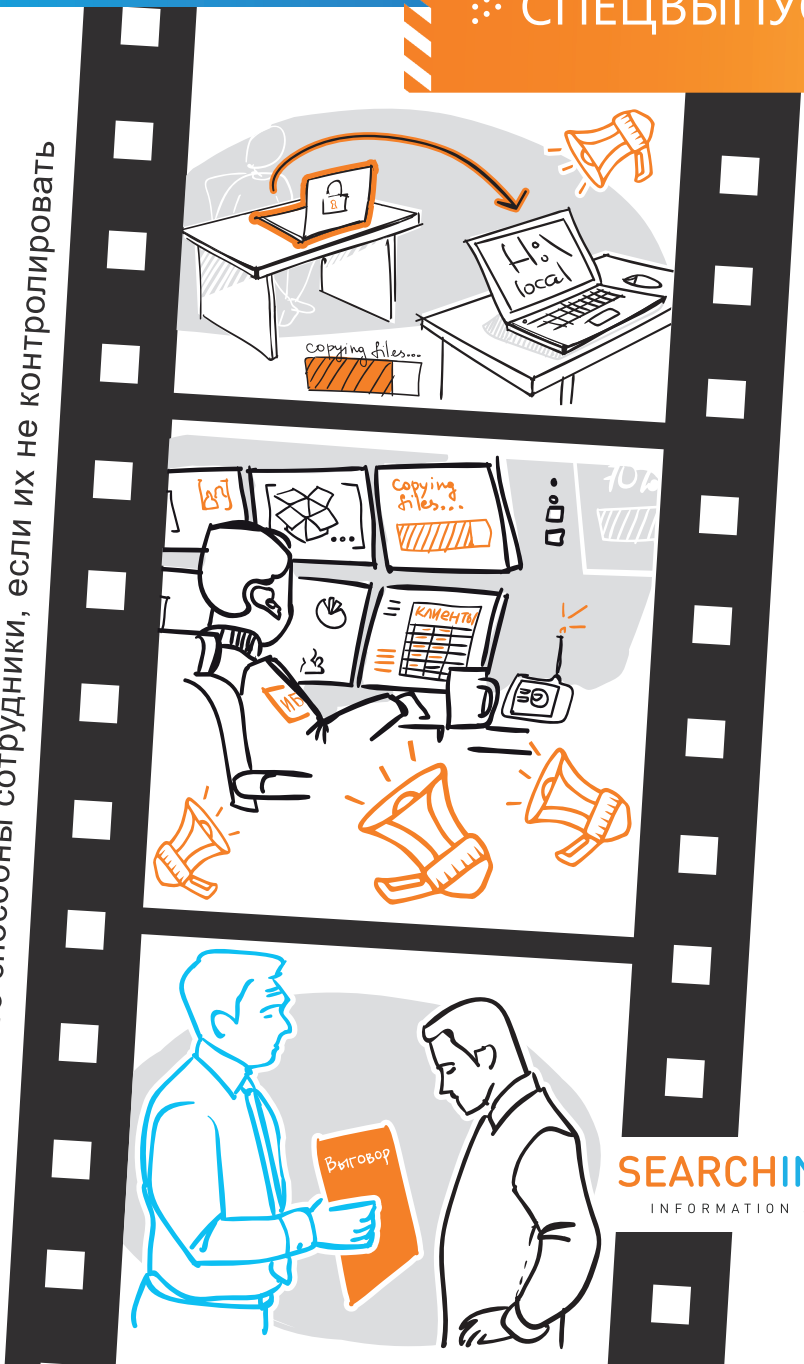
Это не про меня

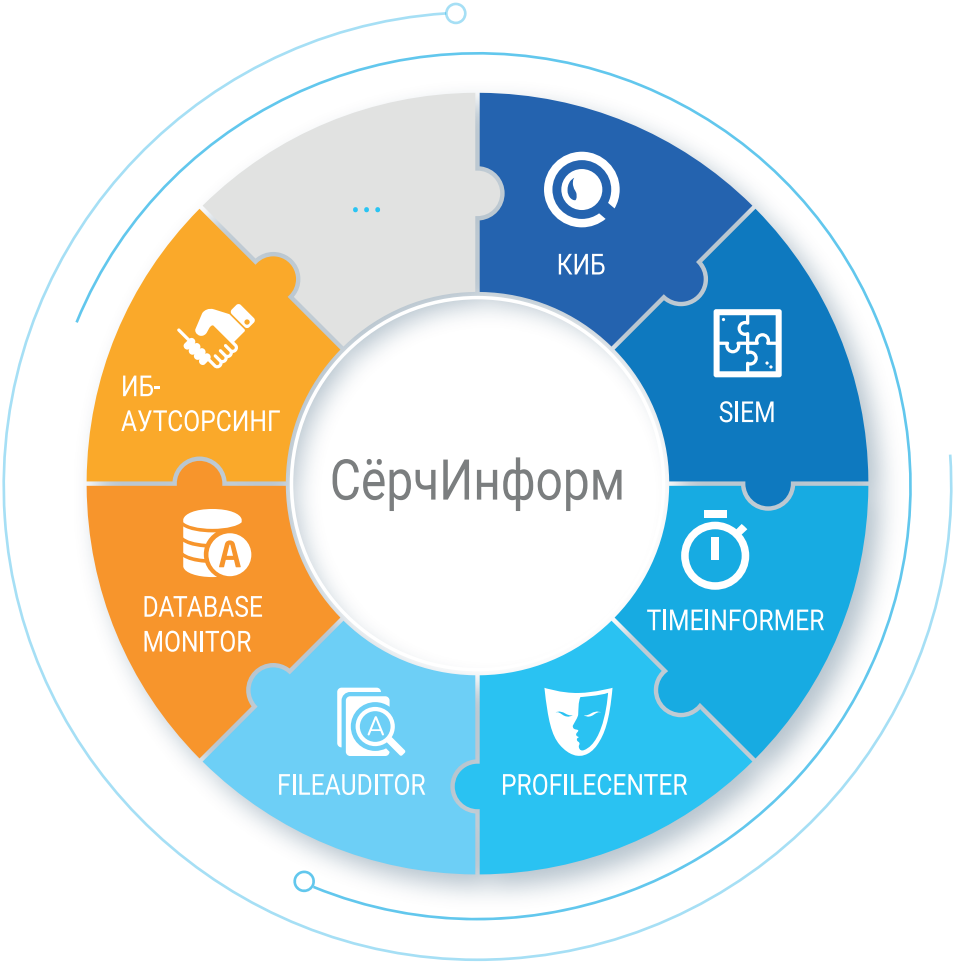
СПЕЦВЫПУСК

На что способны сотрудники, если их не контролировать



SEARCHINFORM
INFORMATION SECURITY

КОМПЛЕКСНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ



Чтобы обнаружить ИБ-угрозы, компаниям нужны мощные инструменты. Продукты «СёрчИнформ» работают в комплексе: контролируют входящий и исходящий трафик, события в IT-инфраструктуре, следят за сохранностью критичной информации на ПК и в БД, наблюдают за действиями сотрудников, оценивают кадровые риски и вовремя сообщают о нарушениях политик безопасности.

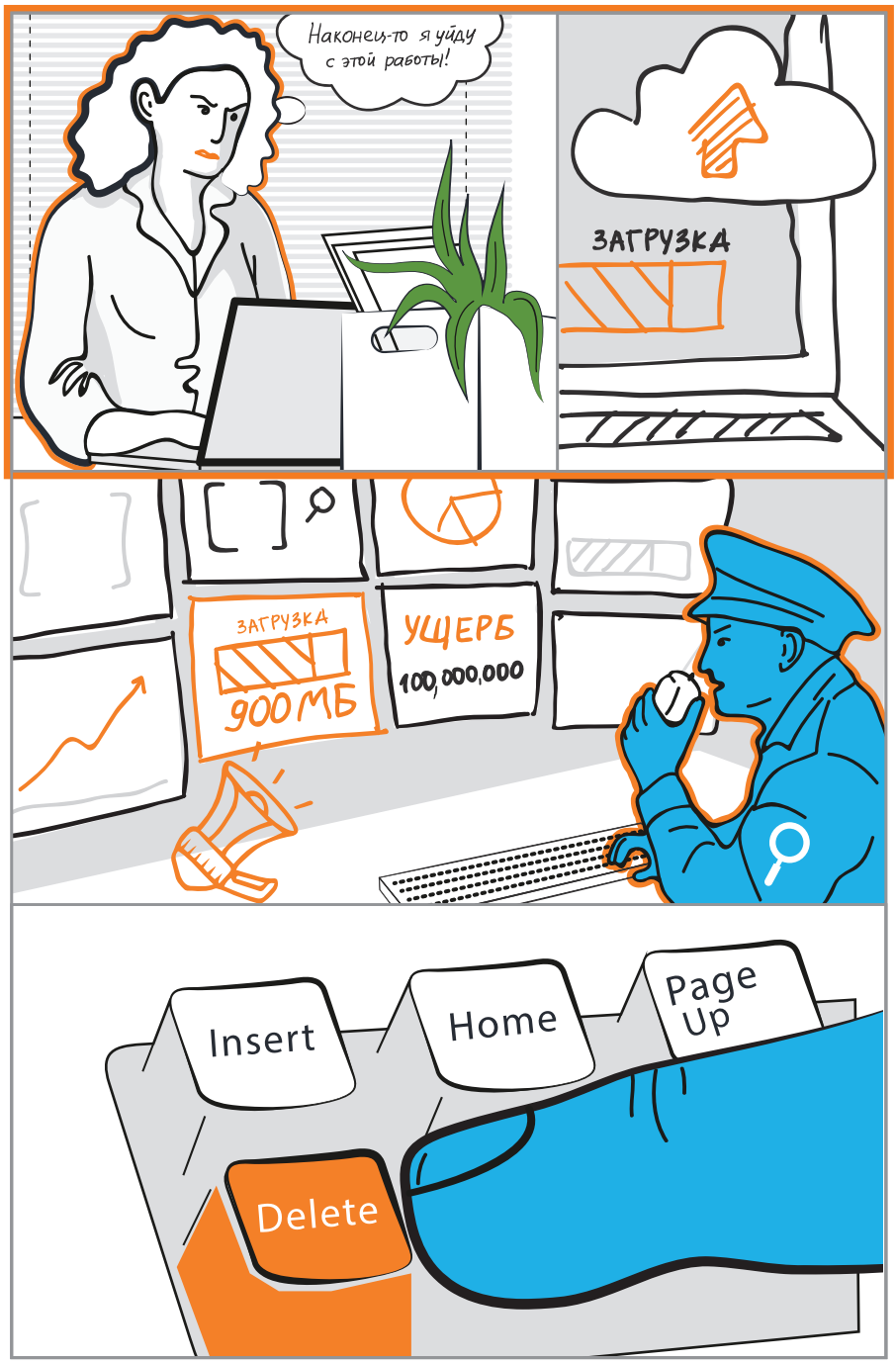
Это не про вас

Пока вы читаете эти строки, где-то в мире крадут или теряют 59 записей данных. Это средняя скорость утечек в секунду.

Вы уверены, что потеря данных не погубит ваш бизнес, но средний убыток от утечек составил 2,5 млн долларов* с учетом коммерческих и репутационных потерь.

Мы собрали реальные истории из практики клиентов, которые доказывают: от утечек и кражи информации, мошенничества и деструктивных действий сотрудников не застрахована ни одна компания.

**По данным международного исследования IBM Security.*


Наконец-то я уйду с этой работы!
ЗАГРУЗКА
ЗАГРУЗКА
900 МБ
УЩЕРБ
100,000,000
Insert
Home
Page Up
Delete

«Сувенир» на память

Сотрудница торгового предприятия, получив отказ в повышении, решила уволиться. Однако перед увольнением загрузила на сторонний ресурс архив объемом около 900 мегабайт.

Анализ архива в DLP показал, что сотрудница украла проекты всех исследований компании по московскому рынку. Итоговая стоимость информации с учетом разработки документации, недополученной прибыли, раскрытия внутренних данных о клиентах и себестоимости продукции составляла около 100 млн рублей.

Благодаря своевременному выявлению инцидента архив был удален со стороннего ресурса.

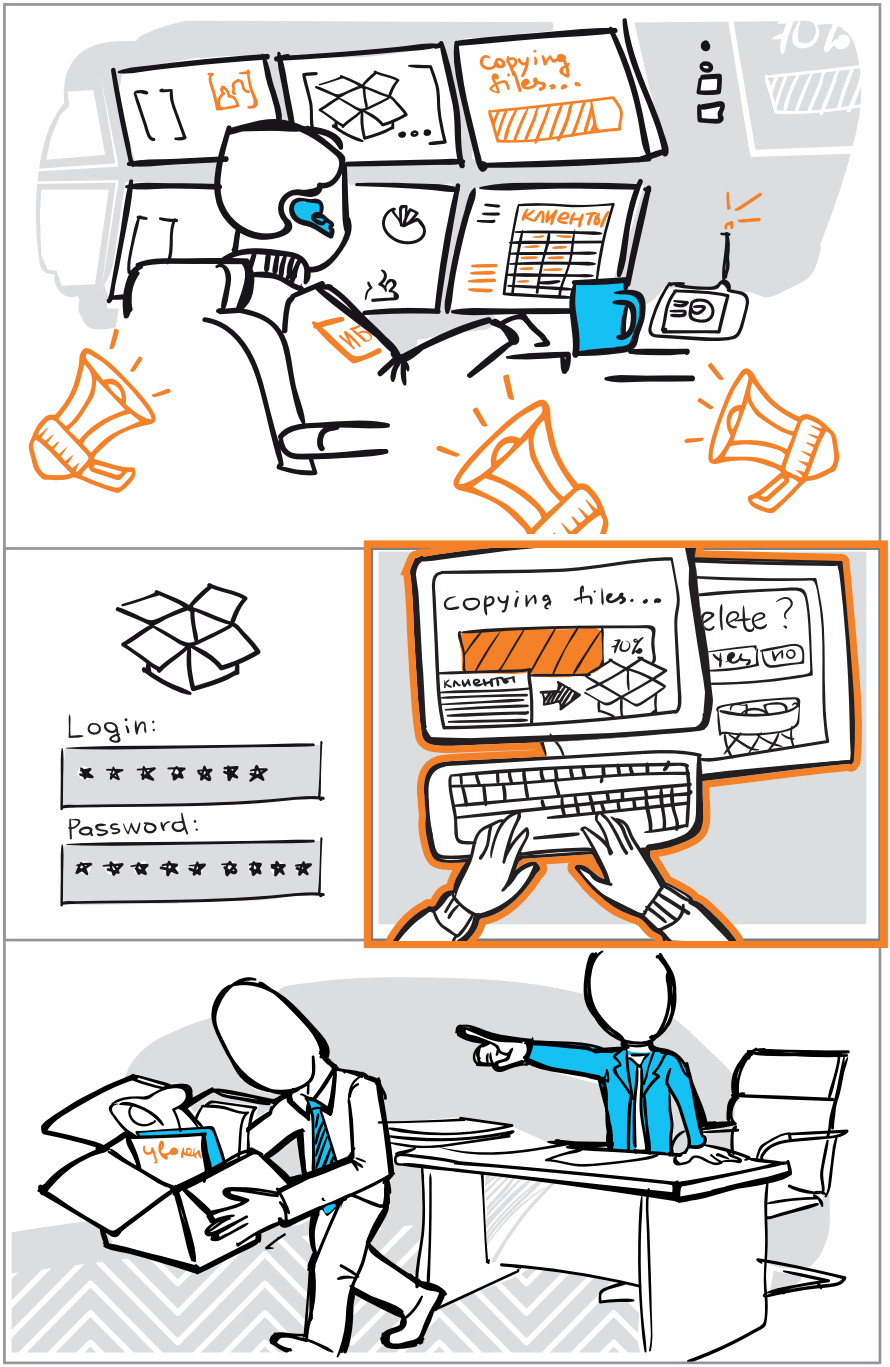
Расследование вскрыло факт подделки бухгалтерской документации. «Обиженная» сотрудница откорректировала финансовую информацию, которая хранилась на файловом сервере. Документы можно было бы восстановить, но своевременное вмешательство сэкономило время и деньги, которые ушли бы на штраф при подаче отчетности в налоговую.

Кроме того, подобный «финт» мог привести к аресту счетов компании, что парализовало бы ее деятельность на период разбирательств и вполне могло привести к банкротству.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ FileAuditor»

«СёрчИнформ КИБ»
(модуль CloudController).


copying files...
клиенты
Login:
Password:
copying files...
70%
клиенты
elete ?
yes
no

«Слив» данных в облако

DLP-система оповестила сотрудников ИБ-отдела о выгрузке аномально большого архива в «облако» Dropbox. Оперативно нашли логин и пароль от учетной записи на облачной платформе и обнаружили, что копирование все еще продолжается.

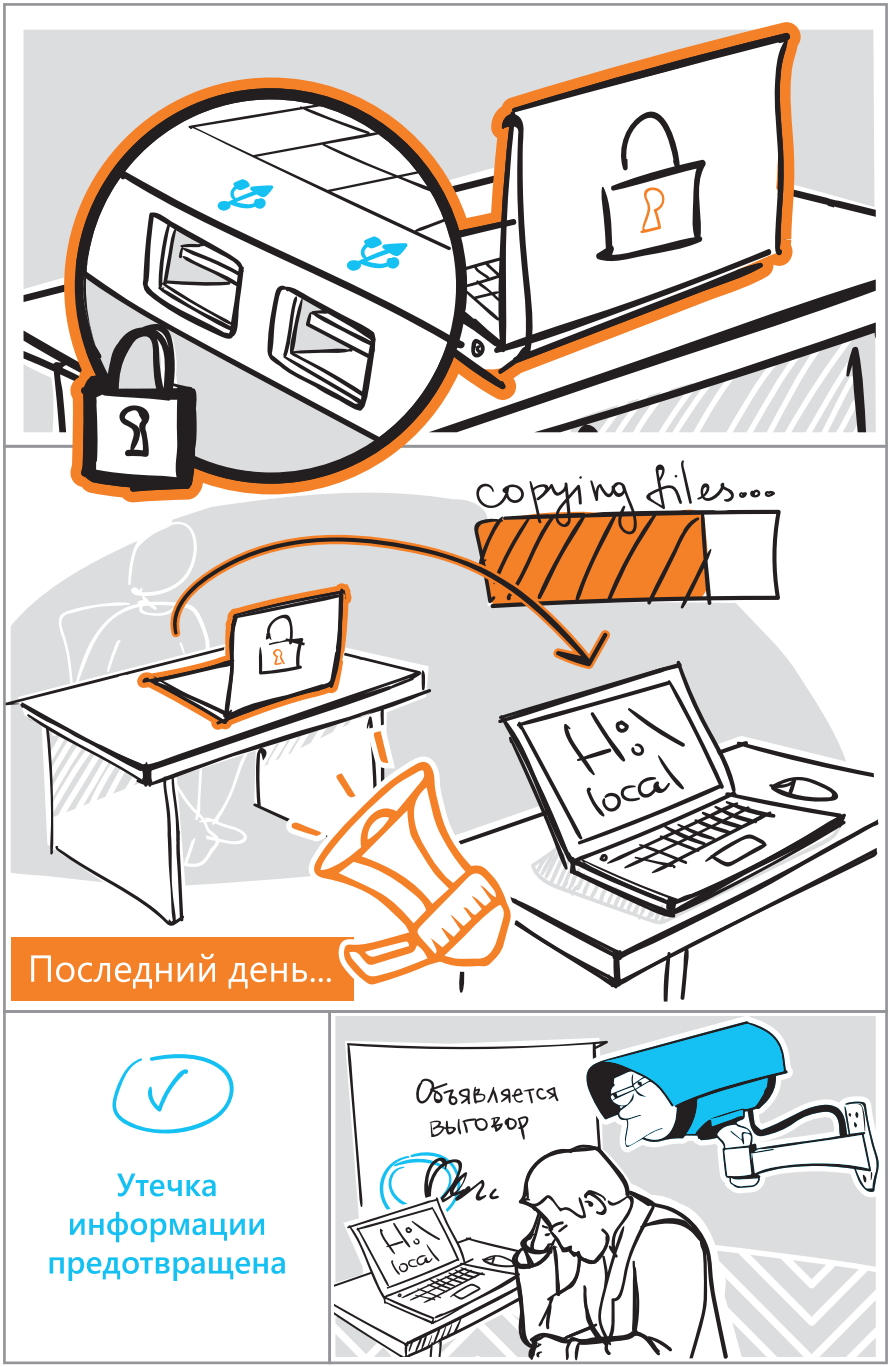
Подключившись к ПК сотрудника в режиме реального времени, ИБ-специалисты увидели, что он копирует клиентскую базу и сразу удаляет файлы на рабочем компьютере.

Реакция специалистов помогла предотвратить инцидент: служба внутренней безопасности успела добраться до рабочего места сотрудника до того, как он завершил копирование. Его попросили удалить документы из облака и уволили.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»

(модули  CloudController,  MonitorController,  Keylogger).


copying files...
Hi
local
Последний день...
Утечка информации предотвращена
Объявляется выговор
Hi
local

Утечка «по дружбе»

На компьютере сотрудника, который оформлял документы на увольнение и поэтому находился на строгом контроле, заблокировали USB-порты. В перехвате MonitorController на скриншотах экрана ИБ-специалист увидел, что сотрудник передает гигабайты информации на некий диск H:\ на компьютере приятеля, который оставался работать в компании.

ИБ-специалист посмотрел историю операций и выяснил, что приятель заранее освободил диск H:\ и тут же предоставил доступ к нему увольняющемуся сотруднику. Тот собирался беспрепятственно забрать документы на флешке.

Утечку информации за пределы компании удалось предотвратить. Друг получил выговор, ИБ-служба взяла его под пристальное наблюдение.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»

(модули FileController, MonitorController).


100 000 $
Исследование рынка
КУПИТЬ
Спустя неделю
Даркнет
Исследование рынка
Получить
Спустя еще неделю
Исследование рынка скача
Исследование рынка
скачать бесплатно
Исследование рынка
скачать бесплатно
Исследование рынка
скачать бесплатно
Доступ к исследованиям
1
2
99
100
Где хранится:
1
2
~ 300 ПК
FileAuditor
Доступ закрыт

Файлы легкого доступа

Ритейл-компания регулярно заказывала дорогостоящие исследования рынка (стоимость одного – около 100 тыс. долларов). Служба безопасности заметила нехорошую тенденцию: через неделю после получения результатов исследование появляется в даркнете, а еще через неделю становится доступным всему Интернету.

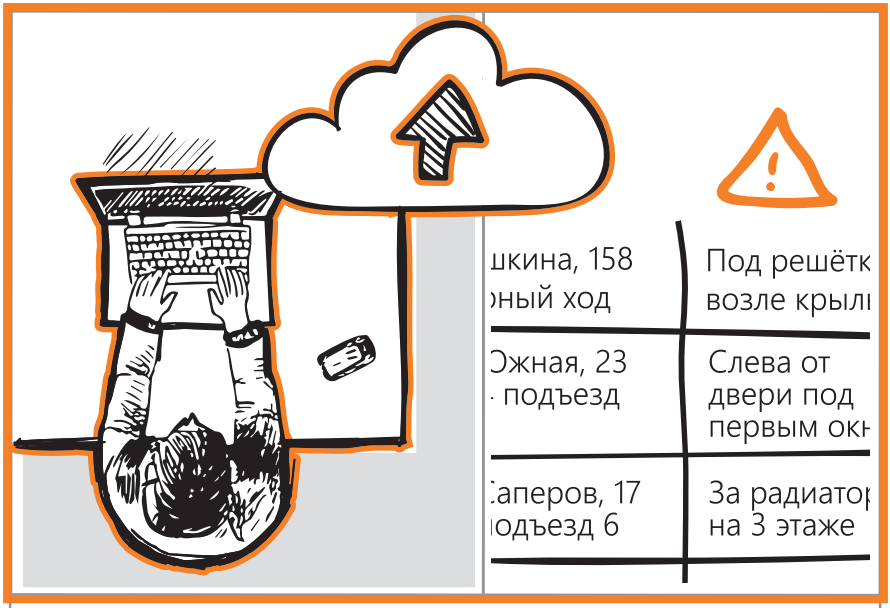
Специалисты по безопасности предложили руководству проверить, у кого есть доступ к исследованиям. Для этого компания установила FileAuditor. По политикам безопасности доступ к документам должен был быть только у 100 специалистов. Аудит показал, что на практике данные хранятся на ПК у почти 300 сотрудников.

После выявления избыточных прав доступ к данным для посторонних закрыли. И провели ретроспективное расследование с помощью DLP, чтобы выяснить, кто и куда сливал документы.

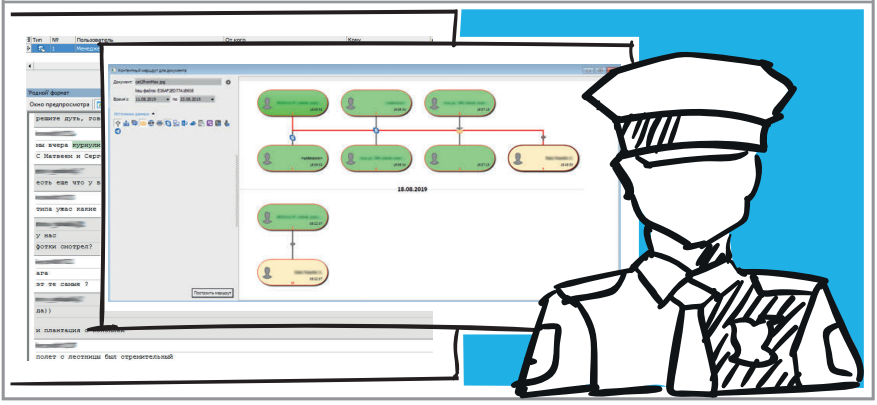
ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ FileAuditor»

«СёрчИнформ КИБ»
(модуль FileController).



шкина, 158 ный ход	Под решётк возле крыл
Ожная, 23 подъезд	Слева от двери под первым окн
аперов, 17 одъезд 6	За радиатор на 3 этаже



Торговля наркотиками

DLP детектировала подозрительное содержание в файле, который сотрудник загружал в «облако». В документе в одной колонке были вписаны граммы, во второй – адрес, в третьей – указание на «закладку», например, «слева от двери под первым окном».

Служба безопасности показала скриншоты документа руководству. Расследование проявило масштаб инцидента, так что ИБ-специалисты решили привлечь компетентные органы.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»

(модули  IMController,  CloudController).


Это ваше новое рабочее место
downloading...

Засланный казачок

На предприятие устроился менеджер по работе с торговыми сетями. Как и к любому новому сотруднику, служба информационной безопасности проявила к нему повышенное внимание, установив за ним пристальное наблюдение.

Бдительность была не напрасной: сотрудник оказался «засланным казачком». Его главной задачей было получение доступа к системе бухгалтерского учета предприятия и последующий «слив» информации конкурирующей компании.

Передача этих сведений конкурентам нанесла бы немалый урон предприятию и привела бы к оттоку клиентов. Все это в совокупности стоило бы компании 12 млн рублей в год.

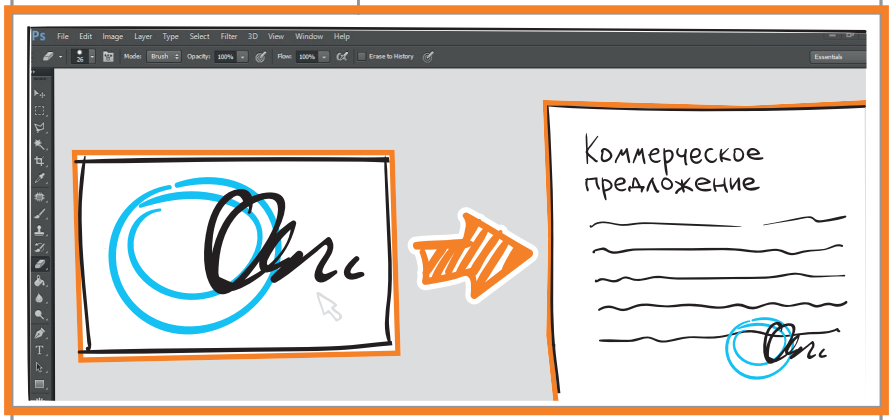
Сотрудник был уволен.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»
(модули DeviceController, FileController).

Коммерческий отдел

Отчёт по суммарной активности процессов



Подделка печатей

Специалист службы безопасности обратил внимание, что на компьютере сотрудника из коммерческого отдела часто активен процесс Photoshop.exe. Работа менеджера по продажам не была связана с дизайном, рекламой или маркетингом – для выполнения его прямых должностных обязанностей графический редактор был не нужен.

Тогда ИБ-специалист обратился к скриншотам и видеозаписи активности, чтобы выяснить, что происходит на мониторе сотрудника во время запущенного процесса Photoshop.exe.

Оказалось, менеджер подделывает ценовые предложения. Он изменял данные и буквально рисовал печати на документах других поставщиков, чтобы лоббировать «своих». Но в итоге вместо дивидендов получил приказ об увольнении.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»

(модули  MonitorController,  ProgramController).


НАЛОГОВАЯ
Сертификат
Регистрация фирмы
"Рога и Копыта"
ФИЛИАЛ
Лучше заключить договор с «Рога и копыта»
ТА
ФИЛИА
ФИЛИАЛ КОМПАНИИ

Фирма-боковичок

Компания, занимающаяся производством оборудования, еще на этапе тестирования «СёрчИнформ КИБ» выявила подозрительную связь между тремя сотрудниками. В течение рабочего дня эти люди не общались друг с другом, обедали порознь и даже работали в разных кабинетах. В то же время, оказалось, что все трое пользуются одним электронным ящиком, зарегистрированным на одном из бесплатных сервисов.

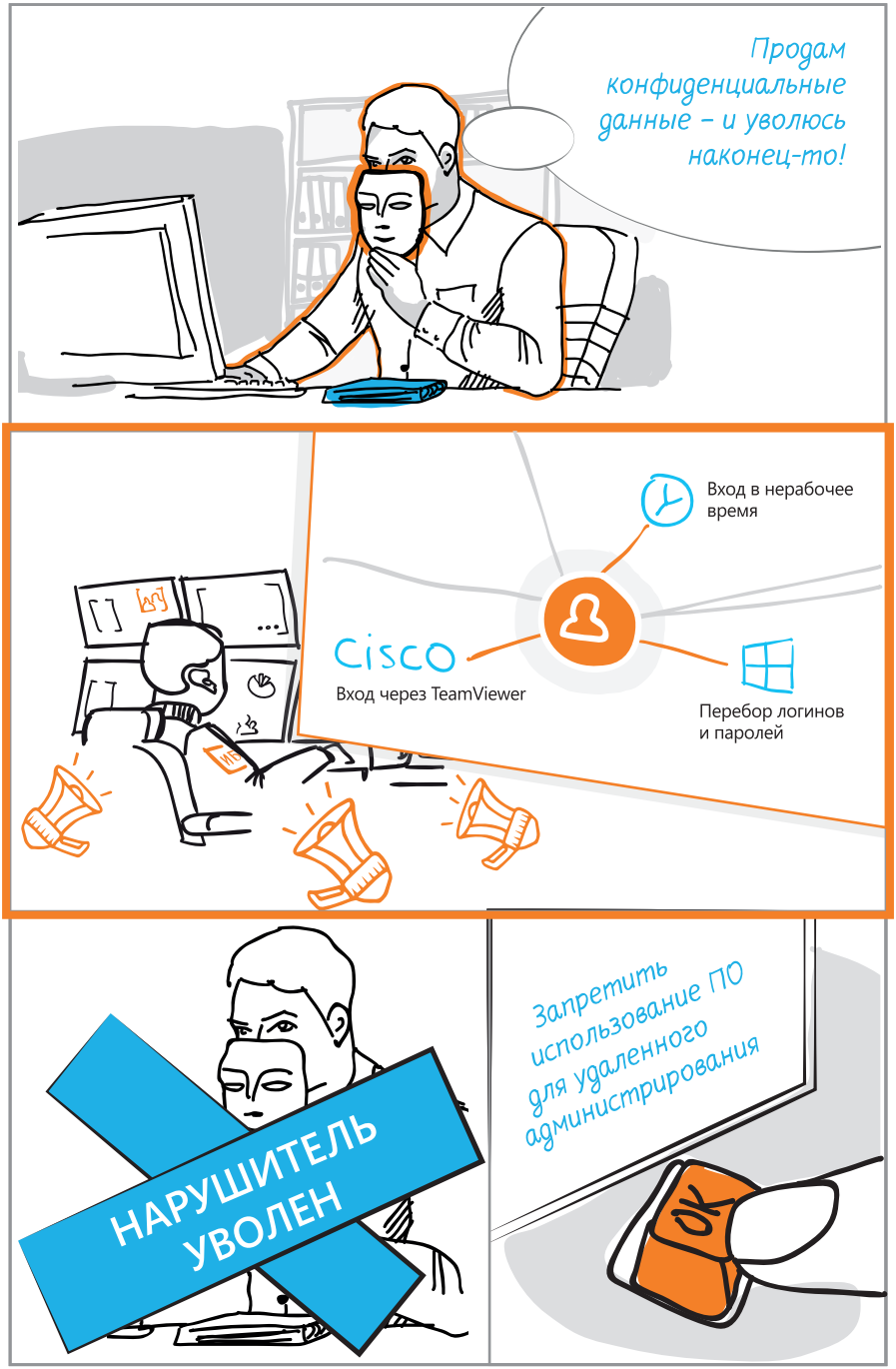
Детальный анализ перехваченной информации позволил установить, что в почтовом ящике был создан черновик, в котором сотрудники обсуждали «боковые» схемы продажи производимого компанией оборудования, но без участия самого производителя. Ущерб от деятельности сотрудников доходил до 4 млн рублей в месяц.

В результате двое сотрудников были уволены. Третий сохранил свою должность, однако к нему были применены иные меры взыскания.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»

(модуль MailController).


Продам конфиденциальные данные – и уволюсь наконец-то!
Вход в нерабочее время
Cisco
Вход через TeamViewer
Перебор логинов и паролей
НАРУШИТЕЛЬ УВОЛЕН
Запретить использование ПО для удаленного администрирования
OK

Махинации с учеткой

«СерчИнформ SIEM» детектировала подозрительную цепочку событий в IT-инфраструктуре компании: перебор логина и пароля и успешный вход в систему через TeamViewer в нетипичное время.

ИБ-служба отследила инцидент и в DLP – система зафиксировала передачу конфиденциальных данных через TeamViewer.

Виновник вскоре нашелся. Им оказался один из менеджеров, который в последнее время был недоволен условиями работы и собирался уволиться.

В итоге сотрудника уволили, а в компании запретили использовать ПО для удаленного администрирования.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ SIEM»

«СёрчИнформ КИБ»
(модуль CloudController).


Avito
смогу достать видеокарту помощнее на следующей неделе, когда придут новые компы
Устройства на компьютере
WIN7
Видеокарта
21.02.2018 Intel(R) Xe...
Винчестер
21.02.2018 (8GB)
Мониторы
21.02.2018 Универсальный
Винчестер
21.02.2018
Видеокарта
21.02.2018
Старая
Новая
Avito
Ущерб компании
Ущерб возмещён
Трудовой контракт

Кража оборудования

DLP-система перехватила подозрительное сообщение, оставленное сотрудником компании на популярной доске объявлений. Автор сообщения обещал «достать видеокарту помощнее на следующей неделе, когда придут новые компы».

Первым под подозрение попал системный администратор. Чтобы собрать доказательства, сотрудники ИБ-отдела вначале изучили отчеты по оборудованию. Обнаружилось, что вместо новых комплектующих, которые в компании регулярно покупали для обновления IT-парка, в системных блоках оказались давно списанные.

Изучив далее архив переписки системного администратора, ИБ-служба установила, что минимум в течение года он заменял видеокарты и жесткие диски на старые, а снятые комплектующие продавал на Avito.

Сотрудника уволили после того, как он возместил причиненный ущерб.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»

(модули HTTPController, ReportCenter).


Никакой премии!
Я отомщу...
BOSS
Downloading...
База данных

Месть сотрудника

В ходе штатного мониторинга активности персонала был выявлен сотрудник, который так и не смог «отойти» от новогодних праздников: помимо ежедневных опозданий на работу, вместо выполнения обязанностей он предпочитал проводить время за игрой в покер и раскладыванием пасьянсов. Реакция руководства была предсказуема: выговор и лишение премии.

Сотрудник воспринял произошедшее по-своему и решил отомстить. Настроенная в DLP политика по поиску негатива выявила переписки работника с друзьями, где он в нелестной форме отзывался о действиях начальства и обещал «устроить им веселую жизнь».

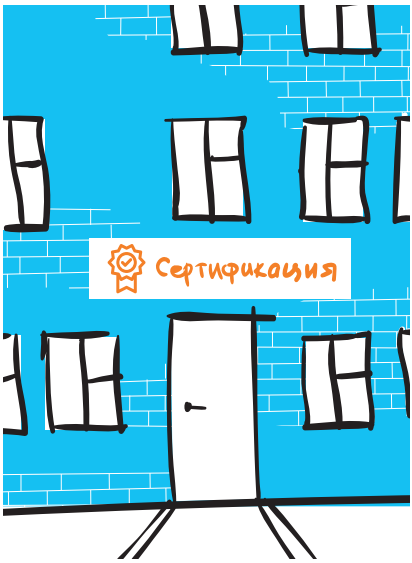
Дальнейшие действия не заставили себя ждать. На следующий день служба информационной безопасности зафиксировала, как сотрудник начал копировать на съемный жесткий диск большие объемы информации: сведения о поставщиках, скидках, клиентах, а также ряд финансовых документов.

Благодаря своевременным действиям службы безопасности покинуть компанию вместе со скопированной информацией сотруднику не удалось. Стоимость данных составляла примерно 7 млн рублей.

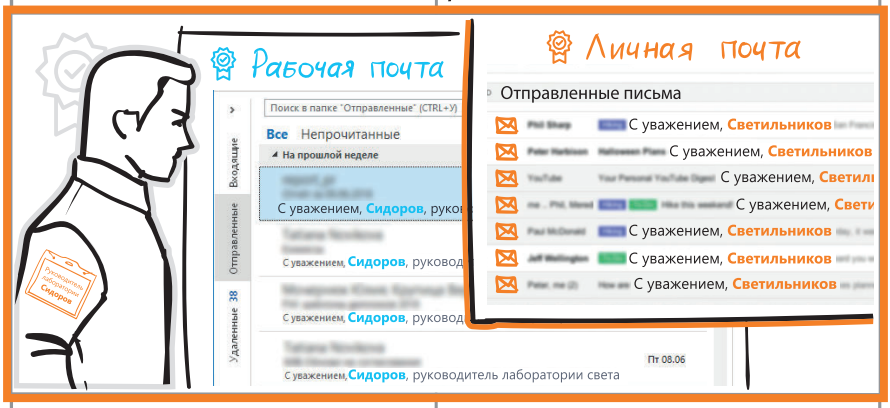
ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»

(модули  DeviceController,  IMController).


Сертификация


Лаборатория света
Руководитель лаборатории
Сидоров


Рабочая почта
Поиск в папке "Отправленные" (CTRL+Y)
Все
Непрочитанные
На прошлой неделе
Входящие
Отправленные
Удаленные 38
С уважением, Сидоров, руков
С уважением, Сидоров, руковод
С уважением, Сидоров, руковод
С уважением, Сидоров, руководитель лаборатории света
Пт 08.06
Личная почта
Отправленные письма
С уважением, Светильников
С уважением, Светильников
С уважением, Светил
С уважением, Свети
С уважением, Светильников
С уважением, Светильников
С уважением, Светильников


Выговор

Фрилансер под прикрытием

В компании, которая проводит обязательную и добровольную сертификацию товаров и услуг, руководитель лаборатории света стал рассылать заметно больше писем с личного почтового адреса.

Особенно службу безопасности заинтересовало, почему руководитель подписывает сообщения и прикрепленные документы вымышленной фамилией – Светильников.

Отдел безопасности пролил свет на обстоятельства дела с помощью DLP. Выяснилось, что руководитель лаборатории выполнял сторонние проекты на рабочем месте. Однако он был ценным сотрудником, поэтому руководство ограничилось замечанием, а ИБ-отдел стал наблюдать за ним более пристально.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»

(модули MailController, HTTPController).


СУББОТА
15:26
398 likes
Уволить!

Разгульные выходные

Каждый зарабатывает в кризис как может. Сотрудники одной компании нашли свой способ: работа сверхурочно по повышенному окладу.

Служба информационной безопасности, анализируя с помощью DLP активность тех, кто выходит работать в выходные дни, выявила, что двое сотрудников исправно выходят на работу сверхурочно, но занимаются преимущественно бездельем: просмотром фильмов, общением в соцсетях и т.д.

Дальнейший анализ выявил грубое нарушение трудовой дисциплины: в один из дней сотрудники решили сфотографироваться на фоне секретного объекта, расположенного на территории предприятия. Затем фотография была размещена на личных страницах работников в соцсетях.

В итоге сотрудники не только получили деньги по повышенному тарифу за «валяние дурака» на рабочем месте, но и скомпрометировали предприятие. За систематическое нарушение трудовой дисциплины и разглашение конфиденциальной информации виновные были уволены.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»

(модули HTTPController, IMController).


назначаем финансовым директором
сегодня вечером отметим назначение у меня!
Заявление
Прошу меня уволить
Уволить финдиректора, а не ценных сотрудников

Продвижение протеже по службе

В производственной компании освободилась должность финансового директора. Один из топ-менеджеров предложил кандидатуру – 28-летнюю сотрудницу бухгалтерии, которая еще не проработала в компании и года. ИБ-служба выступила против.

Во-первых, топ-менеджера и бухгалтера связывали романтические отношения, что подтверждала их переписка в WhatsApp, перехваченная DLP. Во-вторых, в компании как раз тестировали модуль профайлинга. И расчет модуля показал, что бухгалтер любит привлекать внимание, подпитывает собственное эго за счет окружающих и провоцирует коллег, распуская сплетни, а также в силу личностных качеств склонна к махинациям.

Но совет директоров все же утвердил кандидатуру, положившись на авторитет топ-менеджера.

Головокружительный поворот в карьере усилил проявление негативных личностных качеств молодого финансового директора. Через два месяца с помощью сплетен и интриг она разобщила коллектив: появились сложности в управлении персоналом, несколько ценных специалистов подали заявления об увольнении.

Совет директоров решил уволить финансового директора.

ИНСТРУМЕНТЫ РАССЛЕДОВАНИЯ

«СёрчИнформ КИБ»

(модуль IMController);

«СёрчИнформ ProfileCenter»

www.searchinform.ru

+7 (495) 721-84-06
info@searchinform.ru

SEARCHINFORM
INFORMATION SECURITY

Больше кейсов
на канале SearchInform
в Telegram

t.me/searchinform
vk.com/securityinform
facebook.com/SearchInform