



INFOWATCH
INFORMATION WATCH TECHNOLOGIES

Утечки первого полугодия 2008

Аналитический отчёт

Москва - 2008

Оглавление

Введение	3
Откуда утекает информация	3
Как утекает информация	5
Каналы утечек	8
Латентность	13
Крупнейшие утечки	15
Выводы	16
О компании Infowatch	17
Контактная информация	17

Введение

Аналитический центр InfoWatch подводит итоги истекшего первого полугодия и представляет очередное исследование инцидентов внутренней информационной безопасности. Целью проекта было проанализировать все упоминавшиеся в СМИ утечки конфиденциальной информации и выявить закономерности.

Анализировались инциденты во всех странах мира и во всех отраслях, сообщения о которых поступили в первом полугодии 2008 года. Всего таких сообщений 185 — почти точно по 1 инциденту за день. За предыдущие годы удельное число инцидентов было чуть ниже (0,91).

Сведения обо всех инцидентах собираются в базе данных утечек, которая ведётся с 2004 года. Каждому инциденту присваивается ряд параметров, по которым можно производить поиск, подсчитывать статистику и искать корреляции. Неформализованные сообщения об инцидентах публикуются на веб-сайте компании (<http://www.infowatch.ru/threats>).

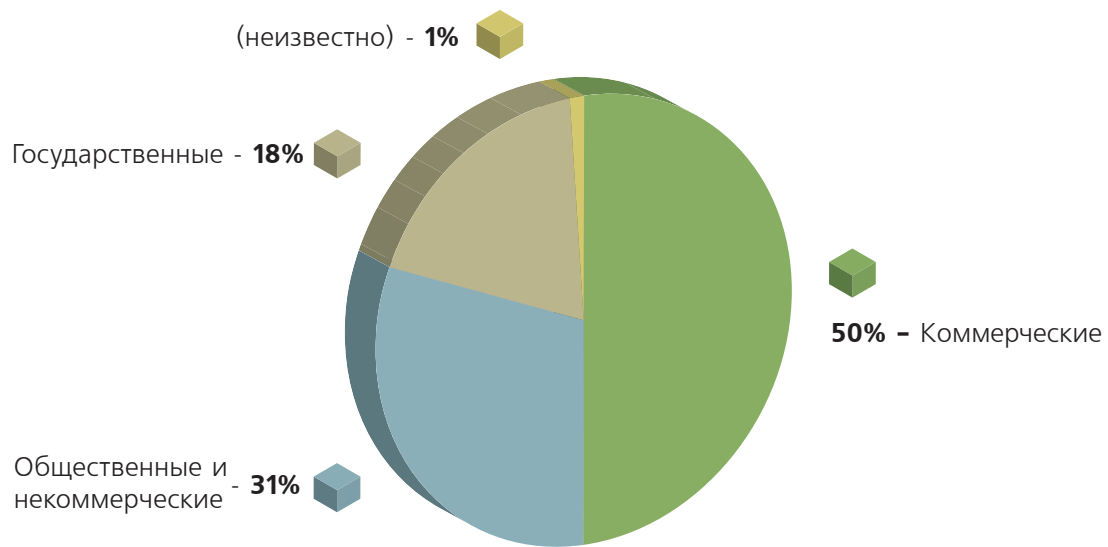
Откуда утекает информация

Предприятия, из которых произошли утечки, поделены на три категории: государственные, коммерческие и прочие. Все учебные заведения отнесены в третью категорию. Хотя формально школы и вузы могут числиться «коммерческими» или государственными. Традиционно учебные заведения довольно сильно отличаются по принятым в них порядкам как от производственных предприятий, так и от государственных органов.

В категорию коммерческих предприятий включены финансовые, страховые, медицинские, производственные, транспортные предприятия, операторы связи и все те, кто занимается коммерческой деятельностью.

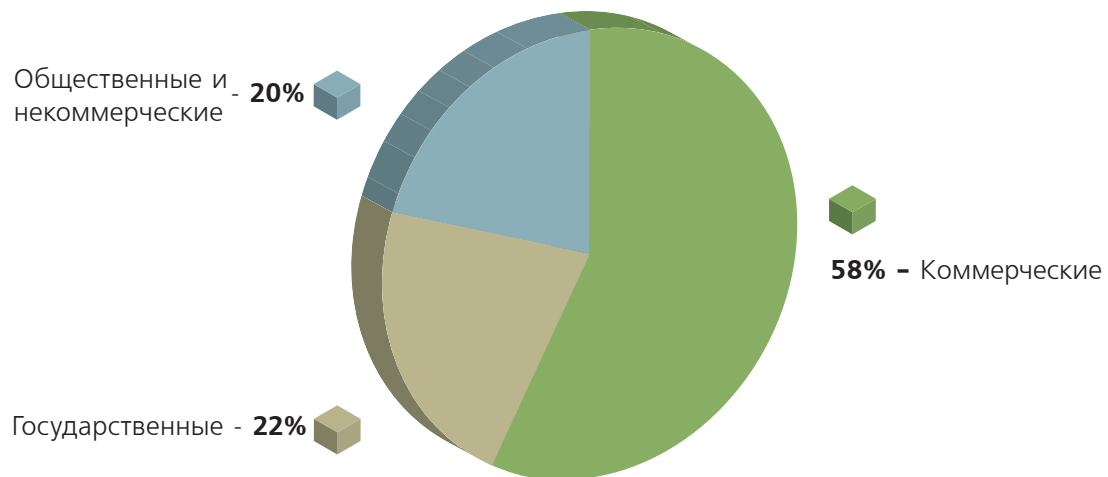
Ниже приведено распределение инцидентов по типам организаций за исследуемый период, а также — для сравнения — за 2007 год.

Рис. 1. Источник утечки, I/2008



Распределение инцидентов по типу организации, 1 полугодие 2008.

Рис. 2. Источник утечки, 2007



Распределение инцидентов по типу организации, 2007

По сравнению с прошлым годом немного увеличилась доля образовательных и некоммерческих организаций за счёт сокращения доли коммерческих. Это изменение не выглядит принципиальным.

Хотя можно сделать замечание о том, что защищённость информационных ресурсов в вузах в среднем слабее. Часто администрирование информационных систем осуществляется студентами.

Кроме того, скрыть имевшую место утечку шансов меньше, чем на предприятии. В последнем случае работники хоть немного заинтересованы в сохранении деловой репутации своего учреждения, обнародование утечки негативно на ней отражается. Получив предписанное законом (для случая США) уведомление об имевшей место утечке, далеко не все сотрудники спешат делиться новостью с прессой. Студенты же, как известно из марксистской теории, являются деклассированными элементами, деловая репутация, стабильность и прочие интересы собственника им не так близки, как среднему классу. Поэтому утечки в университетах, очевидно, чаще попадают в средства массовой информации.

Видимое снижение доли госорганов по сравнению с 2007 годом (с 22 до 18%) находится в пределах статистической погрешности. Но в 2007-м эта доля снижалась. Аналитики объясняли это тем, что растёт число коммерческих предприятий, обрабатывающих персональные данные и иную конфиденциальную информацию в электронном виде. А число госорганов не растёт. Степень же защищённости от утечек в государственном и негосударственном секторе сейчас не сильно отличаются и не будут сильно различаться впредь.

Распределения утечек по типу организации отдельно для умышленных и неумышленных утечек не приводятся в настоящем отчёте, поскольку существенных отличий между ними не обнаружено. То есть, показатель умышленности/случайности не коррелирует с типом организации.

Подытоживая главу, можно сказать, что доля организаций, откуда происходят утечки, определяется в меньшей степени средней защищённостью в этих организациях, а в большей степени — вероятностью огласки инцидента.

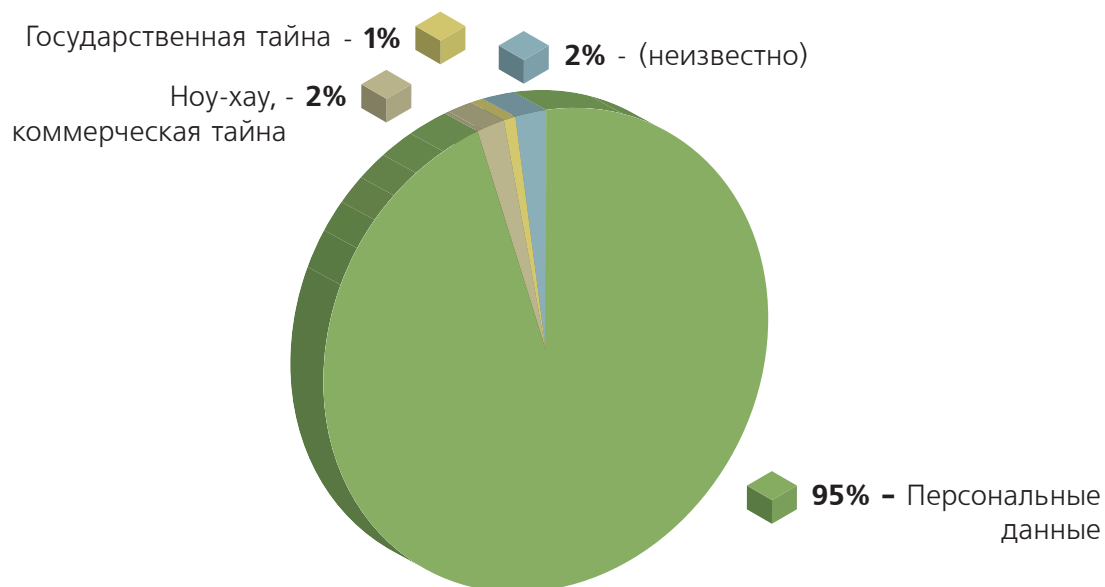
Какая информация утекает

Ниже представлено распределение утечек по типу утекшей информации.

Персональные данные, как и в прошлом году, составляют абсолютное большинство (95%). Ввиду обязательности уведомлений об утечках персональных данных в США, а также ввиду повышенного общественного интереса к этой теме, инциденты с персональными данными чаще попадают в прессу. Зафиксированы сообщения СМИ об мелких утечках, составляющих сотню или всего нескольких десятков записей.

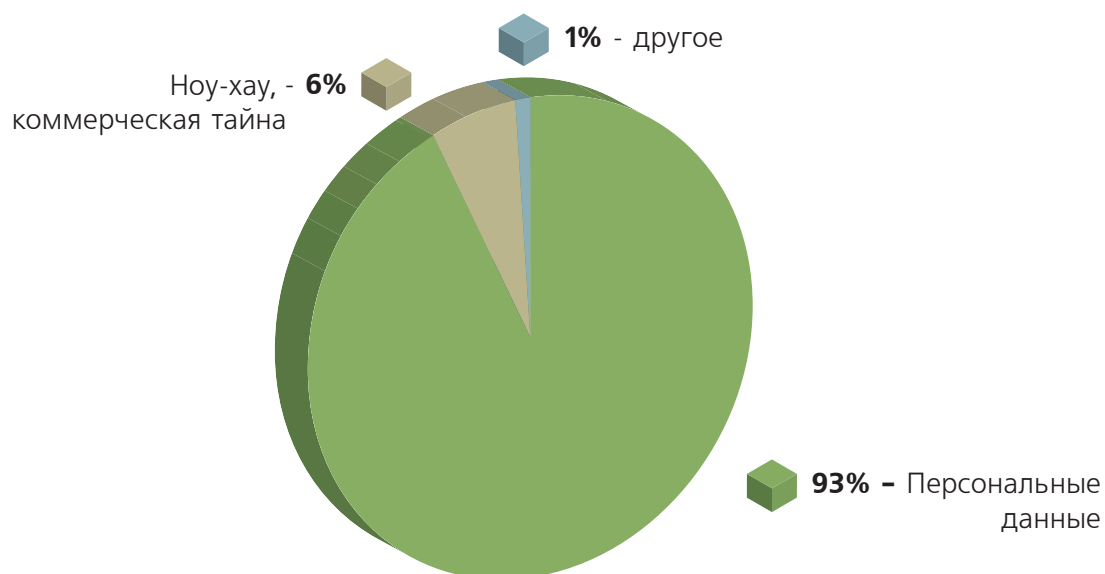
И эти сообщения распространяются по каналам информационных агентств. То есть, в статистику попадает даже мелочёвка местного масштаба. В то же время, коммерческую тайну (а тем более – гостайну) предпочитают терять «молча», ибо огласка инцидента лишь увеличит размер ущерба. И пресса почему-то не торопится распространять по миру сообщения о мелких утечках коммерческой тайны с убытками, например, в тысячу долларов. Даже если об этом становится известно.

Рис. 3. Объект утечки, I/2008



Распределение инцидентов по типу конфиденциальной информации, 1 полугодие 2008

Рис. 4. Объект утечки, 2007



Распределение инцидентов по типу конфиденциальной информации, 2007

Всё дело в актуальности темы. Инцидент с персональными данными каждый читатель осознанно или неосознанно примеряет на себя, как следствие — переживает и сочувствует. В случае с секретом производства или с коммерческой тайной зацепить читателя можно лишь огромным размером убытков, в крайнем случае — суровым приговором для инсайдера. Поэтому в базе инцидентов InfoWatch преобладают и будут преобладать именно персональные данные.

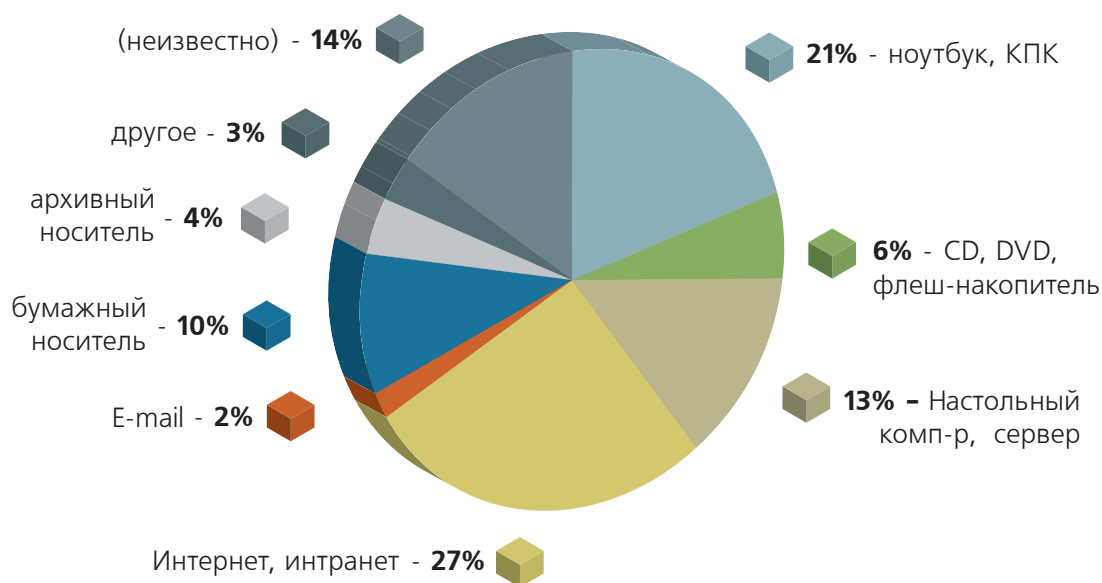
Кстати, в 2006 году в аналогичном исследовании InfoWatch доля персональных данных была ещё ниже — 81%. В будущем ожидается дальнейший рост стоимости персональных данных. Под стоимостью здесь имеется в виду не стоимость их легального получения, обработки и хранения, а ценность персональных данных с точки зрения злоумышленника. Следовательно, утечки будут продолжаться.

Резюмируя, повторим, что защита персональных данных является ныне актуальной (можно сказать «модной») тенденцией. Этой защите уделяется повышенное внимание со стороны общественности и контролирующих органов.

Каналы утечек

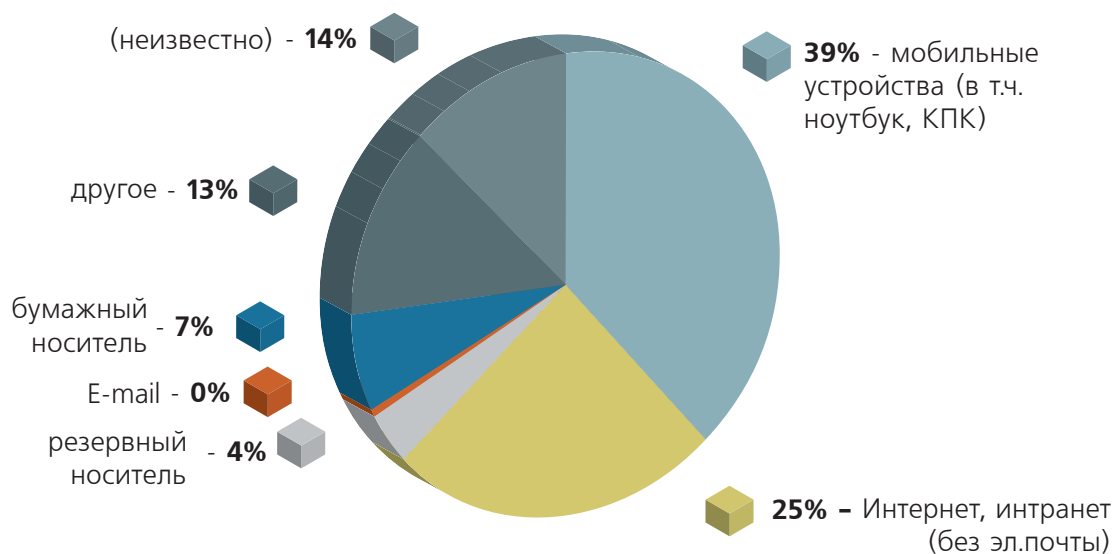
Для разработки организационно-технических средств защиты от утечек, для приоритезации таких работ необычайно важно знать о каналах, по которым несанкционированно передаётся информация. На следующей диаграмме представлено распределение утечек по виду носителя, который использовался для перемещения информации за пределы информационной системы.

Рис. 5. Каналы утечек, I/2008



Распределение утечек по носителям, 1 полугодие 2008.

Рис. 6. Каналы утечек, 2007



Распределение утечек по носителям, 2007.

По сравнению с предыдущим годом, общая картина изменилась не сильно. Практически все изменения лежат в пределах статистической погрешности. Новая категория «настольные компьютеры и серверы» в прошлом году входила в «другое».

По-прежнему очень популярны такие способы утечек, как кражи/потери ноутбуков и случайная публикация в сети («расширивание») файлов.

Не похоже, чтобы кражи ноутбуков начали сокращаться. Дело здесь не в том, что «воруют». Конечно же, воровали, воруют и будут воровать. Да и терять портативные компьютеры и флэшки люди не перестанут, такова уж природа. Однако если конфиденциальная информация хранилась на пропавшем носителе в зашифрованном виде, то такая потеря вовсе не считается инцидентом, в базах данных не учитывается и не имеет правовых последствий в виде обязательного уведомления. Казалось бы, чего проще — поставить программные криптодиски на все путешествующие компьютеры и флэш-накопители. Их выбор широк, в том числе, имеются совершенно бесплатные, но при том удобные утилиты. Но по какой-то причине корпоративные пользователи и их начальники не используют криптодиски. Аналитический центр InfoWatch вынужден признаться, что объяснить этот факт не в состоянии. Видимо, причины лежат где-то в жутких глубинах бессознательного, и достать их оттуда сможет только новый Фрейд.

Объяснить явление, но не указать способы улучшения ситуации — это довольно типично для аналитиков. А в нашем случае ситуация нетипичная, зато позитивно-перспективная. Нет объяснений, но есть несложная рекомендация, которая позволит снизить вероятность утечки сразу на 27%. Все мобильные устройства (ноутбуки, КПК, флэш-накопители) должны быть снабжены криптоконтейнером. Не обязательно вводить шифрование всего диска. Вполне достаточно держать зашифрованными только конфиденциальные файлы, директории или соответствующий раздел диска. Программное обеспечение для этого имеется разнообразное, не дорогое, есть и бесплатные аналоги.

В прошлом, 2007 году доля мобильных устройств сокращалась, а доля сетевых каналов росла. В этом году тоже можно говорить о небольшом сокращении доли мобильных устройств (с 39 до 27%). Впрочем, наши аналитики полагают это изменение не принципиальным за счёт большой доли «не установлено».

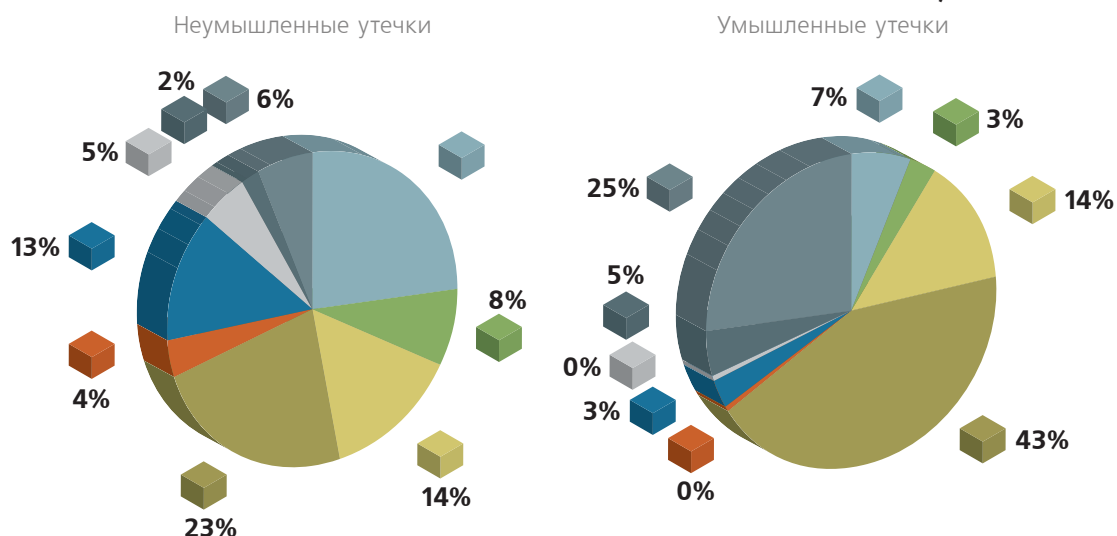
Обращает на себя внимание малое количество утечек по электронной почте (4 случая за полугодие). А в 2007 году зафиксирован всего 1 инцидент с электронной почтой. И это при том, что во всех случаях внедрения DLP-систем (систем защиты от утечек конфиденциальной информации) заказчик требовал обязательного контроля этого канала. А во многих внедрениях канал e-mail был вообще единственным, который контролировался. Столь неразумный подход объясняется двумя причинами. Во-первых, с точки зрения неквалифицированного пользователя отправить конфиденциальный документ по электронной почте – это первое, что приходит в голову. Топ-менеджер, заказывающий DLP-систему, может на этой первой мысли остановиться. Инсайдер же, который замыслил худое, обязательно подумает вторично и подберёт более подходящий канал, например, флэш-накопитель. Во-вторых, электронную почту проще всего проконтролировать технически. Из всех каналов этот – единственный, не требующий онлайн-анализа. Отправляемая и получаемая корреспонденция может несколько минут полежать в очереди, дожидаясь окончания проверок. Ни для http-трафика, ни для распечаток на принтере минутные задержки не приемлемы. Относительная простота реализации привела к тому, что решения для контроля электронной почты появились раньше, стоят дешевле и представлены на рынке в большем разнообразии.

Если подсчитать вышеуказанную статистику отдельно для умышленных и неумышленных утечек, то мы увидим, что утечки по сети (коричневый сектор) более характерны для умышленных действий, в то время как мобильные носители (синий и голубой сектора) больше для случая неумышленных.

Таким образом видно, что если мы решили в первую очередь бороться со случайными утечками, нам надо сосредоточиться на шифровании мобильных носителей (ноутбуков и флэшек,

25% и 8% соответственно), а также на должном уничтожении ненужных бумаг (белый сектор, 13%).

Рис. 7. Неумышленные и умышленные утечки, I/2008

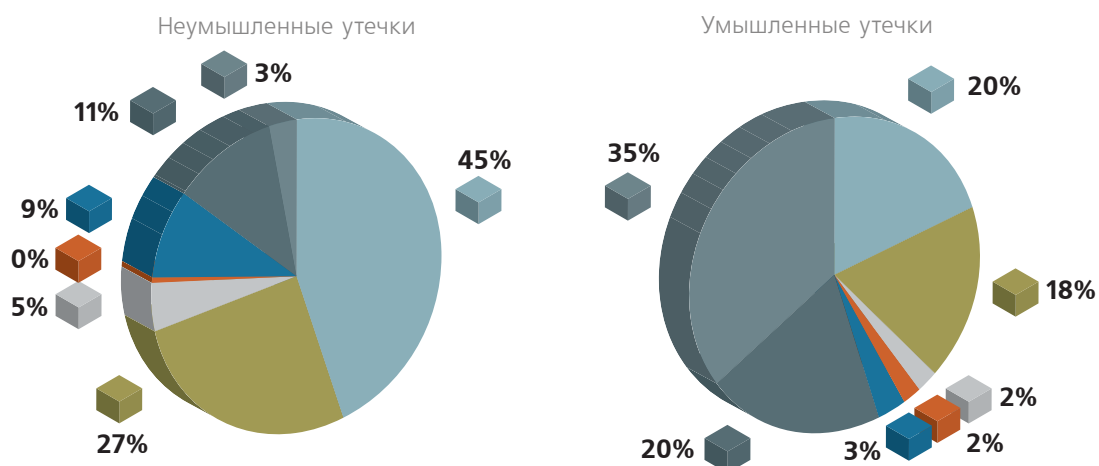


Распределение утечек по носителям отдельно для случайных (слева) и умышленных (справа) утечек, 1 полугодие 2008

Условные обозначения

- мобильные устройства (в т.ч. ноутбук, КПК)
- CD, DVD, флеш-накопитель
- Настольный компьютер, сервер
- Интернет, интранет
- E-mail
- бумажный носитель
- архивный носитель
- другое
- (неизвестно)

Рис. 8. Неумышленные и умышленные утечки, 2007



Распределение утечек по носителям отдельно для случайных (слева) и умышленных (справа) утечек, 2007

Злоумышленник действует разумно и, как правило, знает о системе контроля. Поэтому он постарается воспользоваться иным каналом, тем, который не контролируется. То есть, для противодействия умышленным утечкам важна полнота охвата возможных каналов. Системы защиты, которые способны контролировать меньше трёх различных каналов, вообще не считаются настоящими DLP-системами среди профессионалов.

На следующей диаграмме показано деление инцидентов на умышленные и случайные. Для случая кражи компьютера утечка считается случайной, если умысел вора был направлен на компьютер как дорогостоящую технику, а не на информацию.

Рис. 9. Причины утечки, I/2008

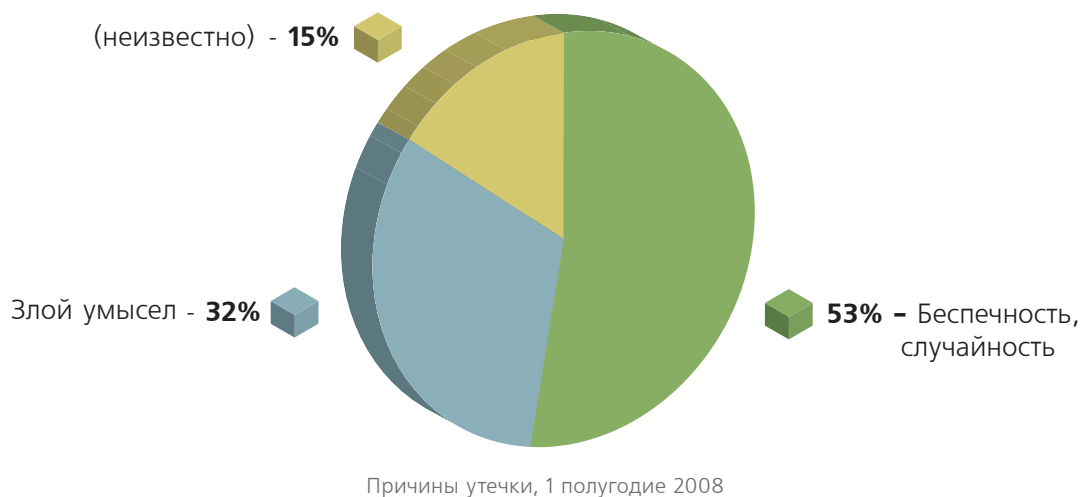


Рис. 10. Причины утечки, 2007



Процент злоумышленных утечек возрос незначительно (с 29 до 32%). В прошлом году он не изменялся по отношению к позапрошлому.

Аналитики InfoWatch предсказывали, что доля неумышленных утечек будет сокращаться. Конечно, полгода — не срок, чтобы тенденции проявились. Возможно, мы увидим их в 2009 году.

Дело в том, что противодействовать случайным утечкам несравненно проще. Почти любая DLP-система (даже система, не достигающая до высокого звания DLP) в автоматическом режиме может предотвратить существенное количество ненамеренных утечек на тех каналах, которые она обрабатывает. А внедрение DLP-систем идёт по всему миру. Что же касается утечек умышленных, то здесь бороться предстоит не со слепой случайностью, а со злым умыслом. Противником DLP-систем и служб ИБ является человек — разумный, хитрый, заинтересованный, а иногда даже квалифицированный. Поэтому эффективность здесь ниже.

Но пока DLP-системы и иные средства борьбы с внутренними угрозами не внедрены на заметном количестве предприятий, упомянутая тенденция не проявится.

Латентность

Значительная часть утечек конфиденциальной информации скрывается. Особенно когда в деле участвует только одна организация. Как можно оценить латентность, то есть процент утечек, не попавших в учёт.

Имеется возможность прикинуть величину относительной латентности. А именно посмотреть, насколько больше скрывается по сравнению с самой открытой в этом отношении страной.

Следующая таблица иллюстрирует латентность утечек персональных данных.

Таблица 1.

Латентность утечек персональных данных по странам мира

Страна	Число утечек	Доля	Утечки на млн. населения
США	148	80.00%	0.505
Великобритания	14	7.57%	0.232
Канада	4	2.16%	0.123
Россия	4	2.16%	0.028
Китай	3	1.62%	0.002
Ирландия	2	1.08%	0.333
Италия	2	1.08%	0.034
Австралия	1	0.54%	0.050
Чили	1	0.54%	0.064
Германия	1	0.54%	0.012
Франция	1	0.54%	0.017
Индия	1	0.54%	0.001
Корея	1	0.54%	0.021
(другие)	1	0.54%	-

В последнем столбце приведено отношение числа утечек, о которых стало известно, к численности населения страны. Резко выделяется показатель для США. В большинстве штатов этой страны закон требует уведомлять субъектов персональных данных об утечке. Понятно, что факт такого уведомления, а следовательно, и факт утечки обычно попадает в СМИ. В других странах, где обязательного уведомления нет, утечки реже становятся достоянием гласности.

Приняв, что в США самый низкий уровень латентности инцидентов с персональными данными, мы можем оценить, насколько этот уровень занижен в других странах. Экстраполируя данные верхней строки таблицы, можно оценить число утечек для развитых стран (то есть для стран с высокой ликвидностью персональных данных) величиной **1 утечка в год на каждый миллион населения** (напомним, учтены данные за полугодие).

Отталкиваясь от этой оценки, можно предположить, что в Великобритании при надлежащей гласности было бы зафиксировано 30 инцидентов вместо 14, в Канаде – 16 вместо 4, в Италии – 29 вместо 2.

Кстати, в Великобритании рассматривается законопроект, предусматривающий уведомление об утечках (<http://www.infowatch.ru/threats?chapter=150685169&id=207733071>). Если он будет принят, удельное число утечек должно подняться до такого же уровня, как в США.

Крупнейшие утечки

В истекшем полугодии можно выделить следующие утечки данных, которые считаются крупнейшими.

Таблица 2.

Крупнейшие утечки данных 1 полугодия 2008 г.

Количество записей	Страна	Дата обнародования	Инцидент (при нажатии открывается источник)	Тип утечки
24 000 000	Италия	22 апреля 2008 г.	Публикация данных о доходах всех налогоплательщиков Италии	Публикация конфиденциальных файлов в сети
8 500 000	Индия-США	29 мая 2008 г.	Крупнейшая кража данных в истории Индии инсайдером	Вскрытие базы данных
6 000 000	Чили	12 мая 2008 г.	Крупнейшая утечка данных в Чили	Взлом серверов
4 500 000	США	21 мая 2008 г.	Bank of New York Mellon потерял персональные данные клиентов	Утеря архивного носителя
4 200 000	США	17 марта 2008 г.	Утечка в сети супермаркетов Ханнафорд	Взлом компьютерной сети
2 200 000	США	11 июня 2008 г.	Утечка из Клиник и госпиталей университета Юты	Утеря архивного носителя
2 100 000	США	17 апреля 2008 г.	Университет Майами потерял данные пациентов клиники вуза	Кража архивного носителя
1 000 000	США	21 марта 2008 г.	Похищение базы данных у Compass Bank инсайдером	Кража архивного носителя
700 000	США	18 апреля 2008 г.	Утечка из Агентства по сбору задолженностей по потребительскому кредиту штата Индиана	Кража сервера
500 000	Германия	23 июня 2008 г.	В 200 городах Германии скомпрометированы персональные данные граждан	Случайная публикация конфиденциальных данных в сети
321 000	США	13 февраля 2008 г.	Банк крови Lifeblood штата Теннесси потерял ноутбуки с персональными данными	Кража портативных компьютеров

Из-за таких крупных утечек, где число пострадавших сопоставимо с численностью населения страны, может сложиться

ситуация, когда персональные данные существенной части граждан обращаются на чёрном рынке.

Хищение информации в корне отличается от хищения материальных ценностей: похищенное практически невозможно найти и вернуть. Однажды попав в обращение, данные навсегда становятся достоянием андерграунда. Даже перевыпустить банковские карты занимает время, а многие скомпрометированные данные заменить трудно.

Аналитический центр InfoWatch пока не может оценить процент персональных данных, которые были скомпрометированы. Однако мы работаем над этим. Если такой процент окажется высок в какой-либо стране или отрасли, то можно будет говорить о снятии защиты этих данных вообще и о переходе на иные методы предотвращения злоупотреблений.

Выводы

1. Персональные данные в настоящее время — модная тема. Их защите уделяется повышенное внимание, об их утечках пресса сообщает сравнительно чаще. Для их защиты предлагается больше новых технических средств и юридическо-организационных методов. Но нельзя сказать, что угрозы, связанные с персональными данными, сильно переоценены.
2. Большая часть утечек происходит неумышленно. Перекрыть возможности случайной утечки означает решить проблему на три четверти. Борьба же с инсайдерами-злоумышленниками — это в среднем менее приоритетная и более сложная задача. При ограниченности средств её следует решать во вторую очередь.
3. Мобильные носители информации (ноутбуки, флэшки и т.п.) и Интернет — это два основных канала утечек. Как намеренных, так и случайных. «Мобильные» ненамеренные утечки достаточно легко перекрыть, введя обязательное шифрование данных.
4. Меры по борьбе с утечками конфиденциальной информации обязательно должны сопровождаться мерами по преодолению последствий утечек. То есть, имеет смысл с самого начала планировать, что делать, когда утечка произойдёт. В некоторых случаях избежать утечки очень трудно, зато сгладить последствия легко.

О компании InfoWatch

InfoWatch – ведущий российский производитель программного обеспечения, разрабатывающий уникальные технологии в области информационной безопасности – защиты от внутренних угроз.

Продукты компании позволяют минимизировать риски 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.

Совместно с традиционными системами защиты – средствами разграничения доступа – InfoWatch позволяет построить комплексную корпоративную структуру информационной безопасности благодаря обеспечению «тыла» – надежной защиты от внутренних угроз.

InfoWatch была учреждена в ноябре 2003 г. компанией «Лаборатория Касперского», ведущего российского разработчика систем защиты от внешних угроз. InfoWatch впитала бесценный 15-летний опыт «Лаборатории Касперского» по внедрению комплексных проектов нейтрализации вирусов, хакерских атак, «спама» и успешно применяет его в области противодействия внутренним угрозам.

Среди наших клиентов – Министерство экономического развития и торговли РФ, ВТБ, РусГидро, Транснефть, ВымпелКом, Федеральная таможенная служба РФ.

Контактная информация

Компания InfoWatch

Российская Федерация, 125363, Москва, проезд №607, д. 30

Тел./факс: +7 495 22 900 22

E-mail: info@infowatch.ru

Веб-сайт: www.infowatch.ru