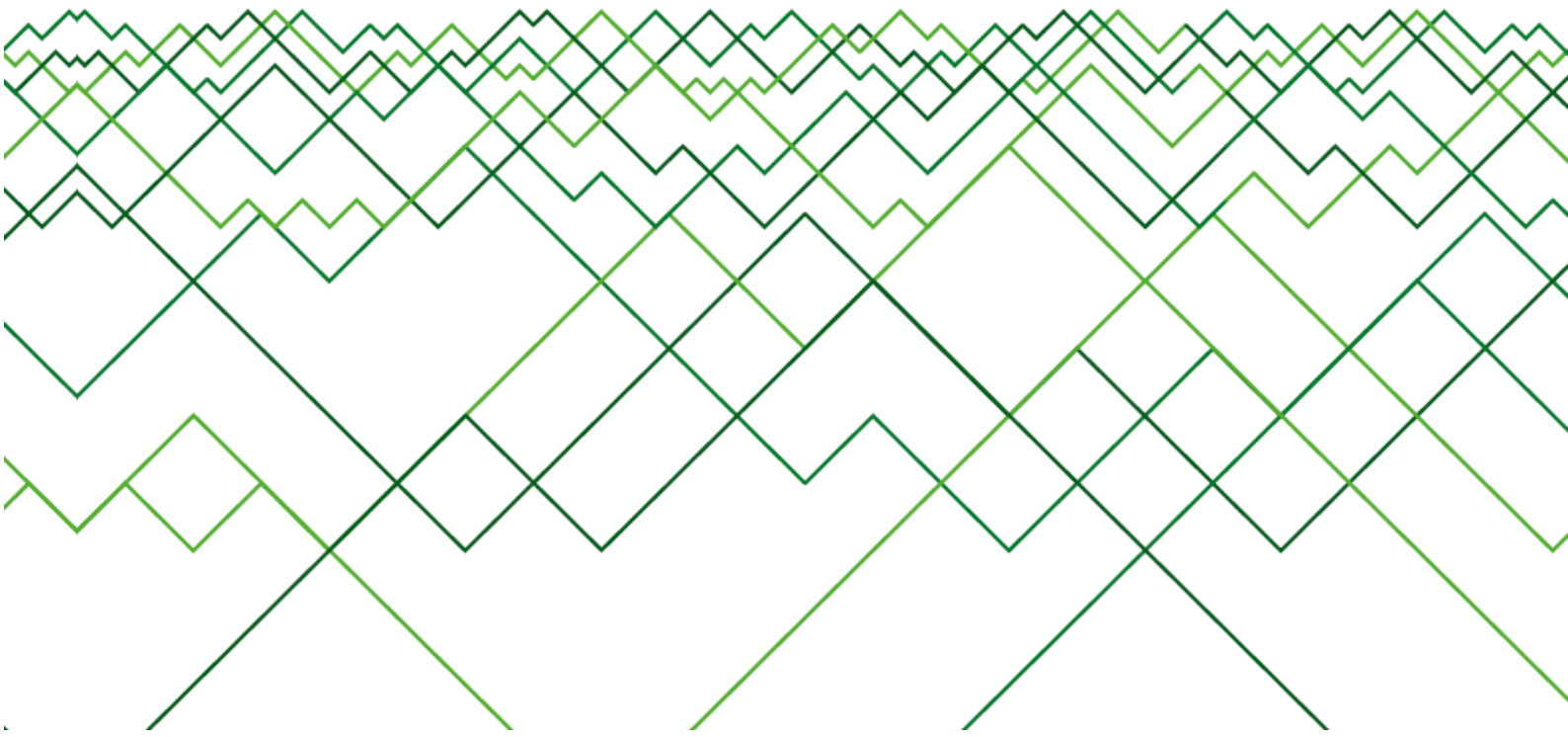
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический Центр InfoWatch

Глобальное исследование утечек корпоративной информации и конфиденциальных данных 2012



INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Оглавление

Аннотация 3
Основные факты 4
Выводы и тенденции 5
Методология 6
Общая статистика 7
Умысел 8
Источники утечек 9
Персональные данные 13
Каналы утечек 14
Региональные особенности 16
Заключение 19
Типичные утечки 2012 20

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Аннотация

Аналитический Центр компании InfoWatch представляет очередное ежегодное исследование утечек информации в мире, зарегистрированных и обнародованных в СМИ за 2012 год.

За все годы исследования предмета аналитики впервые столкнулись с **неоднородностью картины утечек применительно к различным отраслям**. На общем фоне выделяются банки, страховые компании, телеком-операторы, где доля случайных утечек стабильно снижается. Данная картина с небольшими оговорками характеризует весь коммерческий сектор.

2012 год можно **назвать годом утечек в государственных компаниях**. Увеличение доли госструктур в распределении источников утечек примечательно и говорит о недостаточном внимании к проблемам защиты информации в госсекторе. Вторая причина еще более очевидна – массовое использование мобильных устройств (смартфоны, ноутбуки, планшеты), к чему службы информационной безопасности государственных и муниципальных организаций по всему миру оказались явно не готовы.

Подтверждается предсказанная ранее тенденция на снижение доли случайных утечек в целом по миру. Связано это с все большей популярностью средств защиты информации (с одной стороны), а также с особенностью этих систем, более эффективных именно в отношении случайных утечек.

Распространенность средств защиты информации (Gartner утверждает, что около трети компаний уже используют DLP) снимает только одну часть проблемы – случайные утечки, - никак не влияют на злонамеренные. Вопрос здесь скорее в восприятии DLP-систем как софта, способного самостоятельно, без усилий со стороны ИБ-служб, бороться с утечками, что в корне не верно. И если со случайными утечками DLP действительно справляется, то борьба со злонамеренными требует серьезной консалтинговой составляющей в DLP-проектах на этапе подготовки внедрения и сопровождения системы, расследований инцидентов.

В ближайшее время следует ожидать изменение восприятия и отношения к DLP как со стороны вендоров, так и со стороны клиентов. Как следствие – **развитие направления ИБ-консалтинга с последующим повышением культуры информационной безопасности** в компаниях-пользователях систем защиты.

В этом случае можно прогнозировать уже в течение 3-5 лет **снижение «типичных» утечек - «недорогие» умышленные и неумышленные.**

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Основные факты

- ✓ За 2012 год в мире зафиксировано и обнародовано в СМИ **934** случая утечки конфиденциальных данных, что на **16%** превышает показатель прошлого года
- ✓ Официально заявленные в СМИ прямые убытки кредитно-финансовых организаций от утечек в первом полугодии 2012 года составили чуть более **37,8 млн долл**.
- ✓ Скомпрометировано более **1,8 млрд** записей, в том числе финансовые и персональные данные
- ✓ Доля случайных утечек стабильно уменьшается и составляет **38%**
- ✓ Повышается доля утечек в госкомпаниях и муниципальных учреждениях – **29%** (+ 9% по сравнению с 2011 годом)
- ✓ Лидирующий тип утечек – персональные данные – **89,4%**
- ✓ Самый популярный канал утечек – бумажная документация **22,3%**

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Выводы и тенденции

- ✓ Впервые за все годы исследования мы столкнулись с принципиальной невозможностью оценить совокупный ущерб компаний от утечек. Явные убытки по публичным утечкам составляют 37,8 млн. долл. Но это лишь прямые затраты, без учета расходов на судебные разбирательства, рассылку уведомлений, аудит и реструктуризацию систем информационной безопасности и пр. и пр. Очевидно, что с учетом всех расходов цифру потерь необходимо увеличить на порядок. А принимая во внимание то, что видимая часть утечек – это всего лишь несколько процентов, придется получившиеся суммы умножить еще в 30-50 раз. На выходе имеем совершенно фантастические потери – десятки миллиардов долларов.

  Проблема в том, что реальная сумма потерь может очень сильно колебаться в заданном диапазоне величин, и любые попытки точно закрепить ее заранее обречены на провал. Поэтому с 2012 года специалисты Аналитического центра InfoWatch отказались от приведения цифр совокупных потерь, однако сам факт лавинообразного увеличения показателя финансовых потерь сочли необходимым отметить.

- ✓ Второй интересный момент – изменение позиций коммерческих компаний в отношении произошедших инцидентов. Все чаще компании не только не скрывают факт, но сознательно идут на сотрудничество со следствием, подробное расследование инцидента и наказание виновных. Как ни странно, это положительно сказывается на имидже.

- ✓ Третье, но наиболее важное – наметившаяся «специализация» средств защиты от утечек в отношении случайных инцидентов. Следует уже сейчас задумать о смене технологических подходов к созданию систем для того, чтобы информация защищалась равно эффективно и от случайной, и от злонамеренной утечки. Для этого центральным объектом защиты должны стать именно данные, а не каналы связи, не инфраструктура. Причем, вне зависимости от физического местонахождения информации, она должна обнаруживаться и надежно контролироваться – будь то локальное хранилище или глобальная сеть. В этом – новый вызов для всей сферы DLP.

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Методология

Исследование основывается на собственной базе данных, которая пополняется специалистами Центра с 2004 года. В базу утечек InfoWatch включаются инциденты (утечки данных), произошедшие в организациях в результате злонамеренных или неосторожных действий сотрудников и **обнародованные в СМИ** или других **открытых источниках** (включая web-форумы и блоги).

Оговоримся, что исследование охватывает лишь незначительное (не более 1-5%) число от реальных утечек, произошедших в мире. Тем не менее, стабильность основных показателей дает право считать исследование репрезентативным, - 1) распределение параметров (типы утечек, каналы утечек и пр.) на имеющейся выборке год от года меняется плавно, 2) большинство изменений спрогнозировано заранее.

Следовательно, можно утверждать, что тенденции, валидные на выборке публичных инцидентов, выполняются на всем множестве утечек, как обнародованных, так и оставшихся скрытыми.

В настоящее время база утечек InfoWatch насчитывает несколько тысяч зарегистрированных инцидентов. Для каждой утечки фиксируется дата инцидента и дата публикации сообщения в СМИ.

Случаи нарушения конфиденциального статуса информации, произошедшие в результате внешних компьютерных атак, а равно иные инциденты ИБ (DDoS, фишинг и пр.) в данном отчете не рассматриваются.

Классификация и регистрация инцидентов в базе утечек осуществляется на основе результатов анализа, проводимого сотрудниками InfoWatch. В ходе аудита базы, каждой утечке присваиваются различные атрибуты (тип организации, сфера деятельности, тип утечки, финансовый ущерб) и метрики (каналы, типы утекших данных), позволяющие дать представление о масштабе произошедшей утечки, проанализировать возможные причины произошедшего инцидента и спрогнозировать его последствия.

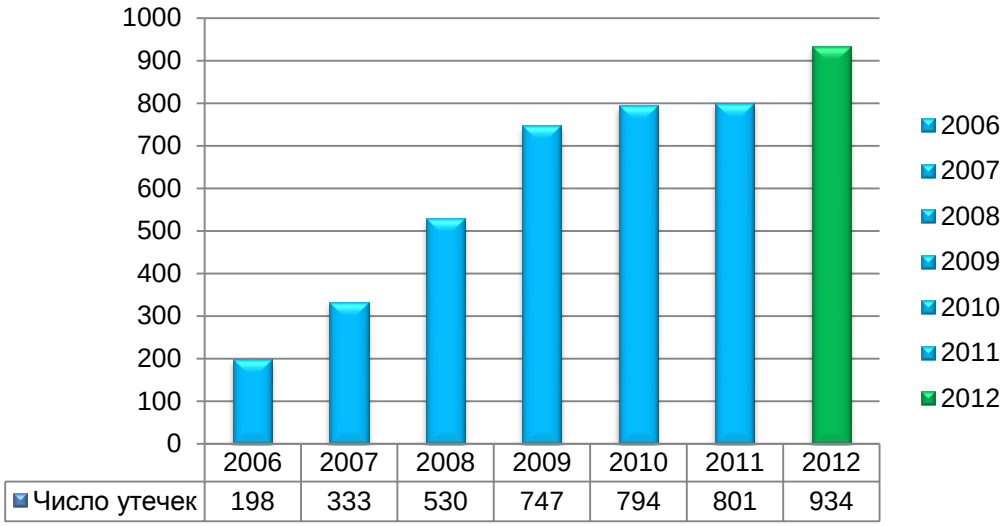
Данные о прямом ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций.

Мы не приводим точной экспертной оценки совокупных потерь компаний, связанных с инцидентами ИБ и ликвидацией их последствий, во избежание ненужных спекуляций вокруг конкретных цифр непрямых потерь.

Общая статистика

В 2012 году Аналитическим Центром InfoWatch зарегистрировано 934 случая утечки конфиденциальной информации, что на 16% больше, чем в 2011 и 2010 гг. (794 и 801 утечка соответственно). Это в среднем 2,5 утечки в день, 75-80 утечек в месяц.

Аналогичный всплеск в последний раз регистрировался в отчете 2009 года. Тогда, по отношению к 2008-му, количество утечек выросло на 40% и было связано с ослаблением внимания компаний и госорганизаций к информационной безопасности на фоне экономического спада.



	2006	2007	2008	2009	2010	2011	2012
Число утечек	198	333	530	747	794	801	934

Рис.1. Динамика числа утечек информации, 2006-2012 гг.

Нынешний рост наоборот объясняется повышенным вниманием регуляторов, государства и других заинтересованных сторон к проблеме безопасности данных. Не секрет, что за рубежом каждый случай утечки персональных данных граждан – повод для судебного преследования нарушителей. Потому пострадавшие и их адвокаты охотно предают огласке все случаи, связанные с нарушением установленных процедур обработки и хранения чувствительной информации с целью увеличить компенсационные выплаты. В результате чего число утечек, попавших в СМИ, закономерно растет.

С другой стороны, регулирующие органы также активно распространяют информацию об утечках. Это характерно для США, где подробности об утечках данных периодически публикуются аппаратом окружных прокуроров в виде сообщений для прессы.

Вывод:

Прошлогодний прогноз Аналитического Центра на стабилизацию числа утечек не оправдался. Виной тому – повышенное внимание всех участников процесса к теме защиты информации, особая роль государства и отраслевых регуляторов. К сожалению, пока это актуально для западных стран в большей степени, чем, например, для России.

Умысел

Баланс умышленных и случайных утечек принципиально не отличается от прошлого года. **Предсказанная нами два года назад тенденция на снижение доли случайных утечек с ростом распространенности DLP проявляется все более явно.** Особенно в отраслях, традиционно ориентированных на защиту данных – банки и финансовые организации, телеком, государственные структуры (в банках доля случайных утечек едва доходит до 20% - см. Глобальное исследование утечек корпоративной информации в банковском сегменте (финансовые и кредитные учреждения) I полугодие 2012).

Аналитики InfoWatch отмечали, что внедрение средств защиты повлияет на соотношение случайных и умышленных утечек. Имеющиеся на рынке средства и методы более эффективны в отношении именно случайных утечек, нежели умышленных. Как видим, процент случайных утечек действительно снижается – в 2012 году доля случайных утечек составила всего 38%. На этом фоне растет доля злонамеренных утечек – 46%. (Процент утечек неясной природы практически не изменился – 16% в 2012 г.).

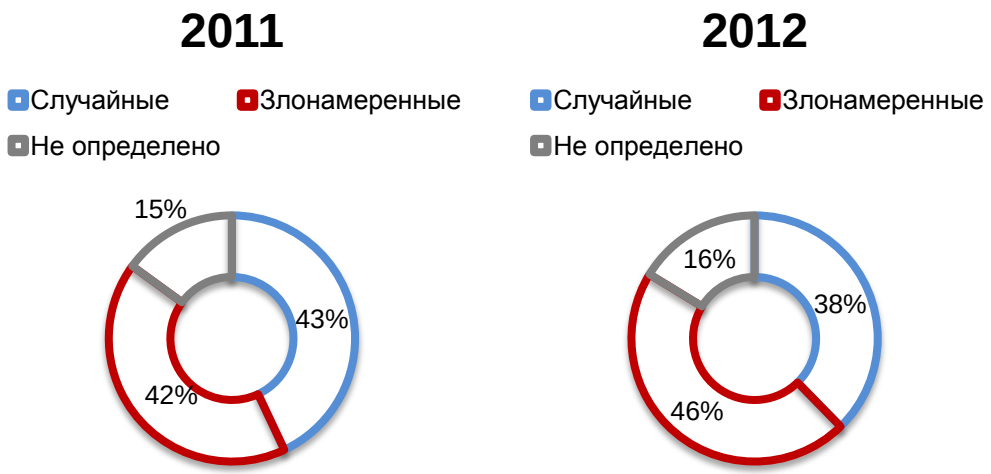


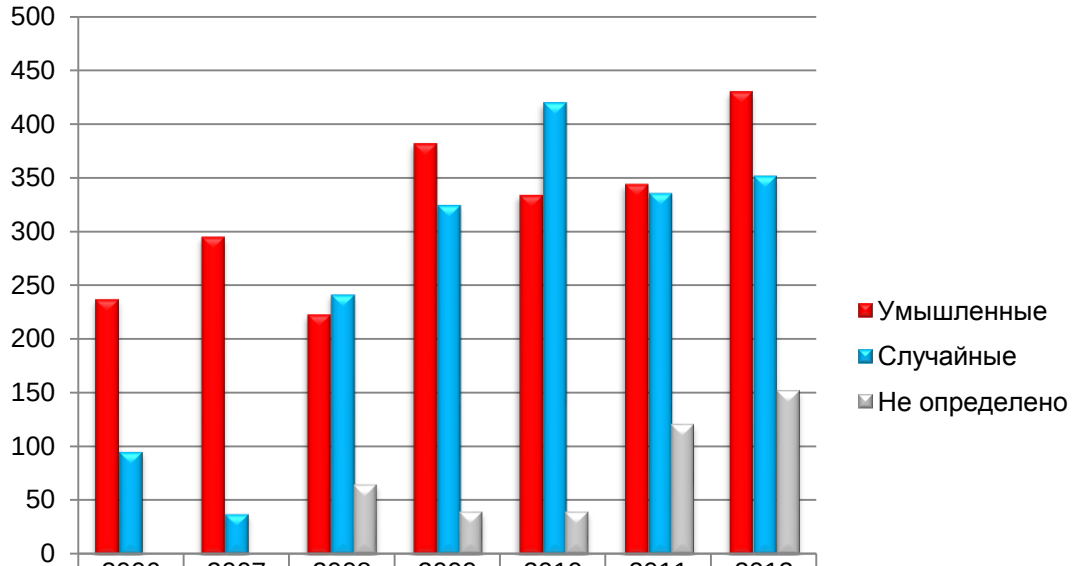
Рис.2. Соотношение случайных и умышленных утечек, 2011-2012 гг.

Во многих инцидентах не представляется возможным установить, была ли утечка умышленной или случайной. Особенно для случаев утраты мобильных носителей, а именно - ноутбуков, наладонников, флешек. Не всегда ясно, потерян носитель или украден. В случае установленного факта кражи также не всегда можно определить, был целью вора сам носитель или записанная на нём информация.

Кроме того, не все источники информации об утечках содержат точные ссылки на носитель. Многие СМИ просто не придают этому значения. В этой связи точно определить намеренность утечки информации становится сложнее, в результате, сектор «Не определено» год от года практически не меняется.

Динамика количественного соотношения злоумышленных и случайных утечек представлена на рис. 3. Примечательно, что в 2012 году мы наблюдаем значительное превышение числа злоумышленных утечек по сравнению с числом

случайных. Последний раз аналогичная ситуация наблюдалась в 2009 году. Схожесть показателей можно объяснить чувствительностью случайных утечек к внедрению средств защиты информации. В 2009 году это был «хвост» от благополучного 2008-го (первая волна массового внедрения средств защиты от утечек). Результаты прошедшего года косвенно подтверждают зарождение второй волны популярности DLP-систем. Как упоминалось ранее, ярче всего указанная тенденция проявляется в «передовых» с точки зрения ИБ отраслях - банки, телеком. Там доля случайных утечек по отношению к злонамеренным еще меньше.



	2006	2007	2008	2009	2010	2011	2012
Умышленные	237	295	223	382	334	344	430
Случайные	96	38	242	325	420	336	352
Не определено	0	0	65	40	40	121	152

Рис. 3. Динамика соотношения случайных и умышленных утечек, 2006 – 2012 гг.

Вывод:

С 2008 года соотношение случайных и намеренных утечек изменилось. Снижение доли случайных утечек в 2012 году знаменует начало предсказанной аналитиками тенденции, связанной с масштабным использованием средств защиты от утечек.

Источники утечек

В связи с широко принятыми в разных странах законами о защите персональных данных, практически все организации, имеющие дело с персональными данными клиентов или предприятия, имеющие большой штат сотрудников, должны принимать меры по защите этой информации.

На деле действительно серьезно к защите информации относятся коммерческие компании (их доля составила 41% и уменьшилась на 5% по сравнению с прошлым годом), образовательные учреждения (доля сократилась практически вполовину,

составив 16%). Откровенно плохо защищаются государственные учреждения (прирост - 9% к 2011 году).

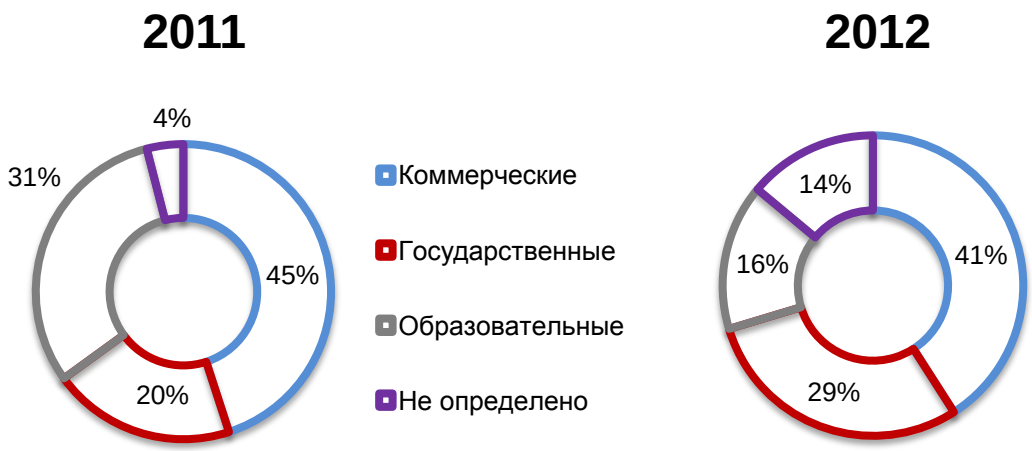


Рис.4. Соотношение случайных и умышленных утечек, 2011-2012 гг.

Интересно, что падение числа утечек в коммерческих компаниях и образовательных учреждениях проявляется и в количественном измерении (см. рис. 5)

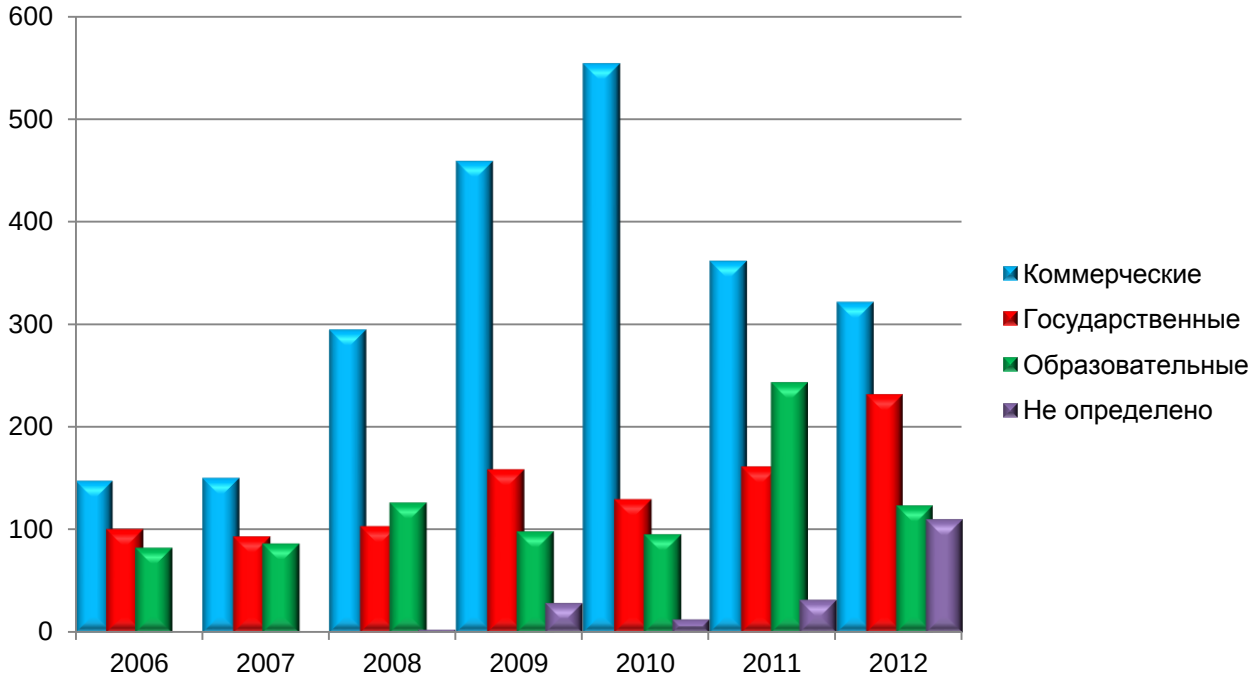


Рис. 5. Динамика утечки информации по типам источников, 2006-2012 гг.

Обратим внимание на распределение случайных и намеренных утечек в коммерческих компаниях (рис. 6). Тут необходимо отметить несколько моментов.

- ✓ В банках преобладают злонамеренные утечки (22% из числа всех злонамеренных утечек), а вот случайных утечек практически нет (4%).

- ✓ В то же время случайные утечки (61%) равно, впрочем, как и намеренные (треть от всех) характерны для медучреждений.
- ✓ Доля ритейловых компаний в обоих случаях незначительна

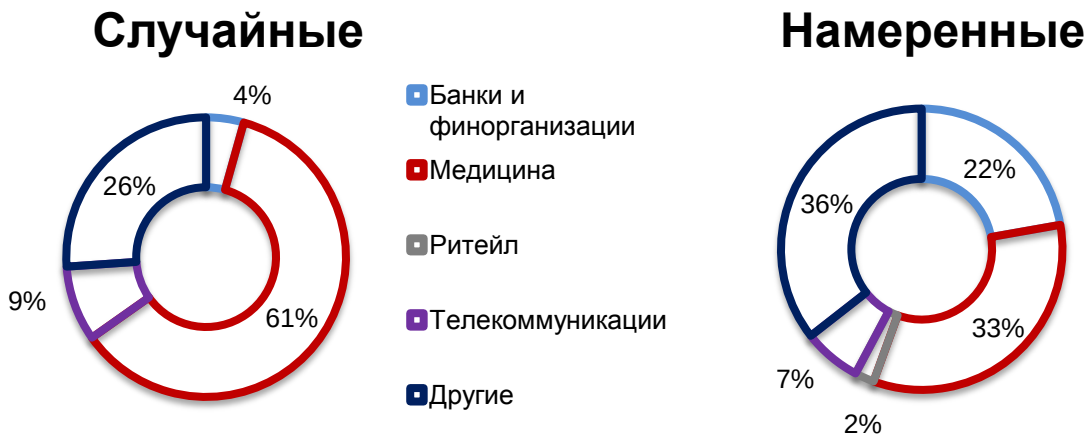


Рис.6. Соотношение случайных и умышленных утечек в коммерческих компаниях, 2011-2012 гг.

Если внимательно посмотреть на динамику изменения долей по основным источникам утечек, заметим, что доля случайных утечек из коммерческих компаний практически не поменялась (около 37%, рис. 7), доля умышленных утечек сократилась.

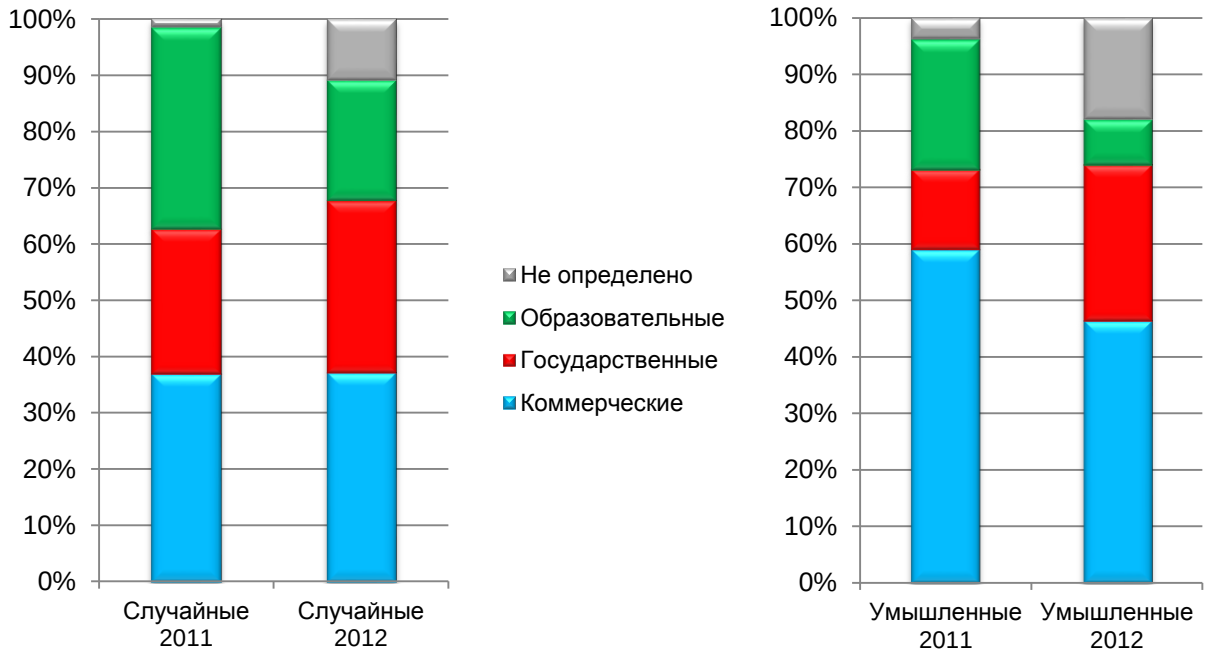


Рис. 7. Соотношение случайных и умышленных утечек по типам организаций, 2011 – 2012 гг.

2012 год стал годом утечек из государственных организаций и муниципальных учреждений. Доля умышленных и случайных утечек для госорганов растет. Очевидно, это связано с объяснимой задержкой внедрения технологий защиты от утечек в забюрократизированных структурах. С другой стороны, госчиновники с охотой не меньшей, чем сотрудники коммерческих компаний, используют личные мобильные устройства. Концепция BYOD работает и в госорганизациях. При этом низкая культура информационной безопасности, недостаточная проработка внутренних политик использования, в части, мобильных устройств создает благоприятные условия для роста числа как умышленных, так и случайных утечек (что на деле и проявляется).

Вывод:

Приведенные данные по коммерческим организациям (в особенности отраслевой разрез) подтверждают тезис о зависимости между ростом популярности DLP-систем и снижением доли случайных утечек. Тем острее встает вопрос об умышленных утечках и путях решения данного аспекта проблемы безопасности информации. По сути, речь идет о том, что уже сейчас необходимо выработать новый подход к защите данных и требованиям к DLP-системам.

Персональные данные

По-прежнему львиная доля всех утечек касается персональных данных — 89,4% (в предыдущем году — 92,4%).

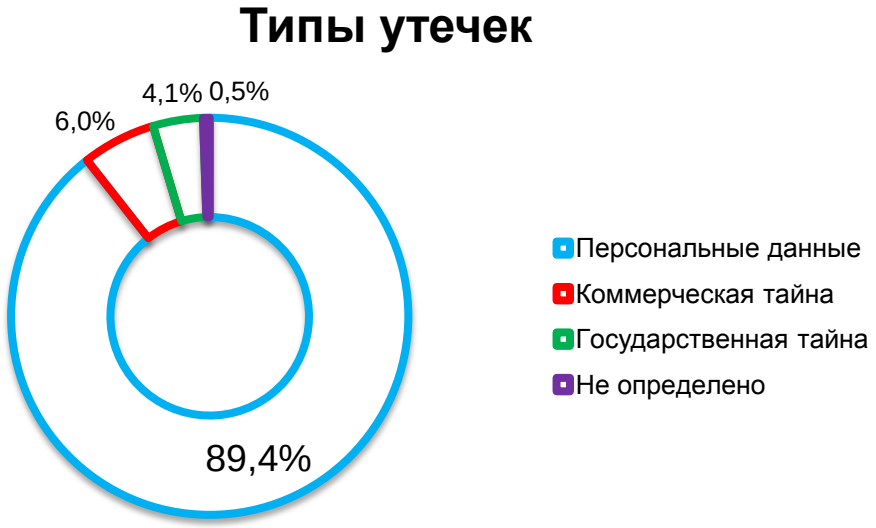


Рис.8. Распределение утечек по типам данных, 2011г.

Отчасти такая высокая доля персональных данных среди утечек определяется законодательными требованиями о публикации инцидентов, связанных с подобными утечками. Другой частью правды является то, что ликвидные персональные данные интересны широкому кругу злоумышленников, так как их можно сбыть на чёрном рынке. **Коммерческая или государственная тайны обычно утекают «на заказ»**. По-настоящему массовыми становятся инциденты, где данные ликвидны и могут быть проданы за деньги широкому кругу покупателей.

Тем более удивительно, что в 2012 году зафиксирован ряд инцидентов, где коммерческая и государственная тайна прямо фигурировали как объект посягательства. В большинстве случаев огласка факта утечки коммерческой тайны имеет под собой желание пострадавшей стороны вывести инцидент в плоскость судебного разбирательства. В большинстве стран кража коммерческой тайны подпадает под действие административного или уголовного законодательства. Как следствие, **компании, пострадавшие от злонамеренной утечки, заинтересованы в том, чтобы наказать виновных (будь то сотрудники или внешние злоумышленники) по всей строгости закона.**

Вывод:

Один из методов противодействия умышленным кражам секретной информации заключается в необходимости затруднить сбыт конфиденциальной информации, сделать невыгодным её хищение «на продажу», усилить законодательную базу. Тогда посягательства на эти данные могут значительно сократиться.

Каналы утечек

Канал утечек – характеристика, которая имеет прямое практическое приложение. В зависимости от частоты утечек по тому или иному каналу (через тот или иной носитель) можно планировать внедрение средств защиты, а также определить приоритет – какими каналами надо заниматься в первую очередь. Но помимо статистических данных нужно учитывать специфику работы организации, какие средства и инструменты чаще всего используются для передачи информации, именно их защищать и контролировать.

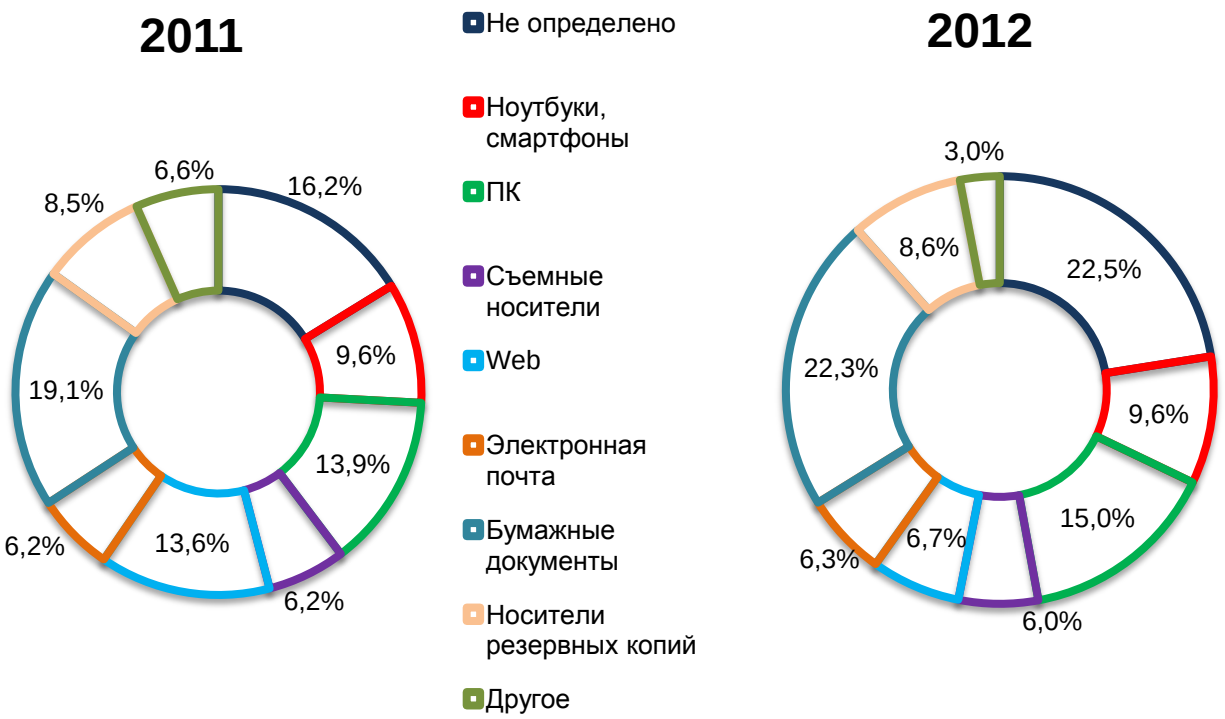


Рис. 9. Распределение утечек по каналам, 2011-2012 гг.

Если принять во внимание все большую популярность средств защиты от утечек информации, следует ожидать падения долей традиционных каналов утечек (где, собственно, технические системы защиты наиболее эффективны). Как видим, для общего распределения это вполне справедливо. Доля web-утечек снизилась вдвое - 6,7%, доли утечек через ПК (+ 1%) , съемные носители (снижение 0,2%), электронную почту – практически не поменялись.

Самое значительное изменение зафиксировано в отношении бумажной документации. Как ни странно, именно организационные меры сегодня являются слабым местом информационной безопасности. В 2012 году этот сегмент прирос еще на 3%, составив 22,3% от всех утечек.

Факты утечки информации, отправленной по электронной почте и переданной огласке, составили всего 6,3%. Этот канал также как и «web» является самым популярным каналом распространения и передачи информации. Большое число утечек через электронную почту в прошлые годы (2007 – 2009 гг.) привели к тому, что

компании стали серьезно контролировать этот канал. В результате наблюдается снижение числа утечек через почту, хотя до идеала, конечно, далеко. И по-прежнему электронная почта остается самым «лакомым» каналом утечки из-за своей простоты. Возможно, доля необнародованных утечек здесь превалирует, поэтому процент утечек по этому каналу не столь велик, как бы можно было предположить.

Последние три года InfoWatch неустанно разъяснял опасности, связанные с утратой мобильных носителей информации. Переносные устройства теряются и крадутся в огромных количествах, а обойтись без них в современной жизни почти невозможно. Поэтому актуальны технические и организационные меры по контролю за подобными мобильными устройствами и информацией, которая на них хранится. Не записывать на мобильные носители секретную информацию без нужды, а если записывать — то в зашифрованном виде. Соблюдение этих правил позволит избежать значительного числа инцидентов в эпоху BYOD.

Теперь рассмотрим, насколько отличаются умышленные и случайные утечки на разных типах носителей.

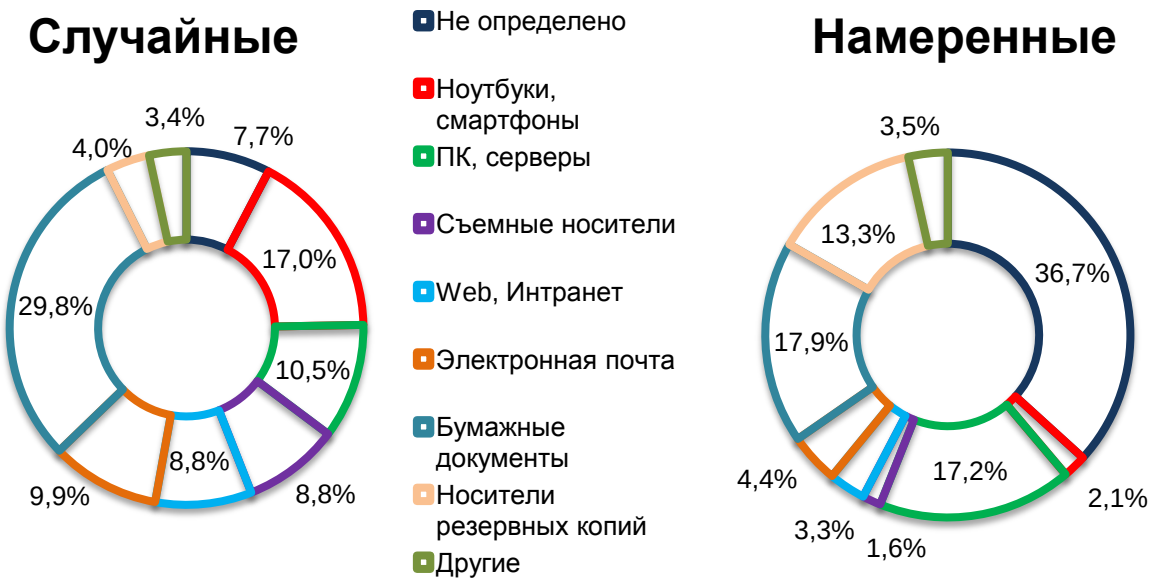


Рис. 10. Распределение случайных и умышленных утечек по каналам, 2012г.

Прежде всего, обращает на себя внимание большая доля неопределенных утечек (не установленный источник), что объяснимо для злоумышленных утечек.

Плачевна ситуация с резервными копиями. Большой процент (13,3%) намеренных утечек по этому каналу говорит о недостаточном внимании служб ИБ к архивной информации (бэкапы). К сожалению, немногие из распространённых систем резервного копирования имеют встроенное шифрование. А похитить архивный диск бывает проще, чем «рабочий» носитель.

Особо следует выделить канал «ПК, серверы». Здесь мы чаще сталкиваемся с умышленной утечкой информации со стационарных рабочих станций или серверов. Причем, как правило, речь идет о неправомерных действиях администраторов сетей. Наряду с бухгалтером, системный администратор – должность, чаще всего фигурирующая в новостях о намеренных утечках. Имея (зачастую) неограниченный доступ к сетевым ресурсам, администраторы злоупотребляют доверием компании-работодателя с намерением извлечь личную выгоду – перепродажа персональных данных, «слив» информации конкурентам и пр.

По-прежнему высока доля случайных утечек через электронную почту (почти 10%), «случайно» течет через смартфоны и ноутбуки (потеря устройств – 17,0%), съемные носители (потеря флэшек – 8,8%).

Треть всех случайных утечек приходится на бумажные носители. Современные DLP-системы умеют проверять все документы, отправляемые на печать, и даже подтверждать наличие в офисе того сотрудника, от имени которого сформировано задание печати. Но после того как документ напечатан, его распространение отследить крайне сложно. За физическим перемещением бумажного носителя ныне можно проследить только организационно-правовыми методами, на технику здесь надежды мало.

Вывод:

Полученные результаты однозначно свидетельствуют о том, что создатели DLP-решений сегодня столкнулись с новым вызовом. Понятие защищенного периметра организаций, по сути, ушло в прошлое, потому системы защиты от утечек должны обеспечить безопасность данных как внутри инфраструктуры компании, так и за ее пределами. Речь идет о необходимости объединить в рамках DLP-систем технологии, позволяющие находить и контролировать принадлежащие компании данные в том числе на просторах глобальной сети.

Региональные особенности

Распределение утечек по регионам в этом году неожиданностей не принесло. США оказались на первом месте как по количеству (576 или 61,7% от всех утечек), так и по агрегированному показателю (утечка на душу населения). Второе место удерживает Великобритания (97 или 10,3%). Третье место за Россией (75 или 8.3%). Напомним, что наша страна не в первый раз входит в число лидеров. В прошлом году третье место досталось Канаде, а вот годом ранее, в 2010 символическая «бронза» за утечки также досталась Российской Федерации.

Количество обнародованных утечек на млн. населения

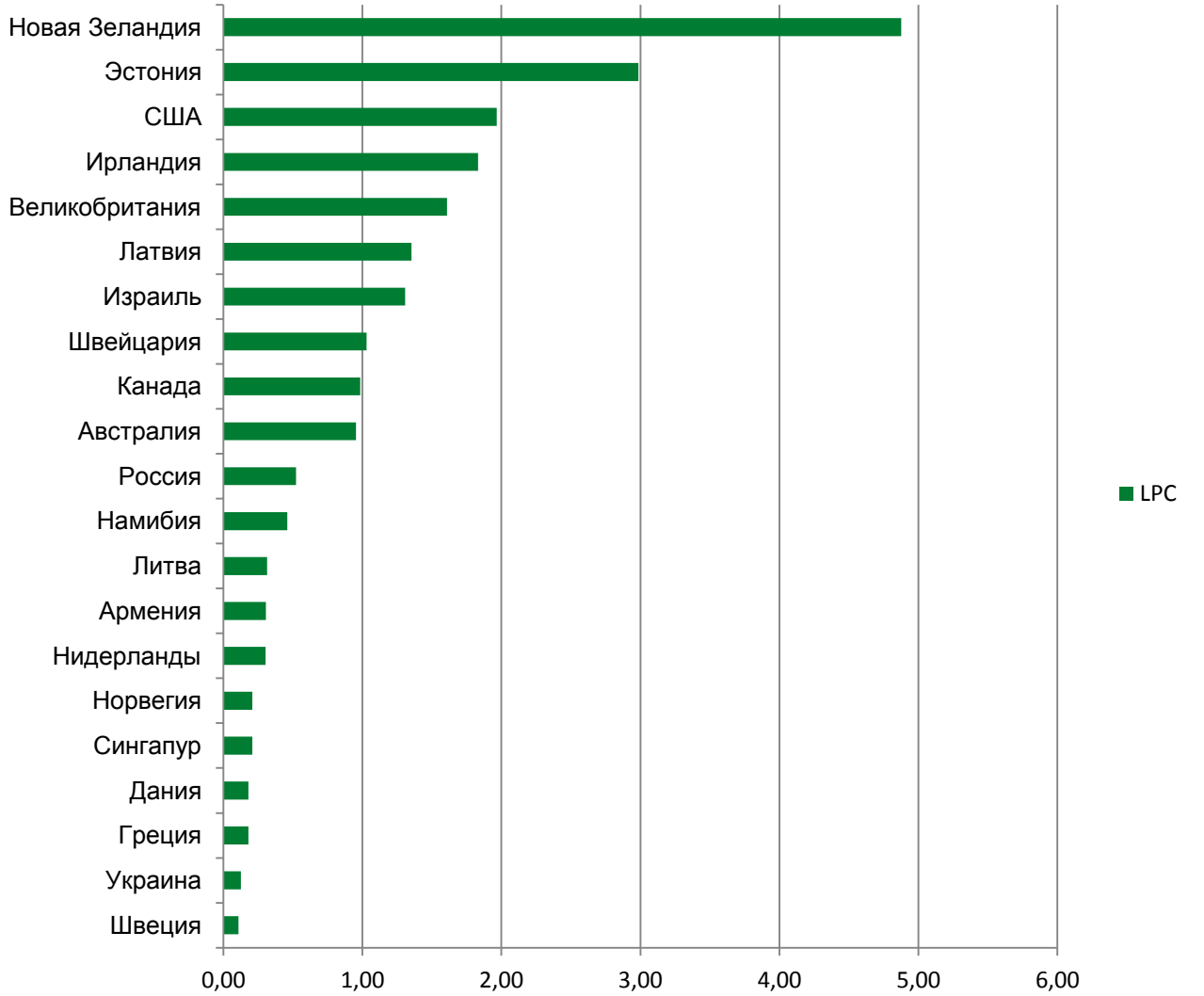


Рис. 11. Распределение утечек по странам, 2012г.
Страны упорядочены по числу утечек на млн. населения (LPM).

Количество обнародованных утечек, шт

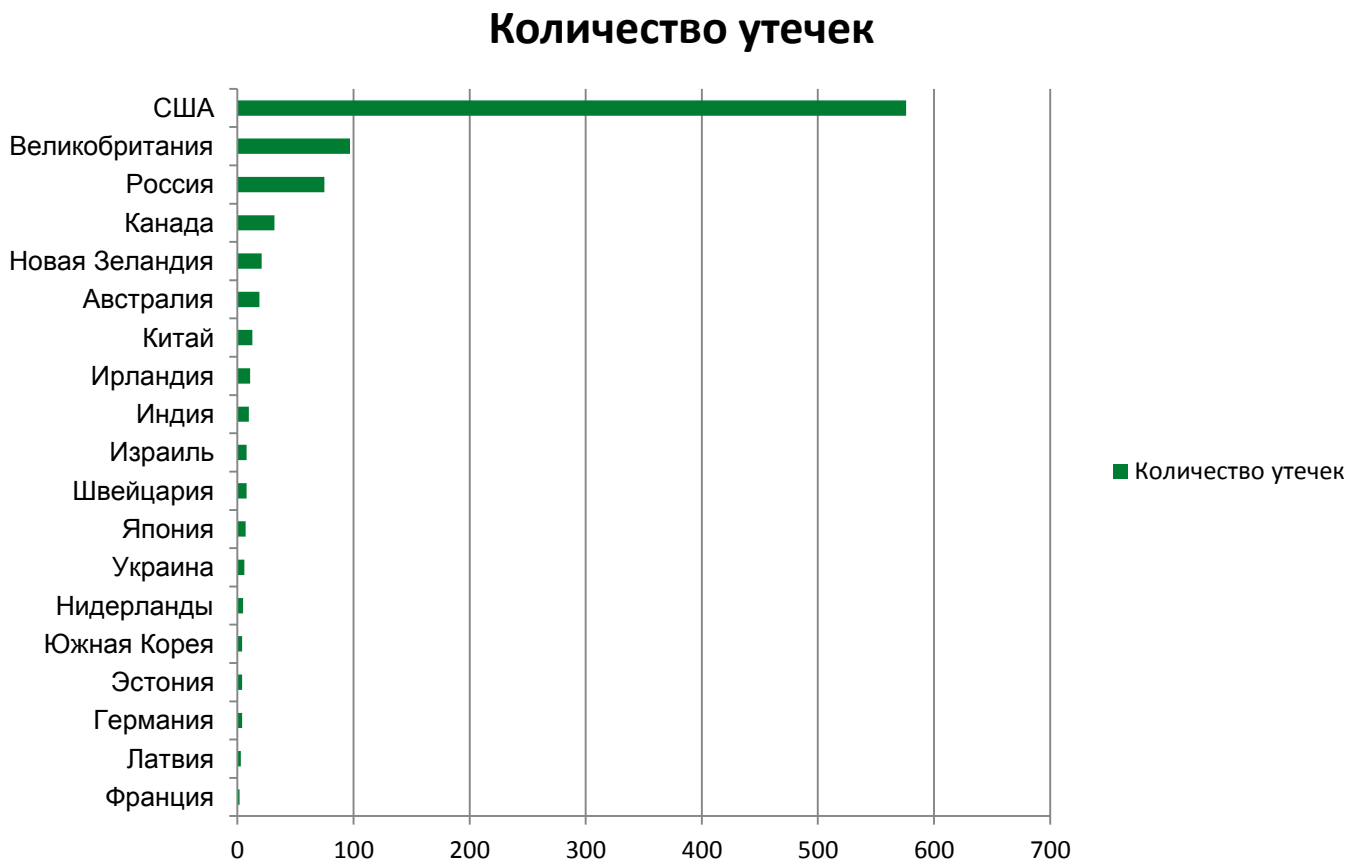


Рис. 12. Распределение утечек по странам, 2012г.

Заключение

В 2012 году Аналитическим Центром InfoWatch зарегистрировано официально заявленных в СМИ **934** случая утечки конфиденциальной информации, что на 16% больше, чем показатель предыдущего года.

Во многих инцидентах не представляется возможным установить, была ли утечка умышленной или случайной, а, следовательно, определить намерение похищения данных становится сложнее. Показательно, что доля неопределенных утечек в распределении умышленных и неумышленных практически не меняется, составляя 16%.

Доля утечек из учебных и некоммерческих организаций подровнялась, что подтверждает во многом случайный пик прошлого года (тогда мы предположили, что рост утечек из образовательного сектора носил случайный характер. В коммерческих организациях доля случайных утечек снижается, что подтверждает высказанную ранее гипотезу о зависимости доли случайных утечек в коммерческом сегменте от темпов проникновения DLP-систем. Однако доля умышленных утечек в них все еще высока, т.к. напрямую связана с возможностью получения выгоды от кражи и распространения конфиденциальной информации. И здесь помимо технических средств защиты важны организационные, правовые и даже законодательные меры.

По-прежнему большая часть утечек касается персональных данных — 89,4%. Одним из методов противодействия умышленным кражам персональных данных может стать затруднение сбыта этой информации, которое возможно только на законодательном уровне. Второй доступный путь – существенное увеличение санкций за неправильную обработку данных в сочетании с последовательной политикой государств в этом вопросе.

Среди самых распространенных каналов утечки информации лидирует категория «бумажная документация». По-прежнему популярны у злоумышленников «носители резервных копий», сами ПК, сетевые хранилища. Примечательно, что в числе популярных каналов для умышленных утечек сократилась доля мобильных устройств (скорее всего, связано с невозможностью точно сказать в каждом случае, имеем мы дело с утечкой или это была банальная кража). Интересно также, что злоумышленники практически не пользуются при организации «сливов» информации средствами электронной почты, что объясняется укоренившимся представлением о подконтрольности данного канала службе ИБ.

Неоднозначность трактовки того или иного случая как умышленной или неумышленной утечки наталкивает на вывод о значительном пересечении природы двух типов утечек. Как следствие, необходимо уже сейчас задуматься о переходе к универсальным технологиям обнаружения утечек и контроля информационных потоков. Очевидно, что контентно-ориентированные системы защиты информации должны работать одинаково эффективно с данными как внутри организации (хранящиеся, обрабатывающиеся, перемещающиеся внутри компании), так и за ее пределами – в глобальной сети.

Типичные утечки 2012

14 миллионов долларов за утечку ПДн

Высший суд графства Аламеда (Alameda, Калифорния, США) обязал фармакологическую компанию Walgreens (основана в 1901) выплатить 14,5 млн долл. в виде штрафа (более 20% от оборота за 2012 финансовый год). Компании вменяется в вину нарушение процедуры обращения с документами, содержащими медицинские данные клиентов.

Аналитик может получить 20 лет за Apple

Американский аналитик Джон Киннакэн (John Kinnucan) обвиняется в незаконной продаже инсайдерской информации о продукции Apple. Против Джона Киннакэна выдвинули обвинения в мошенничестве с ценными бумагами, тайном сговоре и использовании инсайдерской информации. Как говорится в сообщение Bloomberg, Джон получал информацию от поставщиков Apple и продавал ее биржевым спекулянтам, которые заработали на этом, по разным оценкам, около 1,58 млн долларов.

KPMG скомпрометировал данные богатейших людей планеты

Крупнейший представитель «Большой четверки» KPMG оказывал услуги по аудиту брокерской компании MF Global. Для выполнения необходимых проверок MF Global передала KPMG персональные данные своих клиентов, среди которых данные игроков на бирже, банковских служащих и финансовых органов Великобритании. Аудитор, в свою очередь, опубликовал строго конфиденциальную информацию в открытом доступе, в том числе имена, адреса, суммы задолженностей и другие финансовые показатели клиентов MF Global.

Газета Financial Times сообщила, что в результате утечки скомпрометированы имена самых состоятельных людей по всей планете, суммы задолженностей которых составляют сотни тысяч евро.

Инсайдер продал секрет технологии Samsung

Южнокорейская полиция арестовала группу инсайдеров, которая продавала секретную информацию Samsung компании-конкуренту.

Бывший сотрудник Samsung Mobile Display передал конфиденциальную информацию об оригинальной технологии производства AMOLED-дисплеев своему новому работодателю. Секрет технологии, на разработку которой Samsung потратила миллиарды долларов, инсайдер оценил в 170 тыс. долларов.

Citigroup заплатит 2 млн долларов за утечку информации

Главный регулятор по ценным бумагам в штате Массачусетс оштрафовал Citigroup на $2 млн, заявив, что аналитик банка допустил утечку конфиденциальной информации перед провальным IPO социальной сети Facebook.

Младший аналитик Citigroup, назначенный для исследования Facebook, послал электронное письмо двум сотрудникам сайта TechCrunch.com, с полученной Citigroup информацией о Facebook. По некоторым данным, он предложил исследование банка для публикации в СМИ со ссылкой на анонимный источник.

В отношении бывшего сотрудника «Вымпелкома» возбуждено уголовное дело

Оператор «ВымпелКом» официально сообщил о проведении следственно-оперативных мероприятий совместно с правоохранительными органами по факту выявления нескольких случаев передачи конфиденциальной информации третьим лицам бывшим сотрудником компании. Компания заявляет, что действующая на протяжении многих лет система защиты конфиденциальной информации и персональных данных, позволяет на ранней стадии выявлять попытки незаконных действий в отношении персональных данных абонентов. Благодаря этому, были выявлены преступные действия, в отношении бывшего сотрудника возбуждено уголовное дело.

Пермские злоинсайдеры заработали 3 млн рублей

В Перми завершено и передано в суд уголовное дело, возбужденное следователями в отношении организованной преступной группы, совершавшей кражи денежных средств с банковских карт граждан. Следствием установлено, что с марта по апрель текущего года трое жителей Перми договорились между собой систематически совершать денежные операции через Интернет, используя реквизиты банковских карт клиентов одного из банков.

Один из участников преступной группы, являясь студентом, устроился на практику в один из банков. Там он скопировал на флеш-карту конфиденциальную информацию – номера карт, персональные данные их держателей, а также коды CVV на клиентов, необходимые для совершения операций, не требующих чтения данных с магнитной полосы банковской карты и ввода ПИН-кода.

За совершение кражи в особо крупном размере было возбуждено уголовное дело по ч. 4 ст. 158 УК РФ. Статья предусматривает до 10 лет лишения свободы.

Национальная служба здравоохранения Великобритании теряет по 5000 записей пациентов…ежедневно

Великобритания. По последним данным, Национальная служба здравоохранения теряет ежедневно более 5000 записей о пациентах.

Так, медицинские карты и другие записи, содержащие конфиденциальные сведения, неоднократно оказывались в мусорных контейнерах, а электронные записи выставлялись на продажу на сайте интернет-аукциона. Среди прочих нарушений

правил защиты персональных данных — отправка данных о неизлечимо больных пациентах по неправильным номерам, кража медицинских карт и размещение полученных данных, а также кража незащищенных ноутбуков из квартир медицинского персонала.

За 6 месяцев Комиссар по информации Кристофер Грэм оштрафовал учреждения Национальной службы здравоохранения на 1 млн. фунтов стерлингов.

Всего за 2012 год по всему миру скомпрометировано более 1,8 млрд записей, в том числе финансовые данные, номера полисов социального страхования, медицинская информация, иные персональные данные.

Публично обнародована информация о прямых потерях компаний в размере 37,8 млн. долл.

Совокупный ущерб (затраты на ликвидацию последствий утечек, компенсационные выплаты, судебные разбирательства) – несколько миллиардов долларов. С учетом латентного характера утечек информации, можно говорить о том, что счет косвенных потерь компаний идет на десятки миллиардов долларов.