SearchInform

Информационная Безопасность в Банковской сфере

Информационная безопасность банка

Утечки из банка конфиденциальной информации способны не только ослабить его позиции в конкурентной борьбе, но и существенно ухудшить отношение к этому банку со стороны клиентов и государственных структур. В этом плане наиболее опасной оказывается утечка данных о клиентах (как частных, так и корпоративных) и/или о проводимых ими финансовых операциях

Специалисты по банковской безопасности особо выделяют следующий перечень угроз информационной безопасности (утечек)

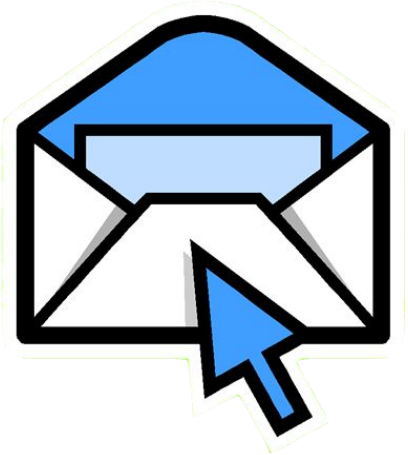
Утечки информации

- Утечка кадров к конкурентам. Уходящие специалисты обычно уносят с собой разного рода конфиденциальную информацию.
- Утечка информации по корпоративным клиентам. Обычно с крупными корпоративными клиентами банки работают индивидуально – на особых условиях.

Утечки информации

- Утечка информации о проводимых банковских транзакциях – кто, куда и какие суммы переводит. Практически всегда обнародованный факт такой утечки приводит к фатальному оттоку клиентов и подрыву доверия к банку. В таких ситуациях особенно важно следить за персоналом.

Утечки информации

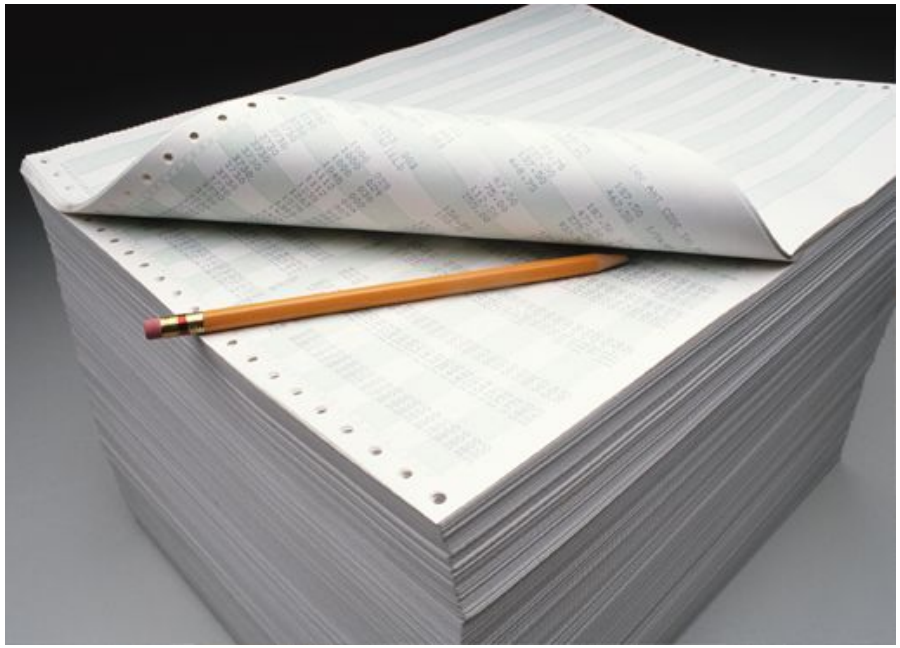


- Очень много информации конкурентам и просто недоброжелателям может дать внутренняя служебная переписка – обсуждение проблем в коллективе, чьих-то ошибок и т.д. Обычно она ведется во внутреннем чате или с использованием программ типа ICQ. При этом доступ к секретной информации могут получать сотрудники, изначально такого доступа не имевшие.

Утечки информации

- Утечки в средства массовой информации.

Утечки информации



- Утечка информации о разрабатываемых маркетинговых программах, инновациях в этой сфере.

- Утечка информации об инвестиционных планах банка. Способна привести к срыву важных и потенциально очень доходных проектов.

Утечки информации

- Утечка информации о системе безопасности банка. Открывает широкие возможности для деятельности криминальных структур.

Утечки информации

- Утечки информации о перемещениях наличных денег (включая выдаваемые наличными кредиты). Следствием может стать банальное ограбление инкассаторов или клиентов.

Стандарт Банка России

С целью дальнейшего предотвращения подобных инцидентов был принят и введен в действие распоряжением Банка России стандарт об «Обеспечении информационной безопасности организаций банковской системы Российской Федерации»

Один из его ключевых постулатов – чтобы положения приведенных в нем документов носили не рекомендательный, а обязательный характер.

Далее предлагаем Вам ознакомиться с некоторыми рекомендациями Банка России, который могут быть в полной мере соблюдены с помощью программных продуктов «SearchInform»

Вот цитаты из рекомендаций с примерами используемых продуктов:

Цитата

3.15. мониторинг информационной безопасности организации банковской системы Российской Федерации (мониторинг ИБ): постоянное наблюдение за событиями ИБ, сбор, анализ и обобщение результатов наблюдения.

3.16. аудит информационной безопасности организации банковской системы Российской Федерации: периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в организациях банковской системы РФ установленных требований по обеспечению информационной безопасности.

5.2. При осуществлении менеджмента документов по обеспечению ИБ рекомендуется … обеспечить выявление документов, созданных вне организации.

Для сбора, обобщения, анализа и контроля за обращением внутренней банковской информации оптимально подходит программный комплекс **SearchInform** – система полнотекстового поиска, ориентированная на корпоративных клиентов. Основное ее преимущество перед конкурентами – запатентованная функция поиска документов, похожих по содержанию на текст запроса. При таком поиске, после обработки запроса, в результатах поиска выводятся документы, максимально похожие на заданный фрагмент текста.

Цитата

5.4. Наибольшими возможностями для нанесения ущерба организации банковской системы обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является нецелевое использование предоставленного контроля над информационными активами, а также сокрытие следов своей деятельности. Внешний злоумышленник скорее да, чем нет, может иметь сообщника(ов) внутри организации.

8.2.6.4. Электронная почта должна архивироваться. Архив должен быть доступен только подразделению (лицу) в организации, ответственному за обеспечение ИБ. Изменения в архиве не допускаются. Доступ к информации архива должен быть ограничен.

SearchInform

Контур информационной безопасности

«Контур информационной безопасности SearchInform» позволяет отслеживать утечки конфиденциальной информации через e-mail, ICQ, Skype, внешние устройства (USB/CD), документы отправляемые на печать и выявлять её появление на компьютерах пользователей.

Контур информационной безопасности

В состав «Контура информационной безопасности SearchInform» входит ряд программ, позволяющих в сжатый период времени составить однозначное, а главное – объективное и подтвержденное документально представление о неформальных информационных потоках внутри банка:

Индексация рабочих станций

SearchInform Server позволяет проиндексировать всю доступную информацию со всех компьютеров в локальной сети предприятия. Администратор может выбрать как любой диск, так и любой компьютер в сети для последующей индексации.

Отслеживание e-mail трафика

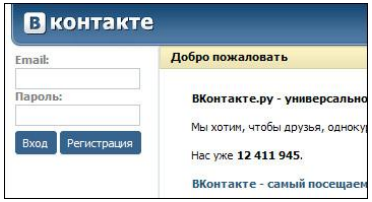
MailSniffer предназначен для перехвата трафика на уровне сетевых протоколов (POP3, SMPT, IMAP, MAPI), индексирования полученных сообщений и осуществления полнотекстового поиска по письмам и вложенным файлам. Это позволяет отследить утечку конфиденциальной информации, создать почтовый архив всей e-mail переписки, и даже при удалении письма из почтового клиента (по неосторожности или намеренно), вся информация, содержащаяся в нем, все равно останется доступна для последующего поиска.

Отслеживание e-mail трафика

MailSniffer способен перехватывать почтовый трафик, который передается через браузер по HTTP протоколу. **MailSniffer** перехватывает письма отправленные через: google.com, rambler.ru, mail.ru, yandex.ru, tut.by, e-mail.ru, open.by, yahoo.com итд. Вся информация сохраняется в базе данных, по которой в последствие можно производить поиск, используя поисковые возможности программы SearchInform.

Отслеживание HTTP трафика

HTTPSniffer способен перехватывать трафик, передаваемый через браузер по HTTP протоколу. **HTTPSniffer** перехватывает сообщения, размещенные в различных блогах, форумах, социальных сетях.



SearchInform

Перехват сообщений интернет-пейджеров

IMSniffer предназначен для перехвата сообщений различных популярных IM клиентов. Программа сохраняет всю переписку в базу данных, по которой в последствие 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 определенной период времени.

Перехват Skype

SkypeSniffer предназначен для контроля сообщений Skype. Программа перехватывает голосовые переговоры, конференции, чаты, sms и передаваемые файлы. Вся информация сохраняется в базе данных, по которой в последствие 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 определенной период времени.

Перехват информации на внешних устройствах

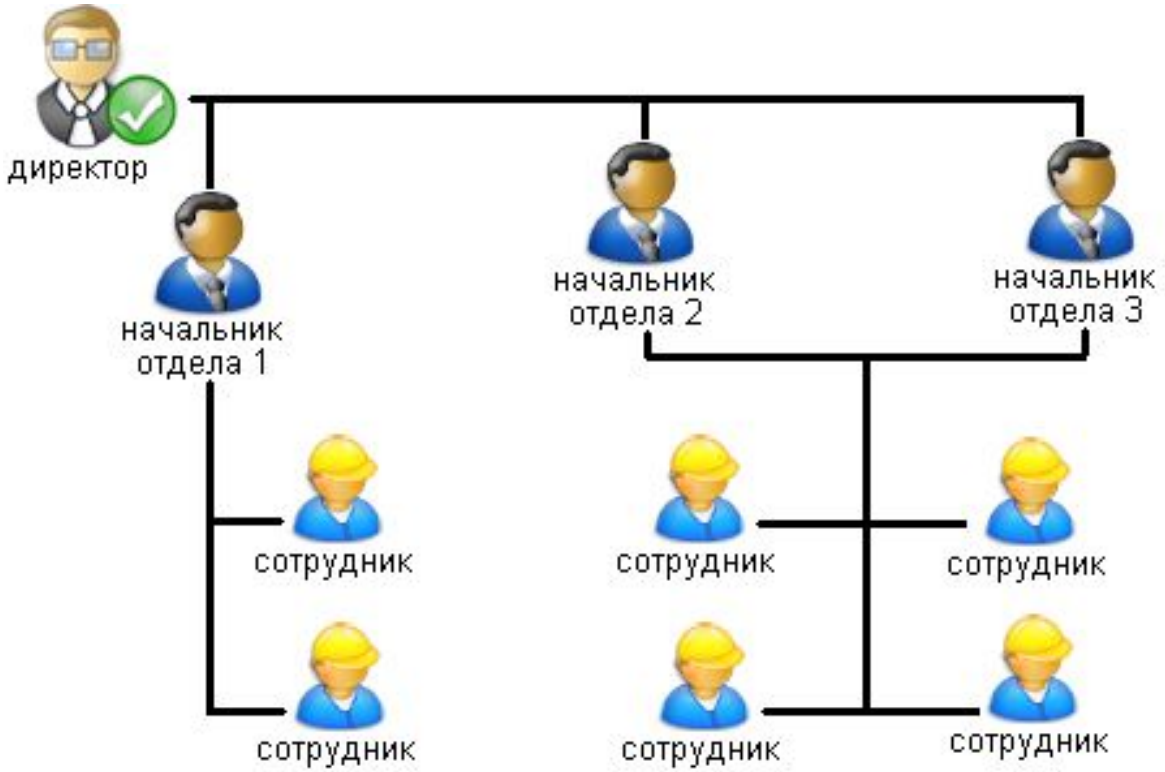
DeviceSniffer – программа, которая перехватывает информацию, записываемую на устройства через порты USB или, например, на CD/DVD диски. После этого информация становится доступной для полнотекстового поиска, а также для уникального «поиска похожих». Таким образом предотвращается возможность утечки информации через сменные носители.

SearchInform

Перехват информации выводимой на печать

PrintSniffer – программа, которая контролирует содержимое документов, отправленных на печать. Все данные перехватываются, содержимое файлов индексируется и хранится в базе заданный промежуток времени. Отслеживая документы, напечатанные на принтере, можно не только предотвращать попытки хищения информации, но также оценить целесообразность использования принтера каждым сотрудником.

Разграничение прав доступа



Важный момент: каждый из компонентов контура информационной безопасности банка согласуется с единой системой разграничения прав доступа. Система обладает рядом гибких настроек и позволяет любым образом выстроить иерархию доступа к конфиденциальной информации, как то и предусматривается рекомендациями Банка России.

Цитата

9.7.1. Для реализации задач развертывания и эксплуатации СМИБ организации рекомендуется иметь в своем составе (самостоятельную или в составе службы безопасности) службу ИБ (уполномоченное лицо). Службу ИБ рекомендуется наделить следующими полномочиями:

- контролировать пользователей, в первую очередь пользователей, имеющих максимальные полномочия;
- контролировать активность, связанную с доступом и использованием средств антивирусной защиты, а также связанную с применением других средств обеспечения ИБ;
- осуществлять мониторинг событий, связанных с ИБ;
- расследовать события, связанные с нарушениями ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, осуществивших противоправные действия, например, нарушивших требования инструкций, руководств и т.п. по обеспечению ИБ организации;

DataCenter

DataCenter – это центр управления всеми индексами, созданными компонентами контура информационной безопасности.

DataCenter позволяет:

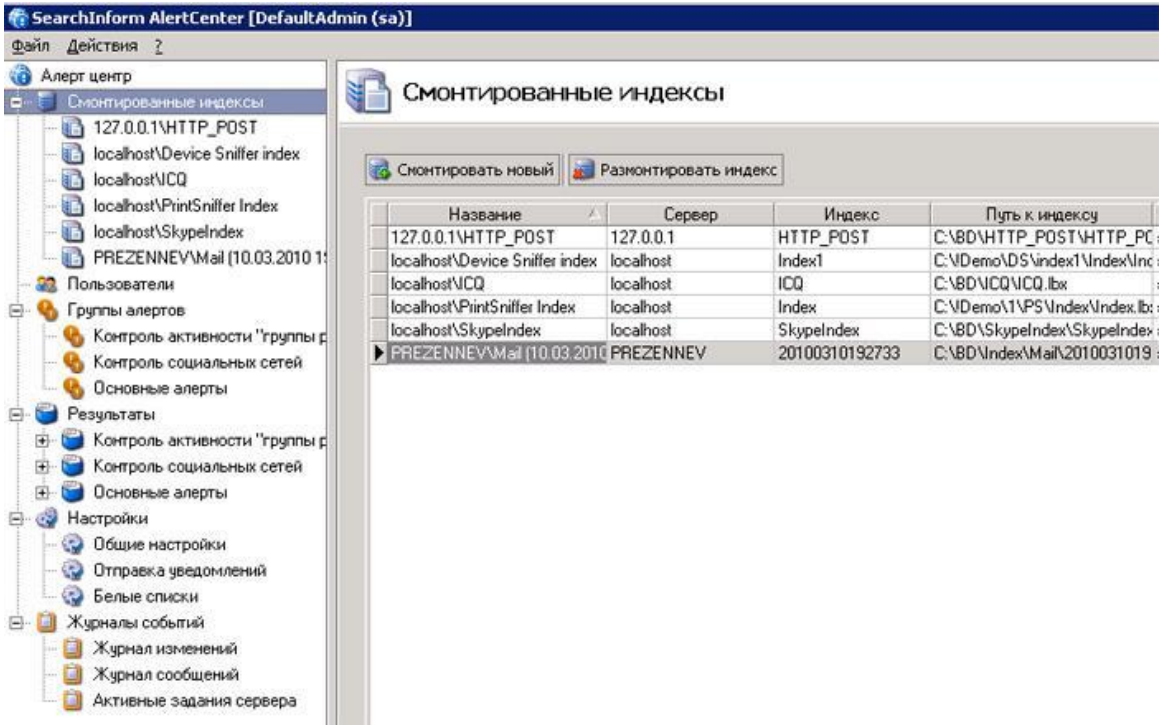
- Разбивать индексы на части, увеличивая производительность поиска информации.
- Задавать определенные параметры (размер, количество документов, время) при достижении которых автоматически создаются новые индексы.
- Следить за состоянием работы всех компонентов контура информационной безопасности и отсылать уведомление на e-mail о каких либо неисправностях.

Центр оповещения

AlertCenter является звеном, связывающим между собой все компоненты в единый контур информационной безопасности компании.
AlertCenter опрашивает все компоненты и, при наличии определённых ключевых слов, фраз или даже фрагментов текста в перехваченной любой из программ информации, немедленно даёт об этом знать лицу, ответственному за информационную безопасность.

Приложение включает в себя консоль сервера и клиент AlertCenter, что позволяет разграничить доступ к оповещениям и настройкам между ответственными за информационную безопасность сотрудниками.

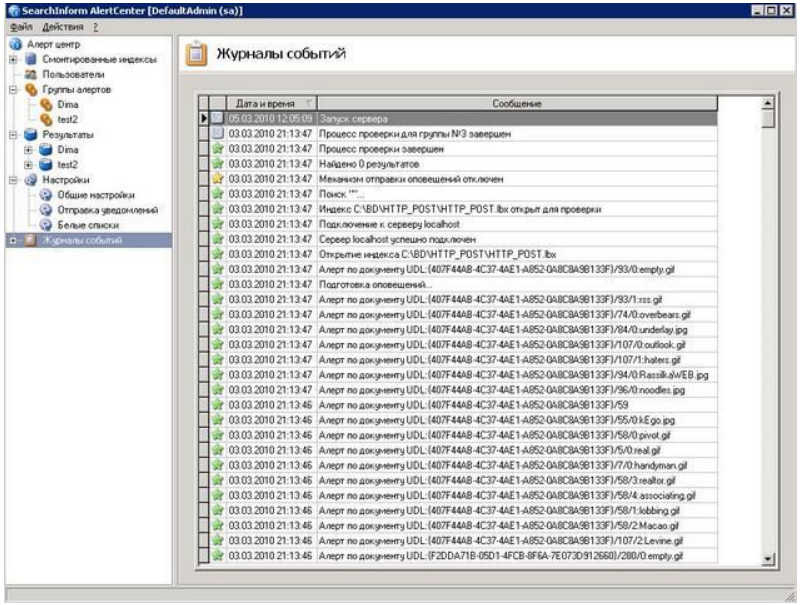
Центр оповещения



AlertCenter является самостоятельным приложением, которое можно подключить к любому индексу, созданному с помощью продуктов «SearchInform», и с заданной периодичностью проверять поисковый индекс на наличие определённых пользователем ключевых слов.

Центр оповещения

Открытие документов, по которым сработали уведомления, в клиентах приложений «Контура информационной безопасности SearchInform» и в сопоставленных приложениях позволит специалистам по безопасности быстро изучать подробности, касающиеся каждого инцидента. «Белый список» пользователей позволит исключить предупреждения для событий, заведомо не ведущих к утечкам информации.



Ведение журнала событий и журнала результатов позволяет оценить эффективность борьбы с утечками информации и работу отдела информационной безопасности.

Итоги

Программные продукты «SearchInform» успешно решают поставленные задачи в банках и финансовых компаниях, государственных структурах и в крупных промышленных, сырьевых, телекоммуникационных и IT-компаниях России и стран СНГ.

SearchInform

Спасибо за внимание