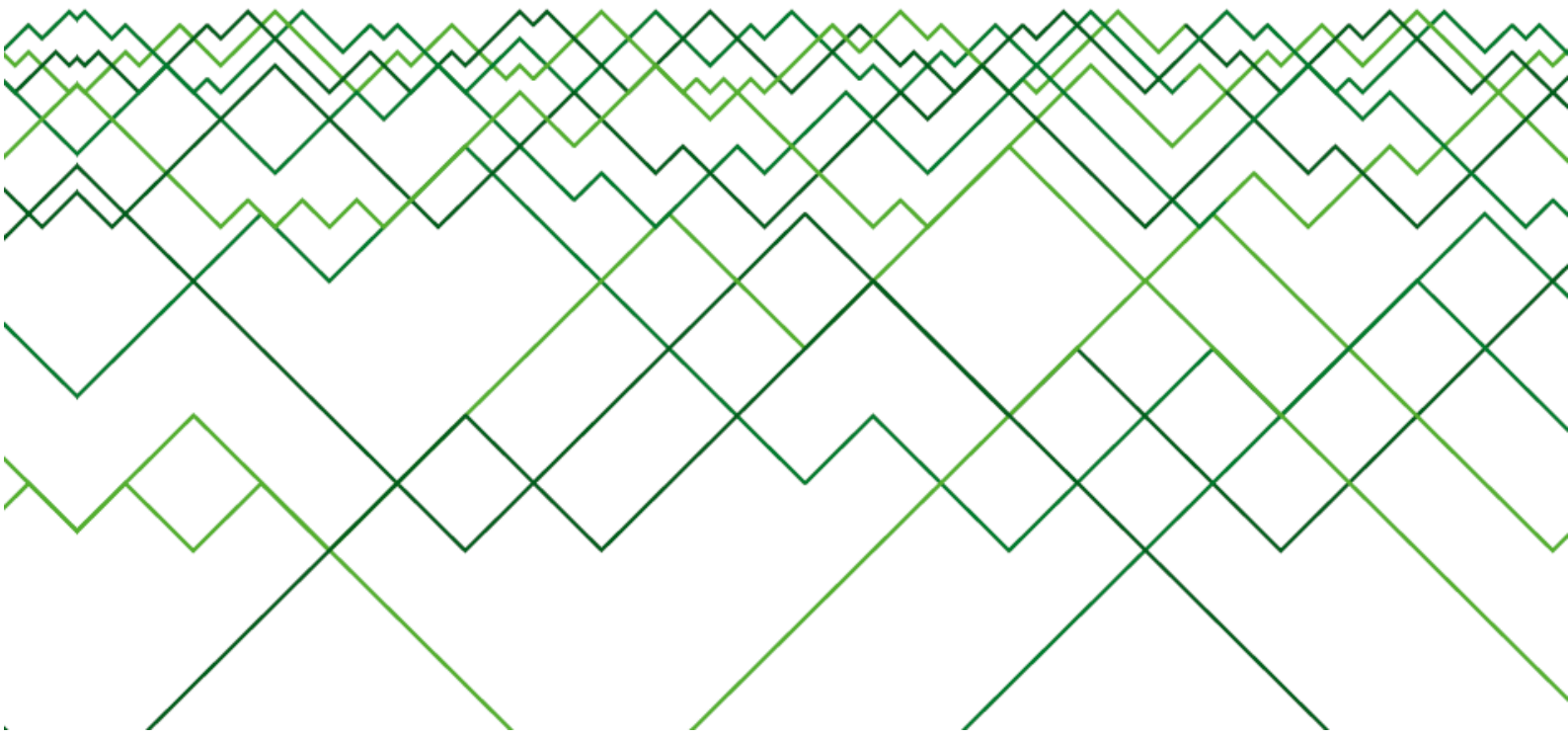
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический Центр InfoWatch

Исследование утечек информации и конфиденциальных данных из компаний и госучреждений России 2012



INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Оглавление

Аннотация

Аналитический Центр компании InfoWatch представляет исследование утечек информации из российских компаний и госучреждений за 2012 год. В основе исследования лежат **обнародованные в СМИ** случаи намеренной или случайной утечки охраняемой информации.

Очередное ежегодное глобальное исследование утечек информации, зарегистрированных и обнародованных в СМИ за 2012 год , Аналитический центр InfoWatch представил в конце февраля 2013 года. По данным отчета, в 2012 году было скомпрометировано более 1,8 млрд. записей, в том числе финансовые и персональные данные. В СМИ было обнародовано 934 случая утечки конфиденциальных данных, что на 16% превышает показатель прошлого года.

Было принято решение сделать специальный отчет по ситуации в России за 2012 год. В результате, исследование выявило ожидаемую неоднородность картины утечек. Ранее мы уже отмечали некоторые отраслевые особенности данного явления (см. Глобальное исследование утечек корпоративной информации в банковском сегменте (финансовые и кредитные учреждения) I полугодие 2012). В этом отчете речь пойдет о региональных отличиях.

2012 год можно **назвать годом утечек в государственных компаниях**. Тренд, характерный для всего мира, проявился и в России. Увеличение доли госструктур в распределении источников утечек примечательно и говорит о **недостаточном внимании к проблемам защиты информации в госсекторе.** Правда, российские утечки из государственных органов мало связаны с «мобилизацией». Случаев **утечки информации через мобильные устройства практически не отмечается**, но это не значит, что их, во-первых, не было, и, во-вторых, что их число не будет расти с увеличением количества смартфонов и планшетов в инфраструктуре госучреждений.

Необходимо отметить довольно высокий (по сравнению с мировым) **процент злонамеренных утечек в распределении по умыслу**. Эта особенность связана с повышенным вниманием российских СМИ к таким фактам, поскольку читатель больше интересуется не тем «что произошло», а тем «кто виноват». Поэтому утечки с героем-злоумышленником «в главной роли» чаще появляются на страницах газет, чем, например, безымянные истории о случайном обнародовании персональных данных.

В ближайшее время мы ожидаем, что проблема роста утечек найдет понимание не только в среде профессионалов, но и на высшем уровне управления компаниями и государственными структурами. Только в этом случае можно прогнозировать **снижение доли и количества «типичных» утечек** («недорогие» умышленные и неумышленные)**.**

INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

Основные факты

- ✓ За 2012 год в России зафиксировано и обнародовано в СМИ **74** случая утечки конфиденциальных данных, что составляет **7,9%** от общемирового количества утечек.
- ✓ Это примерно в 5 раз больше, чем годом ранее. По количеству утечек Россия занимает **третье** место, вслед за США и Великобританией.
- ✓ Более **500 тыс.** человек признаны пострадавшими от утечек.
- ✓ **77%** утечек относятся к разряду злонамеренных. (Доля таких утечек в мире составляет **46%**).
- ✓ На утечки из госучреждений приходится **38%** (на 9 пп. больше, чем в целом по миру). При этом доля утечек из коммерческих организаций также выше мировой – **47%.**
- ✓ Лидирующий тип утечек – персональные данные – **65%.**
- ✓ Самый популярный канал утечек – бумажная документация **28,4%.**

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).

Исследование охватывает лишь незначительное (не более 1-5%) число от реальных утечек, поскольку именно такая доля утечек становится достоянием СМИ. 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) общемировые тренды в основном коррелируют с российской картиной.

Тенденции, валидные на выборке публичных российских 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.

Утечки информации в России

В 2012 году Аналитическим Центром InfoWatch зарегистрировано 74 (7,9% от мировых) случая утечки конфиденциальной информации из российских компаний и госорганизаций. Это почти в пять раз больше, чем 2011 году, когда было зафиксировано «всего» 17 крупных утечек, обнародованных в СМИ. Общемировое число утечек также выросло. В 2012 году зафиксировано 934 утечки, что на 16% больше, чем в 2011-м.

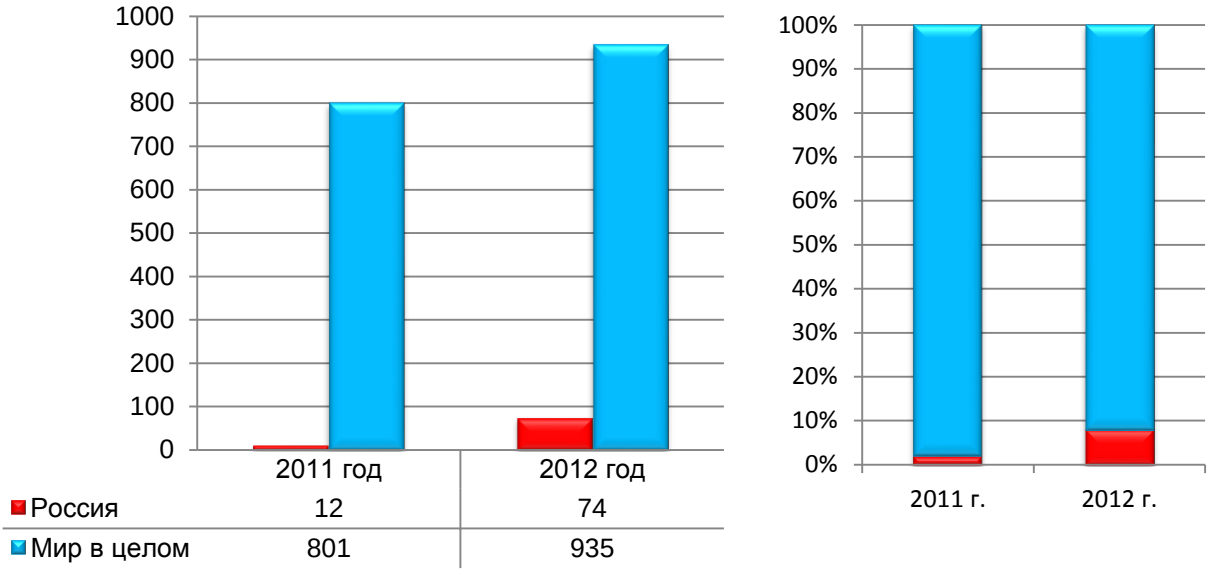


Рис.1. Динамика числа утечек информации и доля России, 2011-2012 гг.

Аналогичная динамика роста мировых утечек в последний раз регистрировалась в отчете 2009 года. Тогда, по отношению к 2008-му, количество утечек выросло на 40% (к 2008 году), что было связано с общим снижением уровня информационной безопасности на фоне экономического спада.

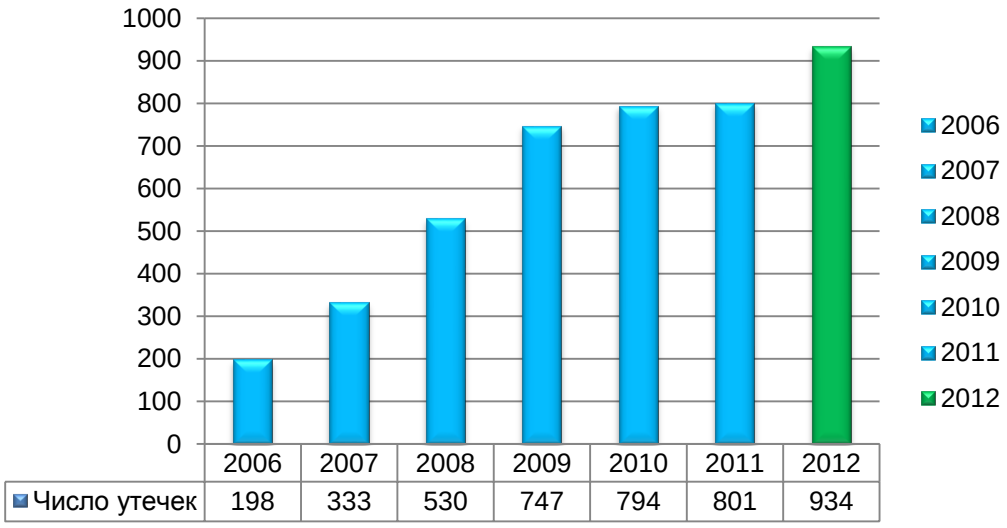


Рис.2. Динамика числа утечек информации в мире, 2006-2012 гг.

Высокие темпы роста количества утечек в мире и, в особенности, в России, во многом объясняются повышенным вниманием регуляторов, государства и СМИ к проблеме безопасности данных. Но если общемировые темпы были вполне прогнозируемы, прирост утечек по России требует отдельного уточнения.

Аналитики InfoWatch увязывают почти пятикратный рост числа утечек с перераспределением долей публичных и непубличных инцидентов. Иными словами, реальных утечек не стало больше в пять раз. Темпы роста числа реальных российских утечек вполне коррелируют с общемировыми, А вот доля «видимых» утечек действительно возросла. Виной тому - интерес общества к данной проблеме, плюс осознание реальности финансовых потерь вследствие утечки, скажем, платежных и клиентских данных.

Рис. 3. Распределение утечек по странам, 2012г.

В 2012 году в СМИ появляется огромное количество сообщений о нарушениях конфиденциальности, публикации персональных данных в открытом доступе и проч. Справедливости ради отметим, что многие из этих сообщений в отчет не попали, поскольку не соответствуют формальным признакам утечки информации, принятым в Аналитическом центре InfoWatch. Но наличие публичного интереса породило спрос и волну публикаций. В результате видимая доля российских утечек действительно выросла в разы.

Вывод:

Прошлогодний прогноз Аналитического Центра на стабилизацию числа утечек не оправдался. Причина – 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, где государственные органы пока скорее реагируют на запрос общества в части регулирования вопросов защиты информации, нежели направляют это самое общество. Отсюда непрогнозируемо высокий скачок утечек в России, который следует объяснить не реальным увеличением числа утечек, а драматическим ростом числа сообщений о них в СМИ.

Умысел

Баланс умышленных и случайных утечек в России в сравнении с общемировой картиной отличается кардинально. **77% всех российских утечек носят явно злонамеренный характер** в то время, как общемировое распределение на протяжении десятка лет колеблется вокруг соотношения 50/50 (без учета утечек неопределенной природы).

Столь низкая доля случайных утечек характерна для сегментов с высоким уровнем информационной безопасности – банки, телеком-операторы. Так, в банковской сфере доля злонамеренных утечек составила 100%, т.е. утечка информации была совершена с целью наживы и перепродажи.

Упоминавшийся выше общественный спрос на «жареные» новости обусловливает повышенное внимание со стороны читателей и слушателей к сообщениям об умышленной краже информации или злонамеренном обнародовании данных и проч. Именно такие сообщения составляют большую часть российских утечек в нашей базе.

В мире же, особенно в англосаксонских странах, утечка становится достоянием гласности вне зависимости от ее «окраски». По самым незначительным фактам нарушения закона, определяющего нормы и правила защиты информации, выпускаются сообщения от имени окружных прокуроров штатов (в США), других уполномоченных лиц в ряде стран. Поэтому картина утечек получается более ровной.

Рис.4. Соотношение случайных и умышленных утечек, 2012 г.

В России всего для 5% инцидентов не было возможным установить, была утечка умышленной или случайной. Особенно это актуально для случаев утраты мобильных носителей, а именно - ноутбуков, планшетов, 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 на общемировом распределении. Относительно небольшой процент «неопределенных» утечек в России связан как раз с акцентированным вниманием СМИ и регуляторов к проблеме – важен не сам факт, но обстоятельства утечки, кто «слил» и как.

Вывод:

Подавляющий процент умышленных утечек в распределении по «окрасу» с большой вероятностью не связан со зрелостью российских компаний и государственных органов. Дело, скорее, в социальном «заказе» со стороны читателей и зрителей, вынуждающем СМИ акцентировать внимание на утечках «с умыслом». Это подтверждается распределением утечек по типам организаций. Если бы в России действительно прослеживался общемировой тренд на снижение случайных утечек вследствие использования систем защиты, прежде всего это бы проявилось в снижении доли коммерческих компаний как наиболее восприимчивых к технологическим средствам защиты. Однако этого не наблюдается (см. ниже)

Источники утечек

Соотношение российских и мировых утечек по источникам (организации, допустившие утечку) в целом сопоставимо. Низкий процент неопределенных утечек связан с отмеченной выше особенностью, характерной для нашей страны - если в мире наблюдается довольно высокий процент утечек с неясным источником (номера соцстрахования обрабатывает целый ряд организаций и компаний), в России, пока, во всяком случае, сообщения об утечках в большинстве своем привязаны к конкретным хозяйствующим субъектам или госструктурам.

Необходимо уточнить, что мы не стали специально разделять муниципальные и бюджетные учреждения, добавив утечки из таковых в раздел «образовательные / бюджетные». Сделано это с единственной целью – отделить «государственные» утечки от утечек в медучреждениях (персональные данные высокой чувствительности), образовательных и бюджетных структурах, где традиционно наблюдается довольно **низкий уровень культуры защиты данных, недостаток финансирования мероприятий по обеспечению безопасности информации**.

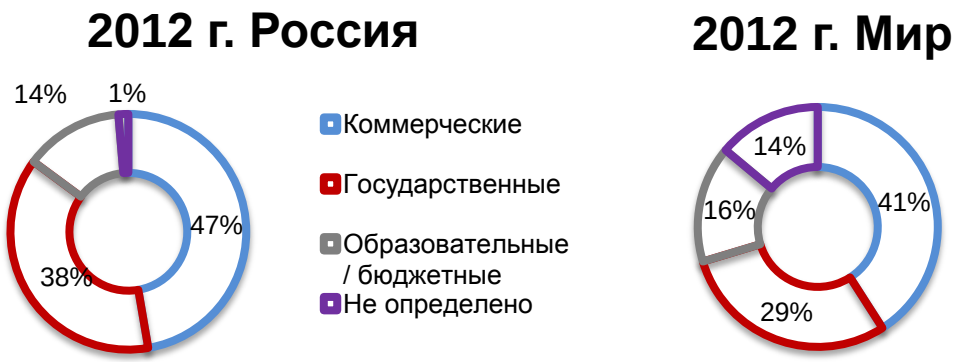


Рис.5. Соотношение случайных и умышленных утечек, 2012 г.

Отмеченный в глобальном отчете рост числа «государственных» утечек в России проявляется еще более ярко. Если по миру мы имеем долю утечек из госучреждений в размере 29%, для России эта цифра составляет 38%.

Вывод:

2012 год можно назвать 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.

Намеренные утечки в коммерческих компаниях

Утверждение, что коммерческие компании более серьезно относятся к защите информации, справедливо и для нашей страны. По миру доля «коммерсантов» в картине утечек стабильно падает (минус 5% к прошлому году), в России динамику мы пока не показываем, но представляется очевидным, что компании, несущие реальные убытки от утечек информации (в виде штрафов, недополученной прибыли и пр.) более заинтересованы в защите данных, чем, скажем, бюджетные образовательные учреждения.

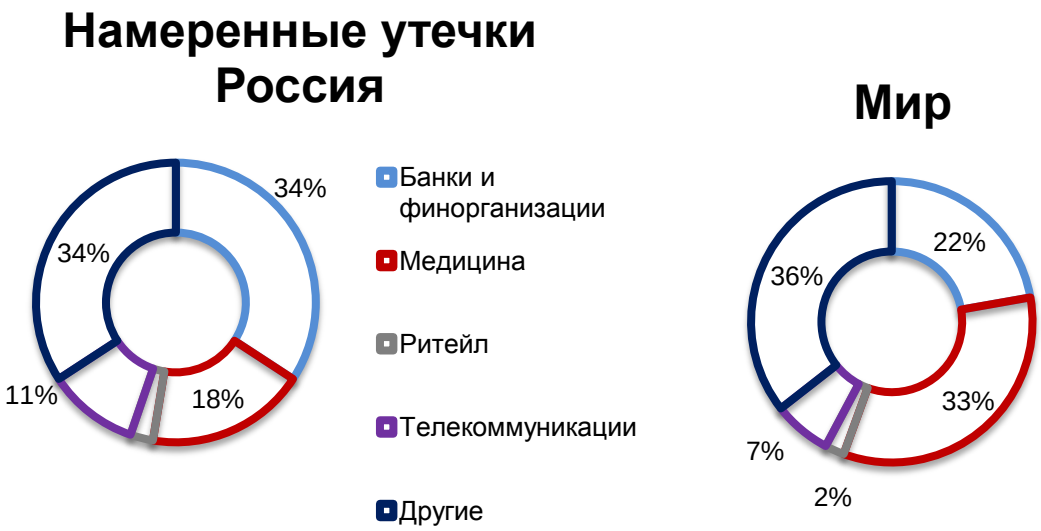


Рис.6. Соотношение умышленных утечек в компаниях, 2012 г.

Вывод:

Отметим запредельно высокую долю умышленных утечек – 34% в российских банках (по отношению к доле банков и финучреждений по миру). Впрочем, этот факт сложно назвать открытием – до четверти всех банковских утечек в мире приходится на российские кредитные учреждения. И это при том, что доля российских утечек (7,9%) в общемировой картине совсем не высока. Остается констатировать, что стремление российских финорганизаций к защите собственной информации и персданных граждан пока проявляется лишь на бумаге.

Типы данных

Наиболее интересной иллюстрацией российской картины утечек будет сравнение типов утекающих данных с общемировыми показателями. В целях большей наглядности мы свели различные виды тайн (служебная, врачебная) в категорию персональных данных, поскольку именно с их компрометацией были связаны конкретные случаи нарушения/ разглашения тайны. Коммерческая тайна намеренно оставлена в отдельной категории, поскольку ее разглашение, по опыту, несет компаниям наибольший материальный ущерб.

Интересно, что коммерческая тайна как самостоятельная категория «оттянула» на себя чуть более четверти всех инцидентов, в то время как по миру доля случаев с утечкой коммерческой тайны не превышает 6%. Это еще раз подчеркивает явный недостаток внимания российских компаний к защите собственных секретов.

Рис.7. Распределение утечек по типам данных, 2012 г.

Вряд ли стоит удивляться подавляющей доле утечек, связанных с персональными данными. Как уже отмечалось, именно утечки персональных данных вызывают в последнее время самый живой интерес общества. К тому же, это наиболее массовый способ заработка злоумышленников, имеющих доступ к защищенной информации. Ликвидные персональные данные интересны широкому кругу злоумышленников, так как их можно сбыть на чёрном рынке.

Сравнительно большие доли утечек, связанных с коммерческой и государственной тайной объясняются еще и тем, что в большинстве случаев огласка факта утечки коммерческой тайны имеет под собой желание пострадавшей стороны вывести инцидент в плоскость судебного разбирательства. 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:

Мировые, и российские компании все чаще используют публичное разбирательство как механизм, позволяющий укрепить дисциплину работы с защищенной информацией. С этим отчасти связана столько большая доля коммерческой тайны в российской выборке.

Каналы утечек

В сравнении с общемировой практикой, ситуация в России не сильно отличается. Однако есть небольшие особенности, которые следует учитывать. Во-первых, несмотря на набирающую популярность концепцию BYOD – принеси свое устройство и работай – утечек через гаджеты и ноутбуки пока сравнительно немного – 1,4% на фоне 9,6% по миру. Означает это ровно то, что россияне, скорее всего, бережнее

относятся и к самим устройствам, и к информации. С другой стороны, корпоративная почта и данные в мобильном телефоне пока еще не повсеместная российская практика. Что, с точки зрения безопасности данных, скорее хорошо.

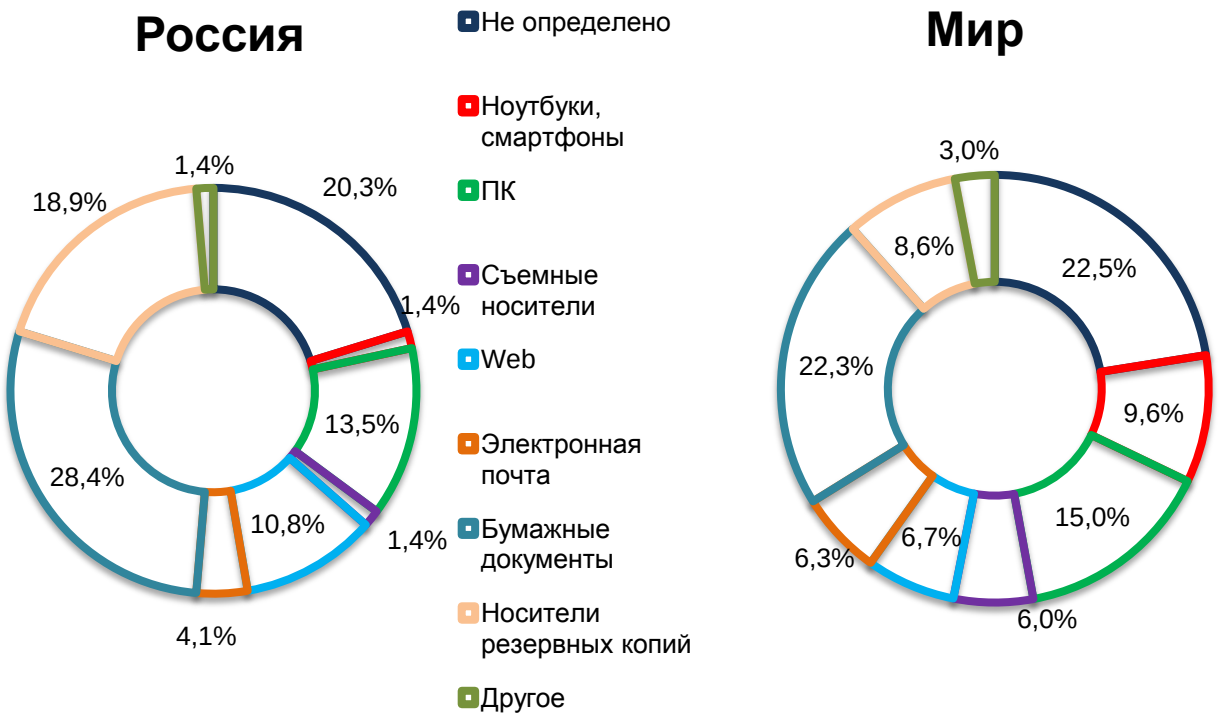


Рис. 8. Распределение утечек по каналам, 2011-2012 гг.

Ожидаемо сопоставимы показатели утечек через ПК и серверы, через веб и почту (тут Россия впереди, но объясняется это недостаточным проникновением средств защиты от утечек даже на уровне крупных компаний и госорганизаций).

Если принять во внимание все большую популярность средств защиты от утечек информации, в России, как и во всем мире, **следует ожидать падения долей традиционных каналов утечек** (где, собственно, технические системы защиты наиболее эффективны). Правда, в отношении нашей страны это справедливо в горизонте 3-5 лет.

Действительно существенно отличаются показатели России по двум каналам – утечка бумажной документации и резервные копии. **В первом случае мы на 6,1% опережаем мировые показатели – через «бумагу» уходит почти треть всей информации.** С резервными копиями разница также составляет десяток процентов – 18,9% утечек в России пришлось на диски и облачный бэкап, в то время, как мировой показатель стабильно держится в районе 10% (8,6% в 2012 году).

Рост утечек через бумажные документы характерен для всего мира. В 2012 году этот сегмент прирос еще на 3%. Как ни странно, именно организационные меры сегодня являются слабым местом информационной безопасности.

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.

Россия в контексте мировых утечек

Распределение утечек по странам 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 (74 или 7.9%). Напомним, что наша страна не в первый раз входит в число лидеров. В 2011 году третье место досталось Канаде, а вот годом ранее, в 2010-м символическая «бронза» за утечки также досталась Российской Федерации.

Ниже приведены агрегированные данные по искусственному показателю Утечка на миллион человек.

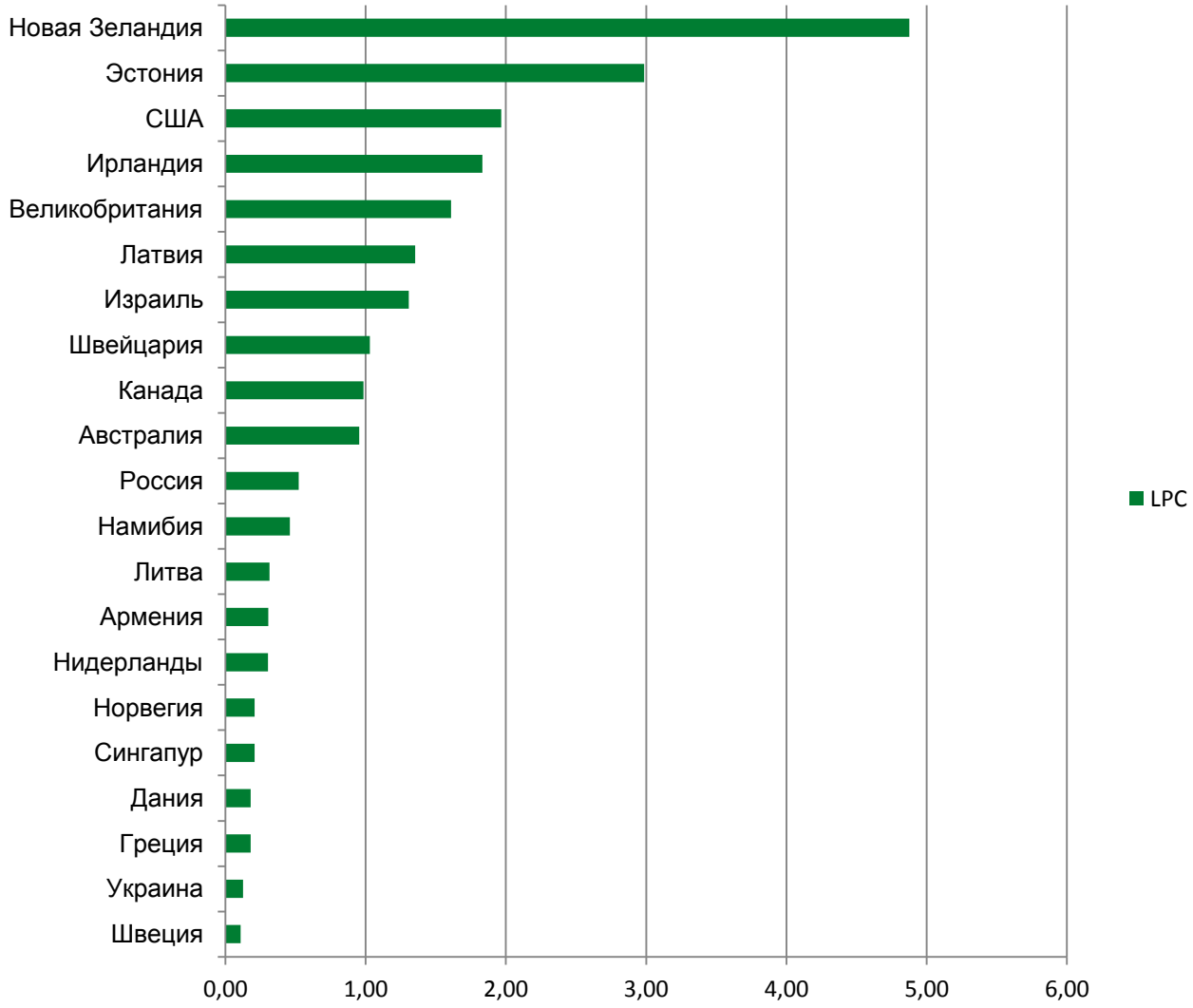


Рис. 11. Распределение утечек по странам, 2012г.
Страны упорядочены по числу утечек на млн. населения (LPM).

Заключение

В 2012 году Аналитическим Центром InfoWatch представлен отдельный отчет, цель которого - показать российскую картину утечек в контексте общемировых трендов. Во многом, мы получили ожидаемые выводы – характерная для российского пространства картина наблюдалась в отчетах InfoWatch трех-пятилетней давности.

С одной стороны, это внушает определенный оптимизм, поскольку говорит о том, что наша страна действительно идет к повышению уровня информационной безопасности, причем как на уровне бизнеса (где преимущества использования средств защиты очевидны), так и на уровне государства – в деле обеспечения безопасности персональных данных граждан. С другой, возникает резонный вопрос – что мешает пройти этот путь быстрее, чем остальной мир?

Оговоримся, львиную долю утечек в нашем глобальном исследовании поставляют страны, давно и серьезно занимающиеся данной проблемой – США, Великобритания. Это означает только одно – с увеличением внимания к теме защиты информации количество публичных утечек не будет снижаться. Наоборот, произойдет рост, поскольку значительная часть случаев, ранее остававшихся «в тени» получит огласку.

Собственно, именно роста количества российских утечек, которые будут преданы огласке в СМИ, мы и ожидаем в ближайшие 3-5 лет. Также можно прогнозировать постепенное снижение числа случайных утечек (вследствие внедрения средств защиты). Кроме того, хочется надеяться, что Россия окажется более удачлива в отношении организационной стороны вопроса защиты. Известно, что в западных странах, несмотря на серьезное проникновение систем предотвращения утечек, огромное число случаев компрометации данных связано с бумажными носителями и резервными копиями. То есть проблема даже не в средствах защиты, а в недостаточной регламентации работы персонала, в низкой культуре информационной безопасности.

В целом же отчет по российским утечкам указывает на неплохие перспективы страны в плане обеспечения безопасности информации. С двумя оговорками – в ближайшие год-два станет понятно, как бизнес-сообщество и регулирующие органы адаптируют концепцию BYOD (пока влияние этого фактора скорее незначительно). Второй момент связан с уже упоминавшийся организационной стороной вопроса. Пока безопасность рассматривается бизнесом как излишнее ограничение, что явно не способствует повышению уровня защиты информации в целом.