ИНФОРМАТИКА

В.Г. Ермошин

Анализ эффективности защиты информации от внутренних угроз в корпоративной среде

Бесконечные вирусные эпидемии и хакерские атаки создают впечатление отсутствия угрозы информационной безопасности (ИБ) изнутри. Тем не менее результаты исследований многих авторитетных аналитических организаций свидетельствуют, что именно внутренние ИТ-угрозы являются одной из наиболее актуальных областей информационной безопасности.

Все аналитические отчеты указывают, что наиболее опасной инсайдерской угрозой является утечка конфиденциальной информации. От утечек конфиденциальной информации страдают как большие корпорации, так и маленькие фирмы. При этом руководители на удивление спокойно реагируют на прямую угрозу своему бизнесу. Даже когда ответственные за безопасность сотрудники предупреждают о том, что важные данные находятся под угрозой, начальство все равно продолжает бездействовать. Может показаться, что потеря нескольких документов не причинит сколько-нибудь значимого вреда. Однако, как показывает практика, сотни тысяч и даже миллионы долларов ущерба – это не редкость. Еще одним заблуждением руководителей является уверенность в том, что наибольшая опасность исходит извне. В действительности собственные работники, партнеры, поставщики и контрактники гораздо опаснее.

В процессе исследования в период с 2004 по 2006 г. компанией Info Watch были опрошены представители 1450 государственных и коммерческих организаций Российской Федерации. Результаты анализа данных опроса приведены на рис. 1.

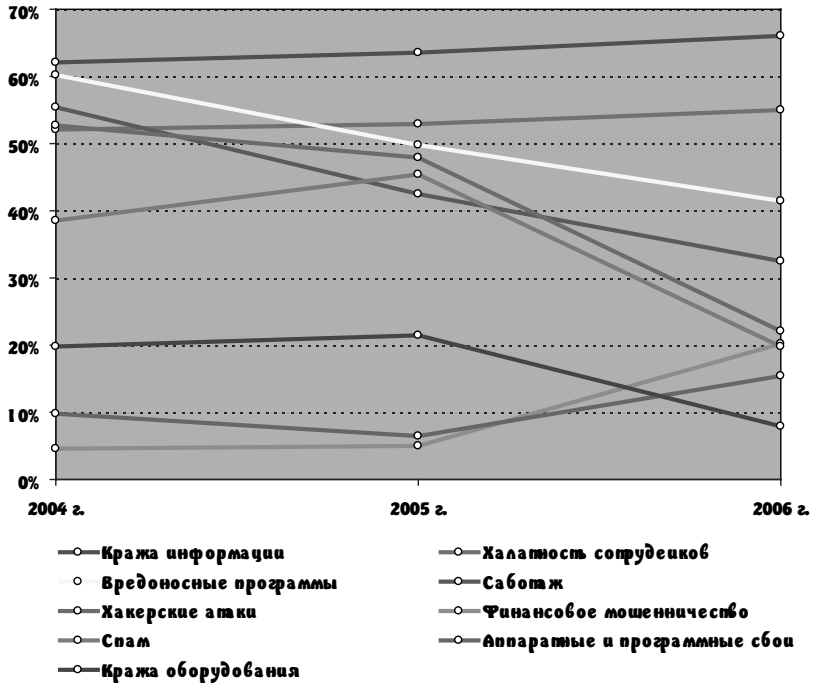

Рис. 1. Динамика изменения видов угроз ИБ

На первом месте находится кража информации (65,8%). Ее индекс опасности вырос 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%). Этого варианта ответа не было в предыдущих исследованиях, поэтому не представляется возможным проследить за динамикой изменения индекса опасности этой угрозы. Вирусные атаки заняли лишь третье место, набрав 41,7% голосов. По сравнению с 2005

годом эта угроза потеряла 7,3%, а с 2004 годом – 18,3%. Именно этот рейтинг опасности позволил такой угрозе, как халатность сотрудников, сразу же занять второе место в списке наиболее опасных угроз ИБ.

На четвертом месте оказалась угроза, которая также не входила в предыдущие исследования Info Watch. Это саботаж (33,5%). Высокий рейтинг опасности саботажа обусловлен тем, что респонденты постепенно утрачивают 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 2005 год эта угроза потеряла 24,6 процентных пунктов, а за два предыдущих года – 28,6%.

На рис. 2 показано соотношение внутренних и внешних угроз ИБ. При построении диаграммы к категории внутренних угроз были отнесены халатность сотрудников, саботаж и финансовое мошенничество, а к категории внешних угроз – вирусы, хакеры и спам. Из диаграммы видно, что инсайдерские атаки превалируют над вирусами, хакерами и спамом.

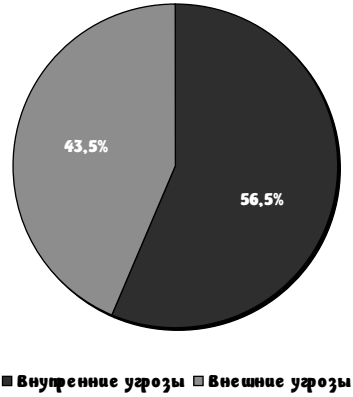

Рис. 2. Соотношение опасности внутренних и внешних угроз ИБ

По данным исследований «National Survey on Managing the Insider Threats», средний ежегодный ущерб в результате утечки информации из расчета на одну опрошенную компанию составляет $3,4 млн. Средний ежегодный ущерб вследствие вирусных атак, согласно исследованиям «2006 CSI/FBI Computer Crime and Security Survey», составляет менее $70 тыс. [1]

Аналитический центр компании Perimetrix также представил результаты исследования в области внутренней информационной безопасности в России. Компания Perimetrix с 10 января по 10 февраля 2008 года провела опрос сотрудников 472 российских организаций. Один из основных вопросов, заданных респондентам, касался угроз ИБ. Наибольшие опасения специалистов вызывают утечки данных (76%) и халатность пользователей (67%), что отражено на рис.3.

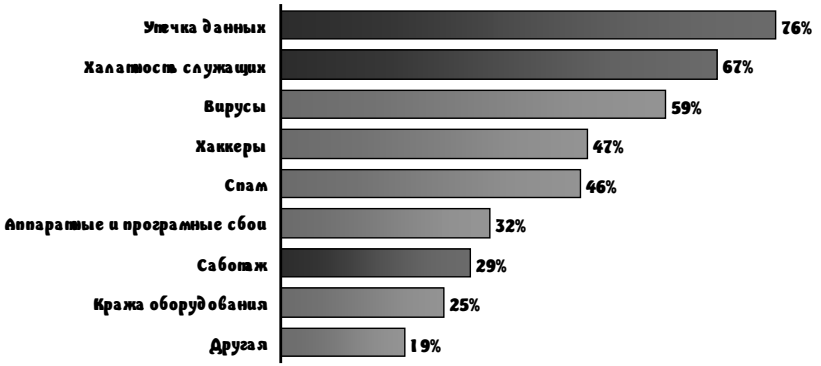

Рис. 3. Наиболее опасные угрозы ИБ

Оба пункта достаточно тесно связаны. Это обусловлено тем, что большое количество информации утекает не только по злому умыслу работников, но и из-за обычной невнимательности или халатности служащих [2]

По исследованию National Survey on Managing the Insider Threats, в ходе которого организация Ponemon Institute опросила 450 экспертов по ИТ-безопасности, 89% респонден-

тов считают атаки инсайдеров наиболее серьезной угрозой. Однако только 50% руководителей компаний согласны со своими подчиненными и признают значимость внутренних утечек. Согласно исследованию 2005 FBI Computer Crime Survey 44% компаний в течение года пострадали от инсайдерских инцидентов, утечки или искажения данных. По сведениям The Global State of Information Security – 2005, по вине инсайдеров происходит около 60% от общего числа инцидентов ИТ-безопасности, а средний ущерб от инсайдерских атак, по данным ФБР, составляет $355 тыс.

Исследование компании Annual Study: Cost of a Data Breach в 2006 году одновременно показывает предельные издержки компаний, пострадавших от утечек конфиденциальных данных и потери клиентской базы. Наибольшие убытки приходятся на непосредственные траты на ликвидацию последствий [3]. Но ущерб от вреда репутации компании может быть несоизмеримо больше. В таблице приведены данные исследований утечек информации по отраслям.

Таблица

Количество исследованных утечек по отраслям

Сфера деятельности	**Количество утечек**		
	Всего	**Внутренни**	**Внешних**
Розничная и интернет-торговля	7	7	0
Финансовые услуги	5	4	1
Аппаратное и программное обеспечение	3	1	2
Аутсорсинг	3	2	1
Здравоохранение	2	1	1
Фармацевтика	2	2	0
Страхование	1	0	1
Гостиничный бизнес	1	0	1
Авиалинии	1	1	0

Продолжение таблицы

Сфера деятельности	Количество утечек		
	Всего	Внутренни	Внешних
Образование	1	1	0
Телекоммуникации	1	0	1
Коммунальные услуги	1	1	0
Автоиндустрия	1	1	0
Другое	2	1	1
ВСЕГО	31 (100%)	22 (71%)	9 (29%)

Количество внутренних утечек информации значительно превосходит количество внешних утечек: 71% внутренних инцидентов против 29% внешних не оставляет в этом никакого сомнения. Особенно хорошо это заметно на примере первых двух отраслей: для сферы финансовых услуг на один внешний инцидент приходится до четырех внутренних. А для розничной и электронной торговли соотношение 7:0 в пользу инсайдеров.

Очевидно, что, борясь с инсайдерами, можно существенно снизить число инцидентов, а значит, уменьшить соответствующие издержки. Для многих организаций хотя бы предотвращение случайных утечек уже оправдывает затраты на систему безопасности.

По мнению экспертов аналитического центра Info Watch, от инсайдеров можно защититься (сохранив свою репутацию) и закрыть все каналы утечки, минимизировать человеческий фактор и запротоколировать все действия инсайдеров с конфиденциальной информацией. На рынке доступны специализированные решения, способные защитить конфиденциальную информацию и предотвратить инсайдерские атаки. Предлагаемые продукты достаточно гибки, так что их можно легко подстроить под корпоративные требования и стандарты. Кроме того, централизованное управление и автоматический контроль обеспечивают высокую эффективность работы даже

при больших объемах трафика, проходящего через почтовые и веб-серверы. Стоимость такого рода решений на несколько порядков меньше прогнозируемых убытков вследствие утечки. Ухудшение репутации компании является одним из наиболее тяжелых последствий инсайдерских атак даже на фоне огромных издержек на ликвидацию последствий утечек и возмещения ущерба пострадавшим.

Список литературы

1. Издание о высоких технологиях – CNews [Электронный ресурс] – Режим доступа: http://www. cnews.ru.
2. PERIMETRIX – защита конфиденциальных данных и секретов от инсайдеров. [Электронный ресурс] – Режим доступа: http://www.perimetrix.ru.
3. *Шаньгин В.Ф.* Информационная безопасность компьютерных систем и сетей. М.: ИД «ФОРУМ»: ИНФРА-М, 2008.
4. *Клейменов С.А., Мельников В.П., Петраков А.М.* Информационная безопасность и защита информации. М.: Издательский центр «Академия», 2006.
5. *Курбатов В.А., Скиба В.Ю.* Руководство по защите от внутренних угроз информационной безопасности. СПБ.: Питер, 2008.
6. Энциклопедия ИТ-аутсорсинга Outsourcing.ru [Электронный ресурс] – Режим доступа: http://www.outsourcing.ru

Научный руководитель – Ф.А. Юн, кандидат технических наук

Наши авторы

Большаков Максим Юрьевич	Аспирант, г. Москва, СГА
Ермошин Василий Геннадьевич	Аспирант, г. Москва, СГА
Ефимов Н. Ю.	Аспирант, г. Москва, СГА
Кононов Виктор Павлович	Кандидат философских наук, Вельск, СГА
Косарев Александр Александрович	Аспирант, г. Калининград, СГА
Куликова Галина Геннадьевна	Помощник директора по воспитательной работе, связям с общественными организациями и СМИ, Новосибирск, СГА
Пеникер Ольга Васильевна	Преподаватель, г. Обнинск, СГА
Павличенко Александр Викторович	Кандидат экономических наук, преподаватель, г. Фрязино, СГА
Селезнева Наталья Николаевна	Студентка, г. Новосибирск, СГА
Роговая Анастасия Владимировна	Аспирант, г. Москва, СГА
Сизов Николай Иванович	Кандидат физико-математических наук, преподаватель, г. Обнинск, СГА
Старков Максим Игоревич	Аспирант, г. Магадан, СГА
Утенков Геннадий Николаевич	Кандидат политических наук, г. Саратов, СГА

Труды СГА

№ 11 ноябрь 2008

Юриспруденция. Экономика. Психология. Образование. Философия. Социология. Политология. Информатика

0000.901.132.08/11.13

Редактор — Н.С. Ковалева
Компьютерная верстка — А.Б. Кондратьева

Сдано в печать 21.11.08
Издательство СГУ
Тираж 700 экз. Заказ

109029, Москва, ул. Нижегородская, 32, корп. 1, к. 206
Телефон: (495)727-12-41 доб. 31-69