Глобальное исследование утечек конфиденциальных данных. Первое полугодие 2009

Компания InfoWatch предлагает вниманию специалистов очередное глобальное исследование статистики по инцидентам, связанным с утечками конфиденциальной информации. Основой для данного отчёта является база данных утечек, которую ведет аналитический центр компании InfoWatch. База инцидентов ведётся с 2004 года, и в неё включаются все инциденты во всех странах мира, информация о которых была опубликована в СМИ, а также блогах, веб-форумах и других сетевых ресурсах.

Качественная характеристика

Количество зафиксированных в расчёте на 1 день утечек продолжает постоянно увеличиваться. Трудно сказать, отражает ли это реальное увеличение числа инцидентов, или дело в том, что наша компания интенсифицировала работу по сбору информации. Скорее, то и другое одновременно. За 1-е полугодие 2009 года была опубликована информация о 413 утечках (2,3 утечки в сутки). Для сравнения: во втором полугодии 2008 было зафиксировано 273 утечки. Таким образом, рост составил 51%.

Тема утечек конфиденциальной информации (особенно персональных данных) продолжает оставаться актуальной в СМИ. Даже инциденты в малоизвестных организациях с десятком пострадавших лиц привлекают интерес публики и освещаются местной прессой. Когда же много потенциальных пострадавших, замешана крупная корпорация, известная личность, то сообщение об утечке быстро расходится по мировым информагентствам, переводится, перепечатывается и обсуждается в Интернете.

Довольно часто стали появляться сообщения об утечках в России. Их за отчётное полугодие зафиксировано 23 (для сравнения: за прошлое полугодие их было всего 2). Это является прямым следствием актуализации темы персональных данных. Новый российский закон «О персональных данных» (152-ФЗ) стал активно применяться государственными органами: набирают обороты проверки Роскомнадзора, компании серьёзно озаботились приведением в соответствие своих информационных систем. Все эти факты породили очередной всплеск интереса СМИ к теме персональных данных и их утечек.

В других странах столь радикального всплеска интереса к теме не наблюдается. Но спада интереса также нет, тема продолжает оставаться актуальной и интересной для широкого круга читателей, не говоря уже про экспертов в области информационной безопасности.

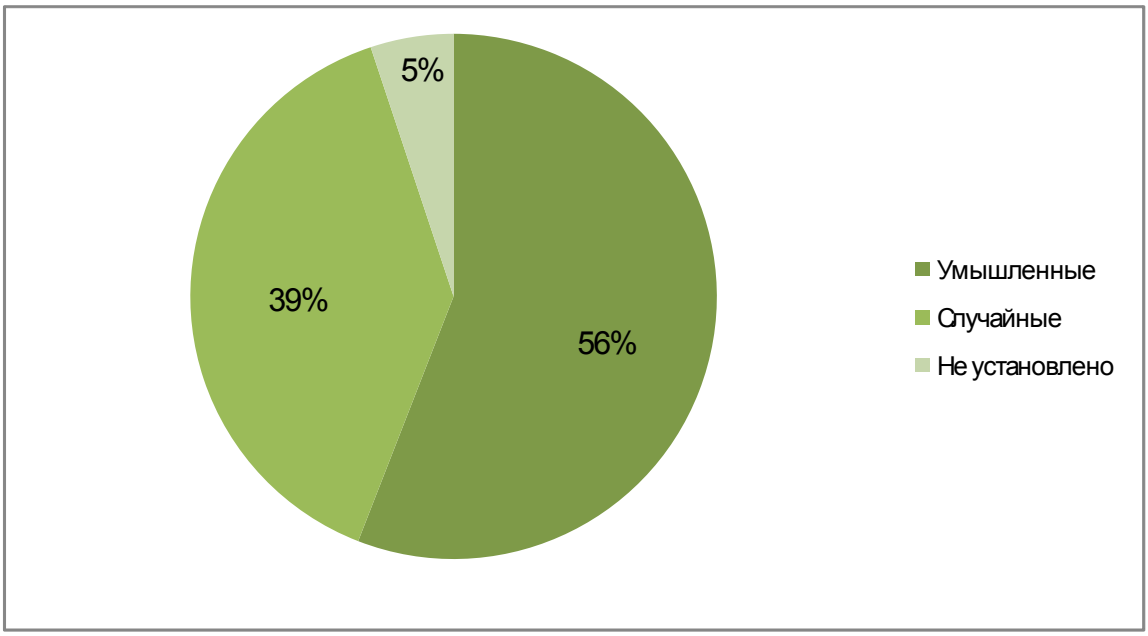
Умысел или случайность?

В 1-м полугодии 2009 года заметно выросла доля умышленных инцидентов. В предыдущие периоды их доля также постепенно увеличивалась, но в пределах статистической погрешности. Теперь же эксперты InfoWatch уверенно констатируют, что умышленных утечек стало больше.

Таблица 1: Доли умышленных и случайных утечек

Вид утечек	1-е полугодие 2009		2-е полугодие 2008	
	Кол-во	%	Кол-во	%
Умышленные	231	55.9%	133	48.7%
Случайные	161	39.0%	105	38.5%
Не установлено	21	5.1%	35	12.8%

Диаграмма 1: Доли умышленных и случайных утечек в 1-м полугодии 2009 года



Разные виды персональных данных имеют разную цену для злоумышленников (многие виды им вообще не нужны). Так, в США и Великобритании (откуда «родом» большинство фиксируемых утечек) прагматично защищают не любые персональные данные, а лишь те, которые злоумышленники могут быстро конвертировать в деньги. Именно за такими данными охотятся злоумышленники. Прежде всего, это данные банковских карт и номера социального страхования (SSN – Social Security Numbers). Сбыт и дальнейшее использование такой информации отлажены. И чем дальше, тем больше возможностей появляется у людей, желающих незаконным образом заработать на продаже ПД, тем шире масштабы этого криминального рынка.

Как видно из диаграммы 1, при неуклонном росте числа как случайных, так и умышленных утечек, количество последних выросло намного больше. В ближайшее время эта тенденция сохранится. Это связано, в первую очередь, с тем, что современные средства противодействия утечкам (в том числе, DLP-системы) достаточно эффективно предотвращают лишь случайные утечки по различным каналам. Для противодействия же умышленным утечкам данных требуется полный контроль всех информационных каналов и грамотные специалисты, способные должным образом настроить систему защиты от утечек и умеющие правильно её использовать.

Таким образом, есть основания полагать, что более широкое внедрение технических методов борьбы с утечками, которое мы отмечаем почти во всех странах, приведёт к выявлению и пресечению утечек обоих видов. Но эти методы будут менее эффективны в случае с умышленными утечками. Следовательно, доля умышленных утечек в ближайшее время будет неуклонно расти.

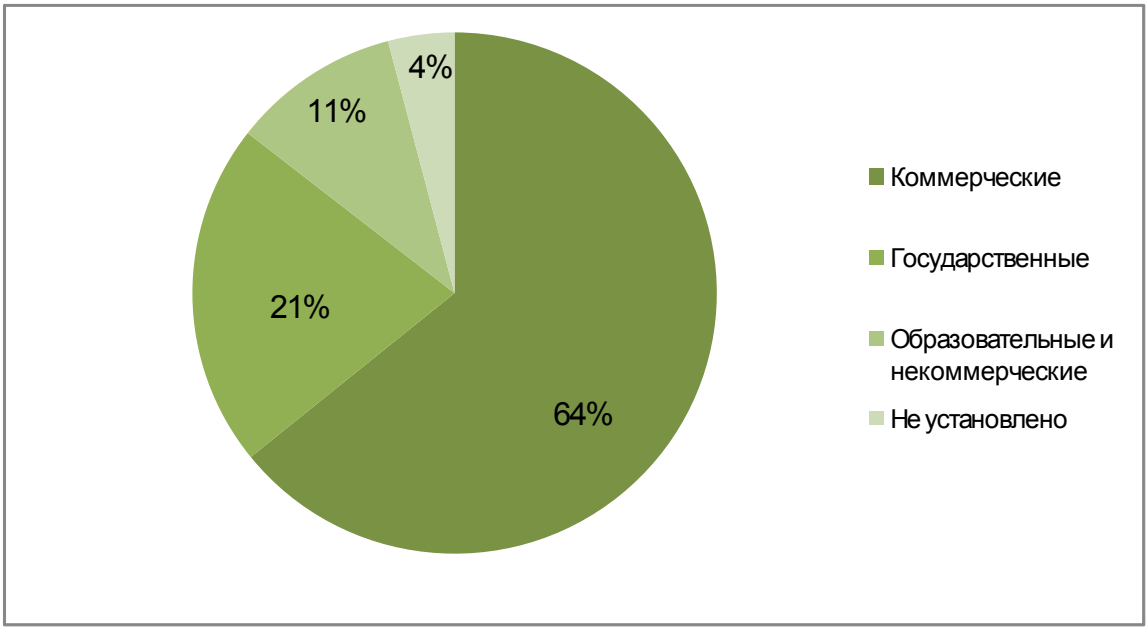
Откуда утекают конфиденциальные данные?

Все предприятия и организации, в которых произошли утечки, ставшие публичными, эксперты InfoWatch подразделяют на три категории: государственные учреждения, коммерческие предприятия, а также учебные заведения и общественные, некоммерческие структуры. Учебные заведения, безусловно, бывают как некоммерческими, так и коммерческими, то есть ориентированными на получение прибыли, тем не менее, эксперты InfoWatch выделяют их в особую категорию, поскольку условия обработки персональных данных студентов не похожи на аналогичные условия в банках, клиниках, магазинах и иных «традиционно коммерческих» предприятиях.

Таблица 2: Распределение источников утечек по видам организаций

Вид организаций	1-е полугодие 2009		2-е полугодие 2008	
	Кол-во	%	Кол-во	%
Коммерческие	265	64.2%	150	54.9%
Государственные	88	21.3%	63	23.1%
Образовательные и некоммерческие	43	10.4%	58	21.2%
Не установлено	17	4.1%	2	0.7%

Диаграмма 2: Распределение источников утечек по видам организаций в 1-м полугодии 2009 года



Как видно из таблицы и диаграммы, в 1-м полугодии 2009 года доля утечек конфиденциальных данных в образовательных учреждениях заметно снизилась за счёт увеличения соответствующего числа на коммерческих предприятиях. Однозначное объяснение такому снижению дать сложно, однако аналитики InfoWatch предполагают, что это может быть связано с мировым финансовым кризисом. В этот период в коммерческом секторе обостряется конкуренция, и происходят массовые увольнения персонала. То и другое способствует увеличению числа утечек данных. На учебные заведения кризис в этом смысле не влияет. Персональные данные студентов не являются инструментом недобросовестной конкуренции, поэтому если их и воруют, то не более интенсивно, чем до кризиса.

Есть этому и другое объяснение. Ещё совсем недавно ситуация в системах

информационной безопасности вузов была столь удручающей, что наведение в ней элементарного порядка (хотя бы установка паролей на доступ к сети, запрета общего доступа к данным на дисках рабочих станций и т.п.) было достаточно для того, чтобы значительно сократить риск утечек ПД студентов.

Если проанализировать статистику умышленных и случайных утечек произошедших в каждом из трёх упомянутых типов организаций отдельно, то существенной разницы обнаружено не будет. Этот результат отличается от того, что был в прошлые годы, когда умышленных утечек было несколько больше в коммерческих организациях, а случайных – в учебных заведениях. На сегодняшний день частичные распределения для случайных и умышленных утечек почти не различаются. Это можно объяснить усовершенствованием методов защиты и профилактики инцидентов. После того, как вопрос о важности защиты персональных данных в течение многих лет обсуждался в СМИ ведущих мировых держав, сегодня в этих странах существует чёткое осознание необходимости обеспечения информационной безопасности во всех типах организаций, включая школы. Везде присутствует хоть какая-то организационная и техническая защита от утечек данных. Следовательно, принципиальной разницы между умышленными и случайными инцидентами для разных типов организаций не будет.

Какие данные утекают?

Если в прошлом году предметом утечек практически всегда являлись персональные данные (98,5%), то в этом году ситуация значительно изменилась. В первом полугодии 2009 года доля утечек персональных данных немного уменьшилась и сегодня составляет только 87,2%. Это произошло, из-за роста количества утечек иных типов информации, и прежде всего, той информации, что составляет коммерческую тайну организации (см. таблицу 3).

Таблица 3: Распределение утечек по типам конфиденциальных данных

Тип конфиденциальных данных	**Инциденты**	
	Кол-во	**%**
Персональные данные	360	87.2%
Коммерческая тайна, ноу-хау	12	2.9%
Государственная и военная тайна	9	2.2%
Другая конфиденциальная информация	28	6.8%
Не установлено	4	1.0%

Диаграмма 3: Распределение утечек по типам конфиденциальных данных в 1-м полугодии 2009 года

Но такие изменения всё же нельзя признать принципиальными. Пресса по-прежнему уделяет наибольшее внимание именно утечкам персональных данных. Иные же виды конфиденциальной информации утекают значительно реже и вызывают меньший интерес публики (поскольку персональные данные каждый невольно примеряет на себя: «а что, если бы это была информация обо мне»). Кроме того, скрывать инциденты с коммерческой тайной несравненно проще – в их отношении либо отсутствуют нормативные акты об обязательном уведомлении, либо уведомляется узкий круг лиц. Утечку государственной или военной тайны скрыть ещё проще.

По каким каналам утекают данные?

Приведённое ниже распределение – самое интересное с практической точки зрения. Носителем или каналом утечки считается тот носитель, находясь на котором данные пересекли охраняемый информационный периметр или стали доступными неавторизированному лицу.

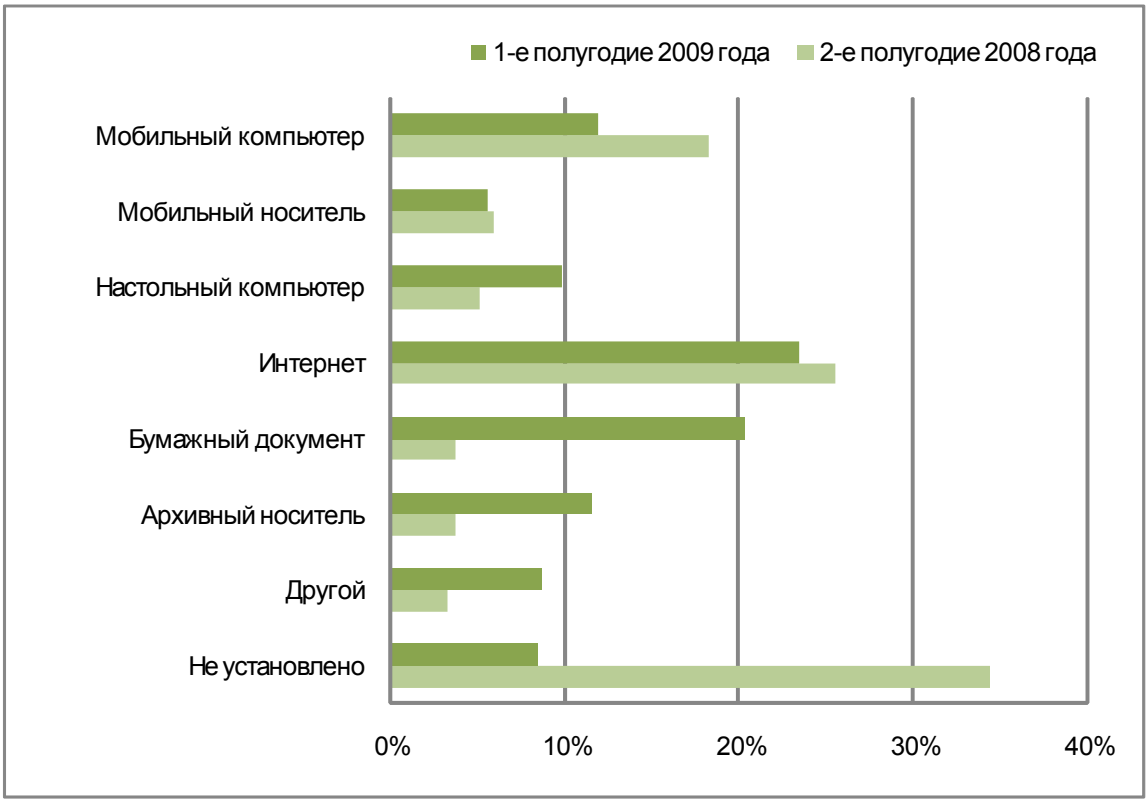
Ориентируясь на тип носителя, можно выбирать средства защиты от утечек и прогнозировать соответствующее снижение рисков.

Таблица 4: Основные каналы утечки данных

Канал утечки	**1-е полугодие 2009**		**2-е полугодие 2008**	
	Кол-во	**%**	**Кол-во**	**%**
Мобильный компьютер (ноутбук, КПК)	49	11.9%	50	18.3%
Мобильный носитель (флэш-накопитель, CD, DVD и т.д.)	23	5.6%	16	5.9%
Настольный компьютер, сервер, НЖМД	41	9.9%	14	5.1%
Интернет	97	23.5%	70	25.6%
Бумажный документ	84	20.3%	10	3.7%
Архивный носитель	48	11.6%	10	3.7%
Другой	36	8.7%	9	3.3%

Не установлено	35	8.5%	94	34.4%

Диаграмма 4: Основные каналы утечки данных в 1-м полугодии 2009 года



Как видно из диаграммы выше, существенным образом снизилось число инцидентов с мобильными компьютерами, а доли утечек через бумажные и архивные носители, наоборот, увеличились.

Первое было предсказуемо, и эксперты InfoWatch прогнозировали это еще в прошлом году. Большое количество публикаций о потере и краже ноутбуков с конфиденциальными данными должно было привести к тому, что пользователи, наконец, озаботятся их защитой. Тем более что это довольно просто технически – надо зашифровать жёсткий диск, раздел диска или хотя бы некоторые файлы. Программ для такого шифрования на рынке имеется предостаточно, в том числе, бесплатных. Но для того, чтобы дело сдвинулось с мёртвой точки, потребовалось значительное время.

Эксперты InfoWatch ожидают, что в будущем доля мобильных носителей и мобильных компьютеров ещё больше сократится, поскольку этот канал утечек успешно закрывается техническими средствами, такими как контроль портов или шифрование.

Небольшое уменьшение доли сетевых утечек объясняется аналогично. Этот вид утечек очень часто освещается в прессе и обсуждается специалистами, а средства защиты от них (современные DLP-системы) хорошо известны и многими уже опробованы на практике.

А вот бумажным и архивным носителям (бэкапам), видимо, не уделялось должного внимания. В результате их доля в числе средств, являющихся каналом утечек, возросла, а для бумажных – особенно сильно. Бумажные документы с конфиденциальными данными чаще всего просто выбрасывают на помойку, где их находят бдительные граждане и сообщают в СМИ. Причём второе имело гораздо большее значение, чем первое. Если раньше мусорные контейнеры проверяли редко, то теперь охотники за славой, начитавшись о подобных случаях в прессе, тщательно проверяют мусорные баки и очень часто находят там конфиденциальные данные. Чтобы обнаружить утечку через веб-сайт компании, исследователю нужна квалификация (как минимум, умение составлять запросы для поисковой системы), в то время как копаться в мусоре можно и

без специальных знаний.

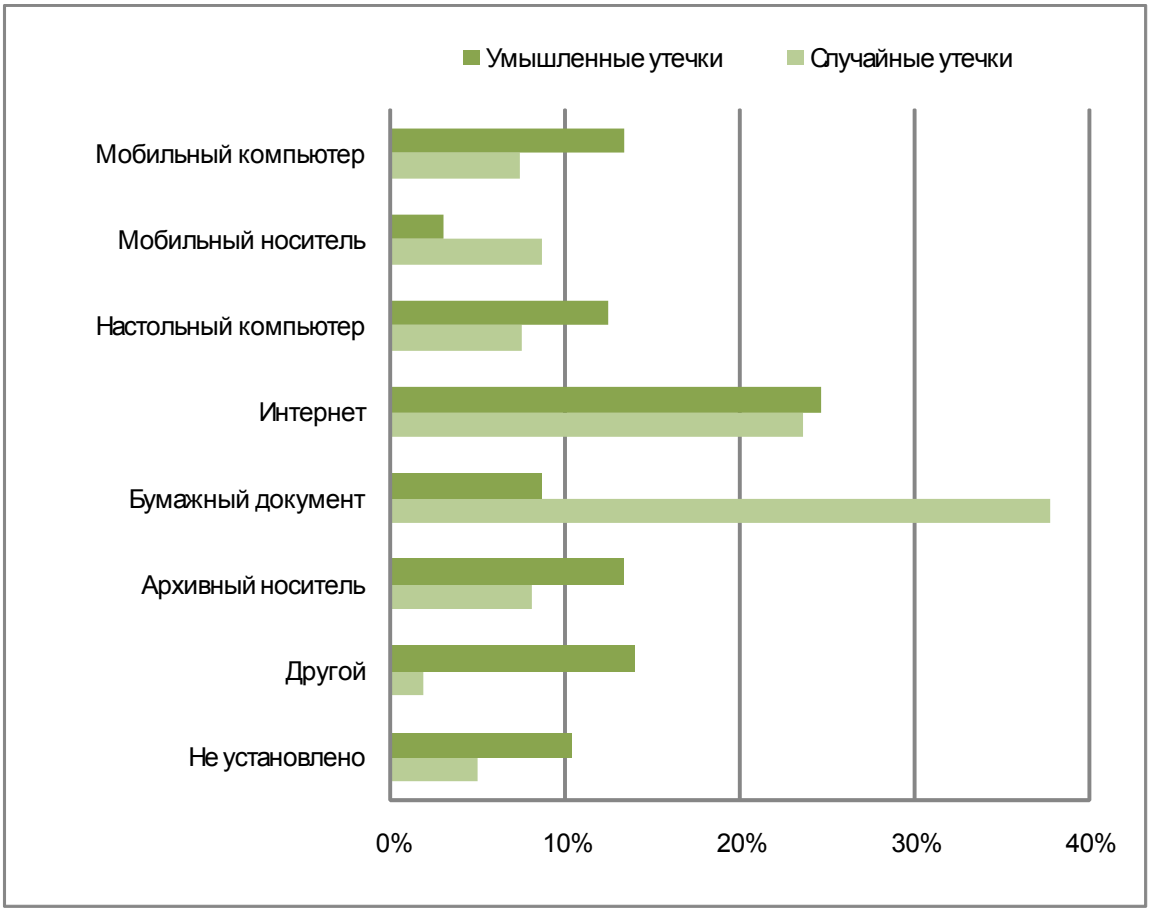
Налицо недостаток внимания служб информационной безопасности к бумажным документам. Некоторые из работников ИБ считают, что когда лист покинул принтер, всё, что на нём напечатано, больше не их забота. Подобный подход и приводит к росту «бумажных» инцидентов. Защита информации не исчерпывается защитой компьютерной информации – об этом в наш кибернетический век легко забыть.

Далее рассмотрим то, как распределены по видам носителей умышленные и случайные утечки по отдельности. Ниже приведены диаграммы для соответствующих типов инцидентов.

Таблица 5: Основные каналы умышленных и случайных утечек

Тип носителя	**Умышленные утечки**		**Случайные утечки**	
	Кол-во	**%**	**Кол-во**	**%**
Мобильный компьютер (ноутбук, КПК)	31	13,4 %	12	7,4%
Мобильный носитель (флэш-накопитель, CD, DVD и т.д.)	7	3,0%	14	8,7%
Настольный компьютер, сервер, НЖМД	29	12,5 %	12	7,5%
Интернет	57	24,7 %	38	23,6%
Бумажный документ	20	8,7%	61	37,8%
Архивный носитель	31	13,4 %	13	8,1%
Другой	32	13,9 %	3	1,9%
Не установлено	24	10,4 %	8	5,0%
Всего	231	100%	161	100%

Диаграмма 5: Основные каналы умышленных и случайных утечек



Методы борьбы со случайными и умышленными утечками – разные. С первыми справиться легче и дешевле. В случае злого умысла противостоять приходится не слепой случайности, лени или невежеству, а умному и заинтересованному противнику. Здесь интеллект играет против интеллекта, хитрость – против хитрости.

Эксперты InfoWatch практически исключают возможность случайных утечек через определённый информационный канал, если он контролируется при помощи современной DLP-системы. В тоже время умышленные инциденты этому правилу не подчиняются: в случае перекрытия одного канала, инсайдер будет искать другой, менее защищенный.

В подтверждение этому колонка «случайные утечки» в таблице 5 говорит нам, с каких каналов нужно начинать внедрять DLP-систему. Колонка «умышленные утечки» не может расцениваться по такому же принципу: защиту нужно ставить на все каналы одновременно, иначе злоумышленник просто обойдёт заслон, воспользуется тем каналом, который недостаточно контролируется или вовсе открыт.

Выше уже говорилось о значительном увеличении доли «бумажных» утечек. Однако, как видно из таблицы 5, данное утверждение справедливо только для случайных утечек. Среди инсайдеров бумажные носители не так популярны, как иные каналы кражи информации.

Распределение утечек по странам

Ещё раз напомним, что в базе данных утечек InfoWatch учитываются инциденты, о которых было сообщено в СМИ (конечно, включая блоги, веб-форумы и пр.). Достоянием гласности становятся далеко не все утечки даже в тех странах, где закон предписывает операторам сообщать о них. Тем не менее, сопоставляя данные разных стран, эксперты InfoWatch могут оценить степень латентности инцидентов, то есть сказать, сколько примерно случаев кражи конфиденциальных данных было скрыто от общественности.

Ниже приводится таблица инцидентов с разбивкой по странам. В последней

колонке указано удельное число утечек в расчёте на один миллион населения.

Таблица 6: Распределение утечек по странам

Страна	Число утечек	%	Утечек на 1 млн. населения
Австралия	6	1.45%	0.301
Канада	14	3.39%	0.431
Китай	1	0.24%	0.001
Куба	1	0.24%	0.087
Чехия	2	0.48%	0.191
Германия	3	0.73%	0.036
Великобритания	69	16.71%	1.145
Ирландия	2	0.48%	0.333
Израиль	1	0.24%	0.164
Индия	1	0.24%	0.001
Япония	7	1.69%	0.055
Нидерланды	1	0.24%	0.061
Новая Зеландия	5	1.21%	1.161
Россия	23	5.56%	0.160
Швеция	1	0.24%	0.108
Сингапур	1	0.24%	0.207
Словакия	1	0.24%	0.186
США	266	64.41%	0.908
Мировой масштаб	4	0.97%	0.001
Не установлено	6	1.45%	

Именно последняя колонка – удельное количество инцидентов – характеризует ситуацию с утечками и их обнародованием в конкретной стране. За отчётный период (1-е полугодие 2009 года) к традиционной паре лидеров (США и Великобритании) присоединилась Новая Зеландия. Эксперты InfoWatch не исключают, что она оказалась в этом списке временно из-за небольшого абсолютного количества инцидентов. Но первые две страны уже давно имеют наибольший показатель выявленных на миллион населения утечек. Это объясняется действующими законами и традициями, которые обязывают предприятия извещать субъектов персональных данных об инцидентах. Такое извещение редко остаётся приватным и чаще всего попадает в прессу.

Россия по этому удельному показателю сильно продвинулась за последние полгода, обогнав Швецию. Китай же по-прежнему остаётся информационно закрытой страной, в то, что там так мало утечек верится с трудом. Не во всех случаях извещение об утечках может быть признано полезным, поэтому вопрос о целесообразности подобного информирования остаётся открытым. Однако точка зрения о необходимости данной процедуры возобладала в США (в 46 штатах), где были приняты соответствующие законы. По стопам США пошла Великобритания. Некоторые другие страны сейчас обдумывают, вводить ли такую же обязанность. Если это произойдёт, их показатель в данной таблице непременно повысится и, скорее всего, остановится на уровне США.

Можно утверждать, что в развитых странах происходит порядка **одной** утечки **в год на каждый миллион населения**. Там, где принято уведомлять граждан или госорганы об инцидентах, большинство из них становится достоянием гласности, в других странах – скрывается от публики.

Также следует обратить внимание на рост числа российских утечек. В первом полугодии 2009 их зафиксировано 23, в то время как за предыдущее полугодие всего 2 (за весь 2008 год – пять). Основной причиной для такого роста количества обнародованных утечек стал закон «О персональных данных», который как раз вводится в действие де-факто (формально он вступил в силу ещё в 2007, но на первых порах не соблюдался). Многие предприятия озаботились приведением в соответствие своих информационных систем. СМИ активно откликнулись на актуальную тему и довольно подробно освещают всё, что связано с защитой персональных данных. Хотя российские утечки ПД и не наносят гражданам материального ущерба, как в США, эта свежая тема продолжает оставаться привлекательной для прессы.

Крупнейшие утечки

Отчётное полугодие не принесло очень крупных утечек, таких как, например, из Deutsche Telekom или сети TJX. Крупнейшие инциденты последних месяцев относительно скромные.

Число записей	Страна	Краткое описание инцидента
7 500 000	Германия	Найдена уязвимость в социальной сети StayFriends GmbH (www.stayfriends.de), которая позволяла получить доступ к персональным данным всех участников
2 500 000	Великобритания	Злоумышленникам удалось получить доступ к БД национальной медицинской службы (NHS), где хранятся данные на пациентов
1 500 000	Япония	Служащий несанкционированно скачал из служебной БД и унёс данные клиентов; часть из них он успел продать.
807 000	США	Утраченная архивная лента содержала данные о подозреваемых лицах за 12 лет, включая номера соцстрахования

Отсутствие многомиллионных утечек в этом полугодии объясняется стечением обстоятельств. Вероятность крупной или очень крупной утечки не сильно отличается от вероятности мелкой. Серьёзность защитных мер зависит больше от ценности информации для оператора, чем от её размера. Большие сети имеют больше компонентов и, следовательно, больше уязвимостей. Мелкий инцидент проще скрыть. Эти факторы и определяют относительно большое число крупных утечек по сравнению с мелкими.

Прогнозы

В следующем полугодии и в последующем году ожидается усиление борьбы с утечками. Следствием этого вряд ли станет сокращение количества зафиксированных инцидентов, поскольку такое усиление невозможно без более тщательного мониторинга инцидентов, что, в свою очередь, увеличивает количество выявленных. Кроме того, ожидается вступление в силу нормативных актов об обязательном уведомлении об утечках персональных данных, что также означает рост статистики.

Поскольку предотвратить случайные утечки проще, дешевле и быстрее, чем намеренные, усиление борьбы, прежде всего, приведёт к сокращению случаев случайных утечек. То есть, их доля должна еще немного уменьшиться.

Выводы

Анализ подсказывает, что риски стать жертвой утечки конфиденциальных данных слабо зависят от типа оператора, обрабатывающего эти данные, будь то

государственный орган, коммерческое предприятие, учебное заведение и т.п. На уровне концепции защиты отдельные решения для каждого типа вряд ли целесообразны.

В России тема защиты персональных данных и тема их утечек становится всё более актуальной и обсуждаемой на всех уровнях: как на уровне руководителей предприятий, так и на государственном уровне.

Эксперты InfoWatch рекомендуют российским предприятиям в ближайшее время обратить особое внимание на защиту конфиденциальной информации на бумажных носителях и контролю печатных устройств. Увеличение роли компьютерной техники привело к тому, что упущен из виду этот весьма опасный канал утечек. Число инцидентов с бумажными документами сильно выросло.

Важно помнить, что интернет и мобильные устройства по-прежнему являются наиболее опасными каналами утечки данных. Содержимое носителей рекомендуется шифровать, а сетевые каналы контролировать при помощи DLP-систем.

Общее зафиксированное количество утечек в мире увеличивается. Относительное же число утечек (на миллион населения) аналитики InfoWatch склонны считать стабильным показателем для развитых стран. То есть рост идёт в основном за счёт выявления и обнародования. Число выявленных и опубликованных утечек быстро растёт в тех странах, где принимаются нормативные акты об обязательном уведомлении заинтересованных лиц при компрометации конфиденциальной информации.