ZECURION
ANALYTICS

«МЫ ПОТЕРЯЛИ 1 МЛРД РУБ. ТОЛЬКО НА ОДНОЙ УТЕЧКЕ ИНФОРМАЦИИ»

практические аспекты защиты информации от утечек в России

www.zecurion.ru | analytics@zecurion.com | +7 495 221-21-60

Оглавление

Введение

Компания Zecurion уже 13 лет специализируется на защите информации. За это время был накоплен высокий уровень экспертизы в области выявления и предотвращения утечек. DLP-системы Zecurion используют несколько тысяч компаний различных отраслей. Их опыт сложно переоценить, он представляет интерес не только для разработчиков специализированных решений, но и для практикующих ИТ- и ИБ-специалистов при реализации проектов по защите конфиденциальных данных.

В рамках работ по совершенствованию продуктовой линейки Zecurion, аналитический центр компании обратился к заказчикам с просьбой поделиться опытом использования DLP-систем. Часть информации, полученной от клиентов компании, была обезличена и легла в основу исследования. Авторы отчёта уверены, что разбор реальных кейсов выявления преднамеренных и случайных утечек поможет специалистам в предотвращении инцидентов и повышении эффективности реализуемых процедур информационной безопасности. Данный отчёт даёт ответы на часто задаваемые в рамках профессиональных сообществ вопросы, на чём компании теряют миллионы долларов, как ловят инсайдеров и каким образом предотвращают случайные утечки.

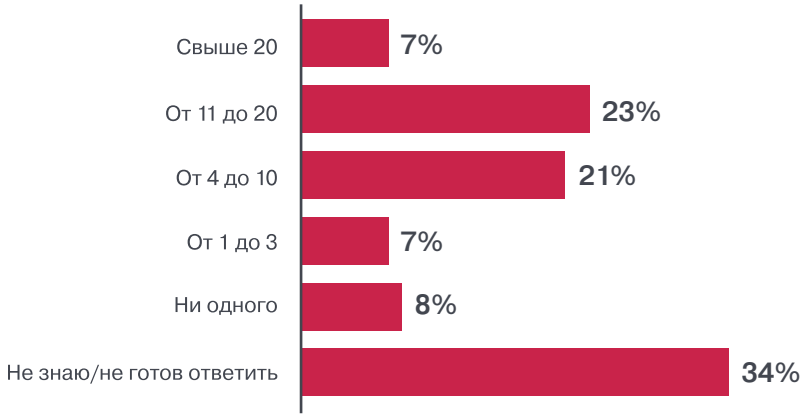
Ключевые выводы

- Максимальный подтверждённый размер финансового ущерба от утечки информации в российской компании — $30 млн.
- Специалисты по ИБ недооценивают возможный ущерб от инцидентов ИБ, связанных с утечкой конфиденциальных данных. Прогнозируемый ущерб (в среднем $310 тыс.) заметно ниже реального (в среднем $820 тыс.)
- Только 8% российских компаний среднего и крупного бизнеса не сталкиваются с утечками данных. Чаще всего компании фиксируют от 11 до 20 инцидентов внутренней ИБ в год. Первые инциденты выявляются уже на этапе тестового внедрения DLP.
- Большое число инцидентов ИБ связано с передачей конфиденциальной информации непосредственно конкурентам. В некоторых случаях — непреднамеренно.
- Компании, внедрившие DLP, но использующие их в режиме мониторинга, продолжают терпеть убытки от утечек конфиденциальной информации.

Частота инцидентов

По статистике, первые утечки информации фиксируются в организациях уже во время опытного внедрения на ограниченном количестве рабочих станций. А часто ли случаются утечки при обычной промышленной эксплуатации DLP-систем? Заказчики Zecurion говорят о том, что инциденты достаточно высокой степени серьёзности фиксируются раз в несколько недель (см. рис. 1). Этот показатель варьируется от отрасли к отрасли и особенно сильно зависит от числа сотрудников, которые имеют доступ к конфиденциальной информации.

Рисунок 1 ▶
Количество инцидентов внутренней безопасности в год

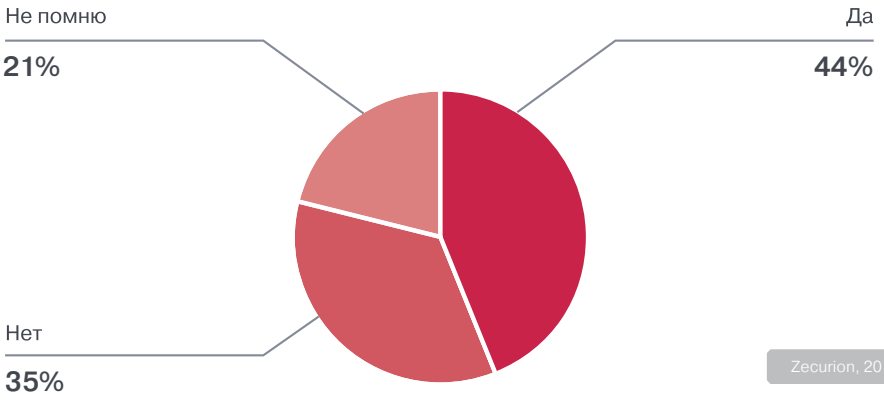


Zecurion, 2014

Правда, масштаб подобных инцидентов сильно различается. Потенциальный ущерб в 500 тыс. руб. может быть незначительным для компании с оборотом в сотни миллионов долларов, но критичным для бизнеса небольшой фирмы.

Формальный признак серьёзного инцидента — тот, о котором докладывают начальству. При этом степень вовлечённости руководства компаний в дела ИБ сильно различается. Отдельный опрос генеральных директоров показал, что менее 50% из них получают отчёты подразделения по защите информации (см. рис. 2). По крайней мере такое число смогло вспомнить наличие отчётов. Вероятно, процент директоров, которые эти отчёты читают — ещё меньше.

Рисунок 2 ▶
Получаете ли вы отчёты подразделений по защите информации?*



Zecurion, 2014

Специалисты по ИБ отмечают, что настоящие утечки информации начинают фиксироваться уже в первые недели тестовой эксплуатации (чаще всего, она проходит в режиме мониторинга). При этом пока настройки системы не отточены, возможна высокая доля ложных срабатываний.

* Респонденты: генеральные директора российских компаний среднего и крупного бизнеса

Во что выливаются утечки

Несмотря на то, что посчитать вероятный (да и фактический) ущерб от утечки информации зачастую довольно проблематично, делать это необходимо хотя бы для обоснования проектов по защите информации. Последствия утечек — вопрос исключительно острый. Как правило, чем больше ущерб от утечек, тем актуальнее оказывается задача защиты информации для компании, тем легче работать специалистам по ИБ, легче аргументировать заявленный бюджет.

То, что примерно в половине случаев респонденты затрудняются оценить стоимость утечек информации указывает на недостаток организационной работы в части классификации информации и оценки информационных рисков. В результате, если проекты по ИБ и ведутся, то без экономического обоснования, а использование конкретных средств не всегда оказывается оправданным.

Тем не менее, вторая половина опрошенных специалистов смогла привести цифры реального ущерба и оценить возможные издержки по предотвращённым инцидентам. Максимальный размер ущерба, который реально понесла компания от утечки конфиденциальных данных составил $30 млн. Источник утечки в этом случае был выявлен среди топ-менеджеров компании. В среднем финансовый ущерб от каждой утечки в опрошенных организациях составил $820 тыс.

Авторы исследования также попросили респондентов оценить возможный ущерб от предотвращённых утечек. Интересно, что оценка специалистов оказалась гораздо более консервативной. В среднем потенциальный ущерб от каждого инцидента мог составить $310 тыс. — намного ниже, чем реальные $820 тыс. По всей видимости, респонденты занижают возможный ущерб или учитывают не все последствия инцидентов.

Рисунок 3 ▶
Ущерб компаний

Zecurion, 2014

Основные статьи ущерба вследствие утечек — это прямые потери, упущенная выгода, а также штрафы со стороны регуляторов. Если говорить о российской практике, наибольшие потери компаний приходятся на косвенный ущерб вследствие ухудшения клиентской базы (особенно в высококонкурентных отраслях) или из-за получения конкурентами других преимуществ.

* Только по инцидентам, которые респонденты смогли оценить в деньгах

** Оценка респондентов по предотвращённым утечкам

Отдельно стоит остановиться на штрафных санкциях. Несмотря на то, что законодательство в области утечек данных в России весьма лояльно, в отдельных случаях именно санкции регуляторов грозят наибольшими потерями для бизнеса. Так, по мнению одного из респондентов, наихудшим последствием утечки информации из отдела промышленной безопасности и охраны труда было бы административное приостановление деятельности компании на срок до трёх месяцев (90 суток), что, по самым скромным оценкам, привело бы к потерям в десятки миллионов рублей.

Утекает из организаций самая разнообразная информация, включая проектную документацию, клиентские базы, сведения об инвестиционной деятельности компании, персональные данные сотрудников, коммерческие предложения, сведения о движениях на счетах клиентов и многое другое.

Нередко на сливе информации попадаются топ-менеджеры компаний. Объясняется это рядом причин. Во-первых, топ-менеджеры имеют легальный доступ к конфиденциальной информации самого высокого уровня, прекрасно представляют её ценность и возможные варианты использования вне компании. Во-вторых, часто руководители не только чувствуют свою безнаказанность, но и буквально провоцируют специалистов служб ИБ нарушать политики. Так, один из заказчиков сообщил, что вынужден был отключить агентские модули Zecurion Zlock у высшего руководства организации по прямому распоряжению сверху.

Ни о какой безопасности в таких условиях речи идти не может. Теряется весь смысл предприятий по ИБ. Можно предотвратить все утечки из линейных подразделений, но всего один инцидент, связанный с топами, поставит компанию на грань банкротства!

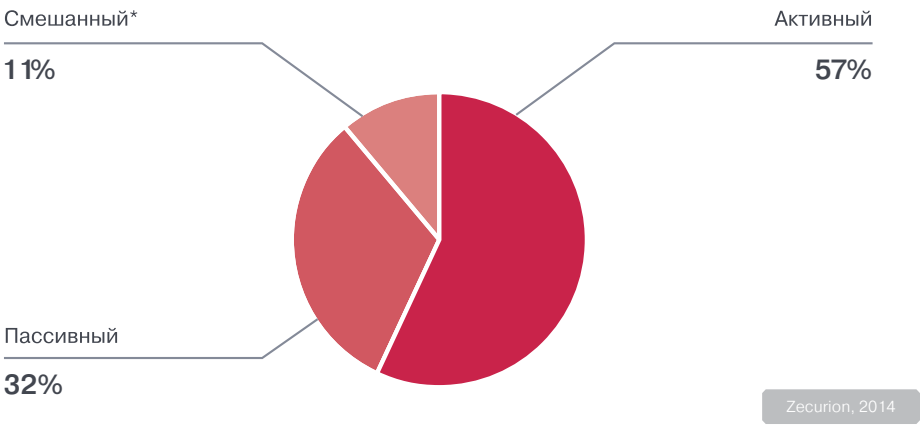
Не стоит думать, что «проблема начальства» характерна только для России. В январе 2013 года стало известно о том, что бывший вице-президент компании AMD и трое его коллег, переходя на работу в Nvidia, прихватили с собой конфиденциальные данные. Среди информации были планы развития и производства, технологические ноу-хау, сведения о заказчиках. Всего более 100 тыс. файлов инсайдеры вынесли на съёмных носителях.

Заблуждение, что работник может распоряжаться по своему усмотрению конфиденциальной информацией, к которой имеет доступ, является очень распространённым. И вряд ли ситуация кардинально изменится в ближайшем будущем. Согласно данным исследования «Защита информации. Что нам готовит будущее?» (http://www.zecurion.ru/upload/iblock/aa3/Zecurion_Students_research_2014.pdf), проведённого в 2013 году, более 80% российских студентов готовы будут скопировать важные для своей деятельности сведения при переходе на новую работу.

Контролировать или только наблюдать?

Блокировать передачу данных, которая нарушает корпоративные политики или не блокировать? Этот вопрос одним из первых встаёт перед специалистами служб информационной безопасности при внедрении DLP-систем. С одной стороны, блокирование (а значит и предотвращение нарушений) является очевидной задачей службы ИБ. С другой стороны, блокирование может нарушать отлаженные бизнес-процессы компании и негативно сказаться на взаимодействии с контрагентами. При реализации мер ИБ всегда необходимо соблюдать баланс удобства доступа к информации и её безопасности. Предпочтения пользователей Zecurion DLP показаны на рис. 4.

Рисунок 4 ▶
Использование режимов работы DLP-системы



При работе DLP-систем можно выделить 3 различных режима работы: активный, пассивный и смешанный. Активный режим подразумевает активное блокирование операций, нарушающих политики безопасности, например, копирование конфиденциального файла на флешку в незашифрованном виде или пересылку его по электронной почте пользователю, который не имеет соответствующих прав доступа. Активный режим чаще всего является стандартным эксплуатационным режимом работы DLP (впрочем, на рынке представлен ряд продуктов, условно относящихся к классу DLP, которые не способны блокировать утечки, а только фиксировать их постфактум).

В пассивном режиме DLP-система не производит блокировку операций, нарушающих политики, однако исправно их фиксирует. На первый взгляд, использование такого режима довольно странно для решений, по определению предназначенных для предотвращения утечек информации. Тем не менее, пассивный режим работы DLP является нужной функцией, и на этапе внедрения или тестового использования без него трудно обойтись (в противном случае возможно серьёзное нарушение бизнес-процессов). Проблема возникает тогда, когда отладочный период затягивается.

Смешанный режим работы DLP по своей сути является разновидностью активного. Важное отличие от активного режима заключается в использовании промежуточного «карантина». В примере с электронным письмом последовательность событий может быть следующей. DLP-система выявляет нарушение политики, информирует об этом офицера безопасности и задерживает отправку письма адресату. После ручной проверки офицер принимает окончательное решение, блокировать доставку или нет. К сожалению, ручная проверка практически не применима к файловым операциям

* Для тех каналов, на которых применимо

(запись на носители) и web-навигации (постинг в чаты, форумы, web-почта) из-за недопустимо больших временных задержек. А в случае с электронной почтой непродолжительные задержки, скорее всего, не будут критичны.

Как правило, DLP-системы, работающие в пассивном режиме, настраивают менее тщательно, что в среднесрочной и долгосрочной перспективах приводит к огромным временным затратам на изучение и реагирование на все инциденты, фиксируемые системой. Единственная выгода — решение по инциденту можно отсрочить. Но к каким негативным последствием для бизнеса это приведёт — большой вопрос.

Оставляя DLP-систему работать в пассивный режиме, службы ИБ затем идут на невероятные уловки, чтобы предотвратить распространение утекшей информации. В качестве примера можно привести историю компании, в которой детектировали утечку через электронную почту. Конфиденциальные сведения инсайдер отправил на свой личный почтовый ящик в популярном почтовом web-сервисе. Угроза миллионных убытков вынудила офицеров безопасности зайти в личную электронную почту злоумышленника и вручную удалить оттуда конфиденциальные письма. И хотя история, можно сказать, закончилась для компании хорошо, инсайдер банально не успел воспользоваться украденной информацией, результаты подобного рейда могли быть гораздо печальнее. Ведь инсайдер вполне мог засудить компанию за взлом своего аккаунта! Вероятно, просто попали на мягкого человека, который согласился уволиться и замять дело по-тихому.

Но готов ли каждый заказчик рисковать подобным образом всякий раз, когда система выявляет утечку?!

Эффективность технологий и средств

По мировой статистике (см. отчёт Zecurion «Утечки конфиденциальной информации 2013»), наибольшее количество утечек происходит через web-сервисы, а также ноутбуки и планшеты. Статистика, которую Zecurion Analytics собрал в рамках опроса пользователей DLP-систем, даёт иные цифры. Различие обусловлено тем, что в мировую статистику не попадают предотвращённые утечки. Именно поэтому в данном отчёте высока доля электронной почты (см. рис. 5), тогда как в общей мировой статистике её доля составляет лишь 7,4%.

Рисунок 5 ▶
Популярные каналы утечек*

* Включая и предотвращённые утечки. Количество ответов более 100%, т. к. респонденты указывали несколько вариантов ответа

Один из наиболее полезных с точки зрения развития продуктов вопросов касался эффективности используемых технологий распознавания и классификации информации. DLP-системы Zecurion используют 10 различных

технологий, позволяющих реализовать гибридный анализ. Каждая из технологий имеет как свои достоинства, так и недостатки (ограничения использования), именно поэтому наилучший результат даёт совместное их использование. Тем не менее, для разработчиков важно понимать, какие из технологий являются наиболее востребованными среди заказчиков. Причём понятие востребованности в данном контексте включает одновременно удобство использования, простоту настройки и точность распознавания конфиденциальной информации (см. рис. 6).

Рисунок 6 ▶
Наиболее востребованные технологии выявления утечек

Ещё один вариант не указан на диаграмме, хотя был назван несколькими респондентами. Его трудно назвать технологией в привычном понимание, скорее это подход. Заключается в том, что система работает в пассивном режиме, фиксируя все перемещения информации в своём архиве. С некоторой периодичностью архив вручную просматривается сотрудником на предмет выявления подозрительных (нарушающих корпоративные политики безопасности) операций.

Архив, безусловно, является важным элементом DLP-системы. Архив всех событий и операций незаменим при настройке системы и расследовании инцидентов. Однако практика ручной инспекции архива как основной технологии выявления утечек порочна — утечки уже невозможно предотвратить, но автоматизация процесса в данном случае минимальна. Точность подобной технологии будет крайне низкой. При большом объёме информации (уже от нескольких десятков рабочих мест) потребуется постоянная загрузка нескольких офицеров безопасности. А DLP в данном случае реализует лишь несколько процентов своего потенциала.

Последствия инцидентов и санкции к нарушителям

В том, что компании стремятся избегать публичности в случаях утечки информации нет ничего удивительного. Репутационные риски могут быть достаточно чувствительными. Но, как показывают результаты опроса, подавляющее большинство организаций также не информирует об инцидентах собственных сотрудников. Между тем, из инцидентов важно делать правильные выводы и доводить их до персонала с тем, чтобы утечки не случались в будущем.

Согласно статистике Zecurion Analytics (см. отчёт «Утечки конфиденциальной информации» за 2013 год), большинство утечек происходит не по злому умыслу, а из-за ошибок или низкой квалификации персонала по вопросам ИБ. Соответственно, для повышения защищённости информации необходимо проводить регулярные тренинги среди работников, учить людей правильно обращаться с конфиденциальными данными, информировать о мероприятиях, реализуемых службой ИБ. И опыт инцидентов имеет в данном случае немалую ценность.

Если в компании ловят злонамеренного инсайдера, полезно будет информировать сотрудников об этом факте хотя бы для того, чтобы повысить бдительность. Целесообразно также рассказать о дисциплинарных мерах, которые были применены к инсайдеру с тем, чтобы уменьшить желание других сотрудников сливать информацию. Хотя чужой пример плохо работает в компаниях с высокой текучкой кадров. Так, большинство офицеров безопасности отмечает, что если работников известить об инциденте (желательно уточнив, какие санкции были применены к нарушителю), большая часть сотрудников становится заметно более осторожной. Но приходят новые люди, и всё возвращается на круги своя.

Рисунок 7 ▶
Меры воздействия на инсайдеров

Респонденты рассказали, какие меры применяются к сотрудникам, которых уличили в сливе информации (см. рис. 7). Санкции сильно отличаются в зависимости от обстоятельств инцидента. Если в действиях сотрудника отсутствует злой умысел, в большинстве случаев всё заканчивается разъяснительными беседами. При серьёзных последствиях непредумышленных утечек работодатели прибегают к официальным выговорам и штрафам (в том числе лишают премий). Если же сотрудники целенаправленно воровали информацию, применяются более жёсткие санкции, инсайдеров увольняют или даже привлекают к юридической ответственности. Впрочем, до суда дело доходит крайне редко — примерно в 2% случаев. Аналогич-

ные цифры приводятся в совместном исследовании кадрового портала Superjob.ru и аналитического центра Zecurion «Офисная небезопасность: почему работники безнаказанно сливают информацию» (http://www.zecurion.ru/upload/iblock/66f/Zecurion_Office_insecure_2013.pdf) — менее чем в 1% случаев компании привлекают инсайдеров к уголовной ответственности. Главные причины, по которым этого не происходит — нежелание афишировать сам факт утечки и трудности с доказательством вины человека. Впрочем, для владельцев DLP-систем технически доказать вину инсайдера не представляется сложным.

Увольнение, даже «по статье», не является слишком строгой мерой наказания инсайдеров, отмечают участники исследования. Особенно, когда сотрудник действовал в интересах конкурентов. Один из респондентов, руководитель службы безопасности, рассказал, что однажды в компании поймали сотрудника, который копировал служебную информацию на внешний жёсткий диск. Инсайдер был оперативно уволен, но «по-тихому, по собственному желанию». А уже на следующей неделе он вышел на работу в конкурирующую компанию.

Обработка инцидентов

Как показывает практика, далеко не всегда обработкой инцидентов занимаются те же службы, что и обнаружением. С точки зрения безопасности разделение полномочий является полезным, однако в некоторых случаях принимает нестандартные формы. Одна из схем, описанных заказчиком, заключается в следующем. Служба ИТ (именно она занимается вопросами технического обеспечения ИБ) фиксирует нарушение политик, создаёт инцидент и передаёт информацию о нём в службу безопасности компании. В свою очередь сотрудники службы безопасности расследуют инцидент и осуществляют все дальнейшие мероприятия по его обработке, докладывая о результатах руководству. Подобная схема не является единичной и используется обычно в тех случаях, когда в организациях отсутствует выделенная служба ИБ, а уровень доверия к службе безопасности высок. Впрочем, большинство классических безопасников не готовы самостоятельно внедрять, настраивать и поддерживать DLP-системы, для чего и привлекают ИТ-специалистов.

Из очевидных недостатков такой схемы следует отметить отсутствие блокировки информации. Что особенно чревато в случае преднамеренных действий сотрудника. Таким образом можно лишь отследить утечку постфактум и попытаться наказать инсайдера, однако в большинстве случаев это не принесёт ничего кроме морального удовлетворения. Утекшую информацию это уже не вернёт.

Ещё один недостаток — отсутствие обратной связи от службы безопасности. Затрудняется настройка решения — в случае, если инцидент создан ошибочно (реально никакой утечки не происходило), следовало бы скорректировать настройки. Хотя при использовании DLP-системы в пассивном режиме не происходит блокирование информации и последствия ложных срабатываний не так критичны для бизнеса, но их разбор в крупной компании существенно осложнит жизнь службы безопасности, отнимет ресурсы от других задач и, в конечном счёте, будет стоить немалых денег.

В целом, практика разделения полномочий при расследовании и обработке инцидентов является оправданной и позволяет уменьшить влияние человеческих ошибок и вероятность сговора сотрудников. Однако весь процесс расследования затягивается в силу усложнения коммуникаций между подразделениями. Кроме того, исключительно важно обеспечивать обратную связь по результатам расследования каждого инцидента для оптимизации работы самой DLP-системы и разработки мер минимизации утечек в будущем.

Среди подобных мер сразу несколько респондентов отмечают изменение порядка назначения прав доступа к информационным ресурсам. А в некоторых случаях вводится ответственность руководителей подразделений за корректное назначение прав пользователей. Это разумно. Именно руководители отделов знают, какая информация находится в их ведении, кому из сотрудников необходим доступ к ней для выполнения рабочих обязанностей, понимают ценность самой информации. Службы ИБ подобными сведениями не располагают и при назначении прав доступа самостоятельно или по заявкам от линейного персонала неизбежно будут ошибаться. Другая проблема связана с тем, что нередко пользователям дают слишком широкие права — просто потому, что так удобно, потому, что так проще работать. А чем шире права доступа, тем выше информационные риски.

Заключение

Авторы исследования провели более 100 интервью и изучили ежедневную работу специалистов по защите информации, чтобы обобщить опыт использования DLP-систем в компаниях различных отраслей и размеров. При этом был выявлен ряд типичных ошибок, снижающих эффективность используемых систем, вызывающих разочарование малоопытных пользователей.

Среди подобных ошибок заказчиков можно отметить недостаточную организационную подготовку к внедрению DLP-системы, отсутствие оценки рисков и регулярной классификации информации. Это значительно увеличивает время внедрения системы и затрудняет процесс эксплуатации. Возможно, именно проблемы, связанные именно с низким качеством подготовительной работы, побуждают компании продолжать эксплуатацию DLP-систем в пассивном режиме работы и после отладочного периода. По сути, отладочный период затягивается навсегда.

Само использование пассивного мониторинга в качестве основного рабочего режима DLP-системы также можно отнести к ошибкам. Мотивацию служб информационной безопасности в данном случае можно понять. Такой подход создаёт меньше проблем в ежедневной деятельности. Нет необходимости скрупулёзно настраивать политики для детектирования настоящих утечек информации. Исключаются разбирательства с начальством по поводу неверной блокировки, недовольства со стороны бизнес-подразделений. Но, самое главное, пассивный режим не позволяет предотвращать утечки, что по определению является первейшей задачей DLP-системы. Получается, что специалисты по ИБ в поисках спокойной жизни мирятся с наличием утечек.

Ещё одна ошибка — отсутствие выделенного специалиста (или даже отдела в крупных корпорациях), который занимался бы обслуживанием DLP-системы. DLP нельзя использовать по схеме «поставил и забыл». Без должного внимания, без регулярной корректировки настроек системы, эффективность её будет стабильно падать. При этом увеличится число ошибок как первого, так и второго рода. Между тем, для контроля и корректировки политик не требуется много времени. Главное, выделять его регулярно. По оценкам заказчиков, 1,5-2 часов в день будет достаточно для обслуживания Zecurion DLP в компании до 500 рабочих мест. В действительно крупных компаниях (с количеством контролируемых пользователей в десятки тысяч), как отмечают опытные безопасники, может потребоваться выделенный аналитик для изучения журналов системы и фиксируемых инцидентов.

Если говорить о последствиях инцидентов, компании часто ведут себя слишком мягко по отношению к преднамеренным инсайдерам. Пойманный с поличным сотрудник редко возражает против увольнения (причём чаще всего, из-за простоты для обеих сторон оформляется «по собственному желанию»). Но после того как инсайдер слил конфиденциальную информацию и, возможно, получил за неё хорошее вознаграждение, увольнение по собственному желанию выглядит прекрасным вариантом для работника. А понесённый ущерб компания уже не возместит.

Некоторые случаи, описанные руководителями служб безопасности, довольно курьёзны. Так, один инсайдер, сливший огромную базу клиентов на личную почту, сообщил, что просто хотел поработать дома. Сложнее оправдаться, когда информация уходит не на личные адреса, а непосредственно конкурентам. Такие случаи не редки. Но к юридической ответственности ин-

сайдеров привлекают не всегда. Как показывает практика, в подобных ситуациях суд становится на сторону работодателя. При этом важно установить в организации режим защиты конфиденциальной информации и правильно оформить трудовые отношения с сотрудником.

* * *

Фраза, вынесенная в заголовок отчёта – это цитата одного из респондентов. После масштабной утечки данных компания оценила финансовый ущерб от инцидента. И он оказался поистине впечатляющим. К сожалению, в тексте сложно передать эмоциональность речи собеседника, но многомиллионный ущерб от инцидентов внутренней безопасности стал для российских компаний суровой реальностью. То, что инциденты не фиксируются компаниями говорит не об их отсутствии, а о заблуждении, в котором пребывают руководители компаний и специалисты по ИБ в отсутствие объективных инструментов анализа. Кажущееся отсутствие инцидентов формирует ложное чувство защищённости, развеять которое способен разве что прямой финансовый ущерб от очередной утечки.

О компании Zecurion

ZECURION

Zecurion (www.zecurion.ru) — крупнейший российский разработчик систем защиты информации от внутренних угроз. DLP-продукты Zecurion позволяют минимизировать риски умышленной и случайной утечки корпоративной информации.

Компания Zecurion более 10 лет профессионально занимается вопросами информационной безопасности. С 2001 года Zecurion является лидером в области шифрования данных, а с 2005 года разрабатывает инновационные решения для защиты от утечек информации. Среди современных продуктов, представленных на рынке DLP, решения Zecurion признаны самыми технологичными (по версии аналитического центра Anti-Malware.ru). В рейтинге CNews Analytics компания Zecurion уверенно удерживает первое место среди разработчиков DLP с 2011 года и входит в число 30 крупнейших ИТ-компаний России в сфере защиты информации. В 2012 году компания провела ребрендинг, прекратив использование старого названия SECURIT.

Линейка продуктов Zecurion реализует полный спектр защиты информации от инсайдеров: контроль всех потенциальных каналов утечки, ведение архива действий сотрудников, защиту данных в процессе использования и хранения, а также управление доступом пользователей к корпоративной сети, приложениям и конфиденциальной информации. Использование DLP-решений компании обеспечивает комплексную защиту информации от утечек на протяжении всего её жизненного цикла — от создания до записи в архив или удаления. Благодаря инновационным подходам и ориентированности решений на требования бизнеса комплексные системы Zecurion используются более чем в 10 000 организаций. Компанию Zecurion поддерживают более 100 бизнес-партнёров из различных регионов России и СНГ, стран Азии и Тихоокеанского региона, Европы и США. В 2013 году компания Zecurion впервые была включена в магический квадрант Gartner в сегменте DLP.

ZECURION
ANALYTICS

Контактная информация

Владимир Ульянов
Руководитель аналитического центра Zecurion

Телефон: +7 909 691-22-12
analytics@zecurion.com

Ксения Головко
Заместитель руководителя пресс-службы

Телефон: +7 967 091-65-50
pr@zecurion.com

129164, Российская Федерация, Москва, Ракетный бульвар, 16

Телефон/факс: +7 495 221-21-60
www.zecurion.ru