

SearchInform



«Контур информационной безопасности
SearchInform»

Содержание

1. ЗАЩИТА ИНФОРМАЦИИ:

«КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ3 SEARCHINFORM»3

1.1. Каналы утечки информации и важность их контроля 3

1.2. Краткое описание продуктов контура 3

1.2.1. SearchInform NetworkSniffer4

1.2.2. SearchInform EndpointSniffer5

1.2.3. Сервер индексации рабочих станций.....6

1.2.4. NetworkSniffer и EndpointSniffer:.....6

преимущества использования обеих платформ.....6

1.2.5. Центр управления6

1.3. Аналитические возможности 8

1.4. Необходимость идентификации сотрудника 9

1.5. Распознавание ухищрений инсайдеров 10

1.6. Необходимость перехвата информации с ноутбуков,.....	10
когда сотрудник работает вне офиса.....	10
2. СРЕДСТВА КОНТРОЛЯ ИНФОРМАЦИОННЫХ ПОТОКОВ.....	11
2.1. Архитектура	11
2.2. SearchInform MailSniffer	11
2.3. SearchInform IMSniffer	12
2.4. SearchInform HTTPSniffer	12
2.5. SearchInform SkypeSniffer.....	12
2.6. SearchInform DeviceSniffer.....	13
2.7. SearchInform FTPSniffer.....	13
2.8. SearchInform PrintSniffer	13
2.9. SearchInform MonitorSniffer	13
2.10. SearchInform FileSniffer и индексация рабочих станций	13
2.11. Контроль ноутбуков	14
3. ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ ПРОДУКТОВ SEARCHINFORM	15
НАШИ КЛИЕНТЫ.....	16
НАШИ КООРДИНАТЫ	17

1. Защита информации: «Контур информационной безопасности SearchInform»

1.1. 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 2,7 млн. долларов. «Контур информационной безопасности SearchInform» позволяет эффективно защищать бизнес от убытков, связанных с утечками информации.

Как «утекает» информация? Существует несколько каналов передачи данных: электронная почта, социальные сети (Facebook, Одноклассники, вКонтакте), форумы, блоги, службы мгновенного обмена сообщениями (ICQ, MSN, Jabber, Mail.ru-Агент), внешние носители информации, принтеры, и, что сейчас особенно актуально, Skype и его аналоги.

Если данные каналы передачи информации в Вашей организации не контролируются, либо контролируются 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.

1.2. Краткое описание продуктов контура

«Контур информационной безопасности SearchInform» – признанный лидер на рынках информационной безопасности России и стран СНГ. Продукт используются во многих крупных организациях, работающих в самых разных отраслях – от банковского дела до машиностроения.

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.

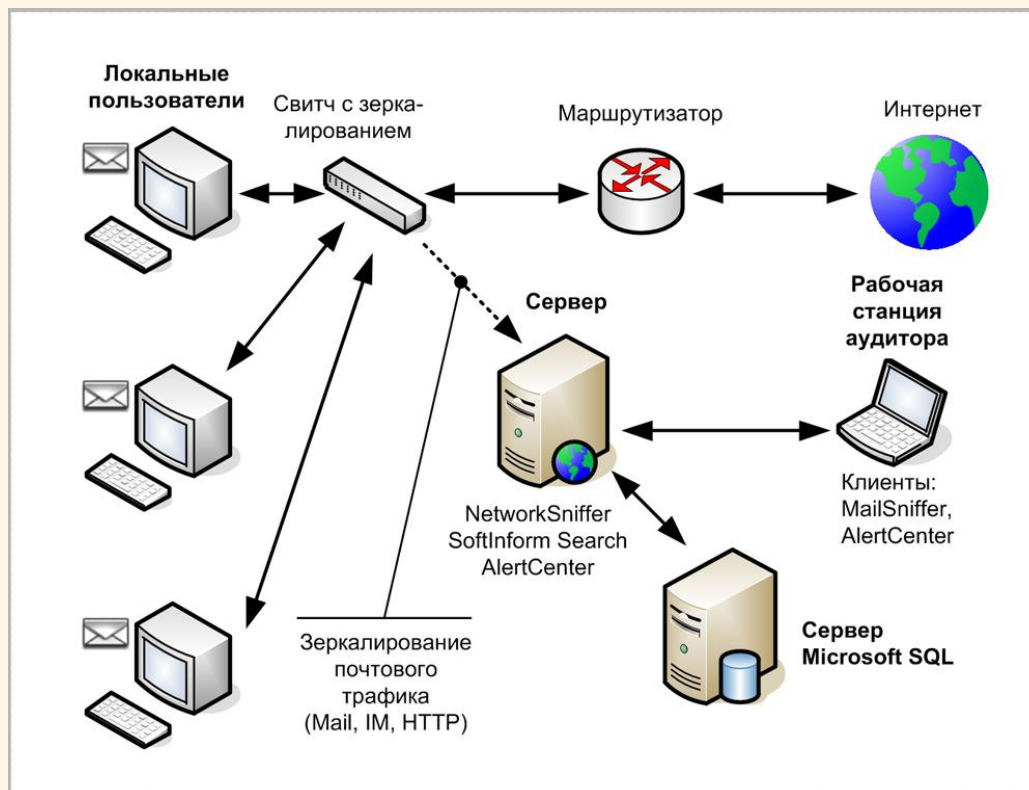
Контур имеет модульную структуру, то есть заказчик может по своему выбору установить только часть компонентов. Все компоненты можно причислить к двум большим группам: суть работы первой – платформа SearchInformNetworkSniffer – в зеркалировании трафика, вторая же – SearchInformEndpointSniffer – задействует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

1.2.1. SearchInform NetworkSniffer

SearchInformNetworkSniffer - платформа для перехвата данных на уровне зеркалируемого трафика, т.е. NetworkSnifferобрабатывает трафик, не влияя на работу корпоративной сети. Перехватываются данные, пересылаемые пользователями по популярным сетевым протоколам и каналам (SMTP, POP3, IMAP, HTTP, HTTPS, MAPI, ICQ, JABBER, MSN, FTP, SIP) на уровне локальной сети, а также внутреннее общение через MSCommunicator/LyncServer). Платформа включает в себя следующие продукты:

- **SearchInformMailSniffer**, позволяющий перехватывать всю входящую и исходящую электронную почту;
- **SearchInformIMSniffer** - сообщения интернет-пейджеров (ICQ, QIP, MSN, JABBER), а также отслеживать общение в популярных социальных сетях;
- **SearchInformHTTPSniffer** - информацию, отправляемую на интернет-форумы, блоги и прочие web-сервисы;
- **SearchInformFTPSniffer** - информацию, передаваемую по протоколу FTP.

Механизм работы NetworkSniffer



- Перехват сетевого трафика производится на уровне сетевых протоколов (Mail, IM, HTTP). Возможна фильтрация по имени пользователя домена, IP- и MAC-адресам.
- Перехваченные сообщения помещаются в базу данных SQL.
- База перехваченных сообщений индексируется при помощи сервера SoftInformSearch. Индекс – особая структура, необходимая для быстрого поиска по перехваченным документам.
- При помощи приложения SearchInformAlertCenter новая информация в индексе с заданным интервалом проверяется на соответствие заранее настроенным политикам безопасности, состоящим из поисковых запросов. Расписание проверок и список запросов настраиваются работниками службы безопасности организации. В случае обна-

ружения совпадений SearchInformAlertCenter незамедлительно высылает ответственному работнику уведомление.

1.2.2. SearchInform EndpointSniffer

SearchInformEndpointSniffer- платформа для перехвата и остановки трафика через агенты. Дополнительно позволяет контролировать сотрудника, находящегося за пределами корпоративной сети - ведь работник может свободно передать конфиденциальные данные с ноутбука третьим лицам. SearchInformEndpointSniffer собирает отправленные данные и передает их для анализа отделу ИБ, либо через Интернет, либо как только лэптоп снова окажется в корпоративной сети.

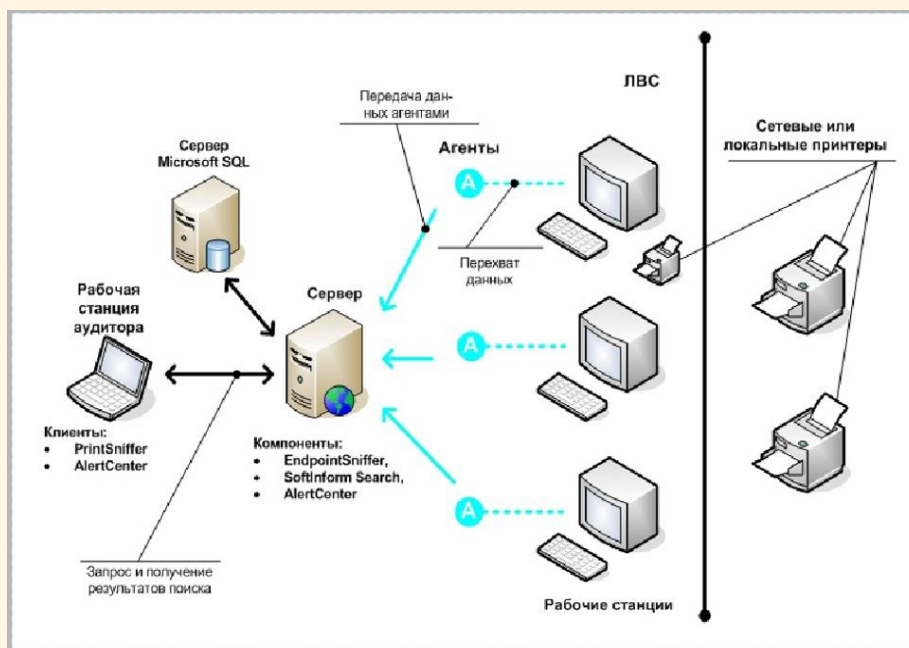
SearchInformEndpointSniffer-агенты позволяют перехватывать:

- **SearchInformMailSniffer** - всю входящую и исходящую (с возможностью блокировки) электронную почту, как через почтовые клиенты (TheBat), так и с доступом через браузер (GMail, Яндекс.Почта);
- **SearchInformIMSniffer** - сообщения интернет-пейджеров (ICQ, QIP, MSN, JABBER, Mail.ru Агент), а также отслеживать общение в популярных социальных сетях (вКонтакте, Facebook);
- **SearchInformSkypeSniffer**- голосовые и текстовые сообщения, а также файлы, передаваемые через Skype;
- **SearchInformDeviceSniffer** - информацию, записываемую на различные внешние устройства (например, USB-флешки, CD/DVD диски);
- **SearchInformFTPSniffer** - информацию, передаваемую по протоколу FTP;
- **SearchInformPrintSniffer** - содержимое документов, отправленных на печать.

А также контролировать и отслеживать:

- **SearchInformFileSniffer**- операции с файлами, хранящимися на серверах и в общих сетевых папках.
- **SearchInformMonitorSniffer**- информацию, отображаемую на мониторах пользователей.

Алгоритм работы EndpointSniffer



Агенты SearchInform EndpointSniffer производят теневое копирование отправленных на печать документов, переговоров в Skype; информации, записываемой на сменные носители, передаваемой по протоколу FTP и отображаемой на мониторах пользователей; отслеживают операции с файлами и направляют полученные данные на сервер SearchInformEndpointSniffer. Сервер помещает перехваченные данные в базу под управлением СУБД Microsoft SQL Server.

Для быстрого поиска по базе и просмотра документов, база индексируется сервером SoftInformSearch. При помощи планировщика обновлений обеспечивается поддержание индекса в постоянно актуальном состоянии. В случае обнаружения фактов нарушения политик безопасности организации SearchInformAlertCenter незамедлительно высылает ответственному работнику уведомление.

1.2.3. Сервер индексации рабочих станций

Сервер индексации рабочих станций позволяет отслеживать появление конфиденциальной информации на компьютерах пользователей, общедоступных сетевых ресурсах и в других местах, для этого не предназначенных.

1.2.4. NetworkSnifferи EndpointSniffer:

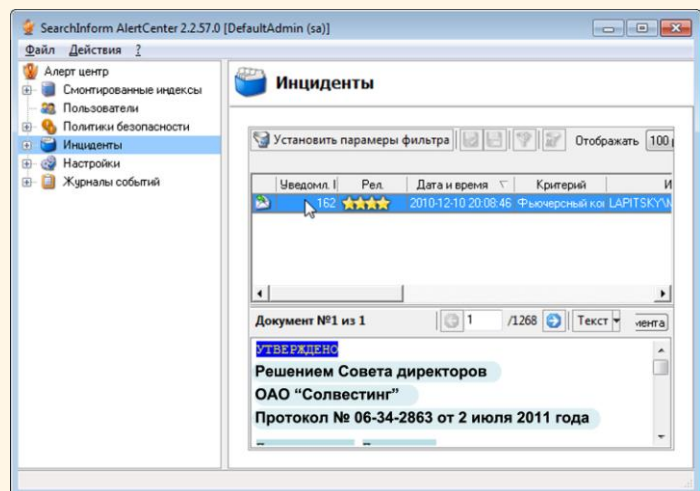
преимущества использования обеих платформ

Для комплексного контроля передаваемых данных целесообразно использовать одновременно и SearchInformNetworkSniffer, и SearchInformEndpointSniffer. 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.

1.2.5. Центр управления

SearchInformAlertCenter

«Мозговой центр» всей системы безопасности. Опрашивает все модули и, при наличии в перехваченной информации определенных ключевых слов, фраз или фрагментов текста, немедленно оповещает об этом офицеров безопасности. Здесь создаются политики информационной безопасности, применяемые к данным, передаваемым через e-mail, ICQ, голосовые и текстовые сообщения скайпа, посты на форумах и в блогах, внешние устройства (USB/CD), в документах, отправляемых на печать.



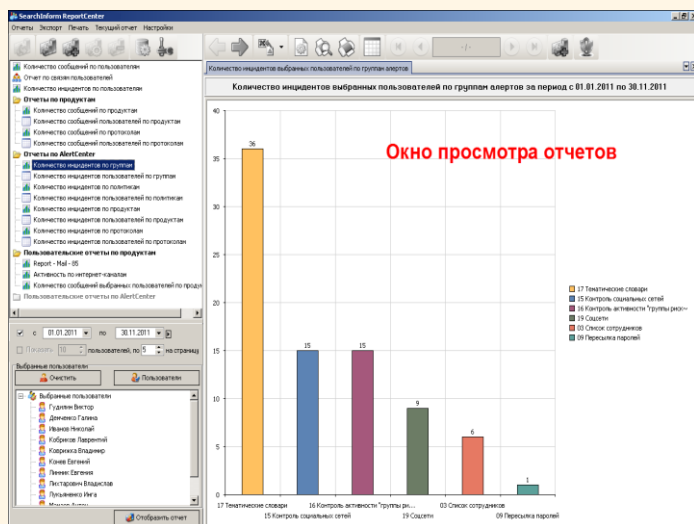
Для идентификации конфиденциальной информации можно использовать методы:

- 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);
- 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 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);
- Использование синонимических рядов;
- Распознавание текста графических документов;
- Поиск документов с умышленно измененным расширением.

SearchInformReportCenter

Позволяет собирать статистику по активности пользователей и инцидентам, связанным с нарушениями политики безопасности, и представлять ее в виде отчетов. Интерфейс программы доступен на двух языках (русский, английский), что позволяет использовать ее в организациях, где есть специалисты по информационной безопасности или руководители, не вла-

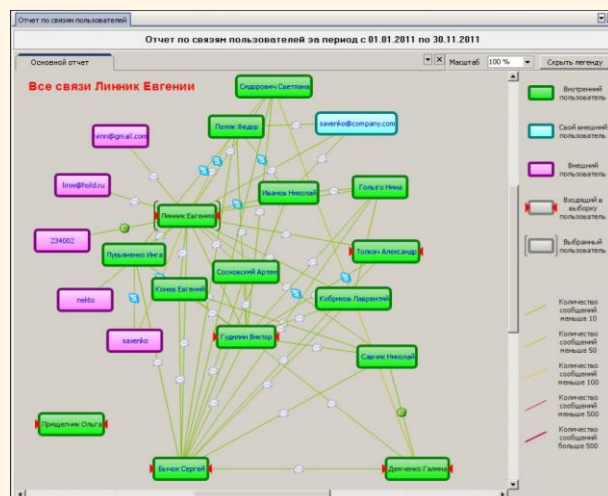


деющие русским языком.

При проведении служебного расследования инцидента можно легко проследить активность пользователя, как с сотрудниками компании, так и с внешними контактами по различным каналам связи - в приложении реализовано схематичное отображение взаимосвязей между контактирующими. Для связей предусмотрена дифференциация по цвету в зависимости от количества переданных сообщений. Также на каждой нити связи отображается иконка информационного канала, по которому было передано сообщение. При наведении курсора мыши на значок продукта, появляется подсказка, которая показывает, какое количество сообщений пользователи отправили друг другу.

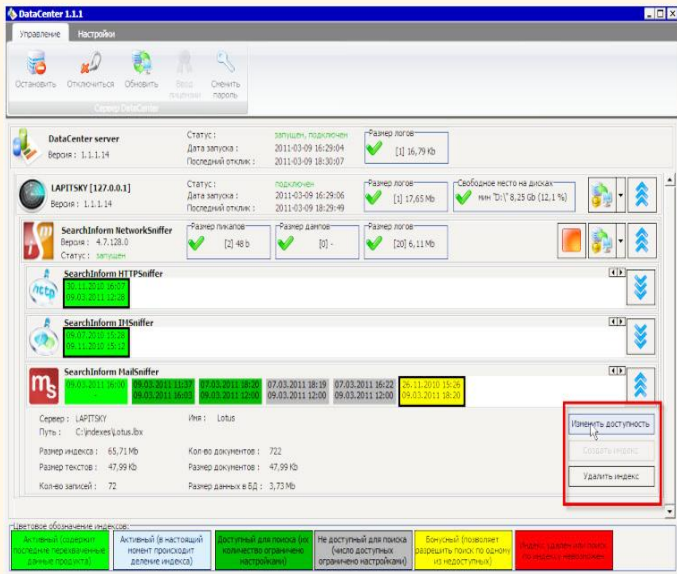
В приложении предусмотрена возможность формирования разнообразных отчетов, позволяющих составить представление о рациональности использования рабочего времени тем или иным пользователем, а также соблюдении им политик безопасности организации:

- «топ» по числу перехваченных файлов и сообщений;
- «топ» пользователей по числу инцидентов;
- распределение инцидентов по группам пользователей и ассоциированным политикам безопасности;
- распределение инцидентов по дням и месяцам.



Каждый из отчетов может формироваться как для всех протоколов передачи данных одновременно, так и для каждого из них в отдельности, что позволит сотрудникам, отвечающим за информационную безопасность, быстрее и точнее анализировать данные о возможных инцидентах.

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



SearchInformDataCenter

Центр управления всеми индексами, созданными компонентами «Контур информационной безопасности SearchInform». SearchInformDataCenter позволяет автоматически разбивать индексы на части для увеличения производительности и задавать правила создания новых индексов за деленный интервал времени для простоты отслеживания данных за необходимые периоды времени.

Также SearchInformDataCenter следит за состоянием работы всех компонентов ра информационной безопасности SearchInform» и отправляет уведомления о неисправностях.

1.3. 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 SearchInform», 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 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.

4. 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.

Основным достоинством метода является высокая скорость работы. К недостаткам можно отнести его неэффективность при внесении в документ значимых изменений и необходимость оперативного создания цифровых отпечатков всех новых документов для возможности их последующего поиска.

5. 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.

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

1.4. Необходимость идентификации сотрудника

Интеграция с доменной системой Windows дает возможность достоверно идентифицировать пользователя, отправившего сообщение по электронной почте, Skype (ниже приведен пример идентификации пользователей Skype), ICQ, MSN, JABBER, оставившего его на форуме или блоге, даже если сотрудник воспользовался для этого почтовым ящиком на бесплатном сервере, подписался чужим именем (никнеймом) или вошел в сеть с чужого компьютера.

№	Тип	Дата/Время	Участни...	Skype пользователи	OS пользователи	Скоб...
11		09.03.2011 9:35:26	2	zorro :58	<unknown> company/savchik	9
12		09.03.2011 14:39:09	2	chilo_pro_5	company/chizik company/iprohor	9
13		17.03.2011 14:37:32	2	space_hero_vrt	company/mamaev company/polyk	8
14		28.02.2011 13:37:20	2	koba7 otto_z	company/kobnikov company/sergeenko	8
15		03.03.2011 14:15:00	2	lulu55 so_so	company/linnik company/savenko	8
16		11.02.2011 13:04:20	2	lulu55 so_so	company/kovtich <unknown>	7
17		02.02.2011 13:48:03	2	lulu shadow	company/lukyan company/stumilin	7
18		13.02.2011 9:46:56	2	vit marinblack	company/polyk <unknown>	6
19		01.02.2011 15:46:56	2	demo slide_on	company/demchenko company/sidorovich	6
20		03.02.2011 10:46:03	2	ivak7 vit	company/ivanov company/polyk	5
21		09.02.2011 13:02:03	2	lulu55 so_so	company/kovtich <unknown>	5
22		07.02.2011 8:26:55	2	chilo so_so	company/chizik company/savenko	5
23		07.02.2011 8:26:55	2	chilo so_so	company/chizik company/savenko	5
24		24.03.2011 12:35:20	2	demo hend_08	company/demchenko company/shilpov	4
25		04.02.2011 11:37:30	2	otto_z lulu55	company/sergeenko company/samohval	4

Оно предпросмотра 0 / 0 Стиль просмотра <HTML>

zorro 09:33:04
Здравствуйте, Николай!

savchik 09:33:20
Здравствуйте!
а вы кто?

zorro 09:33:32
Мы с Вами вчера встречались. Вы мне обещали игру дать поиграть... на флешке

savchik 09:33:44
какую еще игру?
а, да...

zorro 09:34:03
Вы мне ее скачали?
Помните, как мы с Вами договаривались вчера?

Найдено документов: 39 (показано: 39)

Интеграция SkypeSniffer с доменной системой Windows позволяет легко идентифицировать интересующего нас пользователя по его доменному имени в том случае, если сотрудник использует никнейм. Когда имеет место нарушение пользователем либо пользователями политики безопасности организации, мы можем оперативно выявить «подозреваемых», воспользовавшись данными модуля.

1.5. Распознавание ухищрений инсайдеров

Зачастую недобросовестные сотрудники (инсайдеры), пытаясь обмануть службу безопасности, пересохраняют конфиденциальный Word-документ в графическом формате и передают информацию в таком виде, либо запаковывают данные в зашифрованный архив.

«Контур информационной безопасности SearchInform» позволяет осуществлять полноценный контроль:

- распознавать текст в графических файлах и осуществлять поиск по нему;
- обнаруживать передачу зашифрованных архивов по всем каналам возможной утечки информации;
- выявлять пересылку файлов с измененным типом расширения (например, документ, созданный в MS Word, - на графический формат).



1.6. Необходимость перехвата информации с ноутбуков, когда сотрудник работает вне офиса



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 ноутбук снова оказывается в корпоративной сети, все отправленные данные незаметно собираются и передаются для анализа в отдел ИБ.

Поддерживается работа с данными, переданными на печать, отправленными по электронной почте и посредством интернет-мессенджеров, FTP, скайпа.

2. Средства контроля информационных потоков

2.1. Архитектура

Все компоненты системы имеют клиент-серверную структуру. Серверная – это одна из платформ для перехвата данных – SearchInformNetworkSniffer либо SearchInformEndpointSniffer и клиентские приложения, предназначенные для работы с базой перехваченных данных и проведения служебных расследований.

Использование единого поискового аналитического движка позволяет в полной мере использовать все перечисленные поисковые возможности (пункт 1.3.).

2.2. SearchInform MailSniffer

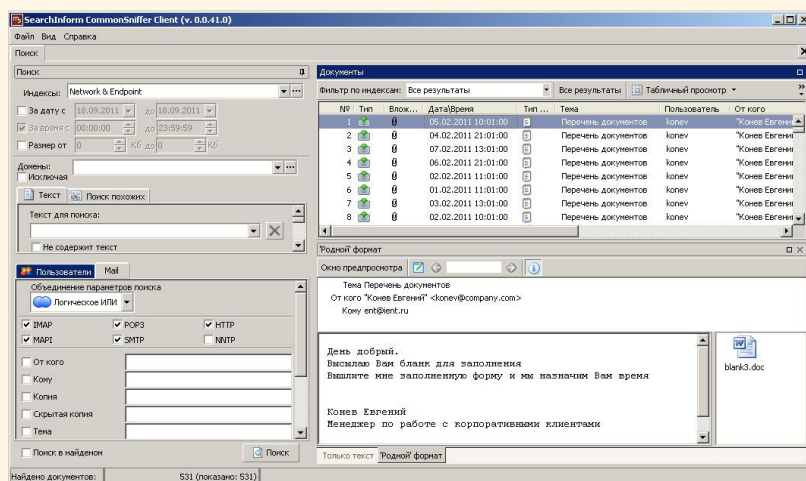
SearchInformMailSniffer предназначен для перехвата почтового трафика на уровне сетевых протоколов, индексирования полученных сообщений и осуществления поиска по ним. Это позволяет отследить утечку конфиденциальной информации.

Для обеспечения информационной безопасности необходимо контролировать передачу электронной почты по следующим протоколам и каналам:

- **SMTP** (исходящая почта через почтовый клиент);
- **POP3** (входящая почта через почтовый клиент);
- **IMAP** (исходящая и входящая почта через почтовый клиент);
- **HTTPs** (исходящая и входящая почта через почтовый клиент);
- **MAPI** (исходящая почта);
- корпоративные почтовые серверы MicrosoftExchangeServer, LotusDomino и другие (средствами интеграции);
- **MSTMG/ISA и прочие прокси-серверы** (средствами интеграции по протоколу ICAP).

Содержимое всех перехваченных писем (включая присоединенные файлы) индексируется и помещается в хранилище. Создается своеобразный архив всей почтовой базы предприятия. И даже 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 SearchInformMailSniffer'ом, будут являться своеобразной резервной копией всей почтовой базы предприятия.

Для просмотра подозрительных документов используется клиентское приложение SIClient.



С помощью клиента можно просмотреть историю почтовых сообщений, переданных пользователями, и сделать срез по дате и активности пользователей.

2.3. SearchInform IMSniffer

Программа SearchInform IMSniffer предназначена для перехвата сообщений различных популярных IM-клиентов.

Программа сохраняет всю переписку в базу данных, по которой впоследствии можно производить поиск, используя поисковые возможности программы SearchInform (морфология, 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, SearchInformIMSniffer позволяет контролировать ведение переговоров и целесообразность использования рабочего времени.

2.4. SearchInform HTTPSniffer

SearchInformHTTPSniffer 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, социальные сети, службы веб-почты или при помощи браузерных IM-клиентов.

При помощи SearchInformHTTPSniffer можно контролировать работу сотрудников и отслеживать их общение в рабочее время.

2.5. SearchInform SkypeSniffer

Программный комплекс SearchInform SkypeSniffer предназначен для перехвата и анализа трафика Skype - сеансов текстовой и голосовой связи, файлов и SMS-сообщений, переданных по скайпу.

Имея репутацию защищенного от прослушивания сервиса, скайп часто используется недобросовестными сотрудниками для передачи конфиденциальных данных компании за пределы организации. С целью предотвратить все возможные утечки информации по этому каналу связи, некоторые руководители его просто «закрывают», что лишь создает дополнительные трудности для делового общения.

SearchInformSkypeSniffer позволяет контролировать, не запрещая. Программный комплекс перехватывает сеансы голосовой и текстовой связи, SMS-сообщения и файлы, передаваемые при помощи скайпа.

2.6. SearchInform DeviceSniffer

SearchInform DeviceSniffer – программа, которая перехватывает всю информацию, записываемую на устройства через USB порты или на CD/DVD диски. Перехваченная информация помещается в хранилище и становится доступной для быстрого полнотекстового поиска. Таким образом, с использованием SearchInform DeviceSniffer контролируется любая возможность утечки информации через сменные носители.

2.7. SearchInform FTPSniffer

Продукт SearchInform FTPSniffer 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 FTPSniffer производит мониторинг документов, загруженных или переданных по простому FTP-соединению, а также переданных по зашифрованному SSL-соединению.

2.8. SearchInform PrintSniffer

SearchInform PrintSniffer - продукт, предназначенный для контроля содержимого документов, отправленных пользователем на печать как посредством сетевых, так и локальных принтеров. Образы и тексты распечатанных документов помещаются в базу данных и доступны для просмотра и анализа. Продукт позволяет проследить «историю» документов: кто распечатал, когда, какое количество экземпляров. Отслеживая документы, напечатанные на принтере, можно не только предотвращать попытки хищения информации, но также оценить целесообразность использования принтера каждым сотрудником.

2.9. SearchInform MonitorSniffer

SearchInform MonitorSniffer предназначен для перехвата информации, отображаемой на мониторах пользователей.

Принцип работы продукта состоит в периодическом перехвате содержимого пользовательских экранов и сохранении полученных снимков в графическом формате в базе данных под управлением Microsoft SQL Server. Функциональность MonitorSniffer обеспечивает также одновременный просмотр активности экрана одного или нескольких пользователей в режиме реального времени.

Перехват снимков экрана происходит незаметно для пользователя.

2.10. SearchInform FileSniffer и индексация рабочих станций

Продукт SearchInform FileSniffer 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.).

Индексация рабочих станций (ИРС) позволяет отследить появление конфиденциальной информации на компьютерах пользователей и местах, для этого не предназначенных.

Совместное использование SearchInformFileSnifferиИРС позволяет:

1) посредством ИРС провести первичный аудит общедоступных сетевых ресурсов, а также рабочих станций пользователей и выяснить, содержат ли они конфиденциальную информацию;

2) посредством SearchInformFileSnifferконтролировать операции с конфиденциальными данными, находящимися на общедоступных сетевых ресурсах и компьютерах пользователей; станций пользователей, попавших в «группу риска» (например, сотрудника, скопировавшего конфиденциальный документ в отдельный файл и изменившего его тип с текстового на графический).

2.11. Контроль ноутбуков

На сегодняшний день SearchInformEndpointSniffer– единственное решение, позволяющее контролировать деятельность сотрудника, работающего за ноутбуком вне офиса– в командировке или дома. Программа собирает отправленные данные, которые будут переданы для анализа отделу ИБ либо при наличии подключения к Интернет, либо как только ноутбук снова окажется в корпоративной сети.

Поддерживается работа с данными, отправленными через электронную почту (IMAP/MAPI, а через SMTP/POP3 - с шифрованием), HTTPиHTTPS, системы мгновенного обмена сообщениями (ICQ, Jabber, MSN Messenger), FTP, Skype, переданными на печать.

Агент SearchInformEndpointSniffer тщательно скрывает свое присутствие на ноутбуке, и обнаружить его непросто даже квалифицированному специалисту.

3.Преимущества использования продуктов SearchInform

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

- **Простота внедрения.** Программный комплекс «SearchInform» можно проинсталлировать всего за несколько часов. Клиент может обойтись силами своих IT-специалистов. В этой ситуации отпадает необходимость предоставлять внутренние документы компании сотруднику компании-разработчика.
- **Сохранение существующей структуры локальной сети.** Внедрение системы не влияет на функционирование существующих информационных систем внутри компании.
- **Комплексность решения.** Позволяет контролировать все каналы утечки информации, а многокомпонентная структура позволяет выбрать только необходимые модули.
- **Единственное решение, которое позволяет контролировать программу Skype.**
- **Полная интеграция с доменной структурой Windows.**
- **Функция «поиск похожих».** Позволяет собственными силами быстро и гибко настроить систему оповещения, не привлекая для этого сторонних специалистов. При этом для эффективной защиты конфиденциальных данных необходимы минимальные трудозатраты на анализ информационных потоков.
- **Контроль ноутбуков.** SearchInformEndpointSniffer - единственное решение, позволяющее контролировать деятельность сотрудника, работающего за ноутбуком вне офиса – в командировке или дома.
- **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.
- **Срез по активностям сотрудника для оперативной работы.** Отследив факт утечки информации по одному каналу, есть возможность просмотреть все активности пользователя по всем каналам.
- **Создание архива перехваченной информации.** Позволяет восстановить последовательность событий в прошлом.
- **Прозрачность ценовой политики и стоимости финального внедрения.**
- **Бесплатная пробная версия.** Предоставляется на 30 дней для проведения полномасштабного тестирования программ в реальных условиях.

Наши клиенты

Общее число клиентов SearchInform на начало июля 2011 года – более 500, 100 из них доверили защиту конфиденциальных корпоративных данных своей компании «Контур информационной безопасности SearchInform» еще в начале текущего года.

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



Наши координаты

Головной офис (Москва, Россия)

Адрес: Москва,
Потаповский переулок, д. 5, к.1, офис 114

Глава офиса: Дмитрий Рябцев

Телефоны:

+7 (495) 721-84-06 (многоканальный)

+7 (495) 664-22-24, +7 (499) 703-04-57

E-mail:

По общим вопросам - info@searchinform.ru

Контакт для прессы –

t.zakharchenko@searchinform.ru

Офис в Новосибирске

Адрес: Новосибирск,
ул. Владимировская, 2/1, офис 204

Глава офиса: Сергей Ананич

Телефон:

+7 (383) 248-90-14

E-mail: s.ananich@searchinform.ru

Офис в Екатеринбурге

Адрес: Екатеринбург, ул. Волгоградская,
193, офис 708

Глава офиса: Дмитрий Стельченко

Телефоны:

+7 (343) 344-50-88, +7 (343) 344-51-38

E-mail: d.stelchenko@searchinform.ru

Офис в Казани

Глава офиса: Владимир Велич

Телефоны:

+7 (843) 212-43-12

+7 (843) 212-43-13

+7 (495) 721-84-06, доб. 112, 126

+7(927)710-22-77

E-mail: v.velich@searchinform.ru

Офис в Санкт-Петербурге

Глава офиса: Евгений Юдов

Телефоны:

+7 (495) 721-84-06, доб. 119

E-mail: e.judov@searchinform.ru

Представительство в Беларуси

Глава офиса: Александр Барановский

Телефон: +375-29-649-77-79

E-mail: ab@searchinform.ru

Представительство в Украине

Адрес: Киев,

ул. Артема, д. 14а, кв. 72

Глава офиса: Николай Луцкевич

Телефоны:

+38-096-505-58-18, +38-044-592-86-03

E-mail: lutskevich@searchinform.ru

Представительство в Латвии

Главы офиса: Виктор Самардакс,
Сергей Найден

Телефоны: +371 67270400,

+371 22086372 (моб.),

+371 67295061 (факс)

E-mail: latvia@searchinform.com

Наши партнеры в Барнауле

«Комплексные системы безопасности»

Адрес: 656049, Алтайский край,

г.Барнаул, пр. Социалистический, 85

Телефоны:

(3852) 36-99-04, 36-99-45,

8-800-200-4488

Отдел по работе с партнерами

Начальник отдела: Галина Сытник

Телефон: +7 (495) 721-84-06

E-mail: g.sytnik@searchinform.ru