



**INFOWATCH**  
INFORMATION WATCH TECHNOLOGIES

# ВНУТРЕННИЕ ИТ-УГРОЗЫ В РОССИИ 2006

Третье ежегодное исследование компании InfoWatch  
в области корпоративной защиты от внутренних угроз  
информационной безопасности

Москва — 2007

# Оглавление

Обращение генерального директора.....	3
Общие выводы.....	4
Методология.....	4
Портрет респондентов.....	5
Угрозы ИБ в России.....	8
Внутренние угрозы ИБ.....	10
Утечка конфиденциальной информации.....	12
Нормативное регулирование.....	15
Средства защиты.....	16
Открытый вопрос.....	20
Заключение.....	21
О компании InfoWatch.....	22

# Обращение генерального директора



## Уважаемые дамы и господа!

Компания InfoWatch представляет вашему вниманию результаты третьего ежегодного исследования проблемы внутренней ИТ-безопасности в России. В этом уникальном по своим масштабам проекте приняли участие 10 компаний, входящих в партнерскую сеть InfoWatch, 5 ведущих отраслевых СМИ и 3 популярных ресурса Интернета, а также несколько десятков клиентов InfoWatch. В результате нам удалось существенно расширить базу респондентов и опросить почти 1,5 тыс. российских компаний.

Отметим, что такое внимание к проблеме внутренней ИТ-безопасности неслучайно. В течение всего 2006 года сообщения об утечках, случаях саботажа и других внутренних нарушениях не сходили с первых полос СМИ. За прошедшие 12 месяцев в базе инцидентов InfoWatch появились почти 200 новых записей. Причем многие из них у всех на слуху. Это базы данных российских банков, белорусских сотовых операторов, хостинг-провайдеров и т.д.

На этом плохие новости, к сожалению, не заканчиваются. Как известно, внутренние инциденты часто приводят к утечке персональных или конфиденциальных данных. Однако из года в год убытки от каждого из этих видов утечек растут на 20-25%. По оценкам аналитического центра InfoWatch, в 2006 году одна лишь экономика США потеряла более 60-65 млрд. долларов вследствие утечек частных сведений. Аппроксимируя этот результат в глобальном масштабе, можно утверждать, что общемировой ущерб от этих инцидентов составляет около 500 млрд. долларов. Между тем, это лишь одна сторона медали, так как не учтенной осталась еще одна угроза – утечка конфиденциальной информации. Исходя из собственного опыта расследования инсайдерских инцидентов, аналитический центр InfoWatch по итогам года оценивает совокупные потери мировой экономики из-за утечки коммерческих секретов в 175 млрд. долларов. Таким образом, все вместе оба вида утечек обходятся ежегодно почти в 700 млрд. долларов. Однако уже в следующем году с учетом инфляции и ежегодного роста убытков на 20-25% эта цифра может превысить 1 трлн. долларов.

Но не будем сгущать краски. На фоне всех отрицательных тенденций есть целый ряд положительных событий. Во-первых, как показало наше исследование, число российских компаний, внедривших системы защиты от утечек, возросло почти в 5 раз за последний год. Этот неудовлетворенный спрос компания InfoWatch почувствовала на себе. Во-вторых, в нашей стране наконец-таки появился закон «О персональных данных». Это лишь первый, но самый трудный шаг, с помощью которого России удастся упорядочить оборот частных сведений граждан. Таким образом, компания InfoWatch с оптимизмом смотрит в будущее. У нас есть все основания полагать, что эффективно защититься от внутренних угроз вполне реально. Более того, наша цель как раз и состоит в том, чтобы помочь в этом российским компаниям.

A handwritten signature in black ink, appearing to be 'Evgeniy Preobrazhenskiy'.

Евгений Преображенский  
Генеральный директор

## Общие выводы

- Обеспокоенность внутренними угрозами ИБ среди российских организаций достигла апогея. Например, индекс опасности утечки информации на 50% опережает аналогичный показатель для любой из внешних угроз.
- Госструктуры и представители частного сектора поставили на первое место утечку информации далеко не случайно. Они отчетливо осознают все отрицательные последствия этого инцидента: прямые финансовые убытки (46%), удар по репутации (42,3%) и потерю клиентов (36,9%).
- Организации начинают присматриваться к своим служащим все пристальнее и пристальнее. Более 40% респондентов уже зафиксировали за 2006 год более одной утечки, а почти 20% - более 5 утечек.
- Доля организаций, внедривших защиту от утечек, возросла за последний год на 500% или в 5 раз. Положительная динамика налицо и это не может не радовать.
- В то же самое время говорить о массовом внедрении не приходится. Пока лишь каждый десятый внедрил эффективное решение на основе ИТ, однако девять из десяти планируют это сделать в ближайшие 2-3 года.
- Есть все основания полагать, что проникновение систем защиты от утечек на российский рынок продолжится и дальше, причем затронет абсолютно все отрасли экономики. Мы находимся на пороге экспоненциального роста данного сегмента.

## Методология

В процессе исследования, в период с 15.11.2006 по 15.01 2007 г., были опрошены представители 1450 государственных и коммерческих организаций Российской Федерации.

Опрос проводился среди заказчиков InfoWatch и клиентов крупнейших системных интеграторов, входящих в партнерскую сеть компании: Энвижн Групп, Ай-Теко, Amphora Group, РусТим, Форус, Эльбрус-2000, LETA IT-company, PolyGor Group, ЮСК, ICL - КПО ВС. Кроме того, в исследовании приняли участие читатели ведущих отраслевых СМИ: «Национального Банковского Журнала», «Вестника Связи», журнала «Мировая энергетика» и «Автоматизация в промышленности», а также представители бизнеса, подписавшиеся на журнал «Экспресс-Электроника». Таким образом, удалось существенно расширить базу респондентов, приходящуюся на банковский сектор, сегменты телекоммуникаций и ИТ, ТЭК, промышленность. Результаты исследования внутренней ИБ в каждом из этих сегментов, а также в госсекторе будет доступно в виде отдельных отраслевых отчетов. Наконец, в сборе первичных данных приняли участие известные в Интернете проекты – Банкир.Ру, SecurityLab.ru и VirusList.ru, благодаря которым также удалось существенно расширить базу респондентов.

Планирование исследования и обработка исходных данных из множественных источников были проведены маркетинговым агентством Rosencrantz & Guildenstern. По инициативе агентства в анкету было включено несколько открытых вопросов, что позволило получить интересные, но совершенно неожиданные ответы.

Сама анкета была составлена аналитическим центром InfoWatch на основе вопросов, предлагавшихся респондентам в 2005 и 2004 годах при проведении исследования по внутренним угрозам информационной безопасности (ИБ). Это позволило проследить динамику изменения ответов за прошедшие 3 года. Между тем, эксперты InfoWatch добавили несколько новых вопросов относительно нормативного регулирования, чтобы в полной мере отследить ситуацию, сложившуюся в области внутренних угроз в России. Опрос проходил непосредственно у самих респондентов, а также по Интернету. Для этого полевые сотрудники маркетингового агентства Rosencrantz & Guildenstern и системных интеграторов, входящих в партнерскую сеть InfoWatch, лично встречались с респондентами и проводили устное интервью, связывались по телефону и электронной почте. Кроме того, опрос аудитории ресурсов Интернета проходил посредством online-анкеты, размещенной на сайтах InfoWatch, Банкир.Ру, SecurityLab.ru и VirusList.ru.

Приведенные ниже данные являются округленными до десятых процентов. В некоторых случаях сумма долей ответов превосходит 100% из-за использования многовариантных вопросов.

## Портрет респондентов

Аналогично исследованиям 2005 и 2004 годов, в данном опросе приняли участие высококвалифицированные специалисты — руководители и ведущие сотрудники отделов ИТ и ИБ. Совокупность участников, род их занятий, сфера деятельности компаний были подобраны таким образом, чтобы наиболее точно соответствовать генеральной совокупности. Все респонденты являются лицами, принимающими решения в области развития корпоративных информационных систем.

Анализ портрета респондентов по количеству сотрудников (рис. 1) показал, что наибольшая доля опрошенных организаций (28,7%) приходится на малый бизнес менее 500 сотрудников). Практически равные доли пришлись на компании с 500 - 1 000 служащих (11,4%) и 5 001 – 10 000 работников (10,3%). Вторая по численности группа респондентов попала в категорию 2 5001 – 5 000 сотрудников (25,8%), а третья на 1 001 – 2 500 служащих (16,7%). Наконец, наименьшее число респондентов – это представители очень крупного бизнеса и федеральных госструктур. На группу 10 001 – 50 000 работников пришлось 6,2%, а более 50 000 сотрудников всего в 0,9% опрошенных организаций.

Обратимся теперь к степени информатизации базы респондентов. Наибольшая по численности доля опрошенных организаций имеет от 251 до 1 000 рабочих станций (35,1%). Следующей идет группа с 1 001 – 5 000 терминалов (24,6%). Другими словами, большинство респондентов (59,7%) приходится на представителей бизнеса выше среднего. Между тем, доля очень крупных организаций составляет 7,2%. Из них 2,3% — это компании с числом рабочих станций более 10 000, а 4,9% - от 5 001 до 10 000 компьютеризированных мест. Наконец, на малый бизнес пришлась почти одна треть всех респондентов (33,1%). Среди них 18,4% составляют компании с числом терминалов от 101 до 250, а 14,7% с числом компьютеров менее 100. Таким образом, суммируя вышеуказанные два показателя, можно сделать вывод, что база респондентов данного исследования состоит преимущественно из представителей крупного бизнеса и сегмента, который можно охарактеризовать, как «выше среднего». Несмотря на это уровень репрезентативности, как малых, так и очень крупных предприятий остается достаточно высоким.

### КОЛИЧЕСТВО СОТРУДНИКОВ 2006 год

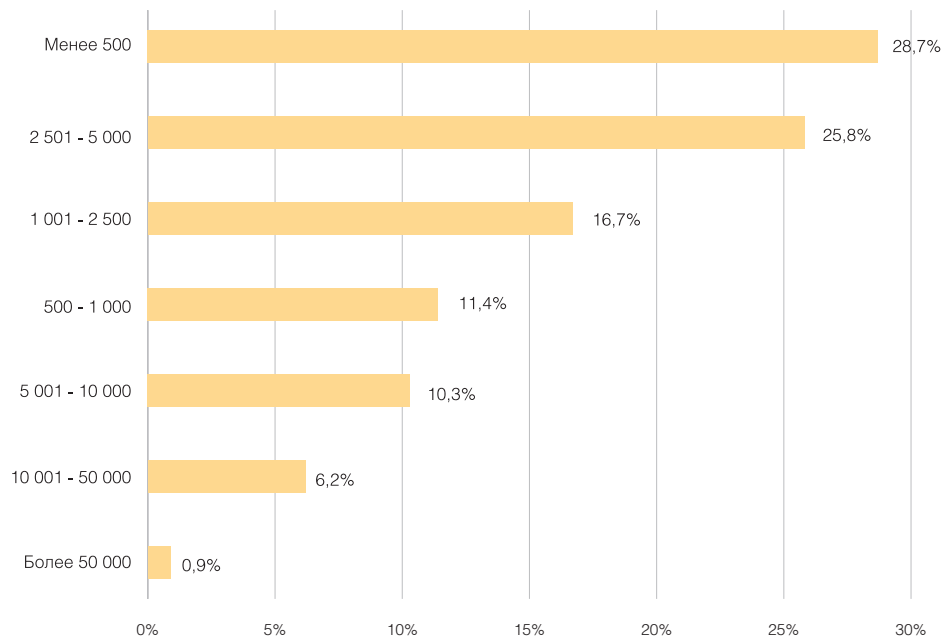


Рис. 1

INFOWATCH · 2007

### КОЛИЧЕСТВО РАБОЧИХ СТАНЦИЙ 2006 год

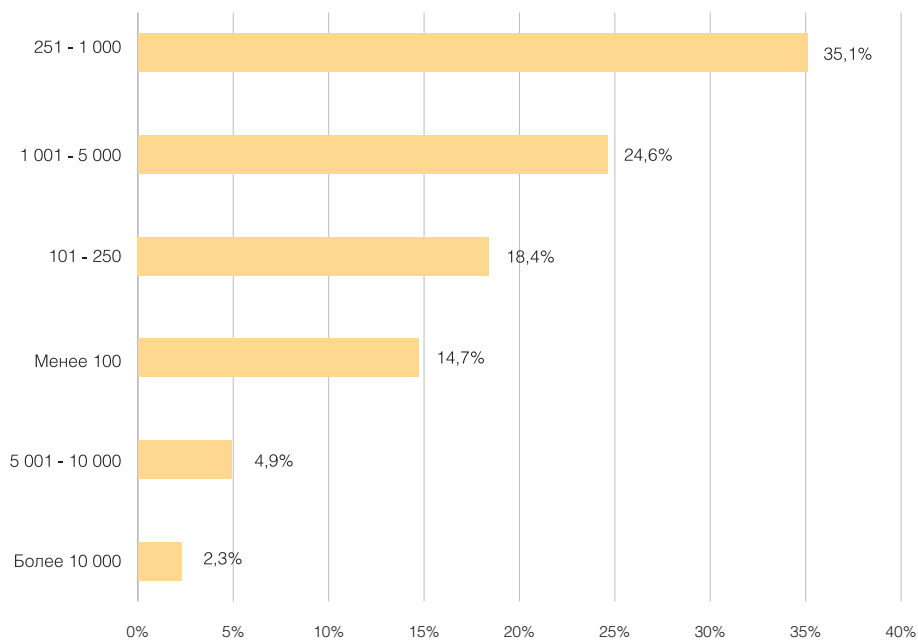


Рис. 2

INFOWATCH · 2007

С точки зрения сферы деятельности (рис.3) в группу лидеров вошли такие сектора экономики как финансовые услуги (21,5%), а также телекоммуникации и ИТ (18,9%). За ними следуют министерства и ведомства (13,2%), производство (12,7%), ТЭК (11,7%) и торговля (10,3%). Наконец, наименьшие доли пришлось на страхование (5,2%) и образование (4,4%).

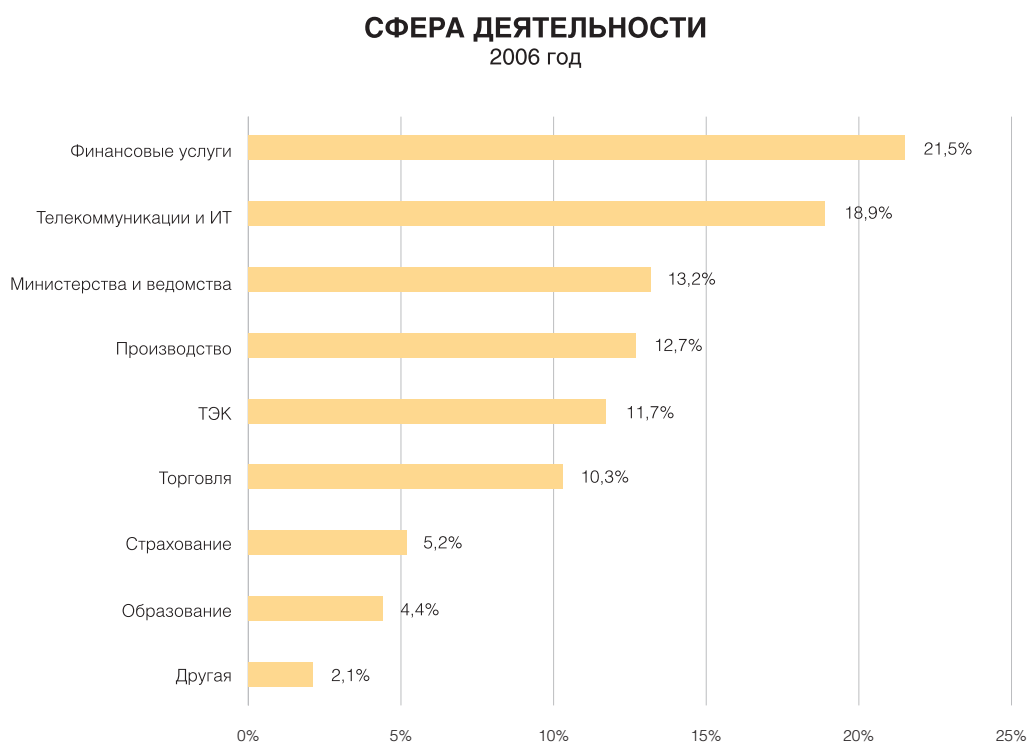


Рис. 3

INFOWATCH • 2007

Анализируя должности респондентов (рис. 4), следует отметить, что по сравнению с прошлым годом несколько снизились доли, приходящиеся на начальников отделов ИТ (40,2%) и ИБ (27,2%). Это вполне объяснимо, так как наличие выделенных служб ИТ и ИБ является признаком зрелости организации, поэтому при увеличении базы респондентов почти в 5 раз логично ожидать снижение зрелости компаний из генеральной совокупности. Между тем, некоторый рост наблюдается в категориях специалистов по ИТ (12,9%) и ИБ (19,3%).

Следует отметить, небольшой рост доли представителей ИБ в общей выборке. В прошлом году этот показатель равнялся 43%, а в этом достиг отметки 46,5%. Это говорит о том, что ИБ все чаще и чаще в российских компаниях становится обязанностью выделенных и квалифицированных специалистов, а не универсальных ИТ-служащих, на которых задачи защиты информации перекладываются в качестве второстепенных. Кроме того, повышение доли представителей ИБ может объясниться изменением структуры базы респондентов в сторону крупного бизнеса и предприятий размера выше среднего.

## РЕСПОНДЕНТЫ ПО ДОЛЖНОСТИ 2006 год

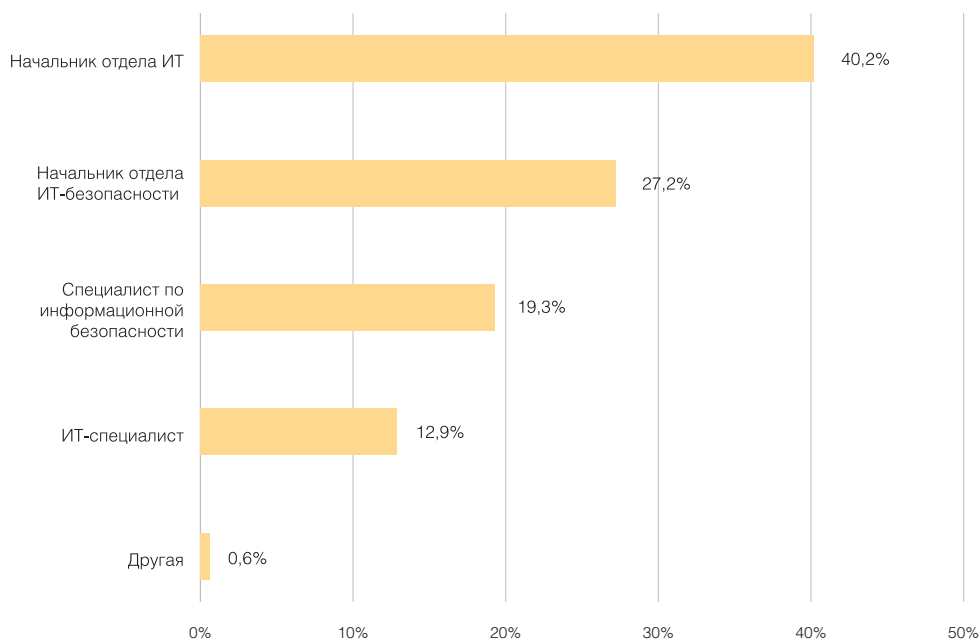


Рис. 4

INFOWATCH • 2007

## Угрозы ИБ в России

По сравнению с прошлым годом несколько изменился ландшафт самых опасных угроз ИБ (рис. 5). На первом месте по-прежнему остается кража информации (65,8%). Ее индекс опасности подрос на 1,8% по сравнению с 2005 годом и на 3,8% по сравнению с 2004 годом. Однако уже на втором месте оказалась халатность сотрудников (55,1%). Тем не менее, уже сейчас можно сделать ряд выводов. Например, вирусные атаки заняли лишь третье место, набрав 41,7% голосов. Если сравнивать с 2005 годом, то эта угроза потеряла целых 7,3 процентных пункта, а если с 2004 годом, то – сразу 18,3%. Вероятно, именно этот рейтинг опасности позволил такой угрозе, как халатность сотрудников, сразу же занять второе место в списке самых опасных угроз ИБ.

На четвертом месте оказалась угроза, которая тоже не входила в предыдущие исследования. Это саботаж (33,5%). Судя по всему, можно снова утверждать, что высокий рейтинг опасности саботажа обусловлен тем, респонденты постепенно теряют чувство страха перед внешними угрозами. Если в случае с халатностью служащих приводился пример снижения рейтинга вирусных атак, то в данном случае налицо потеря лидирующих позиций со стороны хакерских атак. Именно хакерские атаки занимают пятое место с 23,4% голосов. Другими словами, за прошедший год эта угроза потеряла 24,6 процентных пунктов, а за 2 прошедших года – 28,6%.

Таким образом, если пересчитать результаты предыдущего вопроса, разделив все ответы на внутренние и внешние угрозы, то легко видеть, что инсайдеры превалируют над вирусами, хакерами и спамом. Для построения следующей диаграммы (рис. 6) в категорию внутренних угроз были отнесены, халатность сотрудников, саботаж и финансовое мошенничество, а в категорию внешних угроз вирусы, хакеры и спам. После этого суммарный рейтинг опасности каждой категории был нормирован, чтобы сумма равнялась 100%. Отметим, что угрозы кражи информации, различных сбоев и кражи оборудования специально не были отнесены ни к одной из групп. Дело в том, что они могут быть реализованы, как изнутри, так и снаружи или вообще без вмешательства человека (например, аппаратные сбои).

«Конечно, нельзя утверждать, что внутренние риски ИБ опаснее внешних. Однако налицо факт, что угроза со стороны служащих сегодня вызывает гораздо больше беспокойства, чем вирусы, хакеры, спам и т.д. Проблема здесь в том, что от внутренних нарушителей нельзя защититься также легко, как, например, от вредоносных программ. Внедрил антивирус – и все. А с внутренними угрозами так не получится. Это комплексная, но вполне решаемая проблема».

*Юрий Лысенко,  
начальник отдела ИТ-безопасности РосЕвробанка*

Исходя из полученных результатов (рис. 6), респонденты значительно больше обеспокоены внутренней ИБ, чем защитой от внешних угроз. Кроме того, следует учитывать, что неклассифицированные риски, например, кражу информации или оборудования, чаще всего относят к внутренним угрозам. В данном случае это не было сделано, чтобы не придавать угрозам со стороны инсайдеров дополнительного веса. Однако как показали расчеты, даже в этом случае внешние риски существенно уступают внутренним угрозам.

### НАИБОЛЕЕ ОПАСНЫЕ ИТ-УГРОЗЫ 2004-2006 гг.

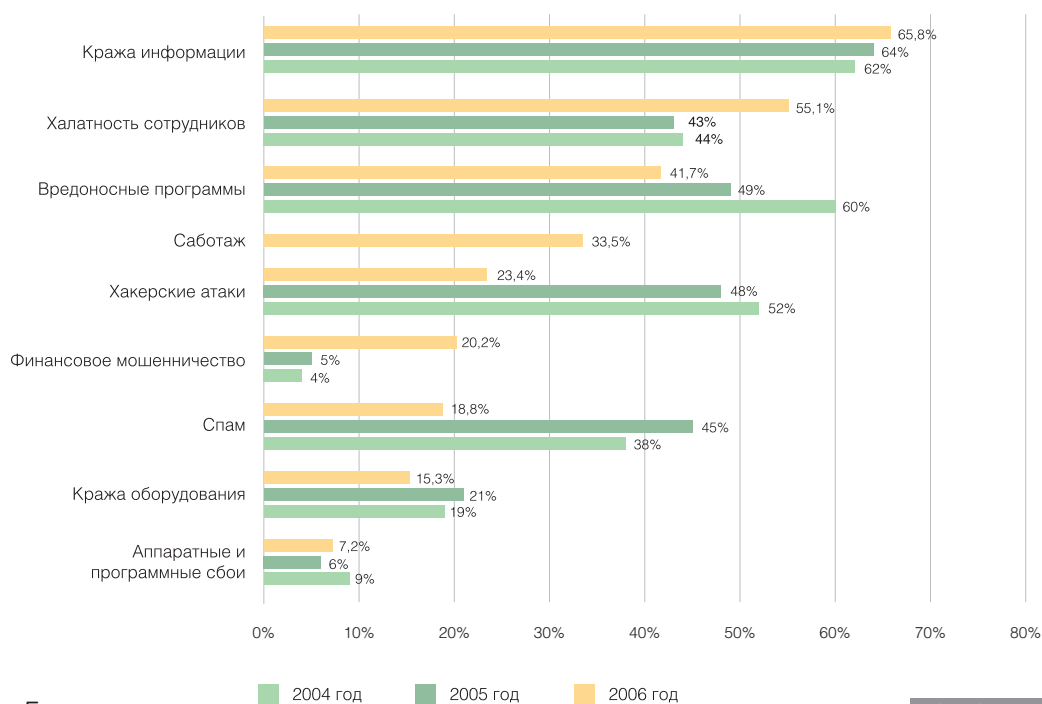


Рис. 5

INFOWATCH • 2007

## СООТНОШЕНИЕ ОПАСНОСТИ ВНУТРЕННИХ И ВНЕШНИХ УГРОЗ ИБ

2006 год

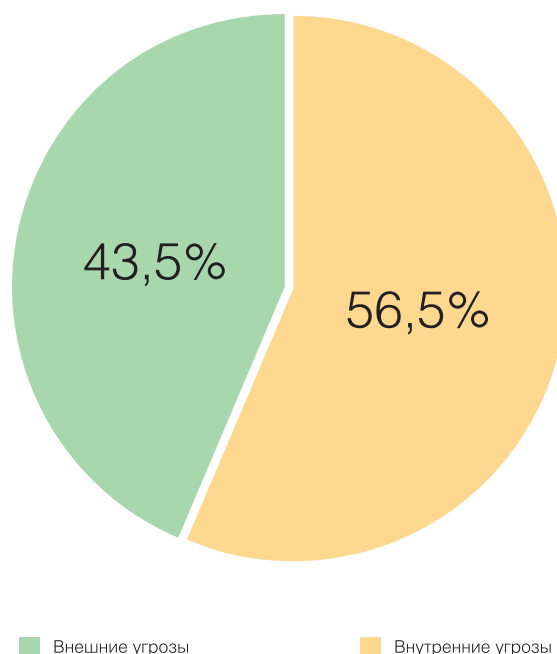


Рис. 6

■ Внешние угрозы

■ Внутренние угрозы

INFOWATCH • 2007

## Внутренние угрозы ИБ

Выяснив, что самые опасные угрозы ИБ исходят изнутри организации, вполне логично изучить структуру инсайдерских рисков. Как показали результаты следующего вопроса (рис. 7), в списке самых опасных внутренних угроз с огромным отрывом лидирует нарушение конфиденциальности информации (70,1%). Ближайший конкурент – искажение информации (38,4%) – отстал на целых 31,7 процентных пункта. Другими словами, риск утечки ценной информации волнует респондентов почти в два раза больше любой другой инсайдерской угрозы.

Между тем, индекс опасности этой угрозой в 2005 году достигал 100%, а в 2004 году – 98%. На первый взгляд может показаться, что обеспокоенность респондентов утечкой конфиденциальной информации за 2006 год несколько снизилась, однако внимательный анализ показывает, что это не так. Прежде всего, в варианты ответов были добавлены две новые угрозы, которые не учитывались в предыдущих исследованиях. Это саботаж (26,2%) и мошенничество (19,3%). Легко видеть, что эти риски заняли третье и четвертое место в списке наиболее опасных угроз, так что включение их в опросный лист было совершенно оправданным. С учетом того, что каждый респондент по-прежнему мог выбрать только три варианта ответа, представляется наиболее вероятным, что две новые угрозы оттянули часть голосов с нарушения конфиденциальности на себя. Кроме того, нет никаких объективных оснований полагать, что риск утечки снизился за прошедший год. Напротив, ушедший год прошел под знаком инсайдеров. На это указывают 5 крупных утечек, которые были зафиксированы в России и СНГ, а также почти [полторы сотни](#) инцидентов внутренней ИБ в других частях света.

## САМЫЕ ОПАСНЫЕ ВНУТРЕННИЕ ИТ-УГРОЗЫ 2004-2006 гг.

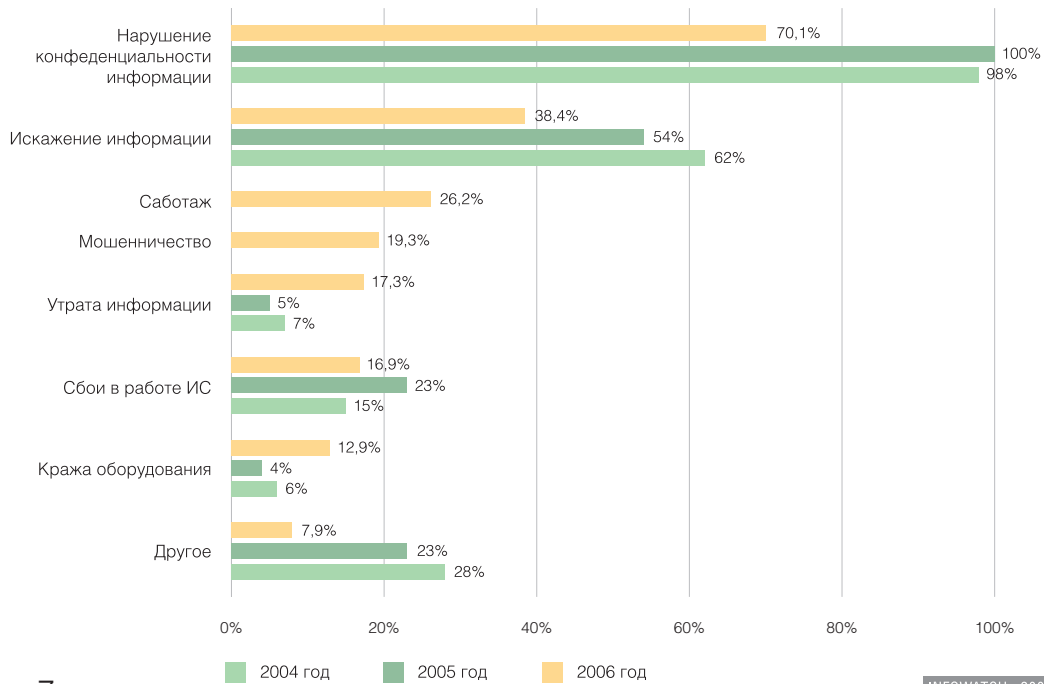


Рис. 7

Комментируя высокий индекс опасности таких угроз, как саботаж и мошенничество, следует отметить, что респонденты совершенно справедливо обратили свое внимание на эти риски. Дело в том, что среди опрошенных компаний преобладают представители крупного бизнеса. Между тем, чем больше компания, тем выше шансы совершения корпоративной диверсии или умышленного искажения финансовых отчетов. Кроме того, проблеме саботажа значительное внимание в 2006 году уделили журналисты и различные исследовательские институты. Один из респондентов во время интервью заметил, что если бы журналисты не стали акцентировать внимание проблеме IT-саботажа и в Интернете не появились отчеты CERT, Секретной службы США и других организаций, то его компания даже не знала бы, что такие риски существуют.

### САМЫЕ КРУПНЫЕ УТЕЧКИ 2006 В РОССИИ И СНГ

Дата	Организация	Потенциальный ущерб
Август	Российские банки, занимающиеся потребительским кредитованием	Удар по репутации и серьезный подрыв доверия к отечественному финансовому сектору
Август	Банк «Первое ОБК» (поглощен Росбанком в 2005 г.)	Ухудшение имиджа, плохое паблисити, массовый отток клиентов
Сентябрь	МЦС (Мобильная Цифровая Связь), владелец марки Velcom	Удар по репутации, потеря лояльных и трудности с привлечением новых клиентов
Октябрь	«Вэб Хостинг» (владелец марки Valuehost)	Массовый отток клиентов, юридические издержки, удар по имиджу
Декабрь	«Русский стандарт», ХКФ-банк, Росбанк, Финансбанк, Импэксбанк и др.	Плохое паблисити, ухудшение репутации всего банковского сектора

# Утечка конфиденциальной информации

Итак, наиболее опасной угрозой ИБ является утечка конфиденциальной информации, совершаемая инсайдерами. В этом году перед респондентами впервые поставили вопрос относительно наиболее плачевных последствий, возникающих вследствие утечек (рис. 8). Как оказалась, более всего респонденты озабочены прямыми финансовыми убытками (46%). На втором месте – ухудшение имиджа и общественного мнения (42,3%), а на третьем – потеря клиентов (36,9%).

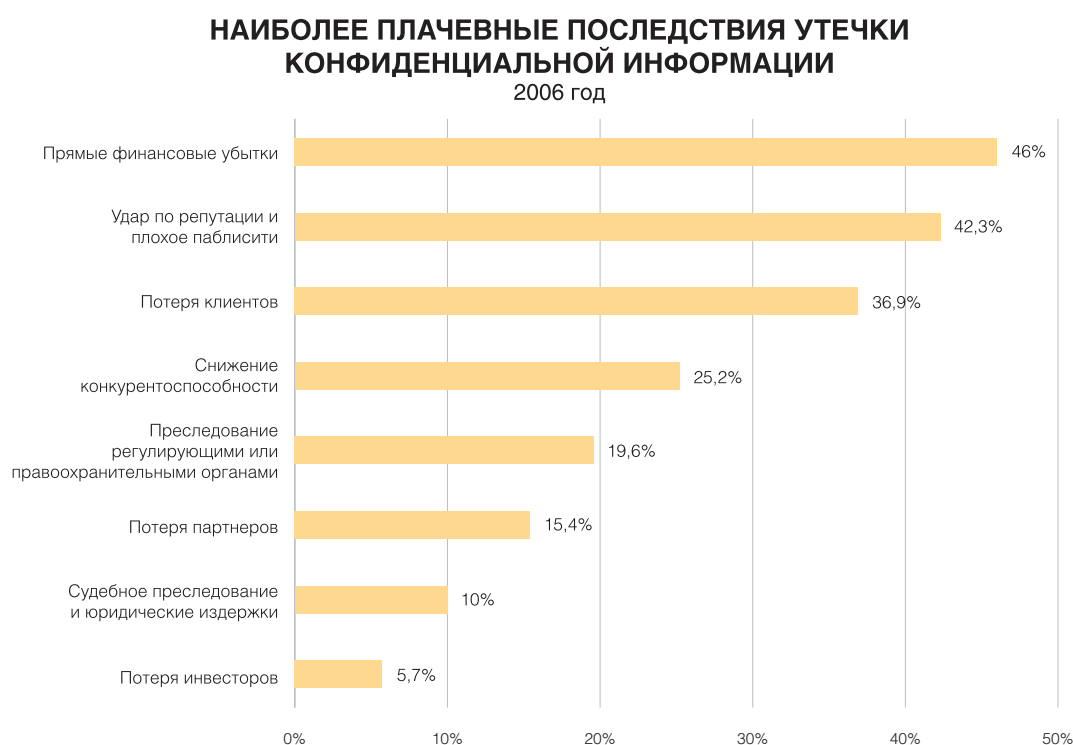


Рис. 8

INFOWATCH • 2007

Кроме того, респонденты озабочены снижением конкурентоспособности (25,2%) организации, что является скорее следствием целого ряда других негативных последствий утечки. Между тем, лишь каждый десятый (10%) упомянул среди наиболее плачевных последствий юридические издержки и судебное преследование, что свидетельствует о неразвитости правоприменительной практики в России. Напомним, что в 2006 году в России был принят закон «О персональных данных», который вступил в силу в феврале 2007 года и создал все предпосылки для того, чтобы компания, допустившая утечку, могла быть привлечена к ответственности. Тем не менее, эксперты компании InfoWatch сомневаются, что одно лишь наличие правильного закона поможет положить конец незаконному обороту персональных данных. Чтобы достичь успеха, необходимо еще вынести несколько судебных решений, наказывающих те организации, которые допускают утечки.

На следующем этапе исследования аналитический центр InfoWatch предложил респондентам указать самые распространенные каналы утечки информации. Распределение ответов представлено на рис. 9. Заметим, что наибольшей популярностью среди инсайдеров пользуются мобильные накопители (86,6%), электронная почта (84,8%) и Интернет (82,2%). По сравнению с 2005 годом первые две позиции не поменялись, а вот Интернет потеснил с третьего места сетевые пейджеры, который в 2006 году набрали только 74,5% процентных пункта и заняли четвертое место.

### КАНАЛЫ УТЕЧКИ ДАННЫХ 2004-2006 гг.

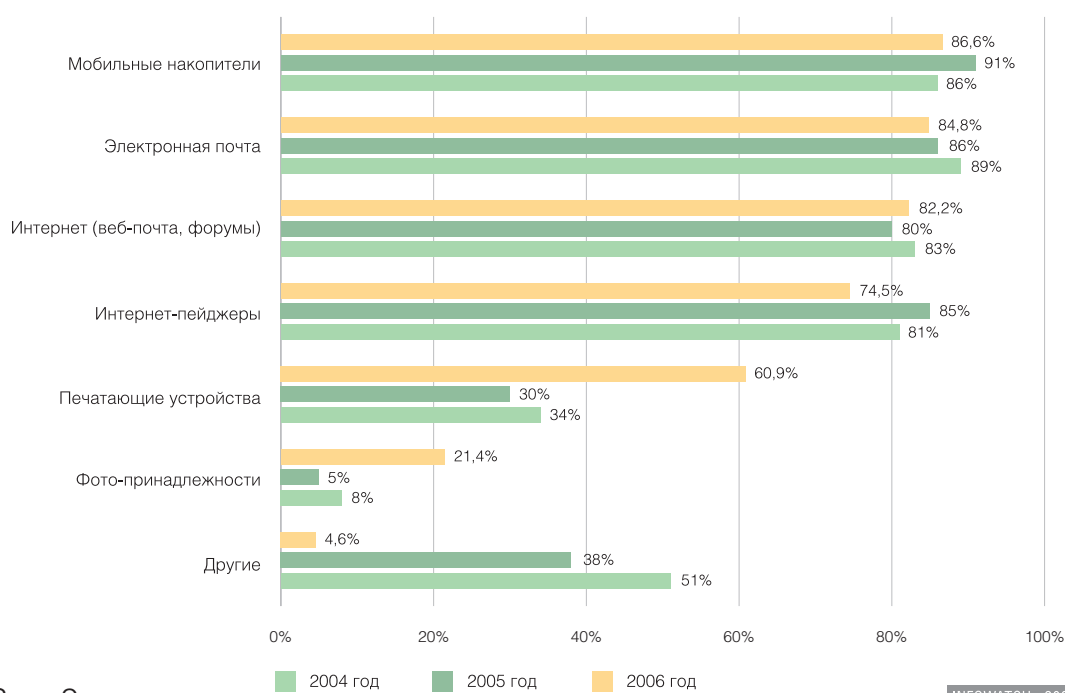


Рис. 9

INFOWATCH · 2007

«В принципе многие внутренние угрозы взаимосвязаны. Например, мошенничество подразумевает искажение информации в финансовых отчетах, а саботаж, в конечном счете, может реализоваться в нарушении конфиденциальности, краже оборудования, утрате данных. Однако сам факт, что утечки (нарушение конфиденциальности) набрали так много голосов, говорит о том, что к этой внутренней угрозе следует подходить наиболее внимательно».

*Василий Окулесский,  
начальник отдела защиты информации ОАО «Банк Москвы»*

Между тем, особое внимание на себя обращает существенно возросший рейтинг опасности печатающих устройств. В 2006 году он составил 60,9%, в то время как в 2005 году был лишь 34 процентных пункта. Дополнительные вопросы респондентам, указавшим на этот канал утечки, помогли выяснить, что многие организации уже имеют достаточно зрелую систему IT-безопасности, которая либо включает средства фильтрации исходящего сетевого трафика, либо ограничительные меры по доступу к внешним сетям. Что же касается принтеров и других печатающих устройств, то они остаются непокрытыми, поэтому инсайдеры переключают свой взор именно на них.

## КОЛИЧЕСТВО УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ 2004-2006 гг.

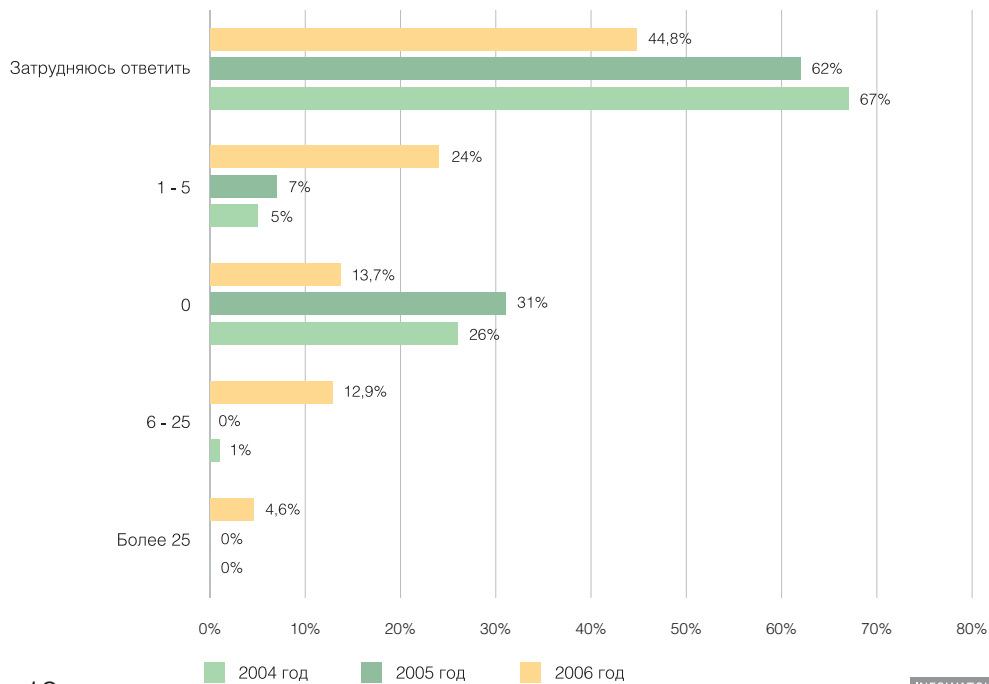


Рис. 10

INFOWATCH · 2007

Наконец, одним из самых важных моментов исследования стал вопрос о количестве утечек конфиденциальной информации, которые респонденты допустили в течение 2006 года (рис. 10). Как в 2005 и 2004 годах, лидером оказалось стандартное «Затрудняюсь ответить», так как слишком многие респонденты еще не используют специализированных решений для выявления утечек. Однако положительный сдвиг уже налицо: если в 2004 году затруднения возникли у 67%, в 2005 году – у 62%, то в 2006 году уже лишь у 44,8% всех опрошенных организаций.

Столь же позитивным выглядит тот факт, что существенно возросла доля респондентов, достаточно точно ответивших о количестве утечек. Так, практически каждый четвертый (24%) сообщил, что его компания допустила от 1 до 5 утечек. В 2005 году об этом заявили лишь 7% организаций. Далее, почти каждый восьмой (12,9%) сообщил, что его компания зафиксировала от 6 до 25 утечек за год. Этот показатель вообще возрос с 0% в 2005 году до 12,9% в 2006 году. Другими словами, у респондентов появилась возможность фиксировать утечки или наблюдать результаты утечек во внешней среде организации. В завершении точно такая же динамика наблюдается у группы, заявившей о более чем 25 утечек. В 2005 году ни один респондент не выбрал данный ответ, а в 2006 году это сделали уже 4,6%.

Остановимся теперь на довольно любопытном ответе – «ни одной утечке не было». Доля этих респондентов сократилась с 31% в 2005 году до 13,7% в 2006 году. Судя по всему, за прошедшие 12 месяцев организации осознали, что точно также подвержены внутренним угрозам и постоянным утечкам, как и весь остальной бизнес. Если раньше респонденты просто заявляли, что у них нет утечек, не основывая свое мнение на каких-либо логических доводах, то теперь эта уверенность испарилась. Многие из тех респондентов, которые входят в 13,7% без утечек, уже установили комплексные системы внутренней ИБ. Однако к этой теме мы вернемся в одной из следующих глав.

# Нормативное регулирование

Впервые в истории российских исследований аналитический центр InfoWatch включил в анкету вопросы, касающиеся нормативного регулирования в сфере ИБ. Как оказалось (рис. 11), подавляющее большинство респондентов (72,1%) не заметили изменение давления со стороны надзорных органов или государства, а еще 3,1% сообщили, что давление либо стало значительно меньше, либо уменьшилось незначительно.

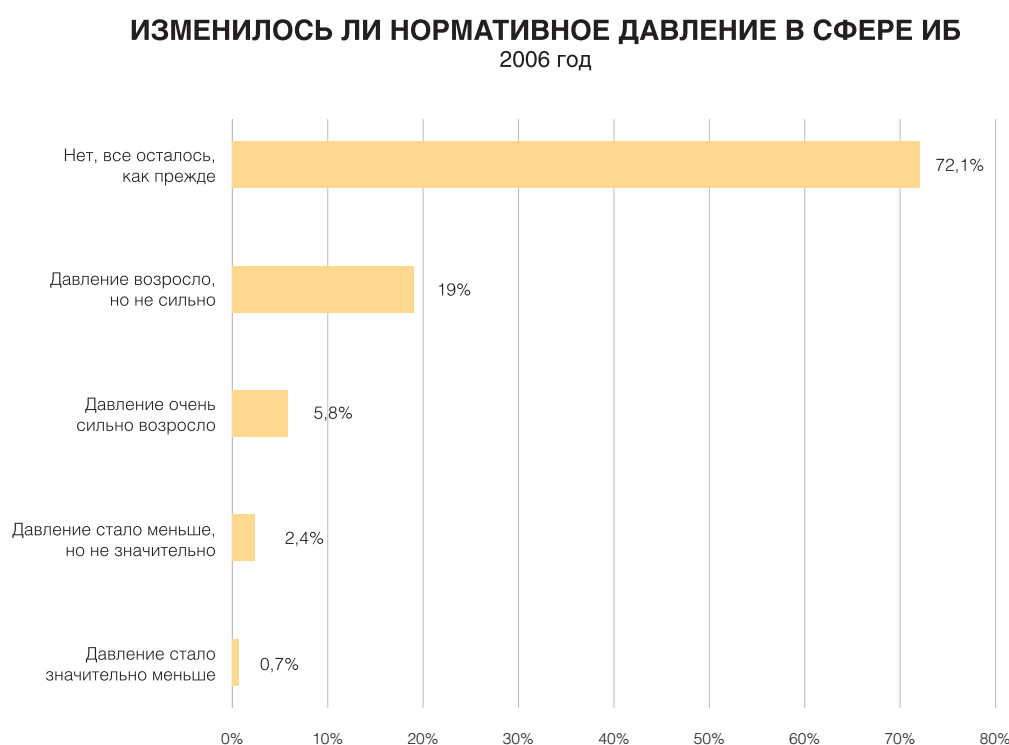


Рис. 11

INFOWATCH • 2007

Тем не мене, определенный интерес представляют почти 25% организаций, зафиксировавших возросшее нормативное давление. Среди них 19% полагают, что требования надзорных органов стали жестче, но не сильно, а еще 5,8% считают, что давление государства возросло существенно.

Дополнительный анализ группы респондентов, относящихся к этим 25%, показался, что данные организации являются либо банками, либо представители сектора телекоммуникаций. Причем углубленное интервьюирование показало, что финансовые компании под нормативным регулированием имеют в виду соглашение Basel II и Стандарт Банка России по ИБ, а телекомы – закон «О персональных данных». Таким образом, определенная обеспокоенность этими нормативными инициативами в банковской и телекоммуникационной сфере присутствует.

## Средства защиты

Среди наиболее популярных средств ИБ за последний год не произошли значительных изменений (рис. 12). По-прежнему пальму первенства удерживают антивирусы (98,6%), межсетевые экраны (73,9%) и контроль доступа (50,8%). Сразу отметим, что небольшое снижение индекса использования антивирусных средств (со 100% до 98,6%) было неизбежно вследствие существенного расширения базы респондентов. В то же самое время на четвертом месте оказались программы защиты от спама, которые за 2006 год прибавили 13,5% и достигли отметки 30,5 процентных пунктов. Далее в рейтинге наиболее популярных средств ИБ находятся системы обнаружения и предотвращения вторжений (23%) и системы защиты от утечек (10,5%). Последний факт необходимо отметить отдельно, так как средства внутренней ИБ впервые опередили популярную технологию VPN (7,5%). Заметим, что опросный лист специально не уточнял, какие именно средства защиты от утечек могут использоваться у респондентов, так что в этот пункт вошли самые разнообразные меры: фильтры исходящего почтового трафика и Интернета, комплексный контроль над рабочим станциями, блокирование USB- и других портов, мониторинг выводимых на печать документов и т.д.

«Честно говоря, для коммерческой организации я бы поставил потерю репутации на первое место. Дело в том, что доброе имя нельзя создать в короткий срок, имея даже очень много денег. Организации тратят годы на то, чтобы сделать свою торговую марку узнаваемой, развивают лояльность марке со стороны клиентов. Между тем, всего одна утечка может разом перечеркнуть долгие годы усилий».

*Олег Смолий,  
главный специалист Управления по обеспечению безопасности ВТБ*

### ПОПУЛЯРНЫЕ СРЕДСТВА ИТ-БЕЗОПАСНОСТИ 2004-2006 гг.

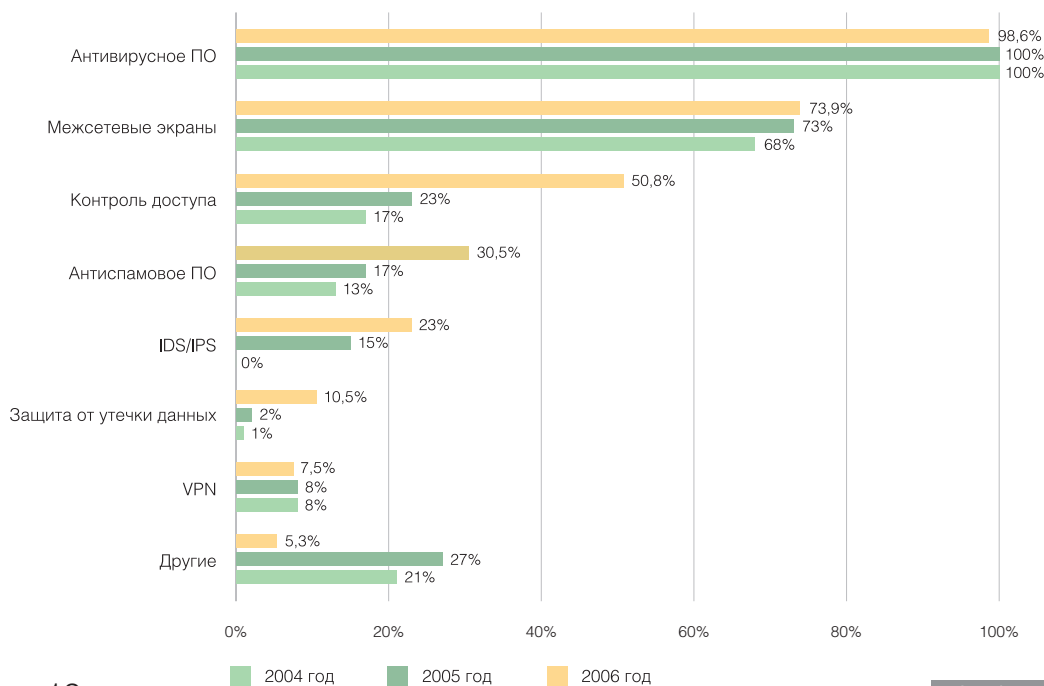


Рис. 12

INFOWATCH • 2007

Таким образом, использование средств защиты от утечек всего за один год возросло практически в пять раз: с 2% до 10,5%. Можно сделать вывод, что начинают сбываться прогнозы, сделанные еще в исследовании «Внутренние ИТ-угрозы в России 2004». Так, около 80% респондентов в 2004 и 2005 годах планировали внедрять системы защиты от утечки в ближайшие два-три года. На основании этих данных аналитический центр InfoWatch еще три года назад прогнозировал взрывной рост рынка внутренней ИБ, что сейчас и происходит. Например, компания InfoWatch по результатам 2006 года увеличила число своих клиентов в 3 раза, а оборот в 2 раза. Более того, топ-менеджмент фирмы отмечает растущий интерес к системам защиты от утечек со стороны ведущих системных интеграторов и представителей, в том числе, среднего бизнеса.

Тем не менее, уровень проникновения в 10,5% нельзя считать удовлетворительным на фоне той угрозы, которую представляют собой внутренние нарушители и утечки конфиденциальной информации. На протяжении двух лет аналитический центр InfoWatch опрашивал респондентов относительно препятствий на пути внедрения системы защиты от утечек. В результате подавляющее большинство организаций затруднялось ответить. Эксперты InfoWatch списывали это на психологическую неготовность российского бизнеса к борьбе с инсайдерами. Следует отметить, что этот вывод нашел свое подтверждение в исследовании этого года (рис. 13).

Итак, наиболее сложным препятствием на пути внедрения защиты от утечки является психологическая неготовность (25,4%). За ней следуют бюджетные ограничения (20,6%), нехватка квалифицированного персонала (17,5%), отсутствие технологических решений (14,8%) и стандартов (12,2%).

### ПРЕПЯТСТВИЯ НА ПУТИ ВНЕДРЕНИЯ ЗАЩИТЫ ОТ УТЕЧКИ ДАННЫХ 2004-2006 гг.

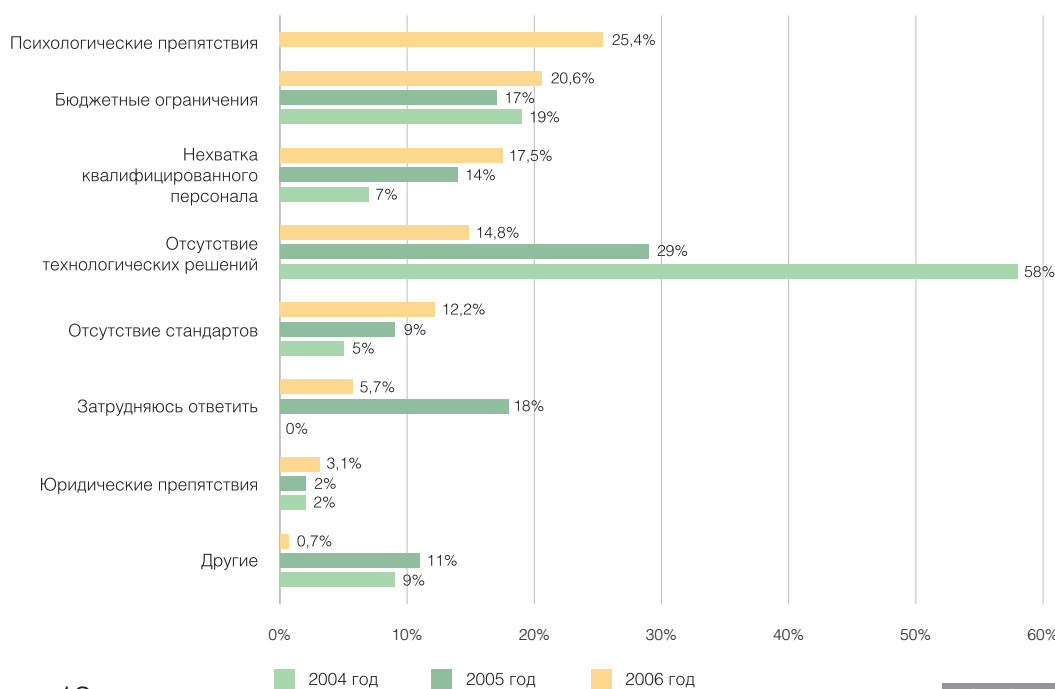


Рис. 13

INFOWATCH • 2007

По сравнению с результатами прошлого года, следует отметить ряд тенденций. Во-первых, в 2006 году только 5,7% затруднились ответить на вопрос. В 2005 году этот показатель был на уровне 18%. Так что за прошедшие 12 месяцев респонденты, как минимум, обратили свое внимание на проблему внутренней ИБ и изучили препятствия на пути реализации эффективных мер противодействия. Во-вторых, доля организаций, указавших на «Отсутствие технологических решений», снизилась за 2006 год с 29% до 14,8%, а за последние два года вообще на 43,2% (с 58% до 14,8%). Оба этих достижения следует приписать на счет грамотному информированию бизнес-сообщества средствами массовой информации, а также эффективной просветительской политике поставщиков. Между тем, если говорить о нехватке персонала и бюджетных ограничениях, то за 2005 год существенных изменений в этих показателях не происходило. Таким образом, респонденты по-прежнему оказываются психологически не готовыми к внедрению эффективных решений для защиты от внутренних нарушителей. Тем не менее, уже достигнутый уровень проникновения в 10,5% являет собой положительную динамику.

На следующем этапе аналитический центр InfoWatch предложил респондентам определить наиболее эффективные пути защиты от утечек (рис. 14). Речь здесь идет о тех решениях, которые представляются организациям наиболее адекватными и приемлемыми для решения проблемы внутренней ИБ, но по ряду причин (см. выше), не используемых респондентами на практике.

Наиболее эффективным средством являются комплексные информационные продукты (44,8%). Эта мера лидирует вот уже на протяжении трех лет, поэтому можно смело утверждать, что именно в этом направлении будет происходить наибольший рост рынка внутренней ИБ в ближайшие годы.

### САМЫЕ ЭФФЕКТИВНЫЕ ПУТИ ЗАЩИТЫ ОТ УТЕЧКИ ДАННЫХ 2004-2006 гг.

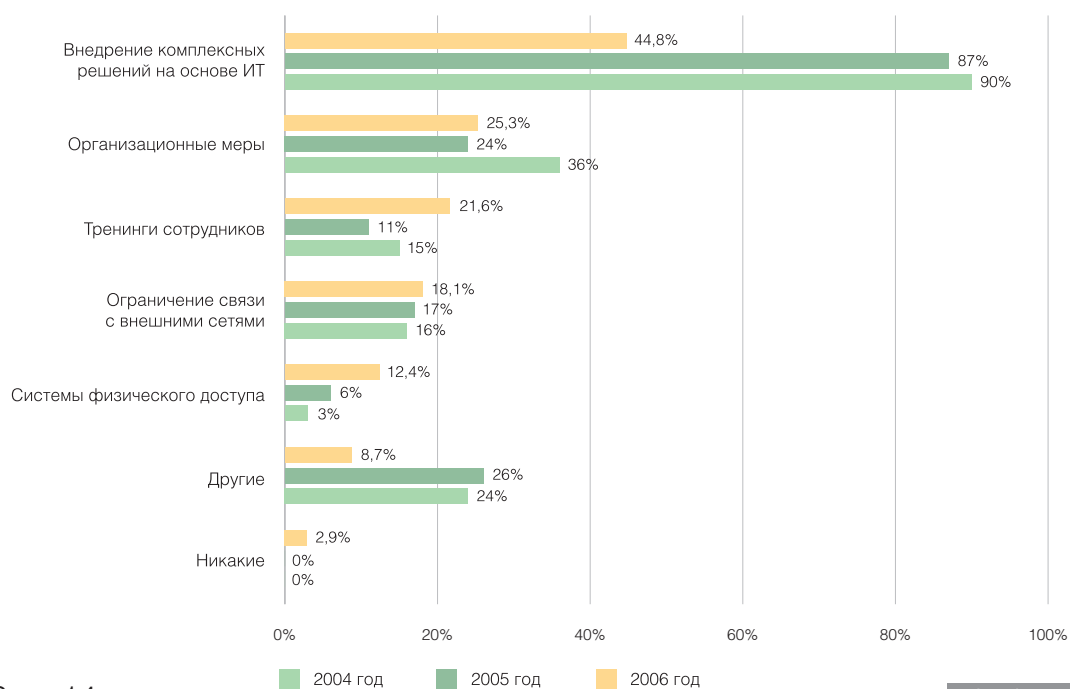


Рис. 14

INFOWATCH • 2007

Далее следуют организационные меры (25,3%), тренинги персонала (21,6%) и ограничение связи с внешними сетями (18,1%). Таким образом, можно рассчитывать, что после преодоления психологических препятствий и бюджетных ограничений (рис. 13) финансовые ресурсы, выделяемые на защиту от утечек, будут распределяться как раз в этих долях. Однако наибольшая часть бюджета придется на комплексные продукты на основе ИТ.

«Респонденты откровенно заявили, что утечки все-таки происходят из их организаций. Причем если почти половина еще действительно не знает об этом, так как не использует никаких средств защиты, то 13,7%, которые заявили – утечек не было, выглядят чересчур самоуверенно. Особенно на фоне того, что только 10,5% респондентов используют специализированные средства защиты».

*Владимир Скиба,  
начальник отдела информационной безопасности ФТС России*

Этот вывод косвенно подтверждают результаты последнего вопроса, в котором аналитический центр InfoWatch предложил респондентам определить свои планы на ближайшие 2-3 года. Согласно распределению ответов (рис. 15), девять из десяти (89,9%) организаций планируют внедрить в ближайшие три года ту или иную систему защиты от утечек.

### ПЛАНЫ ВНЕДРЕНИЯ ЗАЩИТЫ ОТ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ 2004-2006 гг.

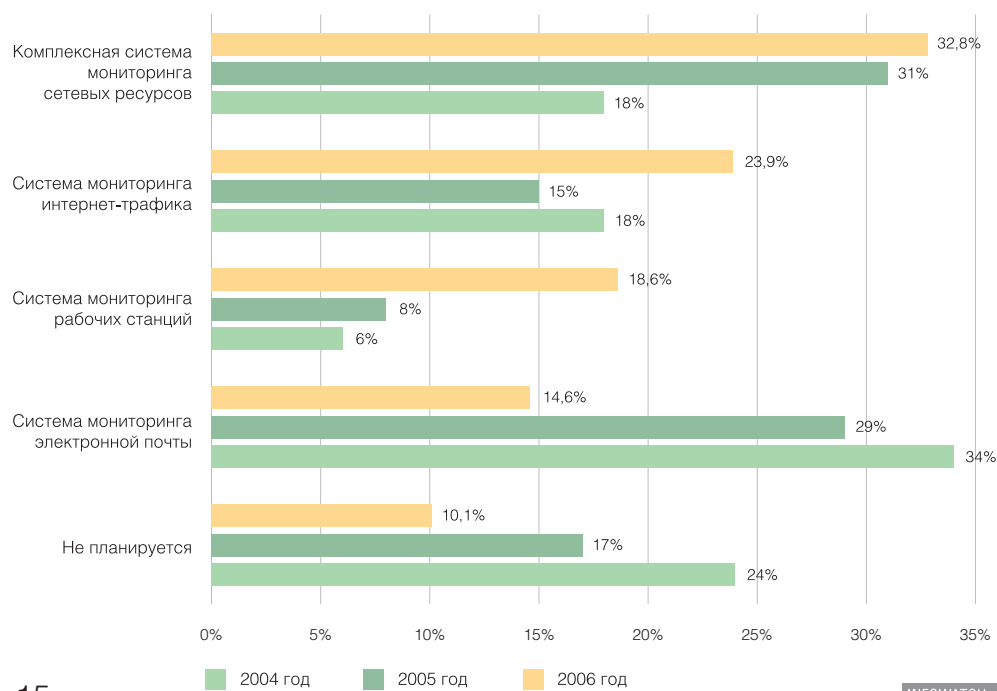


Рис. 15

Наибольшим вниманием респондентов пользуются комплексные решения (32,8%), средства мониторинга Интернет-трафика (23,9%) и системы мониторинга рабочих станций (18,6%). Замыкает цепочку лидеров система мониторинга электронной почты (14,6%). Ее некоторое запоздание может объясняться тем, что часть организаций уже использует фильтры исходящих сообщений.

## Открытый вопрос

В заключение исследования респондентам было предложено просто прокомментировать проблему внутренних нарушителей и высказать свое мнение по любому связанному с ней аспекту. Оказалось, что многие респонденты считают, что внутренние нарушения практически всегда являются следствием человеческого фактора: халатности и безалаберности. Другими словами, лишь несколько российских организаций сталкивались в своей практике с инсайдерами, действующими умышленно. Намного чаще служащие допускают ошибки по незнанию. Именно поэтому большинство респондентов полагают, что технические решения (продукты на основе ИТ) способны эффективно противостоять внутренним нарушениям. Ведь достаточно просто заблокировать пересылку конфиденциального сообщения и выслать уведомление отправителю, чтобы тем самым повысить грамотность этого служащего и показать, что он совершает запрещенное действие. Таким образом, в следующем году аналитический центр InfoWatch планирует включить в анкету вопросы, связанные с мотивами действий тех инсайдеров, которых компаниям уже удавалось выявлять в своей практике.

«Использование различных систем для защиты от внутренних нарушителей действительно становится все более популярным. Однако я хочу предостеречь организации, которые просто пытаются быстро затыкать дыры. Например, раз и отключили USB-порты на рабочих станциях, два и начали фильтровать исходящую почту. Проблема в том, что к внутренним угрозам надо подходить комплексно. Т.е. техническими средствами взять под контроль все каналы утечки, а административными – ограничить доступ к тем, которые контролировать невозможно».

*Дмитрий Мананников,  
директор по ИТ-безопасности СДМ-банка*

В то же самое время у респондентов практически не наблюдалось отношения к проблеме утечек, как к неизбежному злу. В 2005 и 2004 году многие организации даже не знали, что можно предпринять для обеспечения внутренней ИБ. В 2006 году ситуация кардинально изменилась – респонденты ясно понимают, что утечки можно остановить, поэтому концентрируют свое внимание на путях решения проблемы. «Если раньше мы могли просто заявить руководству, что никто не знает, как бороться с утечками, то теперь вопрос стоит совсем иначе. Дайте нам средства, и мы перекроем течь!», - прокомментировал в финале интервью один из респондентов.

В целом опрошенные специалисты и начальники отделов признают, что высшее руководство начинает прислушиваться к их аргументам и выделять средства на реализацию комплексных проектов по защите от внутренних угроз. Конечно, о полноценном преодолении психологической неготовности еще речи не идет, но положительная динамика налицо.

## Заключение

За последние три года внутренние угрозы ИБ ничуть не утратили своей актуальности. По-прежнему наибольшую обеспокоенность респондентов вызывают кража конфиденциальной информации, халатность сотрудников, но теперь в этот ряд еще добавился информационный саботаж. Сравнение индексов обеспокоенности внутренними и внешними угрозами ИБ показывает, что именно инсайдерские риски превалируют в списке наиболее опасных угроз. Более того, наибольший рейтинг опасности приходится на утечку конфиденциальной информации. Как показало исследование, респонденты очень хорошо осведомлены о негативных последствиях этих инцидентов: прямых и косвенных финансовых убытках, долгосрочном ущербе для репутации, потере клиентов и трудности в привлечении новых.

Если говорить о предотвращении утечек, то положительная динамика налицо. Каждая десятая организация уже использует те или иные средства защиты, хотя о по-настоящему массовом внедрении можно говорить в перспективе только ближайших трех лет. Что же мешает бизнесу и госструктурам начать внедрять защиту от утечек прямо сейчас? Оказывается, респонденты психологически не готовы пойти на такой шаг. Правда, девять из десяти планируют установить системы внутренней ИБ уже в ближайшие 2-3 года. Таким образом, тенденция налицо, причем если в прошлом году можно было говорить о ее малых темпах, то сегодня темпы уже впечатляющие: за 2006 год число респондентов, внедривших продукты на основе ИТ, возросло на 500%.

# О компании InfoWatch

InfoWatch — инновационная компания, разрабатывающая уникальные технологии для перспективной области информационной безопасности — защиты от внутренних угроз. В сферу компетенции компании входит минимизация риска утечки, уничтожения данных, саботажа, промышленного шпионажа и других неосторожных и неправомерных действий сотрудников в отношении корпоративной информации.

Уникальные решения компании позволяют контролировать операции с документами внутри корпоративной сети и предотвращать те из них, которые не соответствуют политике безопасности. В частности, InfoWatch обеспечивает проверку почтового и интернет-трафика, а также мониторинг на уровне файловых операций (копирование, удаление, переименование, изменение, печать документов). Совместно с традиционными системами защиты (межсетевые экраны, фильтры, авторизация, крипто-защита и т.д.) InfoWatch позволяет построить комплексную корпоративную структуру безопасности благодаря обеспечению “тыла” — надежной защиты от внутренних угроз.

Среди наших клиентов — Минэкономразвития, Минфин, ФТС, ГидроОГК, Транснефть, ВымпелКом, Мегафон, Внешторгбанк и многие другие.

## Партнеры исследования

### Партнерская сеть InfoWatch



### Медиа-партнеры InfoWatch



### Интернет-партнеры InfoWatch



### Маркетинговое агентство





**INFOWATCH**  
INFORMATION WATCH TECHNOLOGIES

Россия, 123060, Москва,  
1-й Волоколамский проезд, дом 10, стр. 1  
Тел./факс: +7 (495) 797-8700  
[info@infowatch.ru](mailto:info@infowatch.ru)  
[www.infowatch.ru](http://www.infowatch.ru)