Е. Преображенский

ИНСАЙДЕРСКИЕ УГРОЗЫ В РОССИИ`09

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.

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.

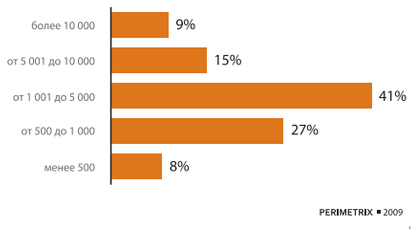
- В подавляющем большинстве случаев нарушители внутренней безопасности не несут практически никакой ответственности. 45% халатных нарушителей наказываются строгими выговорами, а 51% злонамеренных инсайдеров увольняются из компаний по собственному желанию.

- 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 1 000 компьютеров.

Рис. 1. Количество рабочих станций



Сдвиг получившейся выборки респондентов в сторону средних и крупных компаний позволяет получить актуальную картину рынка, поскольку именно 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 коробочные 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.

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 комплекс (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.

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

Рис.2. Сфера деятельности

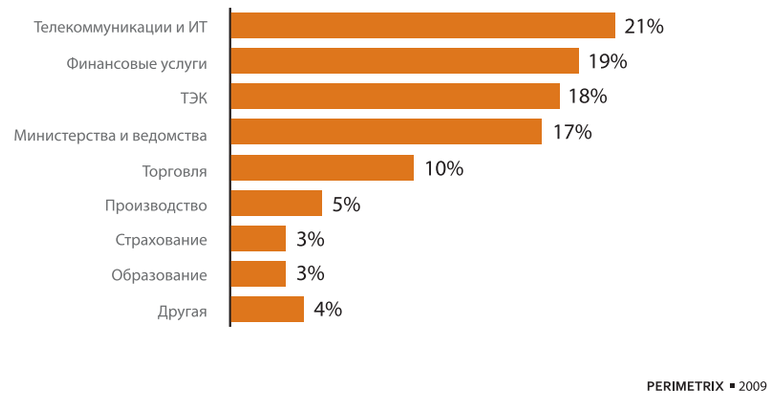
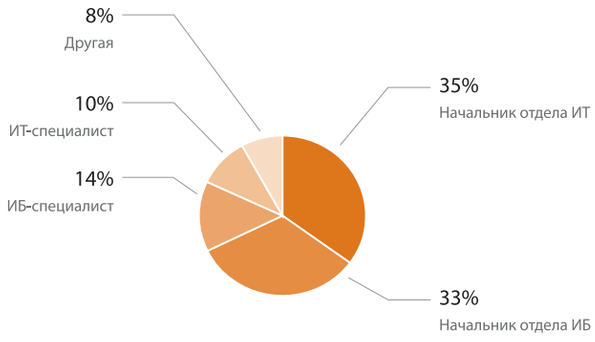


Рис. 3. Респонденты по должности



PERIMETRIX ▪ 2009

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.

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.

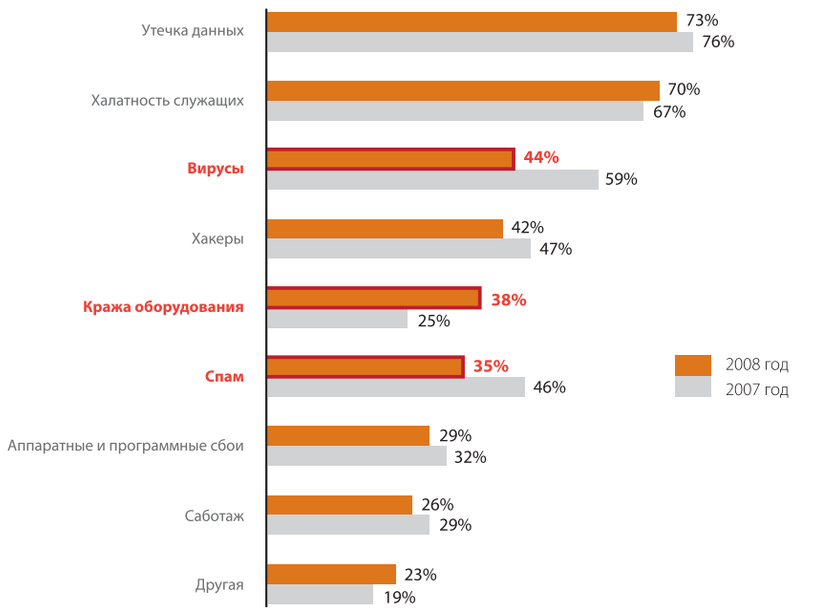
Из получившегося распределения вытекает ряд характерных тенденций.

Во-первых, самыми опасными 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.

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 цифровым носителям, законодательное регулирование). Можно предположить, что опасность данной угрозы будет расти в дальнейшем, поскольку объективных

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



PERIMETRIX ▪ 2009

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.

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 действия трейдера Societe Generale Жерома Кервьеля, который привел свой банк к многомиллиардным убыткам, не имея на это никаких полномочий.

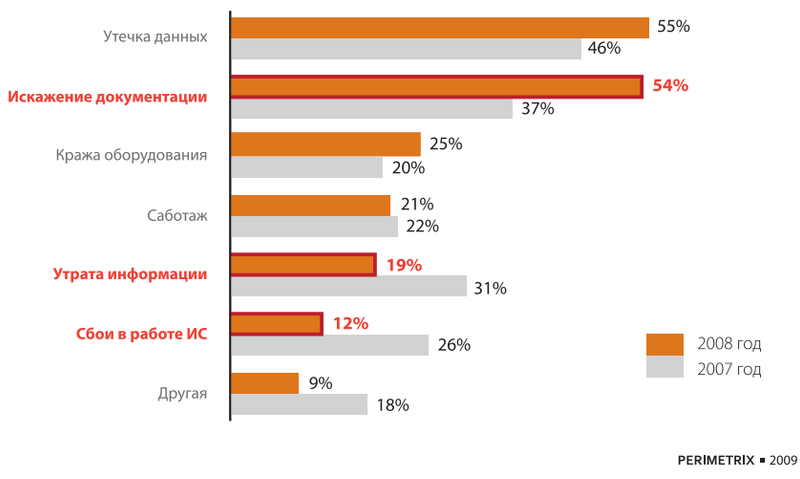
Во-вторых, на ответы респондентов, скорее всего, повлиял мировой финансовый кризис и общая нестабильность современного бизнеса. В таких условиях несанкционированное искажение информации (и тем более, несанкционированные финансовые операции) может привести бизнес к совершенно непредсказуемым последствиям.

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.

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.

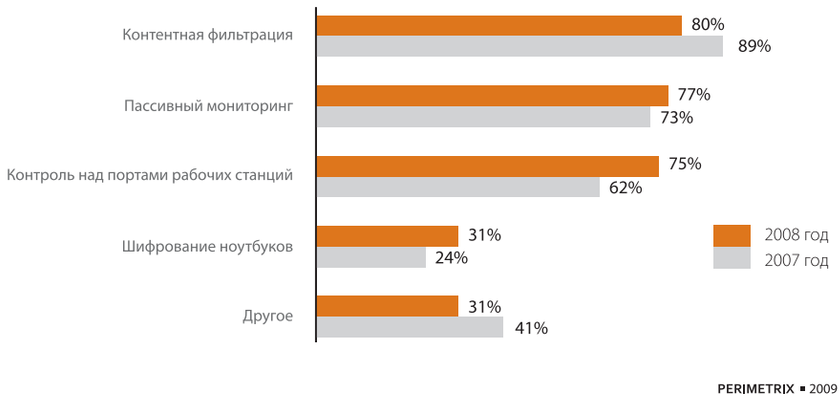
Рис. 5. Наиболее опасные угрозы внутренней ИБ *(возможно выбрать до двух вариантов)*



Информация, наиболее подверженная утечке
(можно выбрать до двух вариантов)

опасных каналов незначительно упали, а «середнячков», напротив, выросли. Возможно, данная тен-

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



зопасности 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.

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 стоит масса нерешенных задач в области создания более качественных продуктов.

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

Рис. 11. Препятствия на пути внедрения защиты от утечек данных

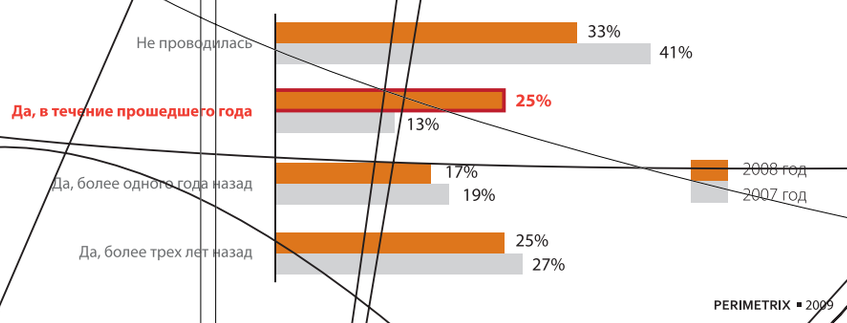
этого процесса при обеспечении информационной безопасности организации. Напомним, что результаты прошлого опроса наглядно показали, что:

- 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.

Проводилась ли в вашей компании классификация данных?



Шифрование данных

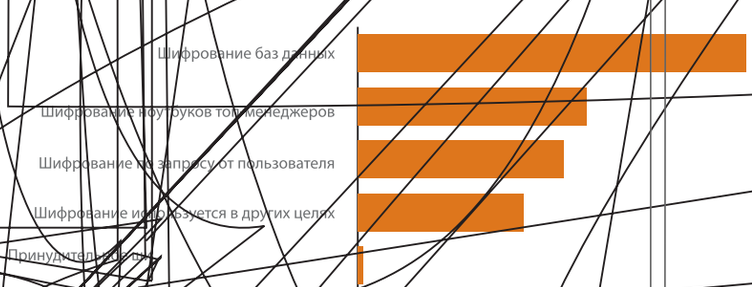
В рамках настоящего исследования респондентам предлагались несколько новых вопросов о внутренней ИТ-безопасности. Специалисты, подтвердившие использование систем криптографической защиты, могли указать, каким конкретно образом применяется эта защита.

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.

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% гарантии, 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 применяет лишь 1% современных компаний.



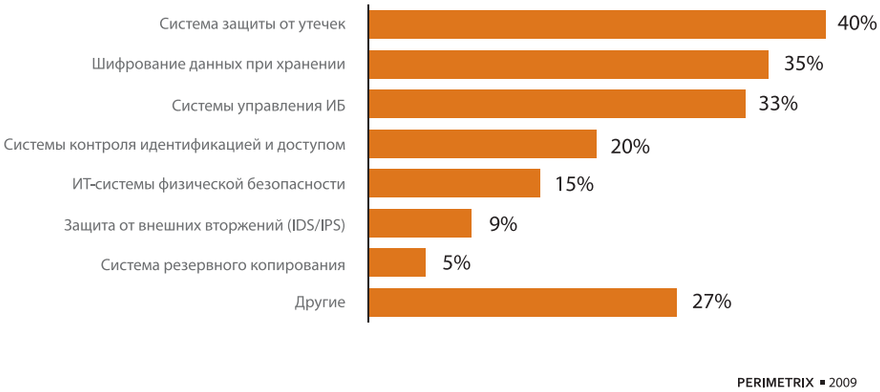
Направлени… развития …

В пре… щих ра…
рассмо… основн…
разв… рынка в…
па…и. Есл…
…расли в…
…тренняя…
направ…
ших…

…й выговор
…меняла

…выносит…
что…
…ндел…
…ор…м,
…ени…
…ост…

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



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.

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 технической 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 судебное преследования или материальные взыскания.

По мнению аналитического центра Perimetrix, в течение ближайшего года рынок внутренней безопасности продолжит 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.

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 года по 23 января 2009 года. В рамках исследования специалисты аналитического центра Perimetrix опросили сотрудников 1 046 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, Insidezi.ru) и сайта компании Perimetrix отвечали на вопросы утвержденной анкеты.

Perimetrix
Российская федерация,
119607,
Москва, Мичуринский проспект, д. 45
Телефон: +7 495 737 99 91
Факс: +7 495 737 99 92
info@perimetrix.com
www.perimetrix.com