Внутренние ИТ-угрозы в промышленности 2006

А.В. Доля (Аналитический центр InfoWatch)

Компания InfoWatch представляет результаты первого отраслевого исследования проблемы внутренней ИТ-безопасности (ИБ) в российской промышленности. В этом проекте приняли участие 10 компаний, входящих в партнерскую сеть InfoWatch, представители отраслевой прессы, а также специализированное маркетинговое агентство. В результате, аналитическому центру InfoWatch удалось опросить 354 российских предприятий.

Исследование ставило своей целью определить отношение респондентов к угрозам внутренней ИБ, обобщить информацию об используемых защитных средствах и технологиях, а также выявить специфику обеспечения внутренней ИБ в российской промышленности. Данный проект уточняет результаты третьего ежегодного исследования "Внутренние ИТ-угрозы в России 2006", в ходе которого было опрошено 1450 российских организаций во всех секторах экономики. Анализ внутриотраслевых результатов и сравнение с аналогичными показателями по всем секторам экономики позволяет выявить специфику промышленных предприятий.

Общие выводы

• Промышленные предприятия более всего обеспокоены именно внутренними угрозами ИБ. Инсайдерские риски превалируют над внешними угрозами в соотношении 6:4 (55% против 45%).

• Наибольшую опасность для промышленности представляют утечки персональных данных клиентов. Такой точки зрения придерживается абсолютное большинство респондентов (84%).

• Опасения предприятий вполне оправданы: 52% опасается, что утечка технологий, промышленных и коммерческих секретов приведет к снижению конкурентоспособности бизнеса.

• 15% компаний заявили, что допустили в 2006 г. хоть одну утечку. Однако 74% вообще не знают о существовании утечек конфиденциальной информации из компании.

• Лишь 9% промышленных компаний используют средства защиты от утечек сейчас, но 96% планируют внедрить те или иные механизмы защиты уже в ближайшие 3 года.

Методология

В процессе исследования, в период с 25.01 по 20.02 2007 г., были опрошены 170 представителей российской промышленности. Опрос проводился среди заказчиков InfoWatch и клиентов крупнейших системных интеграторов, входящих в партнерскую сеть компаний: Энвижн Груп, 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 журналов: "Мировая энергетика" и "Автоматизация в промышленности".

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, традиционно входящих в исследование "Внутренние ИТ-угрозы в России".

Опрос проходил непосредственно у самих респондентов, а также по Internet. 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.

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

Портрет респондентов

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 числу сотрудников показал, что наибольшая доля опрошенных организаций приходится на крупный бизнес: 82% респондентов имеют 1...10 тыс. служащих. При этом 18% организаций с числом персонала менее 1 тыс. представляют малый и средний бизнес, а всего 5% – очень крупные предприятия с числом сотрудников более 10 тыс. человек.

Обратимся теперь к степени информатизации базы респондентов. Оказывается, наибольшая по чис-

ленности доля опрошенных организаций имеет 1...5 тыс. рабочих станций (33%). Следующей идет группа с 5001...10000 терминалов (26%). Другими словами, большинство респондентов (59%) приходятся на представителей крупного бизнеса. Между тем, доля очень крупных организаций с числом рабочих станций более 10 тыс. составляет всего 3%. Что же касается среднего и малого бизнеса, то на него приходится 38%, из которых 21% имеют менее 500 терминалов, а 17% – 500...1000 ПК. Таким образом, можно сделать вывод, что база респондентов данного исследования состоит преимущественно из представителей крупного бизнеса. Несмотря на это, уровень репрезентативности как малых, так и очень крупных предприятий является вполне достаточным.

Анализируя должности респондентов (рис. 1), следует отметить, что подход к ИБ со стороны промышленных предприятий заметно отличается от общеотраслевого. Так, 35% опрошенных организаций имеют в своей штатной структуре выделенный отдел ИБ, в то время как в среднем по всем отраслям этот показатель достигает лишь 27,2 процентных пункта. По мнению аналитического центра InfoWatch, руководство крупных российских промышленных предприятий (а именно они представлены в исследовании больше всего) прекрасно понимает, насколько эффективность и успешность бизнеса может зависеть от ИБ. Тем не менее, многие компании все еще имеют выделенных сотрудников по ИБ в ИТ-департаменте, а некоторые все еще поручают функции ИБ своим штатным ИТ-служащим.

Но даже, когда задачи ИБ возлагаются на ИТ-отделы, опрос руководителей этих департаментов показывает, что они придают задачам ИБ достаточно высокое значение и часто выделяют для этих целей специальных сотрудников, которые в перспективе могут перерасти в выделенную службу.

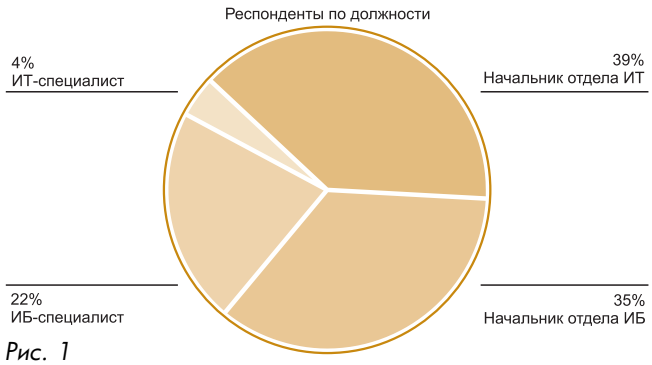

Рис. 1

Рис. 2

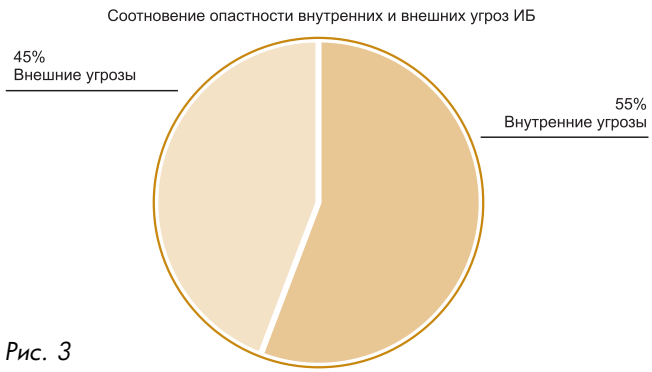

Рис. 3

Угрозы ИБ в России

Отвечая на следующий вопрос, организации имели возможность обрисовать ландшафт самых опасных угроз ИБ. Каждый респондент мог выбрать только три угрозы из предложенного списка (рис. 2). В результате, на первом месте по-прежнему остается кража информации (72%). Далее, на втором месте оказалась халатность сотрудников (61%), которая точно также опередила общеотраслевой показатель на 5,9%. Третье место заняли вирусные атаки (41%), а на четвертой позиции оказался саботаж (33%). Следующие две ступени устойчиво удерживают хакерские атаки (27%) и спам (22%). Все остальные угрозы ИБ набрали менее 20%.

Таким образом, ландшафт угроз ИБ повторяет те же риски, которых опасаются предприятия других отраслей. Незначительные отклонения в более высоком рейтинге опасности кражи информации и халатности сотрудников можно отнести на счет специфики деятельности промышленных предприятий. По сути, весь бизнес в этой сфере построен на технологиях, промышленных и коммерческих секретах.

Между тем, если пересчитать результаты предыдущего вопроса, разделив все ответы на внутренние и внешние угрозы, видно, что инсайдеры превалируют над вирусами, хакерами и спамом.

Для построения следующей диаграммы (рис. 3) 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 ограничить общую сумму ста процентами. 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).

Исходя из полученных результатов (рис. 3), респонденты значительно больше обеспокоены внутренней ИБ, чем защитой от внешних угроз. Кроме того, следует учитывать, что неклассифицированные

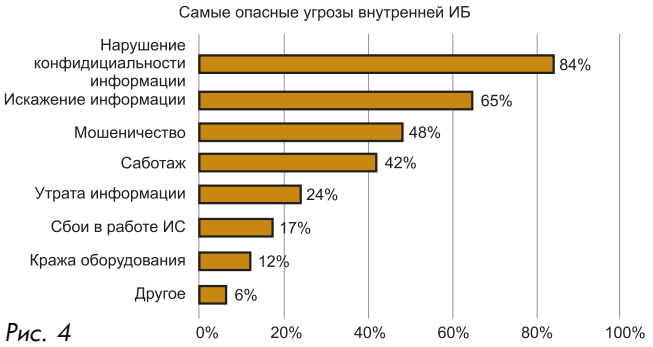

Рис. 4

Рис. 5

Рис. 6

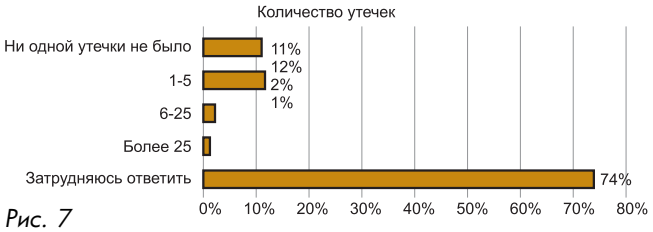

Рис. 7

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.

Внутренние угрозы ИБ

Выяснив, что самые опасные угрозы ИБ исходят изнутри организации, вполне логично изучить структуру инсайдерских рисков. В рамках следующего вопроса респондентам снова предложили выбрать три наиболее опасные угрозы ИБ, но на этот раз рассматривались только внутренние риски. Как показали результаты опроса (рис. 4), в списке самых опасных внутренних угроз с огромным отрывом лидирует нарушение конфиденциальности информации (84%). Ближайший конкурент – искажение информации (65%) – отстал на целых 19 процентных пункта. Другими словами, риск утечки ценной информации волнует респондентов намного больше любой другой инсайдерской угрозы.

Следующие две позиции остались за мошенничеством (48%) и саботажем (42%). Сразу следует отметить, что в этом проявляется некоторая специфика промышленности. Дело в том, что в общеотраслевом исследовании саботаж обогнал мошенничество почти на 15 процентных пунктов. Между тем, например, в учете переданных энергоносителей, мошенничество действительно является одной из самых опасных угроз, так что выбор респондентов вполне обоснован.

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. При этом представитель каждой организации мог выбрать только два варианта из предложенного списка (рис. 5). Оказалось, что более всего респонденты озабочены потерей конкурентоспособности (52%), снижением репутации (43%) и прямыми финансовыми убытками (36%). Далее идет потеря партнеров (28%), которая неминуемо следует за снижением конкурентоспособности.

Сравнивая полученные результаты с общеотраслевым исследованием можно заметить, что представители промышленности намного больше обеспокоены своей конкурентоспособностью по сравнению с предприятиями в среднем по экономике. Дело в том, что конкурентоспособность респондентов как раз базируется на технологиях, промышленных и коммерческих секретах. Поэтому утечка этих сведений неминуемо скажется на успешности бизнеса.

На следующем этапе исследования аналитический центр InfoWatch предложил респондентам указать самые распространенные каналы утечки информации (рис. 6). Отвечая на данный вопрос, респонденты почти полностью повторили результаты общеотраслевого исследования: мобильные накопители (86%), электронная почта (82%) и Internet (81%). Далее следуют Internet-пейджеры (75%) и средства печати (67%).

Наконец, одним из самых важных моментов исследования стал вопрос о числе утечек конфиденциальной информации, которые респонденты допустили в течение 2006 г. (рис. 7). Как и в других отраслях, лидером оказалось стандартное "Затрудняюсь ответить", так как слишком многие респонденты еще не используют специализированных решений для выявления утечек. Причем по сравнению с общеотраслевыми показателями, ответы представителей промы-

Угрозы - оружие тех, кто сам под угрозой.
Д. Боккаччо

шленности указывают на действительно серьезные затруднения. В среднем по экономике проблемы с ответом возникли у 44,8% респондентов, а в промышленности – у 74% организаций. Другими словами, представители данной отрасли хуже всего осведомлены об утечках.

Столь же негативным выглядит тот факт, что только 11% респондентов могут уверенно заявить, что не допустили ни одной утечки в прошедшем году. Этот показатель также на 2,7% меньше общеотраслевого. Таким образом, представители промышленности испытывают серьезные трудности с тем, что хотя бы определить, как часто и в каком направлении конфиденциальная информация пересекает корпоративный периметр.

Средства защиты

Посмотрим теперь, какие средства ИБ используют промышленные предприятия (рис. 8). Среди наиболее популярных инструментов за последний год оказались антивирусы (100%), межсетевые экраны (72%) и контроль доступа (59%). Что касается этих и других средств ИБ, то в целом представители промышленности незначительно отличаются от компаний из других секторов экономики. Тем не менее, определенные опасения внушает низкая доля организаций, использующих защиту от утечки данных (всего 9%). В среднем по всем отраслям этот показатель равняется 10,5%.

По мнению аналитического центра InfoWatch, даже 9% – это хороший показатель для такой новой области, как защита от внутренних угроз ИБ. Следует также учитывать, что на рынке еще не сформировалось единого понимания проблемы, поэтому достигнутые результаты тоже характеризуют прогресс. Тем не менее, очевидно, что поставщикам решений и самим промышленным компаниям еще есть над чем работать, так как сегодня бизнес во многом зависит от сохранения конфиденциальности и целостности информации, а наибольший риск исходит именно от внутренних нарушителей.

В то же самое время логично вернуться к результатам девятого вопроса (рис. 7), отвечая на который 11% респондентов заявило, что в 2006 г. они не зафиксировали ни одной утечки. Получается, что минимум 2% (11% – 9%) из этих компаний не допустили утечек, хотя не используют никаких средств защиты. Более того, из последнего факта вытекает, что такие организации даже не могут отследить, происходят у них утечки или нет. Таким образом, их уверенность в отсутствии утечек не имеет под собой объективных оснований.

Обратимся теперь к следующему вопросу, который логично вытекает из предыдущего. Что именно мешает компаниям внедрять системы защиты от утечек? В предложенном ниже списке (рис. 9) каждый респондент мог выбрать только одну основную причину. Как оказалось, наибольший вес для промышленности имеет отсутствие стандартов (29%). Причем под стандартами здесь понимаются не только нормативные или рекомендательные акты, а еще и единое видение системы внутренней безопасности. Так, многие респонденты отмечали, что сегодня еще не сформировался единый подход к решению проблемы внутренней ИБ. В результате компаниям сложно планировать бюджеты и выбирать продукты для внедрения. Отсюда вытекает еще одна проблема – бюджетные ограничения (23%). Ведь, не имея единого представления внутренней ИБ, компания не может планировать свои расходы и заранее распределять часть бюджета на решение проблемы инсайдеров.

Данные результаты очень интересно сравнить с общеотраслевыми. Так, в опросе всех секторов экономики лидерами среди препятствий стали психологические препятствия (25,4%). В то же самое время отсутствие стандартов оказалось на пятом месте (12,2%). Отсюда напрашивается вывод, что промышленность подходит к проблеме внутренней ИБ намного более зрело, чем другие отрасли. Это проявляется в том, что представители промышленности уже перешагнули психологический барьер и отчетливо понимают, что сегодня необходимо унифицировать процесс защиты от внутренних угроз. С этим мнением полностью согласны эксперты InfoWatch, которые полагают, что выработка единого подхода к решению проблемы инсайдерских рисков просто необходима, и она уже идет сейчас. Но эта работа может занять около 2...3 лет. Таким образом, сложность выбора конкретного решения для защиты от утечек вполне объяснима.

На следующем этапе аналитический центр InfoWatch предложил респондентам определить на-

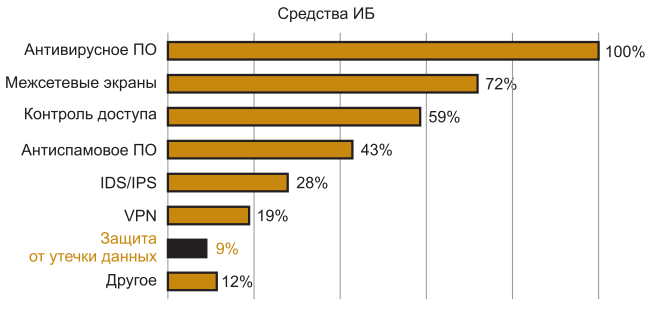

Рис. 8

Рис. 9

Рис. 10

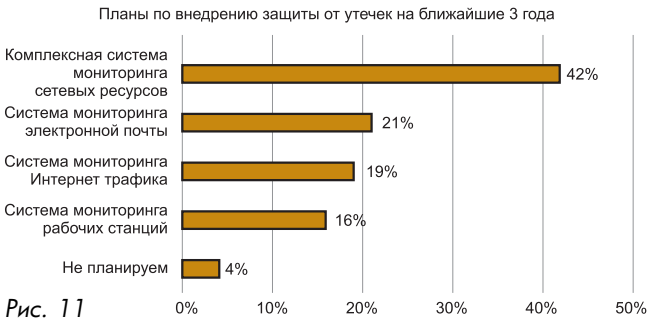

Рис. 11

иболее эффективные пути защиты от утечек (рис. 10). Речь здесь идет о тех решениях, которые представляются организациям наиболее адекватными и приемлемыми для решения проблемы внутренней ИБ, но по ряду причин неиспользуемых респондентами на практике.

Наиболее эффективным средством являются комплексные информационные продукты (48%). Эта мера лидирует вот уже на протяжении трех лет в общеотраслевом исследовании, поэтому можно смело утверждать, что именно в этом направлении будет происходить наибольший рост рынка внутренней ИБ в ближайшие годы.

Далее следуют организационные меры (28%), ограничение связи с внешними сетями (12%) и тренинги персонала (8%). Причем, как полагают эксперты InfoWatch, наиболее эффективным способом минимизации инсайдерских рисков является комбинация различных способов. Правда, базой все равно должно быть комплексное решение на основе ИТ, так как только с его помощью можно закрепить положения политики ИБ на рабочих местах.

Этот вывод полностью подтверждают результаты последнего вопроса, в котором аналитический центр InfoWatch предложил респондентам определить свои планы на ближайшие 2...3 года. Согласно распределению ответов (рис. 11), практически каждый респондент (96%) планирует внедрить в ближайшие три года ту или иную систему защиты от утечек.

Наибольшим вниманием респондентов пользуются комплексные решения (42%). Этот показатель значительно превышает общеотраслевой (почти на 11%), что снова свидетельствует о более зрелом отношении к проблеме внутренней ИБ в промышленности по сравнению с иными отраслями экономики. Среди других планов респондентов следует отметить средства мониторинга Internet-трафика (19%) и электронной почты (21%), а также системы контроля над рабочими станциями (16%).

Открытый вопрос

В заключение исследования респондентам было предложено просто прокомментировать проблему внутренних нарушителей и высказать свое мнение по любому связанному с ней аспекту. Здесь представители промышленности снова высказали свою тревогу относительно отсутствия единого подхода к обеспечению внутренней безопасности. На практике это очень сильно затрудняет выбор конкретного решения, так как организация вынуждена выслушивать очень многих поставщиков, каждый из которых обладает какими-то плюсами, но мало чем пересекается с конкурентами. Кроме того, возникают естественные трудности с планированием бюджета.

Тем не менее, респонденты отмечают, что сегодня уже начинают появляться некоторые точки соприкосновения. Они, прежде всего, связаны с тем, что организации постоянно расширяют число коммуникационных каналов, которые используются в бизнесе: электронная почта, Internet, пейджеры, печать на бумагу, различные беспроводные сети, новые сетевые протоколы и приложения и т.д. Таким образом, при построении системы внутренней ИБ выгодно не концентрировать всю функциональность на каком-то одном канале, а напротив – создавать расширяемую систему, к которой легко добавить новый канал.

Заключение

Несмотря на то, что российские промышленные компании довольно зрело относятся к проблеме ИБ вообще и защите от внутренних угроз в частности, им все равно еще есть куда расти. Во-первых, уровень использования эффективных средств защиты от утечек в организациях данной отрасли еще очень низок. Во-вторых, среди некоторых респондентов бытует мнение, что их компания вообще не допускает утечки, хотя никаких инструментов, чтобы проверить это, данные организации не используют.

Суммируя результаты об уже осуществленных внедрениях в промышленности и планах компаний на ближайшие годы, аналитический центр InfoWatch отмечает в основном положительные тенденции. По сравнению с прошлым годом число организаций, защитивших себя от утечек, выросло в несколько раз (в целом по всем секторам экономики – в пять раз). Причем по прогнозам исследования в будущем году этот показатель снова увеличится в тех же масштабах.

Доля Алексей Владимирович *– руководитель аналитического центра InfoWatch.*
Контактные телефоны/факсы: (495) 797-87-00, 645-79-39.
E-mail:ad@infowatch.com Http://www.InfoWatch.ru