

Это ваша власть  
над информацией



## SearchInform MailSniffer

перехват почтового трафика на уровне сетевых протоколов

### Проблема

Утечка информации в глобальную сеть Интернет посредством электронных писем, является на сегодняшний день, наименее контролируемой областью. 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, становится очень сложно.

### Решение

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

### Основные возможности

#### Поисковые возможности

По всем отосланным и принятым сообщениям MailSniffer может проводить полнотекстовый поиск:

- поиск по словам с учетом морфологии и синонимов
- поиск по фразам с учетом порядка слов и расстояния между ними
- поиск регулярных выражений

#### Запатентованная технология «Поиск похожих»

В качестве поискового запроса используется фрагмент текста. Содержимое сообщений, по которым ведется поиск, анализируется и в поисковой выдаче найденные сообщения выстраиваются в релевантном порядке с указанием процента схожести.

#### Архив всей почтовой базы предприятия

Содержимое всех перехваченных писем (включая не только тело письма и атрибуты, но и присоединенные файлы) индексируется и помещается в хранилище, создаётся своеобразный архив всей почтовой базы предприятия. И даже если корпоративный почтовый сервер выйдет из строя, что несомненно является неприятным происшествием, влекущим огромные временные затраты на восстановление, то данные перехваченные MailSniffer'ом будут являться своеобразным бэкапом всей почтовой базы предприятия.

## Функция «История переписки»

Позволяет посмотреть всю переписку сотрудника с адресатом. Отображаться будут все письма, которые были отправлены на указанный адрес и полученные с него. Вся переписка будет показана в хронологическом порядке.

## Масштабируемость

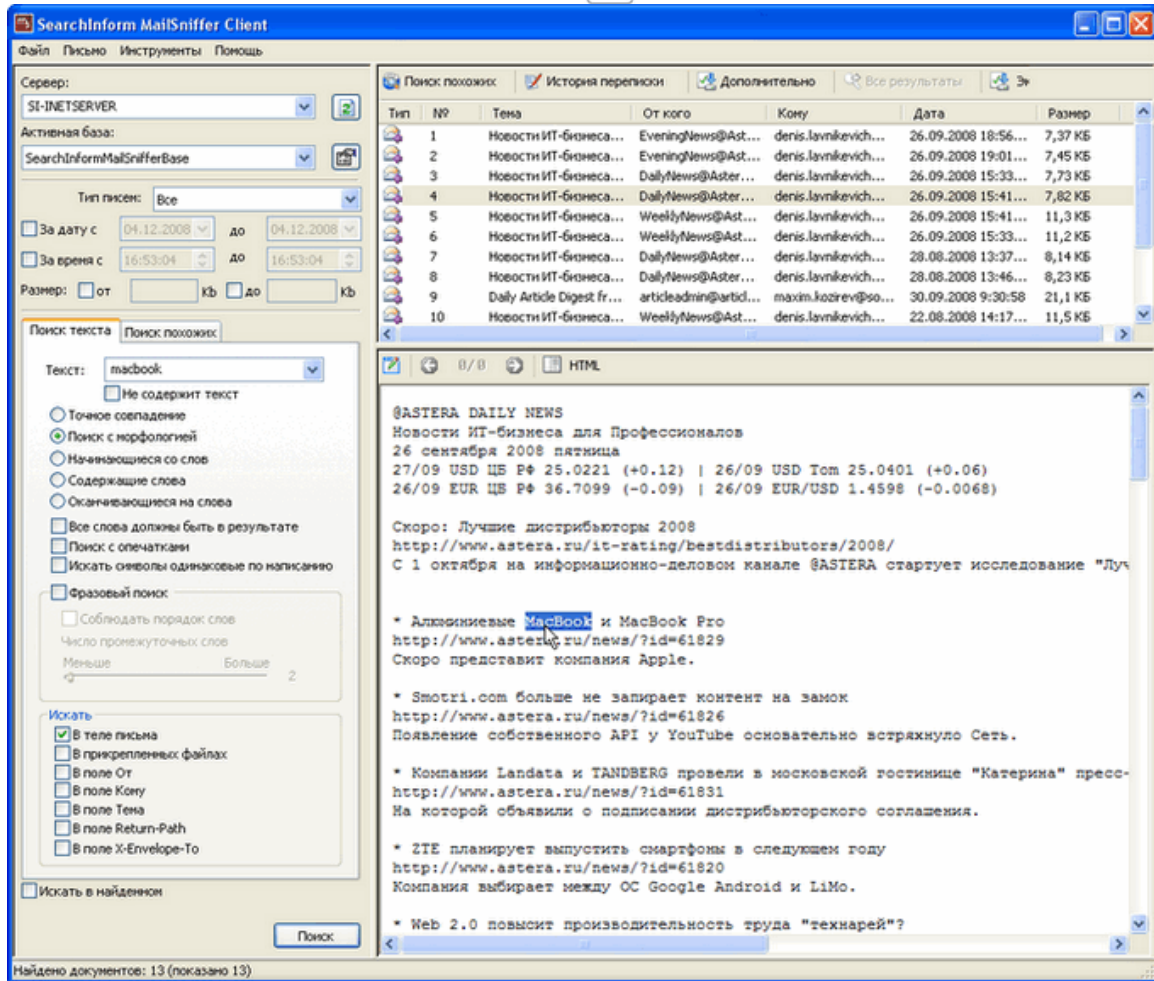
Возможность работы с большими объемами данных и трафика.

## Алгоритм работы



- Все сообщения, которые посылаются или принимаются с рабочих станций, перехватываются зеркалируемым свитчем и отправляются в NetworkSniffer Server (платформа для перехвата почтового трафика и сообщений IM-клиентов (ICQ, MSN, QIP), которая работает с различными сетевыми протоколами (POP3, SMTP, ICQ, MSN)).
- Далее информация передается в базу данных SQL, а затем в SearchInform Server.
- Перехваченные документы индексируются при помощи SearchInform Server. Индекс – особая структура, необходимая для быстрого поиска по перехваченным документам.
- При помощи приложения AlertCenter, созданный индекс опрашивается по списку заданных ключевых слов, выражений и фрагментов текста. Расписание проверок и список запросов настраиваются работниками службы безопасности организации.
- В случае обнаружения совпадений, AlertCenter незамедлительно высылает ответственному работнику уведомление.
- Для полноценного просмотра подозрительных документов, необходимо клиентское приложение MailSniffer.

Это ваша власть  
над информацией



## Системные требования

| Минимальные:          |                        | Рекомендованные:      |                        |
|-----------------------|------------------------|-----------------------|------------------------|
| Процессор:            | 2 GHz                  | Процессор:            | 3,2 GHz                |
| Оперативная память:   | 1,0 Gb                 | Оперативная память:   | 4,0 Gb                 |
| Винчестер:            | 1 Gb и более           | Винчестер:            | 5 Gb и более           |
| Сетевая карта:        | 100 Mbit               | Сетевая карта:        | 1 Gbit                 |
| Операционная система: | Windows 2000, XP, 2003 | Операционная система: | Windows 2000, XP, 2003 |