



# ИНСАЙДЕРСКИЕ УГРОЗЫ '09 В РОССИИ



Медиа-партнеры

KEEPING SECRETS SAFE





ВСТУПИТЕЛЬНОЕ СЛОВО

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

ОБЩИЕ ВЫВОДЫ

ПОРТРЕТ РЕСПОНДЕНТА

УГРОЗЫ ИБ

ИНСАЙДЕРСКИЕ УГРОЗЫ

СРЕДСТВА ЗАЩИТЫ

КЛАССИФИКАЦИЯ ДАННЫХ

ШИФРОВАНИЕ ДАННЫХ

ОТВЕТСТВЕННОСТЬ НАРУШИТЕЛЯ ВНУТРЕННЕЙ ИБ

НАПРАВЛЕНИЕ РАЗВИТИЯ РЫНКА

ЗАКЛЮЧЕНИЕ

О КОМПАНИИ PERIMETRIX

О МЕДИА-ПАРТНЕРАХ



## Уважаемые дамы и господа!

Аналитический центр компании Perimetrix представляет результаты второго ежегодного исследования в области внутренней информационной безопасности (ИБ). С момента выхода первого исследования существенно изменилась глобальная ситуация, однако проблема защиты от внутренних ИТ-угроз по-прежнему беспокоит большинство российских компаний.

Несмотря на огромный масштаб проблемы (убытки от утечек могут измеряться сотнями миллионов долларов) и возрастающий спрос на комплексные системы безопасности, ситуация с защищенностью бизнеса почти не изменилась. С нашей точки зрения, эта негативная тенденция связана с ограниченностью предложения на рынке, недостаточной информированностью заказчиков и пассивностью некоторых вендоров.

Нам кажется, что будущий год станет переломной точкой в развитии российского рынка комплексных систем защиты конфиденциальности данных. Этот рынок по-прежнему очень молод, и мощные глобальные потрясения, такие как мировой финансовый кризис, могут нанести ему существенный удар. Те вендоры, которые сумеют пережить это непростое время, создадут себе задел для дальнейшего развития и получат очевидные конкурентные преимущества.

Мы искренне надеемся, что результаты нашего исследования помогут российским компаниям лучше понять специфику внутренней безопасности и принять все необходимые меры защиты.

Евгений Преображенский  
Генеральный директор

## МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

Исследование «Инсайдерские угрозы 2009» проводилось при непосредственной поддержке ряда медиа-партнеров. Авторы выражают перечисленным организациям (представлены в алфавитном порядке) искреннюю благодарность за оказанную помощь в сборе первичной статистической информации и популяризации идеи защиты от внутренних ИТ-угроз на российском рынке.

- Журнал «Защита информации. Инсайд»;
- Компания «Практика Безопасности»;
- Журнал «Экономическая безопасность».
- Портал Anti-malware.ru;
- Портал Bankir.ru;
- Журнал Information Security/Информационная безопасность;
- Портал Securitylab.ru.

Исследование «Инсайдерские угрозы в России 2009» проводилось с 01 декабря 2008 г. по 23 января 2009 года. В рамках исследования специалисты аналитического центра Perimetrix опросили сотрудников 1046 российских компаний различных отраслей экономики. Респонденты из числа посетителей сайтов медиа-партнеров (Anti-Malware.ru, Bankir.ru, SecurityLab.ru, ITsec.ru, EkonBez.ru, Security-practice.ru, Inside-zi.ru) и сайта компании Perimetrix отвечали на вопросы утвержденной анкеты.

## ОБЩИЕ ВЫВОДЫ

- Внутренние угрозы безопасности по-прежнему беспокоят компании значительно больше внешних угроз. Наибольшие опасения вызывают угрозы утечки информации (73%), а также халатность служащих (70%)
- Главной причиной актуальности внутренних проблем являются продолжающиеся утечки информации — только 5% компаний заявили об отсутствии подобных инцидентов за последний год. Специалисты по безопасности осознали собственную незащищенность перед утечками — сразу 42% респондентов затруднились назвать точное количество утечек.
- Проникновение систем защиты от внутренних угроз за последний год выросло, однако не слишком сильно. Криптографические системы используют 41% компаний, а комплексные системы защиты от утечек — 29%.
- Спрос на системы внутренней безопасности достаточно высок, однако он сдерживается рядом объективных факторов. Главным из них являются бюджетные ограничения (46%), которые приобрели особенную актуальность во время финансового кризиса.
- В подавляющем большинстве случаев нарушители внутренней безопасности не несут практически никакой ответственности. 45% халатных нарушителей наказываются строгими выговорами, а 51% злонамеренных инсайдеров увольняются из компаний по собственному желанию.
- В ближайший год рынок внутренней безопасности продолжит свой рост, однако он вряд ли окажется слишком быстрым. Прорыва на рынке следует ожидать через 2-3 года, по мере стабилизации финансовой ситуации и активного развития новых игроков.

## ПОРТРЕТ РЕСПОНДЕНТА

Как и в исследовании прошлого года, полученная выборка имеет явный уклон в сторону средних и крупных компаний (рис. 1). На долю небольших организаций, имеющих менее 500 рабочих станций, пришлось только 8% респондентов, в то время как почти две трети компаний (65%) используют в своей корпоративной сети более 1000 компьютеров.

Сдвиг получившейся выборки респондентов в сторону средних и крупных компаний позволяет получить актуальную картину рынка, поскольку имен-

но такие организации испытывают максимальные трудности в области внутренних проблем безопасности. Нельзя забывать и о специфике предложения — на рынке присутствуют системы защиты для крупных заказчиков, но почти не представлены корпоративные решения для небольших организаций. Последние предпочитают решать проблему другими способами — смежными продуктами и организационными мерами. На данный момент проблему внутренней безопасности и защиты конфиденциальности данных уместнее всего рассматривать через призму крупного бизнеса.

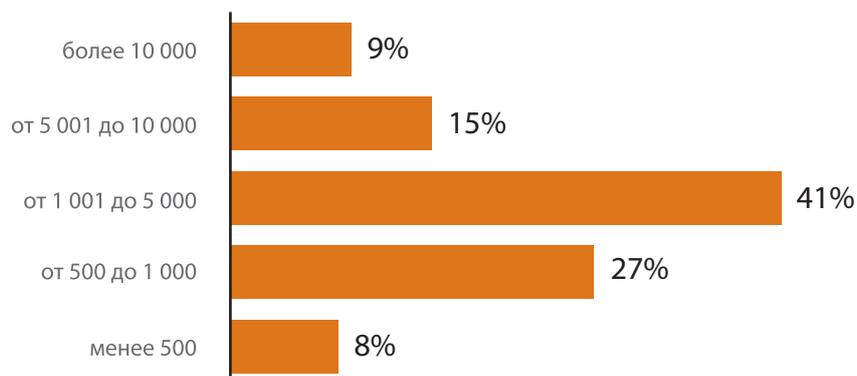


Рисунок 1. Количество рабочих станций

Отраслевое распределение респондентов оказалось вполне стандартным для такого рода исследований (рис. 2). Первые строчки в этом распределении традиционно заняли секторы телекоммуникаций (21%) и финансовых услуг (19%), всегда являвшиеся лидерами в области внедрения систем защиты. Вслед за ними расположились более консервативные отрасли — топливно-энергетический ком-

плекс (18%), а также предприятия государственного сектора (17%).

По сравнению с прошлым годом существенно (с 6 до 10%) выросла доля торговых компаний (прежде всего, розничных сетей), которые приняли более активное участие в исследовании. А вот количество респондентов из производственных фирм и страховых компаний, напротив, несколько уменьшилось.

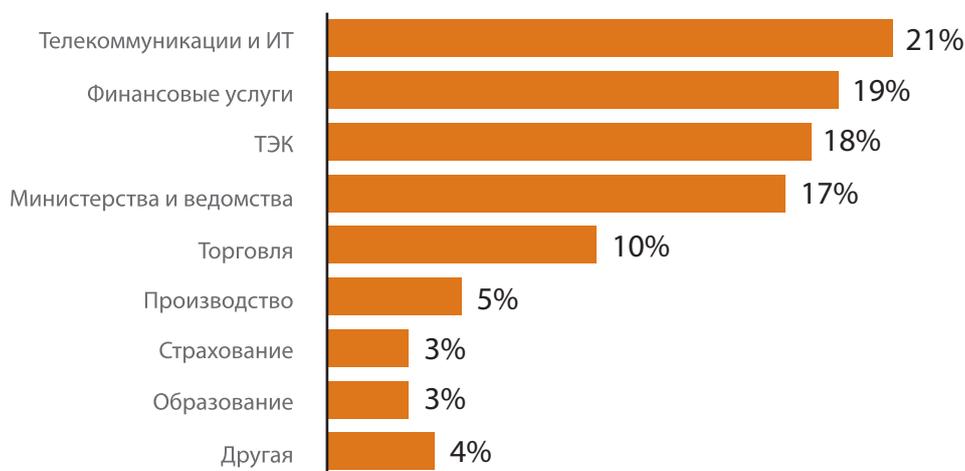


Рисунок 2. Сфера деятельности

Подавляющее большинство респондентов (как минимум 92%) задействованы в принятии решений по внедрению ИТ и ИБ систем. Две трети опрошенных специалистов являются руководителями — 35% респондентов возглавляют ИТ-отдел, а еще 33% — отдел информационной безопасности. Таким образом, можно с уверенностью утверждать, что выборка

специалистов обладает вполне достаточной компетенцией для ответа на поставленные далее вопросы, и полученные в результате исследования данные неплохо отражают текущую ситуацию на рынке. А поскольку респонденты определяют развитие ИБ-систем в своих организациях — по их ответам можно строить схемы дальнейшего развития отрасли.

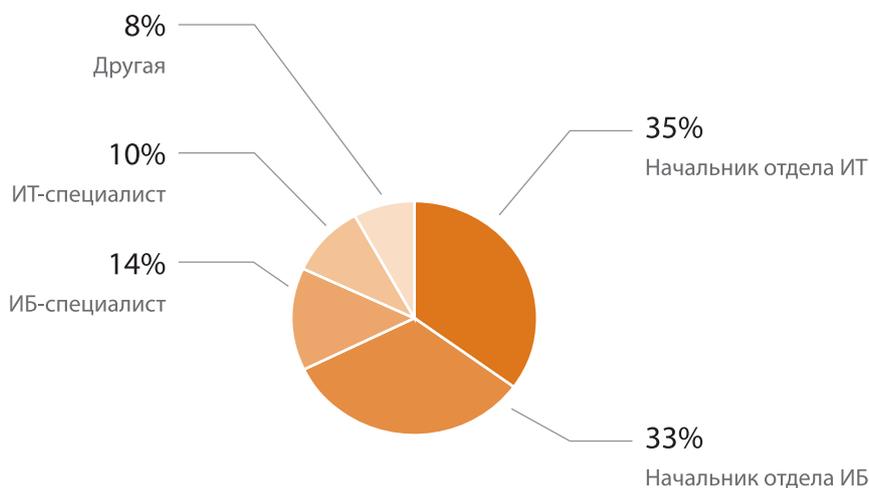


Рисунок 3. Респонденты по должности

## УГРОЗЫ ИБ

Один из основных вопросов исследования касался наиболее опасных угроз внутренней безопасности. Респондентам предлагалось выбрать четыре наиболее опасные угрозы ИБ из общего списка существующих рисков. Результаты их выбора в сравнении с показателями годичной давности представлены на рис. 4.

Из получившегося распределения вытекает ряд характерных тенденций. Во-первых, самыми опасны-

ми угрозами по-прежнему остаются утечки информации и халатность персонала — доли этих угроз изменились незначительно, и эти изменения находятся в рамках погрешности исследования. А вот опасность практически всех внешних угроз (вирусов, хакеров и спама), напротив, существенно уменьшилась. По-видимому, этот тренд объясняется общей успокоенностью компаний в отношении угроз внешней безопасности.

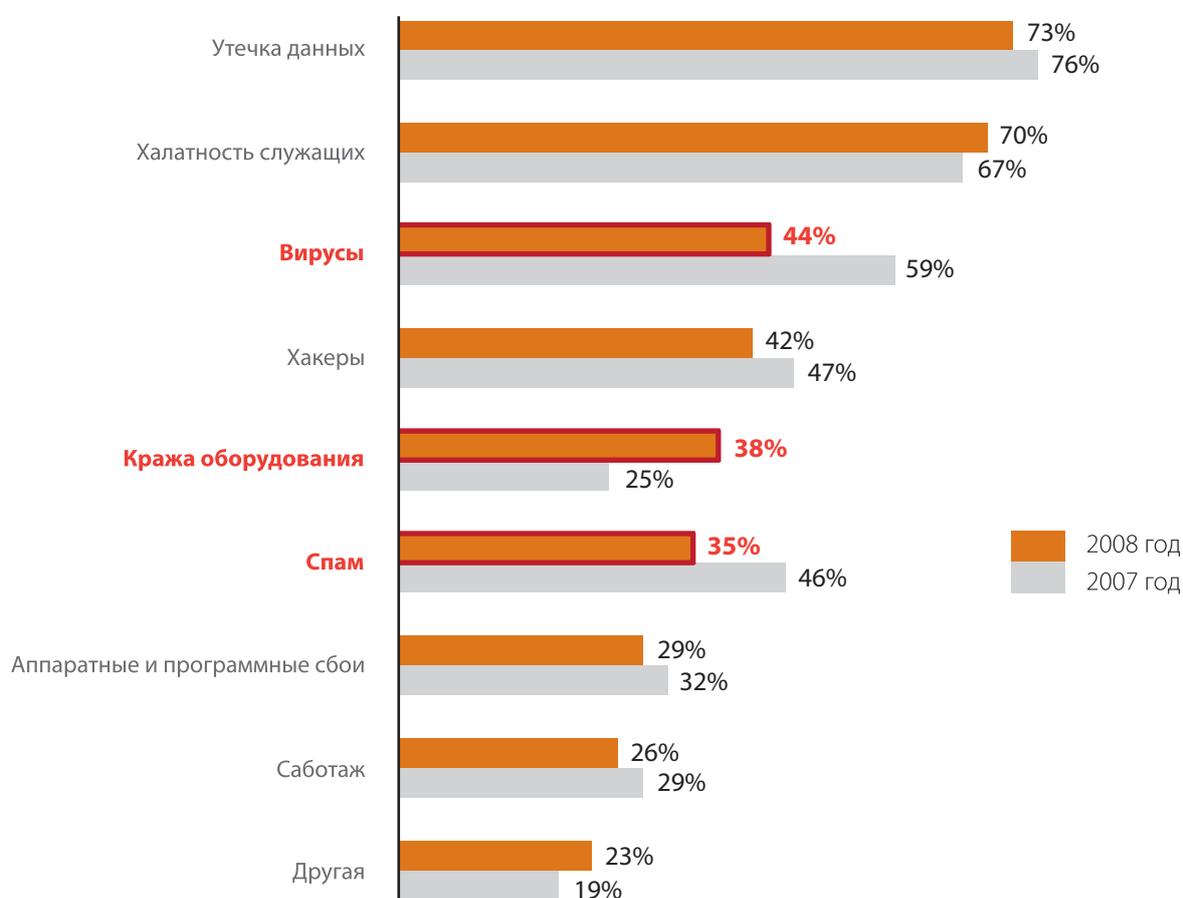


Рисунок 4. Наиболее опасные угрозы ИБ\* (возможно выбрать до четырех вариантов)

\* Здесь и далее наиболее явные тенденции отмечены красным

На самом деле, большая опасность внутренних угроз была заметна еще в прошлом году — угрозы утечки информации и халатности служащих опережали атаки внешних злоумышленников уже тогда. Этот долгосрочный тренд объясняется рядом вполне объяснимых причин — более высоким ущербом от внутренних утечек информации, меньшим проникновением средств защиты и принципиально новой постановкой задачи безопасности. За год ситуация кардинально не изменилась, однако приоритеты специалистов продолжили движение в сторону внутренних угроз, и потому опасность внешних угроз продолжила закономерно падать.

Среди остальных трендов выделим резкий рост опасности угрозы кражи оборудования (с 25 до 38%), которая также непосредственно связана с утечками информации. Действительно, в случае кражи любого носителя (флэшки, ноутбука и даже персонального компьютера или сервера) возникают существенные риски утечки. Рост опасности кражи оборудования можно объяснить как субъективными факторами (публикации в прессе, появление негативной аналитики\*), так и объективными тенденциями отрасли (внимание грабителей к циф-

ровым носителям, законодательное регулирование). Можно предположить, что опасность данной угрозы будет расти в дальнейшем, поскольку объективных факторов для ее покрытия на рынке пока не наблюдается.

Оставшиеся угрозы — аппаратные и программные сбои и саботаж — не дотянули до своего прошлогоднего уровня, но и не показали существенных трендов к снижению. Это означает, что требование непрерывности бизнеса по-прежнему остается приоритетным примерно для 30% современных компаний. Последний тезис, впрочем, не означает, что для оставшихся 70% респондентов данное требование не принципиально — для них важнее более явные угрозы, которые приводят организацию к явным материальным убыткам.

Отметим, что угрозы саботажа и аппаратно-программных сбоев чаще всего беспокоят крупные компании, ИТ-системы которых обрабатывают огромные масштабы информации. Даже незначительный простой подобных систем автоматически приводит их владельца к масштабным потерям и серьезной упущенной выгоде.

\* Например, по данным исследования Dell и Ponemon Institute «Airport Insecurity: The Case of Lost Laptops», 2008, только в крупнейших американских аэропортах теряется более 600 тыс. ноутбуков в год.

## ИНСАЙДЕРСКИЕ УГРОЗЫ

Следующая группа вопросов исследования касалась специфики угроз внутренней безопасности или инсайдерских угроз. На каждый из следующих трех вопросов респондентам предлагалось выбрать два наиболее подходящих ответа.

Как и в прошлом году, наиболее опасной угрозой внутренней ИБ была признана утечка информации, которую отметили более половины (55%) респондентов. Однако наибольший рост показала вторая по опасности угроза, связанная с искажением корпоративной (и преимущественно финансовой) документации. В нынешнем году ее опасность подскочила сразу на 17% и практически сравнялась с опасностью утечек информации.

По мнению аналитического центра Perimetrix, данная тенденция является значимой и объясняется целым рядом причин. Во-первых, в 2008 году произошел ряд громких инсайдерских скандалов, непосредственно связанных с искажением корпоративной документации и финансовым мошенничеством. Именно в эту категорию угроз можно отнести дей-

ствия трейдера Societe Generale Жерома Кервьеля, который привел свой банк к многомиллиардным убыткам, не имея на это никаких полномочий. Во-вторых, на ответы респондентов, скорее всего, повлиял мировой финансовый кризис и общая нестабильность современного бизнеса. В таких условиях несанкционированное искажение информации (и тем более, несанкционированные финансовые операции) могут привести бизнес к совершенно непредсказуемым последствиям.

И, в-третьих, рост обеспокоенности данной угрозой можно объяснить неспособностью современных решений с ней бороться. Если утечки конфиденциальной информации вполне реально отследить, то сделать это с несанкционированными искажениями значительно труднее — особенно если эти искажения вносятся санкционированным пользователем. На данный момент единственный способ борьбы с такого рода угрозами находится в плоскости логгирования и архивирования всех действий пользователей с конфиденциальными документами.

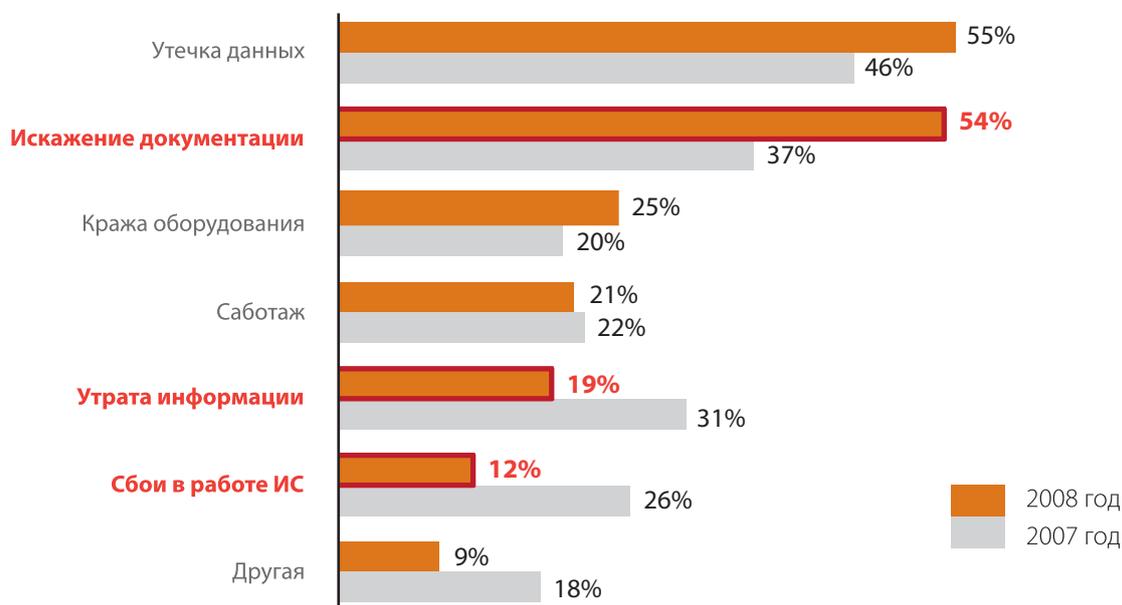


Рисунок 5. Наиболее опасные угрозы внутренней ИБ (возможно выбрать до двух вариантов)



Ситуация с оставшимися угрозами внутренней ИБ оказалась весьма предсказуемой — опасность кражи оборудования выросла, саботажа — почти не изменилась, а угроза утраты информации и сбоев резко упала. Падение опасности сбоев, скорее всего, связано с большим количеством DoS-атак, которые относятся к категории внешних, а не внутренних угроз. А резкое уменьшение опасности утраты информации объяснить труднее — по-видимому, ему способствовал рост проникновения различных систем резервного копирования.

Какая информация чаще всего «утекает» из российских компаний? Ответ на этот вопрос (рис. 6) практически не изменился по сравнению с прошлым годом — в группу особого риска по-прежнему попадают персональные данные, набравшие 68% голосов респондентов (на 11% больше, чем в год

назад). Впрочем, по мнению аналитического центра Perimetrix, данная тенденция говорит не о росте количества утечек персональных данных, а об обеспокоенности современных компаний за их защищенность.

Действительно, 2008 год ознаменовался усилением нормативного прессинга со стороны регуляторов рынка. За этот период времени появились сразу несколько подзаконных актов и постановлений, направленных на защиту именно персональных данных, как наиболее критичной категории конфиденциальной информации. Несмотря на то, что ряд участников рынка высказывают определенные сомнения в качестве и непротиворечивости этих актов, ужесточение нормативного прессинга наблюдается уже сегодня. Как следствие, растет и обеспокоенность компаний за сохранность обрабатываемых персональных данных.



Рисунок 6. Информация, наиболее подверженная утечке (возможно выбрать до двух вариантов)

Опасность утечки других категорий информации за последний год существенно не изменилась. Компании по-прежнему опасаются утечек сведений о деталях конкретных сделок (40%), финансовых отчетов (41%), интеллектуальной собственности и бизнес-планов (по 19%).

Похожая ситуация наблюдается и в отношении популярных каналов утечки (рис. 7), опасность которых осталась на прошлогоднем уровне. Наиболее опасным каналом по-прежнему остаются мобильные накопители (70%), за которыми следует электронная почта (52%) и интернет-каналы (33%). Опасность печатающих устройств за последний год несколько выросла (с 18 до 23%), а интернет-пейджеров, напротив, упала (с 17 до 13%).

В целом, говоря о каналах утечки, можно заметить слабый тренд к уравниванию их опасностей. Распределение нынешнего года оказалось чуть более равномерным, чем прошлогодние результаты — показатели наиболее опасных каналов незначительно упали, а «среднячков», напротив, выросли. Возможно, данная тенденция говорит о более четком понимании проблемы утечек, которую можно решить, только закрыв все возможные каналы — от мобильных накопителей до фото-принадлежностей. Ведь даже один незакрытый канал автоматически означает уязвимость, потенциальную угрозу безопасности и отличный шанс для злонамеренного инсайдера.



Рисунок 7. Самые популярные каналы утечки (возможно выбрать до двух вариантов)



Весьма интересные результаты были получены после анализа ответов на следующий вопрос — о количестве зафиксированных утечек (рис. 8). Если прошлогодние респонденты были уверены в своих ответах, то чуть ли не половина (42%) участников нынешнего опроса затруднилась назвать точное количество инцидентов.

Эксперты аналитического центра Perimetrix, объясняют полученные результаты ростом осведомленности специалистов и их профессиональным развитием. Специалист по безопасности может быть уверен в точном количестве утечек, только если в его компании развернуто сразу несколько специализированных систем защиты — а в большинстве случаев, та-

кого положения дел не наблюдается. В этом свете совершенно неудивительно, что в нынешнем году к респондентам пришло понимание собственной незащищенности в области защиты от внутренних угроз.

Если не учитывать последний вариант ответа и проинформировать данные по остальным вариантам, то можно сделать вывод о незначительном увеличении среднего количества утечек. Данный тренд логично объясняется общей канвой развития отрасли и наращиванием компетенции компаний в области информационной безопасности. За последний год защищенность компаний могла только увеличиться, а вместе с ней, выросло и количество обнаруженных утечек.

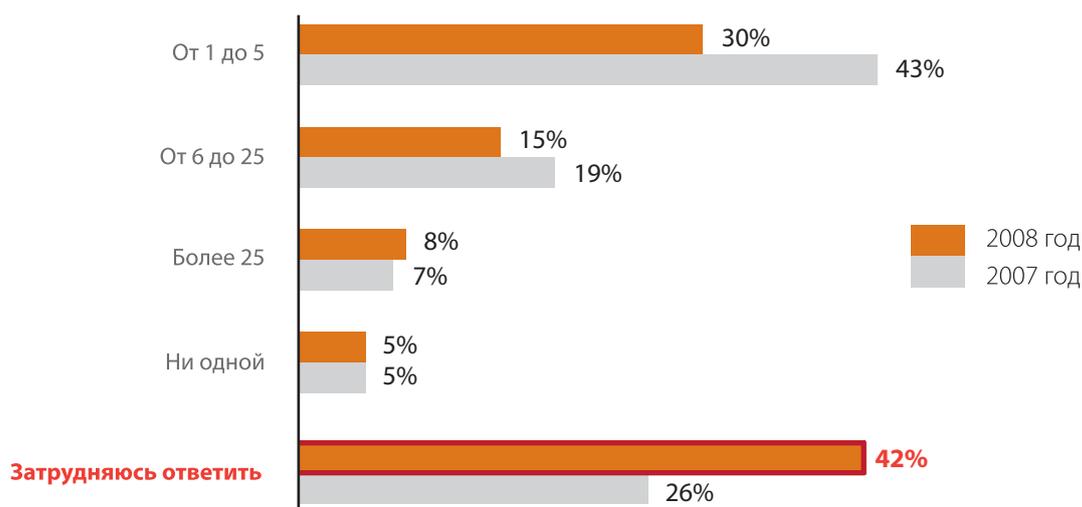


Рисунок 8. Количество утечек в 2008 году

## СРЕДСТВА ЗАЩИТЫ

После детального описания существующих угроз логично перейти к статистике используемых средств защиты. Их краткий список приведен на рис. 9.

Легко заметить, что абсолютно все респонденты используют в своей работе антивирусы, межсетевые экраны и те или иные средства контроля доступа.

Вслед за ними располагаются системы обнаружения/предотвращения вторжений (70%), антиспам-фильтры (75%) и инструменты для создания виртуальных частных сетей (63%). Отметим, что все перечисленные средства защиты направлены на защиту внешних угроз, опасность которых (как следует из предыдущего раздела), неуклонно падает.

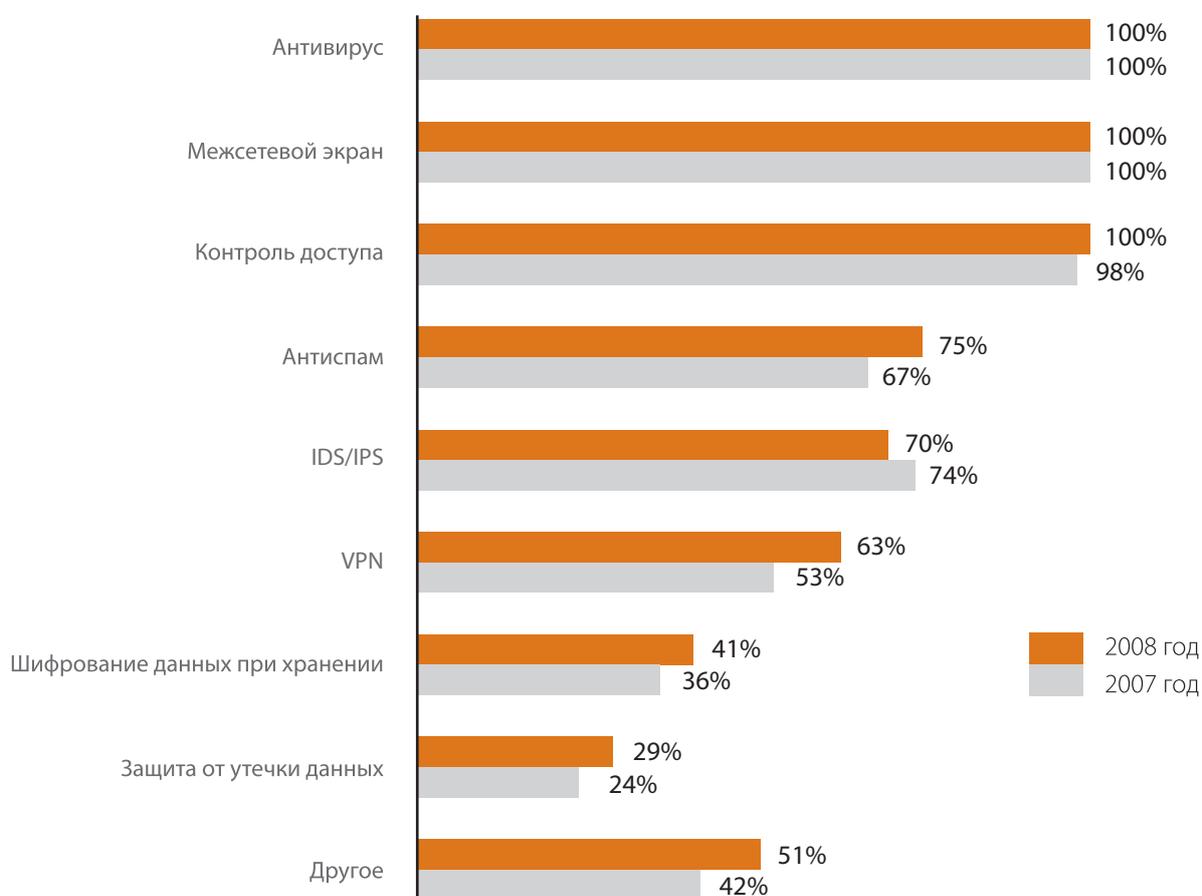


Рисунок 9. Самые популярные средства ИБ (возможно выбрать неограниченное число вариантов)

Впрочем, и резкого роста популярности решений для внутренней защиты в нынешнем году не случилось. Проникновение криптографических продуктов и специализированных систем защиты от утечек осталось примерно на том же уровне. Несмотря на огромную актуальность внутренних проблем, компании не спешат приобретать продукты, которые представлены на современном рынке.

Почему же ожидаемый скачок так, по сути, и не случился? Сегодня существует сразу несколько ответов на этот вопрос. Во-первых, большинство представленных на рынке продуктов имеют длительный цикл внедрения, и ожидать от них резкого роста проникновения бессмысленно. А во-вторых, на рынке систем защиты от утечек было ограничено предложение — больше половины года на нем присутствовал только один традиционный игрок (InfoWatch). Компания Perimetrix официа-

льно представила свой продукт только в сентябре 2008 года, а западные вендоры (Symantec, Websense и др.) вели весьма пассивную политику и концентрировались на продвижении других классов продуктов.

Среди систем внутренней безопасности по-прежнему лидируют решения на базе контентной фильтрации, которые используют 80% компаний, решившихся внедрить системы защиты от утечек. По сравнению с прошлым годом, доля контентной фильтрации упала с 89 до 80%, что косвенно говорит о неэффективности данной технологии. Вместе с контентной фильтрацией компании используют пассивный мониторинг (77%), а также внедряют контроль использования портов рабочих станций (75%). Один из наиболее действенных методов защиты — шифрование ноутбуков — постепенно, хотя не слишком быстро, набирает популярность.

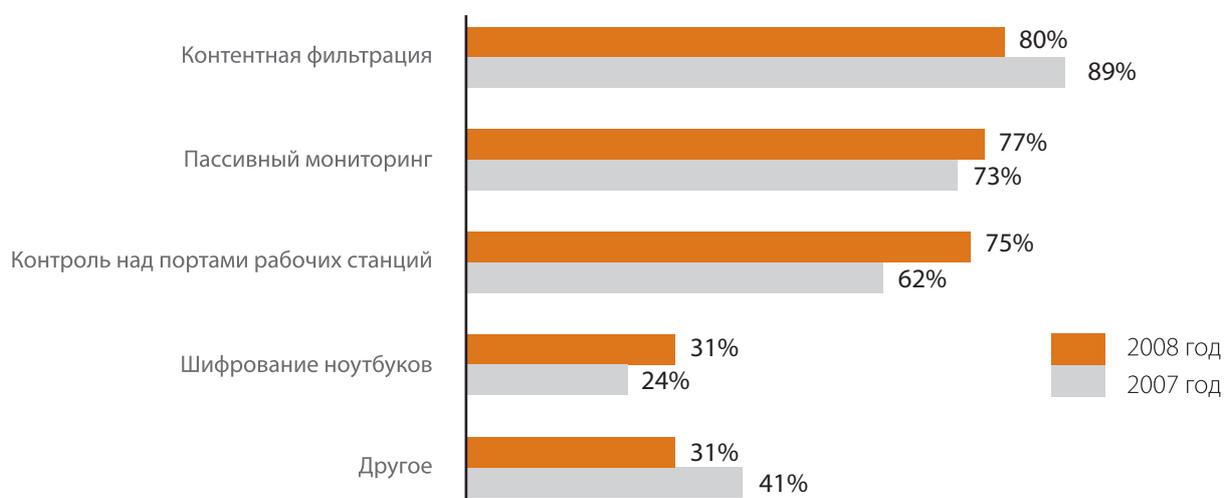


Рисунок 10. Самые популярные средства защиты от утечек (возможно выбрать неограниченное число вариантов)\*

\* Среди респондентов, внедривших средства защиты от утечек



Чтобы обрисовать краткосрочные перспективы развития рынка, обратимся к вопросу о наиболее актуальных препятствиях к внедрению систем защиты (рис. 11). Структура этих препятствий в нынешнем году серьезно поменялась — на первое место вышли бюджетные ограничения, доля которых выросла практически в два раза, с 26 до 46%. Причина данной тенденции непосредственно связана с кризисом ликвидности и банальной нехваткой свободных денег среди компаний-заказчиков.

Вместе с тем, потенциальные заказчики не слишком довольны и эффективностью представленных на рынке решений. По-видимому, значительное падение доли (с 49 до 35%) не говорит о росте эффективности решений и объясняется «кризисным» перераспределением голосов респондентов в сторону других ответов. Таким образом, перед вендорами по-прежнему стоят масса нерешенных задач в области создания более качественных продуктов.



Рисунок 11. Препятствия на пути внедрения защиты от утечек данных

На основании полученной статистики можно делать выводы о перспективах дальнейшего развития российского рынка систем защиты от утечек информации. По мнению аналитического центра Perimetrix, в ближайшем году этот рынок будет устойчиво, но не слишком быстро расти. Благодаря незащищенности компаний и низкому проникновению систем защиты, спрос на подобные решения будет достаточным большим, а предложение — ограниченным. Новые игроки рынка вряд ли сумеют за ближайший год раскрутить маховик продаж, а старые — не смогут реализовать много технологически отсталых продуктов. К негативным

факторам необходимо также отнести влияние кризиса и падение платежеспособности потенциальных заказчиков.

Однако в среднесрочной перспективе (2-3 года) на рынке должен произойти резкий скачок вперед. Спрос на системы безопасности не будет к этому времени удовлетворен, на рынке начнут полноценно работать новые игроки, влияние кризиса постепенно сойдет на нет, и у заказчиков появятся свободные ресурсы. Не стоит забывать и об ужесточении регулирующих мер государства, которые также приведут к стимулированию спроса на комплексные защитные системы.



## КЛАССИФИКАЦИЯ ДАННЫХ

Ряд вопросов исследования касался технологических аспектов защиты от внутренних угроз. Как и в прошлом году, респондентам был предложен вопрос о классификации данных и использовании этого процесса при обеспечении информационной безопасности организации. Напомним, что результаты прошлого опроса наглядно показали, что:

- Классификация данных помогает усилить безопасность в целом и защиту от утечек в частности;
- Проводить классификацию данных достаточно трудно — это требует вовлечения едва ли не всех сотрудников организации;
- Однако еще труднее поддерживать классификацию в актуальном состоянии по прошествии какого-то времени.

Все перечисленные тезисы являются универсальными и практически не зависят от времени. Поэтому респондентам нынешнего исследования не задавались вопросы о пользе классификации, которая и так практически всем очевидна. Вместо этого, аналитический центр Perimetrix снова спросил специалистов, насколько давно они проводили классификацию корпоративных данных?

Полученные ответы обнадеживают, особенно в сравнении с прошлогодними результатами. Количество компаний, проводивших классификацию в течение прошедшего года, выросло практически в два раза, достигнув психологической отметки в 25%. При этом, правда, нельзя забывать, что столько же компаний провели классификацию данных более трех лет назад, а 33% организаций вообще никогда ее не проводили.

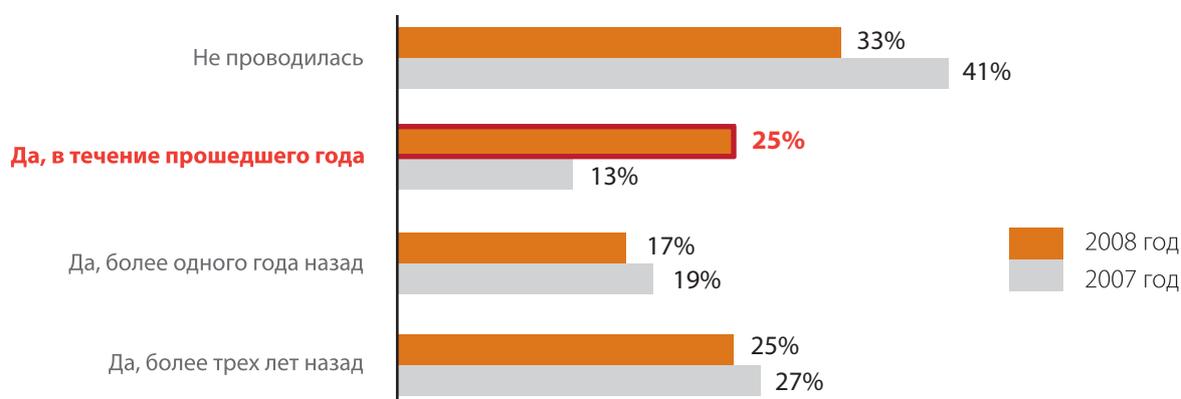


Рисунок 12. Проводилась ли в вашей компании классификация данных?

## ШИФРОВАНИЕ ДАННЫХ

В рамках настоящего исследования респондентам предлагались несколько новых вопросов о внутренней ИТ-безопасности. Специалисты, подтвердившие использование систем криптографической защиты, могли указать, каким конкретно образом применяется эта защита.

Как выяснилось, в большинстве (68%) случаев она применяется для защиты различных баз данных и хранилищ конфиденциальной информации. Такой подход является обязательным требованием ряда

отраслевых актов и стандартов (например, стандарта PCI DSS), однако он практически никак не защищает компанию от внутренних угроз безопасности.

Действительно, шифрование баз данных способно обеспечить защиту в случае физической кражи носителей, но в подавляющем большинстве случаев эти носители располагаются в серверах, которые, в свою очередь, находятся в защищенных дата-центрах. Проникнуть туда трудно, а украсть оборудование — еще труднее.



**Рисунок 13.** Каким образом используется шифрование в вашей компании (возможно выбрать неограниченное число вариантов)\*?

С точки зрения бизнеса значительно логичнее шифровать не базы данных, а мобильные носители — ноутбуки, флэш-накопители и портативные диски — поскольку именно эти носители часто теряются или становятся мишенью грабителей. Шифрование ноутбуков топ-менеджеров, содержащих особенно секретную информацию, применяется в 40% случаев, а шифрование мобильных носителей по запросу от пользователя — в 36%. Отметим, что ни тот, ни другой способ не дает 100% га-

рантии, поскольку пользователь устройства может забыть зашифровать информацию или не сделать это умышленно.

Комплексную защиту может обеспечить лишь принудительное прозрачное шифрование информации на всех ноутбуках и мобильных носителях. Однако эта технология на сегодняшний день является слишком сложной — ее применяют лишь 1% современных компаний.

\* Среди компаний, использующих системы шифрования данных

## ОТВЕТСТВЕННОСТЬ НАРУШИТЕЛЯ ВНУТРЕННЕЙ ИБ

Еще одной интересной темой нынешнего исследования стала ответственность нарушителей внутренней безопасности. В рамках опроса респондентам предлагалось описать карательные меры, которые применяются к халатным сотрудникам и злонамеренным инсайдерам.

Как выяснилось (рис. 14), в случае случайной утечки информации сотруднику редко грозят серьезные санкции типа увольнения (9%) или материального взыскания (13%) — в большинстве случаев (45%) компании предпочитают простить сотрудника, сделав ему строгий выговор. Отметим, что в 15% случаев инсайдеры и вовсе остаются безнаказан-

ными, а 11% компаний принимают меры в зависимости от тяжести потерянной информации.

Ситуация со злонамеренными инсайдерами во многом аналогична — как и в случае халатных сотрудников, компании редко идут на самые жесткие меры (рис. 15). В большинстве случаев (51%) инсайдера попросту увольняют, а вернее — побуждают его написать заявление об уходе по собственному желанию. До судебного разбирательства дело доходит крайне редко (9%), поскольку компании резонно предпочитают не выносить сор из избы. Понятно, что громкие инсайдерские скандалы привлекают внимание прессы и негативно влияют на репутацию компаний.

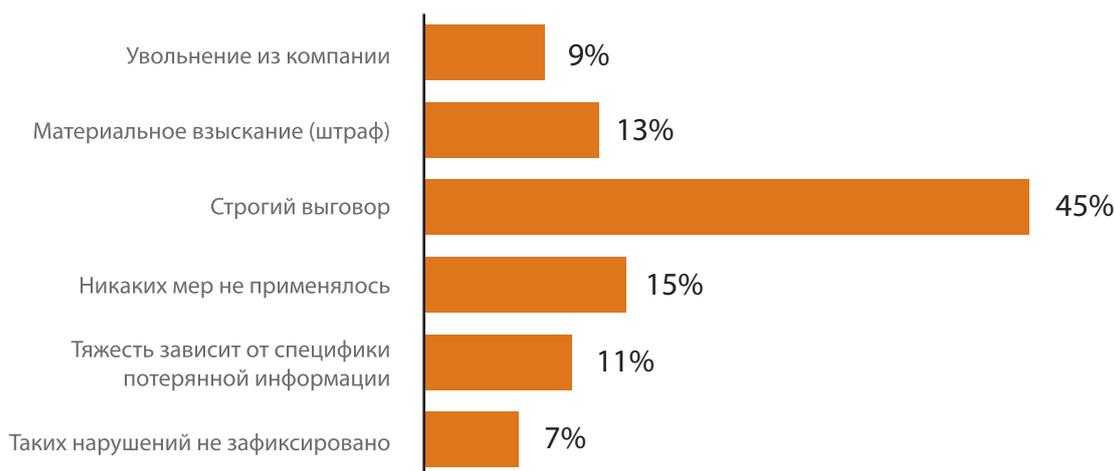


Рисунок 14. Какие меры обычно применяются к сотрудникам, допустившим случайную утечку информации?



**Рисунок 15.** Какие меры обычно применяются к сотрудникам, допустившим **спланированную** утечку информации?

Таким образом, и халатные, и злонамеренные инсайдеры, как правило, остаются практически безнаказанными. Для первой категории нарушителей утечка, скорее всего, обернется легким испугом, а для

второй — увольнением с работы и, может быть, подрывом деловой репутации. Такие последствия вряд ли могут напугать нарушителя, что, в свою очередь, приводит к росту опасности инсайдерской угрозы.

## НАПРАВЛЕНИЕ РАЗВИТИЯ РЫНКА

В предыдущих разделах мы рассмотрели основные тенденции развития рынка внутренней безопасности. Если же говорить об ИБ-отрасли в целом, то именно внутренняя безопасность должна стать основным драйвером этого направления в течение ближайших трех лет.

На данный момент примерно 40% российских компаний (рис. 16) заявляют о планах внедрения защиты от утечек в течение ближайших трех лет. 35% организаций собираются внедрить криптографические системы для хранящихся данных, а еще 33% — системы управления информационной безопасностью. Следом располагаются системы контроля идентификацией и доступом, а также ИТ-системы физической безопасности.

Таким образом, сегодня можно выделить два основных вектора развития рынка. Первый из них смотрит в сторону внутренней безопасности, второй — в сторону интеграции разрозненных систем и построения единой управляющей инфраструктуры. Последняя задача особенно важна, поскольку в современных (и особенно крупных) компаниях используется целый зоопарк практически не связанных друг с другом систем защиты. Естественно, компаниям становится крайне тяжело всем этим зоопарком управлять.

Что же касается внутренней безопасности, то причины популярности данного вектора очевидны — компании стремятся построить адекватную защиту для до сих пор непокрытых угроз.



Рисунок 16. Планы по наращиванию систем ИБ в ближайшие три года

## ЗАКЛЮЧЕНИЕ

В целом настоящее исследование показало, что ситуация с внутренней безопасностью в российских компаниях по-прежнему остается весьма плачевной. Организации практически всех отраслей и размеров продолжают допускать утечки — только 5% респондентов заявили об отсутствии каких-либо инцидентов в течение последнего года. Вместе с тем, имеются и положительные тенденции — гораздо большее количество специалистов стали осознавать собственную незащищенность и уязвимость своей компании перед действиями инсайдеров.

Уровень проникновения систем защиты от внутренних угроз в течение 2008 года вырос, хотя и не слишком значительно. Больше половины компаний до сих пор пытаются бороться с утечками исключительно с помощью административных мер, не решаясь на внедрение технических системы защиты. Отметим, что не слишком значительный рост рынка отчасти объясняется ограниченным предложением и низким качеством доступных заказчикам продуктов.

Одним из негативных факторов, повышающих опасность внутренних угроз является слишком слабая ответственность нарушителей — халатные инсайдеры, как правило, наказываются строгим выговором, а злонамеренные — увольнением из компании без негативных записей в трудовой книжке. Нарушителям внутренней безопасности редко грозят серьезные санкции, такие как судебные преследования или материальные взыскания.

По мнению аналитического центра Perimetrix, в течение ближайшего года рынок внутренней безопасности продолжить расти, однако не слишком быстро. Такая ситуация связана как с внешними факторами (финансовым кризисом), так и с внутренними реалиями рынка (прежде всего, ограниченностью предложения и ресурсов вендоров). Высокий спрос на комплексные системы защиты, впрочем, имеется уже сегодня, однако он будет реализован только спустя два-три года, по мере стабилизации финансовой ситуации и активного развития новых игроков.

## О КОМПАНИИ PERIMETRIX

Компания Perimetrix разрабатывает уникальные решения для реализации режима секретности конфиденциальности данных. В отличие от конкурентов Perimetrix концентрирует свой потенциал, инновационный подход и уникальный опыт на создании корпоративной платформы внутренней информационной безопасности и интеграции с актуальными бизнес-процессами, организационной и технологической инфраструктурой заказчика. Наша цель — повышение стоимости бизнеса заказчиков за счёт поддержания непрерывности бизнес-процессов, минимизации риска утечки, повышения конкурентоспособности, а также установления плодотворных отношений с инвесторами и партнерами, соответствия государственным требованиям.

Благодаря реализации революционной концепции Secret Documents Lifecycle Perimetrix обеспечивает защиту секретных документов на всех этапах жизненного цикла, мониторинг каналов коммуникаций и аудит электронных операций. Технологическая основа системы — знание объекта защиты, контроль доступа и действий пользователей с целью предотвращения нарушения корпоративной политики.

Компания основана в 2007 году командой профессионалов, стоявших у истоков создания современных систем защиты от внутренних угроз информационной безопасности, и входит в Группу компаний «КомпьюЛинк» — лидирующий альянс на российском рынке информационных технологий.

## О МЕДИА-ПАРТНЕРАХ



[www.inside-zi.ru](http://www.inside-zi.ru)

## О ЖУРНАЛЕ «ЗАЩИТА ИНФОРМАЦИИ. ИНСАЙД»

«Защита информации. Инсайд» — единственный в России информационно-методический журнал в области защиты информации. Издание содержит оперативную информацию о значимых событиях и мировых тенденциях на рынке защиты информации, комментарии о новых продуктах и технологиях, вопросы формирования методического аппарата для решения проблем, связанных с защитой информации, а также сведения о регулировании российского рынка и актуальные интервью. Журнал «Защита информации. Инсайд» выходит шесть раз в год.



[www.security-practice.ru](http://www.security-practice.ru)

## О КОМПАНИИ «ПРАКТИКА БЕЗОПАСНОСТИ»

«Практика Безопасности» — консалтинговое бюро по информационной безопасности. Основной специализацией компании является построение систем информационной безопасности «под ключ» для любых предприятий, где есть сложные IT-процессы, конфиденциальная информация и персональные данные.

«Практика Безопасности» сфокусирована на процессном подходе к построению систем управления информационной безопасностью. Команда бюро состоит из опытных консультантов-практиков, способных решить любые вопросы информационной безопасности для процветания бизнеса клиента.

Результат работы «Практики безопасности» — современная система менеджмента информационной безопасности, которая эффективно противостоит угрозам и не требует неоправданных затрат.



[www.econbez.ru](http://www.econbez.ru)

## О ЖУРНАЛЕ «ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ»

Информационно-аналитический журнал, приоритетной задачей которого является своевременное и объективное информирование читателя о наиболее значимых событиях, имеющих отношение к проблемам экономической безопасности и суверенитета России. Издание поможет руководителям предприятий и организаций выбрать законные средства и способы обеспечения экономической безопасности как компании в целом, так и отдельной личности, как субъекта экономических отношений.





[www.anti-malware.ru](http://www.anti-malware.ru)

#### О ПОРТАЛЕ ANTI-MALWARE

Anti-Malware.ru — первый в России независимый информационно-аналитический портал, посвященный программным средствам защиты от вредоносных программ.

Портал основывается на сильном сообществе экспертов и профессионалов в области информационных технологий и информационной безопасности, участвующих в во всех аспектах жизни портала.

Anti-Malware.ru был основан в 2005 году и за время своего существования добился широкого признания среди большого числа экспертов и профессионалов в области информационной безопасности.

Одним из основных принципов работы Anti-Malware.ru является равноудаленность от всех участников рынка. Администрация портала стремится в равной мере освещать все представленные на российском рынке продукты. Объективно проводить тестирования, сравнения и обзоры различных программ, а также методов защиты от всех видов современных угроз, которые попадают под определение «malware».



[www.bankir.ru](http://www.bankir.ru)

#### О ПОРТАЛЕ BANKIR.RU

Главное направление деятельности Банкир.Ру — активное участие в развитии банковского бизнеса в России, улучшение качества и расширение спектра финансовых услуг клиентам российских банков. Мы считаем, что банковская система РФ должна и может быть конкурентоспособна по отношению к ведущим мировым финансовым системам. Наша цель — продвижение и развитие банковского дела в России, повышение квалификации банковского персонала.

Развитие банковского рынка зависит не только от деятельности государственных органов управления и Центрального Банка РФ, но и не в последнюю очередь от самих кредитных организаций, от их понимания законов развития бизнеса, от намерений расширения деятельности. Коммерческие банки, банковские ассоциации и союзы, Центральный Банк РФ должны объединить усилия для достижения общих целей, наладить конструктивный диалог, способствовать профессиональному росту специалистов банковского дела.

На сайте Банкир.Ру любой посетитель найдет ответ на интересующий его вопрос по банковской деятельности и не только; познакомится с последними новостями, аналитическими материалами и интересными людьми; узнает много нового и интересного о действующих кредитных организациях; сможет найти новое место работы или подобрать квалифицированного специалиста для работы в банке.

**InformationSecurity**  
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

[www.egovernment.ru](http://www.egovernment.ru)

#### О ЖУРНАЛЕ INFORMATION SECURITY/ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Журнал «Information Security/Информационная безопасность» — продолжает серию печатных изданий: журналов и каталогов, издаваемых компанией «Гротек». Тема журнала — информационная безопасность и все, что с ней связано. По мере развития IT технологий, проблема их безопасного использования становится год от года все актуальнее. Вот почему главной задачей журнала «Information Security/Информационная безопасность» является ориентирование потребителя в море новых решений в этой области.

Ядро издания составляют технические обзоры, тесты новых продуктов, а также описания комплексных интегрированных решений, внедренных в России в коммерческих структурах и в государственных организациях. Авторы журнала — сотрудники основных фирм-участников рынка безопасности, среди которых как производители, авторы решений в области безопасности, так и потребители. Журнал «Information Security/Информационная безопасность» — это профессиональный взгляд на отрасль. С его помощью потребители узнают о новейших решениях в области безопасности, о тенденциях рынка и его проблемных вопросах; ознакомятся с расчетами информационных рисков в различных сферах промышленности, банковской и финансово-кредитной сферы Российской Федерации.

Издание выходит тиражом 10000 экземпляров и распространяется по модели B2B (business-to-business). Основная аудитория журнала это руководители служб связи и IT, безопасности, финансов крупных и средних компаний разных отраслей, а также государственных и контролирующих органов. География распространения журнала охватывает пространство от Москвы и Санкт-Петербурга, до Урала, Сибири и Дальнего Востока.



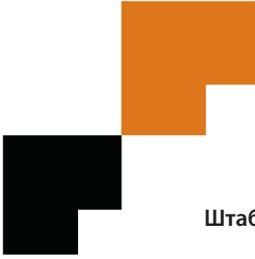


[www.securitylab.ru](http://www.securitylab.ru)

### О ПОРТАЛЕ SECURITYLAB.RU

SecurityLab.ru — информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях.

SecurityLab.ru единственный ресурс в русскоязычном Интернете, который оперативно публикует полную информацию обо всех опубликованных уязвимостях на русском языке, анализирует эту информацию и выдает конкретные рекомендации по ее устранению. Информация, представленная в этом разделе, позволяет оперативно и объективно оценить риски бизнеса, связанных с потенциальным взломом сетевой инфраструктуры и предпринимать соответствующие меры по минимизации этих рисков.



**Штаб-квартира Perimetrix**

Российская Федерация,  
119607, Москва,  
Мичуринский проспект, д. 45

Телефон: +7 495 737 99 91  
Факс: +7 495 737 99 92

[info@perimetrix.com](mailto:info@perimetrix.com)  
[www.perimetrix.com](http://www.perimetrix.com)

KEEPING SECRETS SAFE

