КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DLP-СИСТЕМА НА 100%

Что такое DLP-система?

Что такое DLP-система и зачем она нужна?

Утечка информации может нанести серьезный вред любой организации.

Каналов утечки информации множество - уследить за всеми одновременно человеку самостоятельно практически невозможно.

DLP-система - это технология предотвращения утечки информации.

Современные DLP-системы способны не только перехватывать информацию, но и автоматически обрабатывать и анализировать ее.

Контроль каналов утечки информации

Основными каналами утечки информации являются:

- съемные носители: флешки, CD/DVD диски, съемные жесткие диски и пр.;
- электронная почта, в том числе личная;
- распечатанные с компьютера документы;
- социальные сети, Skype, ICQ и пр.

Современная система информационной безопасности должна:

- позволять сотруднику использовать все каналы для передачи информации;
- при этом перехватывать и анализировать информационные потоки, идущие по этим каналам.

Информационная безопасность – это контроль всех каналов передачи информации: реализация комплексной политики информационной безопасности невозможна при наличии хотя бы одного неконтролируемого службой безопасности канала потенциальных утечек.

Ключевые возможности DLP-системы

1. Автоматический перехват и обработка информации.

Перехваченная информация бесполезна, пока она не проанализирована!

Читать «по-старинки» все и у всех невозможно.

DLP-система способна к **автоматическому анализу информации** с помощью различных поисковых алгоритмов и **автоматической отработке** заданных политик безопасности.

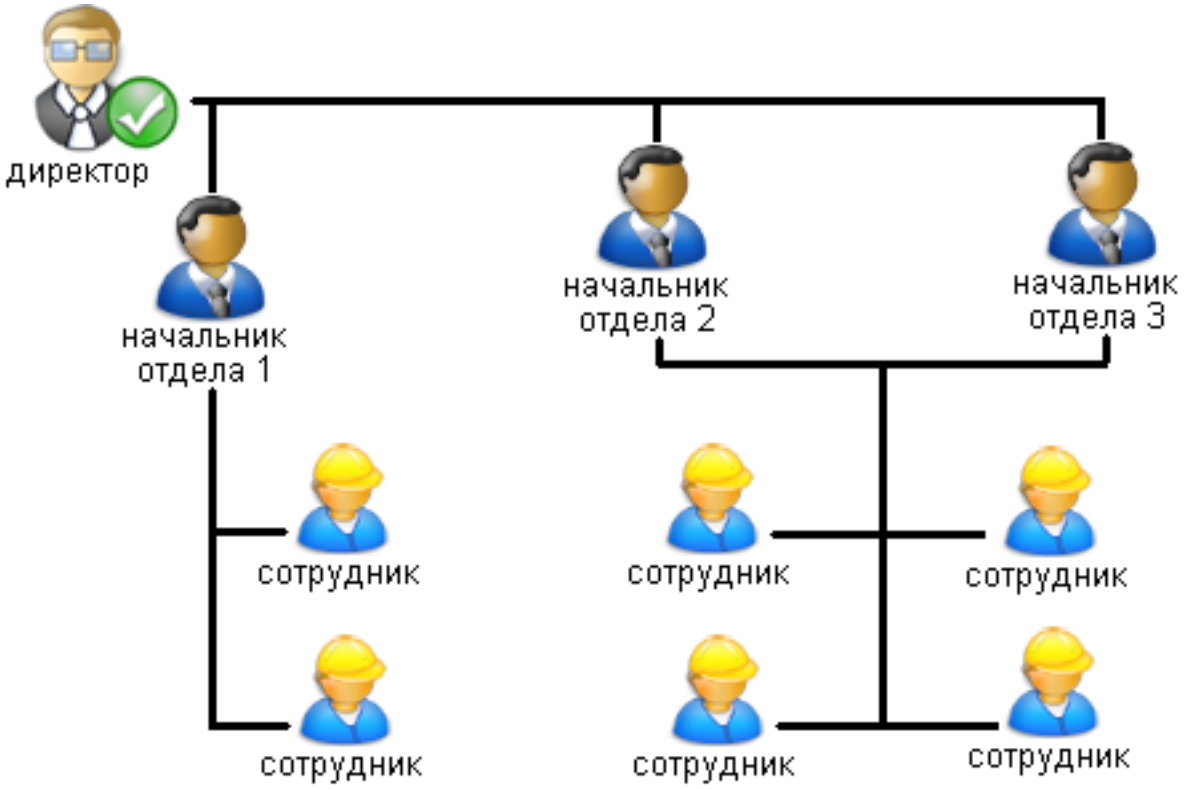
Таким образом, 1 специалист службы безопасности способен контролировать 1000-1500 сотрудников.

2. Интеграция с доменной системой.

Интеграция с доменной системой Windows дает возможность достоверно связать совершенное действие с конкретным компьютером и конкретным пользователем, из-под учетной записи которого оно произошло.

Ключевые возможности DLP-системы

3. Разграничение прав доступа.



DLP-система обладает рядом гибких настроек и позволяет **выстроить иерархию доступа** к конфиденциальной информации любым образом.

Три кита информационной безопасности

1. Предотвращение утечек.

Задача ИБ-системы состоит не только, и не столько, в том, чтобы зафиксировать сам факт утечки, но в предотвращении инцидента на стадии созревания негативного намерения у потенциального инсайдера (инсайдеров).

2. Работа с коллективом.

DLP-система отслеживает настроения в коллективе путем мониторинга сообщений сотрудников в интернет-мессенджерах (Skype, ICQ и т.д.) и соцсетях в рабочее время.

3. Оптимизация работы.

С помощью DLP-системы можно контролировать реакцию коллектива на нововведения и в соответствии с ней эффективно корректировать внутреннюю политику предприятия.

Состав DLP-системы «Контур информационной безопасности»

Архитектура системы

Все компоненты системы имеют **клиент-серверную структуру:**

- **серверная** – это одна из платформ для перехвата данных – **SearchInform NetworkSniffer** либо **SearchInform EndpointSniffer**;
- **клиентские приложения** - предназначены для работы с базой перехваченных данных и проведения служебных расследований.

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

SearchInform NetworkSniffer - платформа для перехвата данных на уровне зеркалируемого трафика, т.е. NetworkSniffer обрабатывает 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) на уровне локальной сети.

Платформа включает в себя следующие продукты:

Архитектура системы

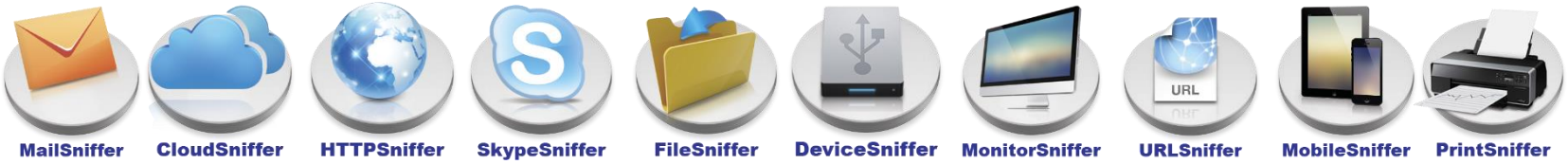
SearchInform EndpointSniffer - платформа для перехвата трафика посредством агентов.

Дополнительно позволяет контролировать сотрудников, находящихся за пределами корпоративной сети - они могут свободно передать конфиденциальные данные с ноутбука третьим лицам.

SearchInform EndpointSniffer собирает отправленные данные и передает их для анализа отделу ИБ, как только лэптоп выходит в Сеть.

Преимущества работы агентов IMSniffer и MailSniffer на платформе SearchInform EndpointSniffer в том, что они обладают повышенной устойчивостью к различным сбоям (даже если сервера станут недоступными, перехват будет осуществляться), способны перехватывать и те данные, которые передаются по защищенным протоколам.

SearchInform EndpointSniffer-агенты:



Элементы Контура информационной безопасности

SearchInform NetworkSniffer позволяет осуществлять перехват информации, передаваемой через интернет. Поддерживаются все распространенные протоколы, которые могут использоваться инсайдерами. Предлагается поддержка прокси-серверов - как программных (Kerio, Squid и т.д.), так и аппаратных (BlueCoat, IronPort и т.д.) - через стандартный протокол ICAP.

MailSniffer

Электронная почта – один из наиболее опасных каналов утечек, так как поддерживается пересылка больших объемов данных. Поддерживаются протоколы SMTP, POP3, MAPI, IMAP.

HTTPSniffer

Возможны утечки информации в социальные сети, блоги, на форумы, а также через Web-приложения для отправки электронной почты и SMS, Web-чаты.

CloudSniffer

Облачные хранилища предназначены для хранения больших объёмов информации. Дополнительную опасность представляет автоматическая синхронизация хранилищ с устройствами работника. Следует контролировать такие сервисы, как: Dropbox, Google Drive, Office 365 и др.

Элементы Контура информационной безопасности

ADSniffer

Контроль и анализ событий журналов Active Directory позволяет выявлять подозрительные действия, которые могут совершаться системным администратором компании. ADSniffer позволяет отслеживать и сохранять в свою базу данных только те события, которые представляют потенциальную угрозу безопасности системы.

PrintSniffer

Этот модуль 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 и избежать перерасхода бумаги и тонера.

FTPSniffer

Этот протокол - важнейшее средство передачи больших объемов данных, и может использоваться недобросовестными сотрудниками для передачи целых баз данных, детализированных чертежей, пакетов отсканированных документов и пр.

Элементы Контура информационной безопасности

SkypeSniffer

Первое решение в области информационной безопасности, обеспечивающее перехват не только голосовых и текстовых сообщений, но и файлов, передаваемых через Skype.

IMSniffer

Перехват служб мгновенного обмена сообщениями.
Поддерживаются протоколы ICQ, MSN, Mail.ru Агент, JABBER, активно используемые офисными работниками.

ViberSniffer

Единственное решение, позволяющее осуществлять полный контроль Viber.
Перехватываются чаты, звонки, отправляемые файлы, контакты.

Элементы Контура информационной безопасности

DeviceSniffer

Программа, выполняющая аудит внешних носителей, подключенных к компьютеру (флэшки, компакт-диски, внешние винчестеры), а также перехват записываемых на них файлов благодаря функции «теневого копирования». Предусмотрена возможность шифрования всей информации, записываемой на внешние носители. С помощью этой программы вы можете избежать утечки больших объемов данных, которые инсайдер переписывает на внешние носители из-за невозможности их передачи по интернету.

MonitorSniffer

Предназначен для снятия снимков и видеозаписи экранов рабочих станций сотрудников и сохранения полученной информации в базе данных. Поддерживается контроль экрана одного или нескольких пользователей в режиме реального времени, можно отслеживать состояние экранов пользователей терминальных серверов, работающих по RDP-соединению (протоколу удаленного рабочего стола).

Элементы Контура информационной безопасности

FileSniffer

Контролирует работу пользователей на общих сетевых ресурсах, которые содержат большие объемы конфиденциальных данных, не предназначенных для распространения за пределами компании. Копируя документы с этих ресурсов, сотрудники могут торговать корпоративными секретами. SearchInform FileSniffer позволяет контролировать все операции с файлами на общедоступных сетевых ресурсах, защищая информацию, находящуюся на них.

Индексация рабочих станций

Позволяет в режиме реального времени отслеживать появление, копирование, перемещение и удаление конфиденциальной информации на рабочих станциях пользователей. Подобный аудит пользовательских компьютеров во всей локальной сети предприятия позволит вовремя обнаружить сотрудника, собирающегося передать закрытые корпоративные документы третьим лицам.

Больше, чем DLP

MicrophoneSniffer

Позволяет при включенном ноутбуке записывать разговоры вокруг или прослушивать их в режиме реального времени.

Видеорежим в MonitorSniffer

Непрерывная запись действий сотрудников за компьютерами. Алгоритмы сжатия позволяют уместить 8 часов непрерывного «кино» всего в 300 мегабайт.

Шифрование информации, записываемой на внешние носители

Если сотрудник потеряет носитель или захочет передать его третьим лицам, данные не будут скомпрометированы.

- В папку с ограниченным доступом зашел кто-то еще. Что он там делал?
- Знаете ли вы, чем занимается ваш системный администратор? Кому создавал/блокировал учетные записи? Кому изменял права?

Вы можете знать гораздо больше!

Совместное использование модулей FileSniffer и ADSniffer обеспечивает наиболее полный контроль над действиями IT-службы.

Дополнительные функции DLP-системы

- ✓ Контроль ноутбуков сотрудников
- ✓ Контроль работы системных администраторов
- ✓ Контроль рабочего времени сотрудников
- ✓ Аудио-, видеоконтроль
- ✓ Контроль связи коллектива с уволенными сотрудниками
- ✓ Контроль нелояльных сотрудников
- ✓ Работа с группой риска

Контроль ноутбуков

DLP-система позволяет полноценно контролировать ноутбуки по всем каналам, даже когда они находятся за пределами корпоративной сети.

Агент EndpointSniffer тщательно скрывает свое присутствие на лэптопе, и обнаружить его непросто даже квалифицированному специалисту. Он собирает отправленные данные, которые будут переданы для анализа отделу ИБ сразу же, как только лэптоп обнаружит соединение с сетью.

Пример из жизни

Одна компания очень удивила своих сотрудников: закупила **150 ноутбуков** и раздала менеджерам высшего и среднего звена. Вскоре корпоративная щедрость окупилась в десятки раз.

Наблюдалась устойчивая тенденция: **в течение трёх месяцев** с момента получения корпоративных ноутбуков сотрудники перестали разделять личное и рабочее пространство. В итоге, и на работе, и дома люди использовали корпоративные машины, что обеспечило приток важной с точки зрения ИБ информации, позволившей вскрыть **несколько крупных мошеннических схем**.

Кто контролирует контролеров?

Проверить добросовестность выполнения обязанностей системных администраторов – сложная задача.

Сделать это незаметно для людей, чья работа напрямую связана с IT, **практически невозможно**. Но оставлять проблему без решения нельзя – системные администраторы и их действия являются основой информационной безопасности компании.

«Золотая середина» в контроле за IT-службой – это своевременное выявление подозрительных действий с их стороны.

- Если сисадмин повышает права учётной записи, а спустя некоторое время возвращает «всё как было» – это повод задуматься.
- Если сисадмин периодически почитывает конфиденциальные корпоративные документы – это повод задуматься всерьёз.
- Кроме того – никто не отменял халатность.

Контроль рабочего времени сотрудников

Наряду с защитой конфиденциальной информации и борьбой с инсайдерством, важной задачей сегодня является выявление неэффективных сотрудников. Иначе говоря, бездельников.

ProgramSniffer – модуль, входящий в «Контур информационной безопасности» – помогает решить задачу выявления неэффективных сотрудников, предоставляя специалисту службы безопасности отчеты о:

- ✓ времени прихода и ухода сотрудника с работы и на работу;
- ✓ времени реальной работы за компьютером;
- ✓ статистику и время использования приложений;
- ✓ времени, проведенном на конкретных сайтах.

Вирус разгильдяйства

Присутствие сотрудника на рабочем месте не гарантирует того, что он будет заниматься своими непосредственными обязанностями.

Типичные **симптомы вируса разгильдяйства** у сотрудника:

- социальные сети;
- развлекательные ресурсы;
- онлайн-игры;
- перекуры;
- лень.

Неэффективное использование рабочего времени наносит компании больший вред, чем кажется на первый взгляд.

Последствия вируса разгильдяйства для бизнеса:

- прямые потери от того, что человек занимается ерундой в рабочее время
- «заражает» всех остальных: если он бездельничает, то почему я должен работать?
- недополученная прибыль

Аудио-, видеоконтроль

Запись звука целесообразна не только «в целях повышения качества обслуживания», но и для выборочного контроля сотрудников, подозревающихся в мошенничестве. «Талантливые» менеджеры по продажам на переговорах могут договориться не только о том, что затем будет записано на бумаге.

Пример из жизни

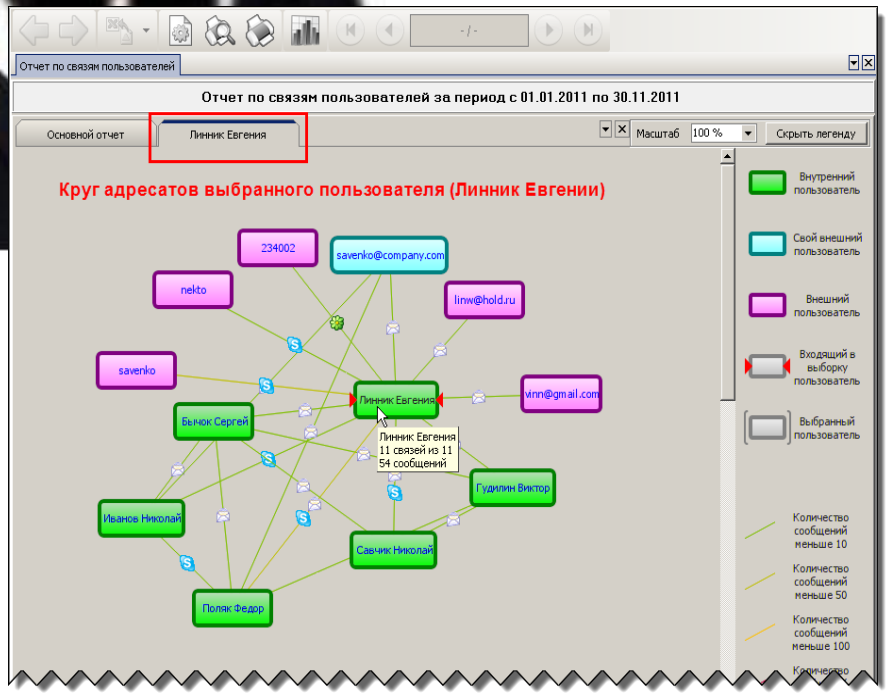
В компании, занимающейся закупками, завелся «умный» менеджер. Отработав некоторое время, девушка собрала «коллекцию» различных коммерческих предложений и разработала мошенническую схему: перед закупкой, вместо того, чтобы «честно» собирать КП партнеров, менеджер договаривалась с какой-либо компанией на откат, а остальные предложения «рисовала» в Photoshop, подставляя заведомо невыгодные цены. Тем самым, создавалась видимость, что «нужное» КП действительно самое выгодное, хотя это было не так.

Нарушительницу удалось установить благодаря просмотру видео, перехваченного с помощью **MonitorSniffer.**

Уволенный / обиженный сотрудник

Общение с бывшими – это прямая угроза переманивания.

Представьте себе: человек уходит в другую компанию, а затем общается с бывшими коллегами, узнавая у них конфиденциальную информацию, рассказывая, как ему хорошо на новом месте и хорошо бы перейти в эту фирму всем отделом.



Важно отслеживать коммуникативные связи между работниками, выявлять неформальных лидеров в коллективе, а также контролировать общение сотрудников с бывшими коллегами.

Нелояльный сотрудник

Посещение сайтов по трудоустройству.

Это действие сотрудники совершают перед тем, как сесть за составление резюме. Сотрудник может ничего не отправлять на сайт, а «просто смотреть». Поэтому отслеживаем даже факт захода. Дополнительно отслеживаем факты отправки резюме.

Нецензурные и негативные слова.

Мат + негативные слова вместе с фамилиями топ менеджмента и названием компании дают пищу для размышлений о лояльности сотрудников.

Группа риска

Такие люди могут стать объектами для манипуляций и шантажа.

Люди в этой группе не являются инсайдерами или нелояльными сотрудниками, но могут стать таковыми при определенных обстоятельствах.

К группе риска относятся люди:

- с зависимостями (алкоголь, наркотики);
- с финансовыми проблемами (долги, кредиты);
- с нетрадиционной сексуальной ориентацией;
- и другие.

К группе риска относится больше людей, чем Вы думаете.

Возможно создать словарь специальных терминов, по которому можно выявлять разговоры или посты определённой тематики.

При правильной работе с группой риска Вы не только не навредите компании, но наоборот, укрепите лояльность сотрудников к ней.

Предотвращение утечки информации

У каждой компании, вне зависимости от сферы ее деятельности, есть свои «секреты», требующие защиты.

Необходимо контролировать движение в корпоративной сети и доступ к документам, содержащим:

- список фамилий;
- список компаний-партнеров;
- товарные позиции.

Ключевые преимущества DLP-системы

Преимущества Контура информационной безопасности

1. Простота и скорость внедрения. Процесс инсталляции занимает всего несколько часов и не влияет на функционирование существующих информационных систем внутри компании.
2. Возможность контроля всех каналов передачи информации, включая Skype, социальные сети, принтеры, а также работу пользователей на файл-серверах.
3. Функция «поиск похожих». Позволяет собственными силами быстро и гибко настроить систему оповещения, не привлекая сторонних специалистов. При этом для эффективной защиты конфиденциальных данных необходимы минимальные трудозатраты на анализ информационных потоков.
4. Полная интеграция с доменной структурой Windows позволяет достоверно идентифицировать пользователя.
5. Расширенные поисковые возможности позволяют эффективно защищать конфиденциальные данные при минимальных трудозатратах на анализ информационных потоков (достаточно 1 «безопасника» для контроля 1000 – 1500 рабочих станций в организации).

Спасибо за внимание

ООО «Нордкомп»
167000, Республика Коми, г. Сыктывкар,
ул. Первомайская, д. 20.

Тел.: +7 (8212) 310-310
E-mail: info@nordcomp.ru
Сайт: www.nordcomp.ru

Приобретая DLP-систему, нужно использовать ее возможности на 100%.