочих станциях программного обеспечения, история его установки и удаления;
- хронология событий над агентами: их установка, обновление и удаление;
- количество сообщений относительно каждого компьютера и продукта.

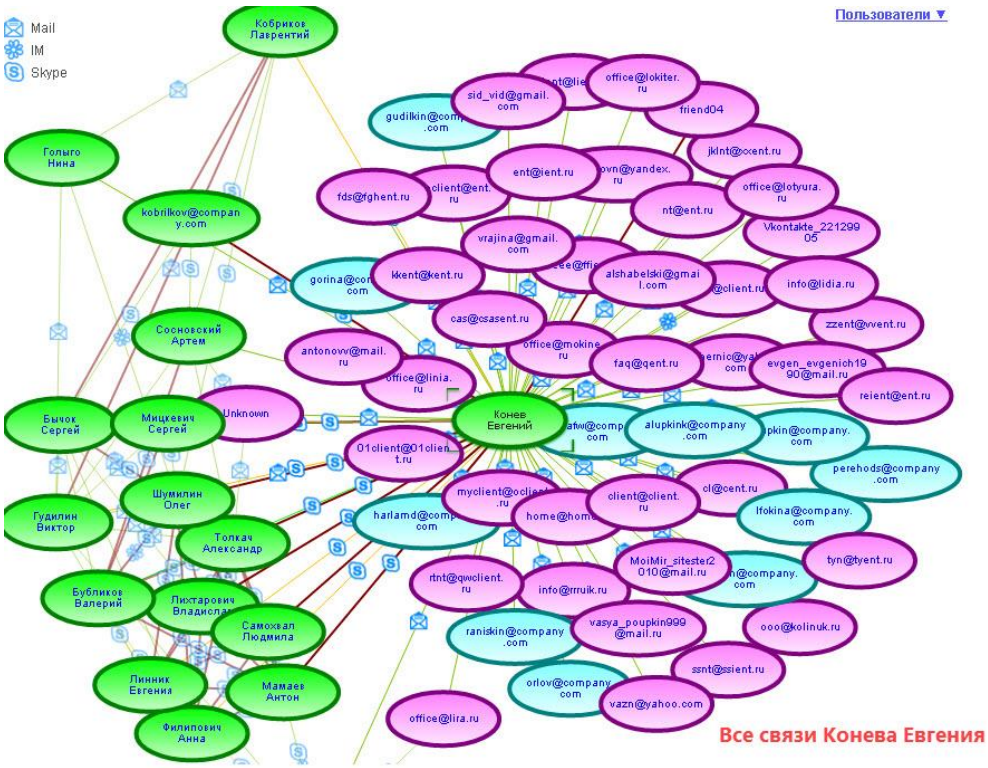
Каждый из отчетов может формироваться как для всех протоколов передачи данных, так и для каждого из них в отдельности, что позволит сотрудникам службы информационной безопасности быстрее и точнее анализировать данные о возможных инцидентах.

Отчет может быть сформирован в формате таблицы, диаграммы, временного графика, а также в виде графа отношений, представляющего собой регулируемую визуализацию связей между пользователями, находящимися в контакте.



Граф отношений, будучи наделен свойствами интерактивности, дает наглядное представление о связях внутри коллектива по всем основным каналам

коммуникации, а также о круге общения того или иного пользователя. Выявить, с кем устанавливались контакты с данной учетной записи на компьютере на протяжении заданного периода времени, теперь не составляет труда.



Компонент ReportCenter может формировать отчеты как за весь период работы «Контура информационной безопасности», так и за указанный пользователем временной период. Для некоторых отчетов доступна также функция выбора пользователей, позволяющая отобразить отчет только для интересующих пользователей.

Помимо ряда стандартных шаблонов отчетов, предусмотрена возможность добавления пользовательских шаблонов. При этом можно настроить:

- название отчета и его тип,
- параметры фильтрации, которые будут учтены при построении отчета,
- временной период,
- дополнительные параметры, индивидуальные для каждого типа отчета,
- при доступности, параметры формирования и отправки оповещений.

Любой сгенерированный отчет может быть сохранен как отдельный (пользовательский) шаблон.

Все отчеты открываются на отдельных вкладках из клиентской консоли SearchInform ReportCenter и могут быть выведены на печать либо экспортированы в форматы PDF, HTML, TXT, XLS, XML.

Аналитические возможности

Наиболее важным компонентом любой системы информационной безопасности является аналитический модуль. Совместное использование всех типов поиска позволяет максимально эффективно защищать конфиденциальные данные в корпоративной сети и, что особенно важно в современных условиях, - резко сократить трудозатраты на их анализ. Поисковые механизмы, встроенные в «Контур информационной безопасности Серчинформ», 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 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.

4. **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.

5. **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.

6. **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.

7. **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.

Интеграция с доменной системой Windows позволяет легко идентифицировать интересующего Вас пользователя 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.

«Контур информационной безопасности Сёрчинформ» 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 лэптопы, 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 лэптоп снова оказывается в корпоративной сети, все отправленные данные незаметно собираются и передаются для анализа в отдел 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.

Средства контроля информационных потоков

Архитектура

Все компоненты системы имеют клиент-серверную структуру.

Под серверной частью подразумевается одна из платформ для перехвата данных (SearchInform NetworkController либо SearchInform EndpointController), под клиентской – клиентские приложения, предназначенные для поиска и просмотра перехваченных данных в целях проведения служебных расследований.

Использование единого поискового аналитического движка позволяет в полной мере использовать богатые поисковые возможности.

SearchInform 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 продукт SearchInform 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 SearchInform 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)** (*Exchange Web Services* – исходящая и входящая почта, *Kerio Outlook Connect* – исходящая и входящая почта, *Outlook Web App и Outlook Web App light* – исходящая почта, *Zimbra Web Client* – входящая и исходящая почта, исходящая и входящая корреспонденция с почтовых веб-сервисов yandex.ru, tut.by, gmail.com, outlook.com, mail.ru, rambler.ru, office 365, ukr.net, yahoo.com, qip.ru, Google Sync).

Возможна интеграция с:

- почтовыми серверами **Microsoft Exchange**, **Lotus Domino** и др.;
- **Microsoft ISA / Forefront TMG** и прочими прокси-серверами, работающими по протоколу **ICAP**.

SearchInform 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 продукт SearchInform IMController предназначен для перехвата сообщений популярных IM-клиентов.

Программа сохраняет всю переписку в базу данных, по которой впоследствии можно производить поиск, используя поисковые возможности программы SearchInform Client (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:

- **OSCAR** (ICQ/QIP);
- **MSNP** (Windows Live);
- **XMPP** (Jabber, Google Hangouts);
- **MMP** (Mail.ru Agent);
- **HTTP IM** (Facebook, Мой Мир@Mail.Ru, Одноклассники.ru, Linkedin, ВКонтакте, Google+);
- **SIP** (X-Lite и др.);
- **Gadu-Gadu** (Gadu-Gadu);
- **YAHOO** (Yahoo! Messenger);
- **Viber** (Viber Desktop);
- **Microsoft Lync**.

SearchInform 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 компаниям критически и по-новому взглянуть на себя. С другой стороны, использование новых способов коммуникации приводит к росту уязвимости. Сотрудники могут использовать социальные сети, блоги, чаты для незаконных действий, способных причинить урон репутации и финансовой деятельности компании.

Программный продукт SearchInform 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, чаты, службы веб-почты или при помощи браузерных IM-клиентов.

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

- электронная почта с доступом через веб-интерфейс;
- блоги;
- интернет-форумы;
- формы обратной связи;
- веб-чаты;
- социальные сети (Facebook, ВКонтакте, Одноклассники.ru, Мой Мир@Mail.ru, Google+, Linkedin);
- Браузерные IM-клиенты (ICQ, MSN, QIP и т.д.).

Также перехватываются GET-запросы поисковых систем.

SearchInform SkypeController

SearchInform SkypeController используется для перехвата и анализа Skype-трафика:

- текстовых сообщений;
- передаваемых файлов;
- сеансов голосовой связи;
- SMS-сообщений.

Обмен по Skype текстовыми и голосовыми сообщениями давно стал полноценным способом ведения деловых переговоров и передачи корпоративной информации. Среди других каналов коммуникации Skype выделяется своим надежным методом шифрования данных, что в значительной мере повышает безопасность при передаче информации.

В то же время, данное преимущество может нести серьезные угрозы для компании в случае передачи конфиденциальных данных на сторону инсайдерами, поскольку трафик Skype практически невозможно расшифровать. С целью предотвратить все возможные утечки информации по этому каналу связи, некоторые руководители его просто «закрывают», что в свою очередь создает дополнительные трудности для делового общения.

SearchInform SkypeController позволяет контролировать, не запрещая. Приложение перехватывает сеансы голосовой и текстовой связи, SMS-сообщения и файлы, передаваемые при помощи Skype.

SearchInform 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.

SearchInform 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 полнотекстового поиска.

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

Дополнительные возможности:

- Частичная и полная блокировка устройств хранения данных, когда данные разрешается использовать для чтения с одновременным запретом всех других операций (запись, создание, копирование, переименование).
- Использование «белого» и «черного» списков устройств.
- Шифрование данных, записываемых на USB-flash.
- Ограничение доступа к папкам и дискам.

SearchInform FTPController

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

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.

Продукт SearchInform 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.

SearchInform PrintController

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

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.

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

Образы и тексты распечатанных документов помещаются в базу данных, индексируются и становятся доступными для просмотра и анализа. Продукт позволяет проследить «историю» документов: кто распечатал, когда, какое количество экземпляров.

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

SearchInform MicrophoneController

Продукт предназначен для записи разговоров, ведущихся сотрудниками внутри офиса, либо в командировках. Запись голоса производится с помощью любого обнаруженного микрофона (в гарнитуре, ноутбуке, веб-камере…). Перехваченные агентом записи сохраняются в базу данных, после чего с помощью клиентского приложения к ним можно применять атрибутный поиск, а также прослушивать.

Программное приложение может оказать неоценимую помощь в ходе проведения служебных разбирательств.

Программный продукт может быть установлен на любую рабочую станцию. Запись разговоров происходит незаметно для пользователя.

Режим LiveSound позволяет подключаться к рабочим станциям и прослушивать разговоры, ведущиеся сотрудниками, в режиме реального времени.

Предусмотрена возможность настройки условий записи:

- перехват только речи или всех звуков;
- внутри офиса или за его пределами;
- при записи речи – редактирование верхней и нижней границ алгоритма Voice Activity Detection, позволяющего распознать человеческую речь среди фонового шума или тишины;
- длительность звуковых файлов;
- уровень подавления шума;
- перечень процессов, при запуске которых будет производиться запись;
- расписание для активации звукозаписи.

SearchInform MonitorController + Keylogger

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.

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

Принцип работы продукта 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 режиме реального времени.

Продукт 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.

Режим LiveView позволяет осуществлять одновременный просмотр активности экрана одного или нескольких пользователей в режиме реального времени.

С помощью KeyLogger реализован мониторинг текстовых данных, помещенных в буфер обмена и вставленных из него.

SearchInform FileController

На файл-серверах может храниться огромное число документов, в том числе содержащих конфиденциальную информацию. Сотрудники могут получить доступ к документам, содержащим конфиденциальную информацию, и использовать их вразрез с существующими политиками, например, для передачи за пределы организаций.

Продукт SearchInform FileController предназначен для контроля операций с файлами, хранящимися на серверах и в общих сетевых папках. Посредством установленных на рабочих станциях и файл-серверах агентов, приложение регистрирует любые операции, совершаемые пользователями с файлами (открытие, копирование, изменение и т.д.).

Продукт FileController может производить мониторинг следующих операций: создание, чтение, перемещение, переименование, запись, удаление, выполнение, копирование, запрет доступа, изменение прав доступа, изменение расширения.

Производить мониторинг можно как на уровне файл-серверов, так и на уровне рабочих станций пользователей.

SearchInform 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, 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.

SearchInform CloudController предназначен для контроля входящих и исходящих данных облачных сервисов. Модуль позволяет отслеживать следующие облач-ные хранилища данных:

- Google Drive
- OneDrive
- Office 365
- Dropbox
- Evernote
- Yandex Disk
- cloud.mail.ru
- iCloud Drive
- DropMeFiles
- Amazon S3
- в том числе при использовании клиентов Google Drive Client, Dropbox Client, Yandex Drive Client, Mail.ru Client, Evernote Client, OneDrive Client.

Также осуществляется контроль файлов, передаваемых при помощи MS SharePoint.

SearchInform ProgramController

Трудно представить руководителя, которого бы не интересовало, каким образом сотрудниками используются корпоративные вычислительные средства в рамках выполнения ими своих служебных обязанностей. Например, какую долю времени сотрудник уделяет выполнению своих служебных 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.

SearchInform 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 ProgramController 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 заданным пользователям, компьютерам, MAC- и IP-адресам, именам запущенных процессов и продолжительности работы в них.

Преимущества использования продуктов SearchInform

«Контур информационной безопасности Сёрчинформ» разработан с учётом специфики работы крупных компаний и обладает рядом достоинств:

- **Простота внедрения.** Программный комплекс SearchInform можно проинсталлировать всего за несколько часов силами собственных IT-специалистов. При этом нет необходимости предоставлять внутренние документы сотрудникам SearchInform. 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 1500 различными компаниями позволяет оперативно создавать уникальные наборы политик безопасности, ориентированные непосредственно на деятельность организации.

Наши клиенты

Общее число клиентов SearchInform на данный момент – более 1700, около ста из них доверили защиту конфиденциальных корпоративных данных своей компании «Контуру информационной безопасности Сёрчинформ» еще в начале текущего года.

Ввиду специфики назначения системы по предотвращению утечек данных, приводим ниже лишь некоторую часть наших клиентов.

Наши координаты

Адрес: г. Москва, Скатертный переулок, д. 8/1, строение 1, помещения 1-12

Телефоны:
+7 (495) 721-84-06 (многоканальный)
+7 (499) 703-04-57
E-mail:
По общим вопросам – info@searchinform.ru
Контакт для прессы – pr@searchinform.ru

Учебный центр
Телефон:
+7 (495) 721-84-06 доб. 120, 138

Офис в Новосибирске
Адрес: Новосибирск,
ул. Владимировская, 2/1, офис 109
Глава офиса: Сорокин Николай
Телефон: +7 (495) 721-84-06, доб. 106
E-mail: n.sorokin@searchinform.ru

Офис в Екатеринбурге
Адрес: Екатеринбург,
ул. С. Дерябиной, 24, офис 801
Глава офиса: Алексей Попов
Телефоны:
+7 (343) 344-50-88
+7 (343) 344-51-38
E-mail: a.popov@searchinform.ru

Офис в Казани
Адрес: Казань,
ул. Островского, 57В, офис 301-303
Глава офиса: Латушкина Татьяна
Телефоны:
+7 (843) 212-43-12
+7 (843) 212-43-13
+7 (965) 600-53-07
E-mail: t.latushkina@searchinform.ru

Офис в Санкт-Петербурге
Адрес: Санкт-Петербург,
Коломяжский пр., 27, лит. А, пом. 27Н
Глава офиса: Евгений Юдов
Телефоны: +7 (812) 309-73-35
E-mail: e.judov@searchinform.ru

Офис в Беларуси
Адрес: Минск,
ул. Измайловская, 30
Глава офиса: Александр Барановский
Телефон: +375 (29) 649-77-79
E-mail: ab@searchinform.ru

Офис в Украине
Адрес: Киев,
ул. Глубочицкая, д. 33-37, офис 206
Глава офиса: Алена Бугаенко
Телефоны:
+38 (067) 476-15-18
+38 (044) 592-86-13
E-mail: a.bugaenko@searchinform.ru

Офис в Хабаровске
Адрес: Хабаровск,
ул. Пушкина, 54, офис 403
Глава офиса: Денис Кириленок
Телефон:
+7 (4212) 47-59-92
+7 (914) 201-69-86
E-mail: d.kirilenok@searchinform.ru

Офис в Казахстане
Адрес: Алматы,
ул. Ауэзова, 84, офис 200
Глава офиса: Дмитрий Стельченко
Телефон: +7 (727) 222-17-95
E-mail: d.stelchenko@searchinform.ru