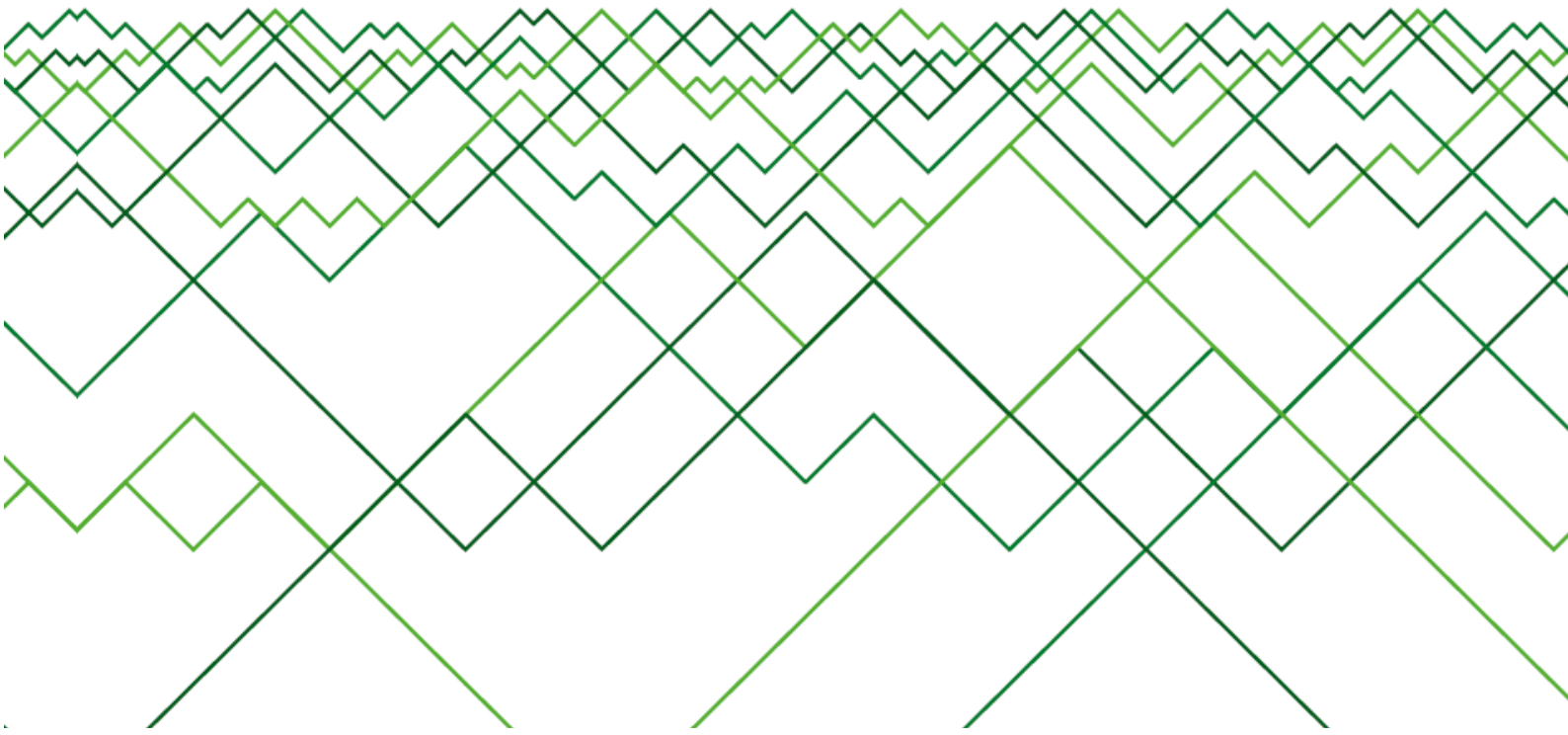
INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аналитический центр InfoWatch

Глобальное исследование утечек корпоративной информации в банковском сегменте (финансовые и кредитные учреждения) I полугодие 2012



INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Оглавление

Аннотация 3
Методология 3
Основные факты 4
Выводы: 5
Вклад банков в картину утечек 6
Умысел 7
Каналы утечек 8
Что утекает 9
Российские особенности 10
Тенденции 11
Заключение 12
Типичные банковские утечки 1-2Q 2012 13

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Аннотация

Аналитический Центр компании InfoWatch представляет первое отраслевое исследование утечек информации в кредитных и финансовых учреждениях за 1-2 кварталы 2012 года.

В эпоху мгновенного распространения информации, социальных сетей и электронных СМИ репутация компании настолько хрупка, что впору стелить соломку повсеместно. Банки это остро чувствуют, ведь любое сообщение о дырах в их системах безопасности прямо сказывается на лояльности клиентов.

Меж тем число таких сообщений растет год от года. Внешние атаки, случаи мошенничества в системах дистанционного банковского обслуживания, утечки данных о пользователях – лакомые темы для журналистов. И любая публикация такого рода надежности банку в глазах его клиентов не добавляет.

Данное исследование имеет единственную цель - дать обобщенную картину угроз, связанных с утечками конфиденциальной информации в банковском сегменте. Показать тенденции, характерные для банковского сегмента.

Методология

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

В частности, это означает, 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. Распределение параметров (типы утечек, каналы утечек и пр.) на имеющейся выборке год от года меняется плавно. Большинство изменений спрогнозировано заранее.

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

Данные о прямом ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций. **Мы не приводим экспертной оценки совокупных потерь компаний, связанных инцидентами ИБ и ликвидацией их последствий, во избежание ненужных спекуляций вокруг конкретных цифр непрямых потерь.**

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Основные факты

- ✓ Прямые убытки кредитно-финансовых организаций от утечек в первом полугодии 2012 года составили чуть более **2 млрд долл**.
- ✓ Скомпрометировано более **2 млн** записей, в том числе финансовые и персональные данные
- ✓ Лидирующий тип утечек – финансовая информация - **до 60%**
- ✓ Несмотря на ежегодное снижение доли утечек в коммерческих компаниях по отношению к общему числу утечек, доля «банковских» утечек остается неизменной – **5-7%**
- ✓ В банковском сегменте доля случайных утечек значительно ниже, чем в целом по всем индустриям (**20%** и **37%** соответственно)
- ✓ Также интересно, что в банках информация практически «не течет» через электронную почту, веб и съемные носители. Зато здесь значительно выше доля утечек через носители резервных копий – **41,7%**
- ✓ **24,7%** случаев от всех утечек пришлись на российские банки. При этом доля российских утечек в общей картине остается незначительной (см. глобальное исследование утечек за 2011 год)

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Выводы:

- ✓ Соотношение случайных и злонамеренных утечек (крен в сторону последних) в совокупности с незначительной долей «популярных» каналов (веб, почта, мессенджеры) говорит о безусловной эффективности используемых банками технических средств. С другой стороны, доля банковских утечек в общей картине не снижается. Очевидно, что технические средства, уверенно справляющиеся со случайными утечками, пасуют перед злонамеренным нарушителем. Такая ситуация характерна в случае, если массово применяются решения, ориентированные **только на контроль каналов передачи данных, но не самой информации**.
- ✓ Причины относительно слабого успеха банков в деле борьбы с утечками данных также кроются в **недостаточно высокой ИБ-культуре персонала** (неправильное хранение бумажных документов, потеря ноутбуков и пр.), **неэффективности применяемых организационных мер**.

В целом банковский сегмент показал себя более зрелым в отношении информационной безопасности. Можно с уверенностью прогнозировать скорый переход ИБ-специалистов банков от понимания проблемы к оценке эффективности средств и методов ее решения. Проще говоря, специалисты уже понимают, что информационная безопасность – это не конечный по времени проект, но постоянный процесс. И, находясь внутри этого процесса, мало достичь какого-то уровня безопасности (внедрить систему защиты) – **нужно поддерживать этот уровень постоянно.**

Вклад банков в картину утечек

Доля финансовых и кредитных учреждений в общей статистике утечек сравнительно невысока – **5,76%.** При этом утечки в банках - пятая часть (**18%**) от всех утечек в коммерческих компаниях. Интересно, что число утечек из коммерческих компаний утечек год от года снижается. В то же время доля «банковских» остается стабильной.

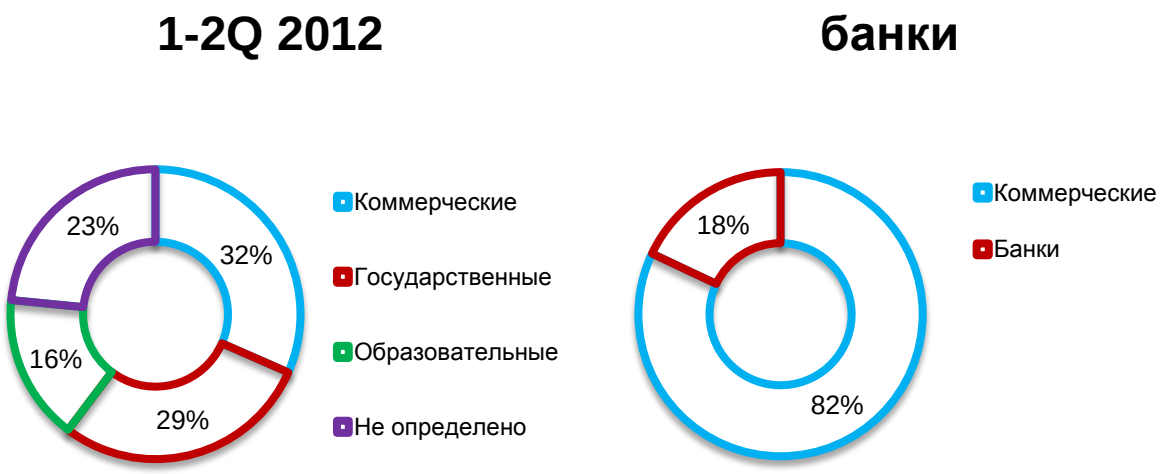


Рис.1. Распределение утечек по организациям. Доля банков, 1-2 кв. 2012г.

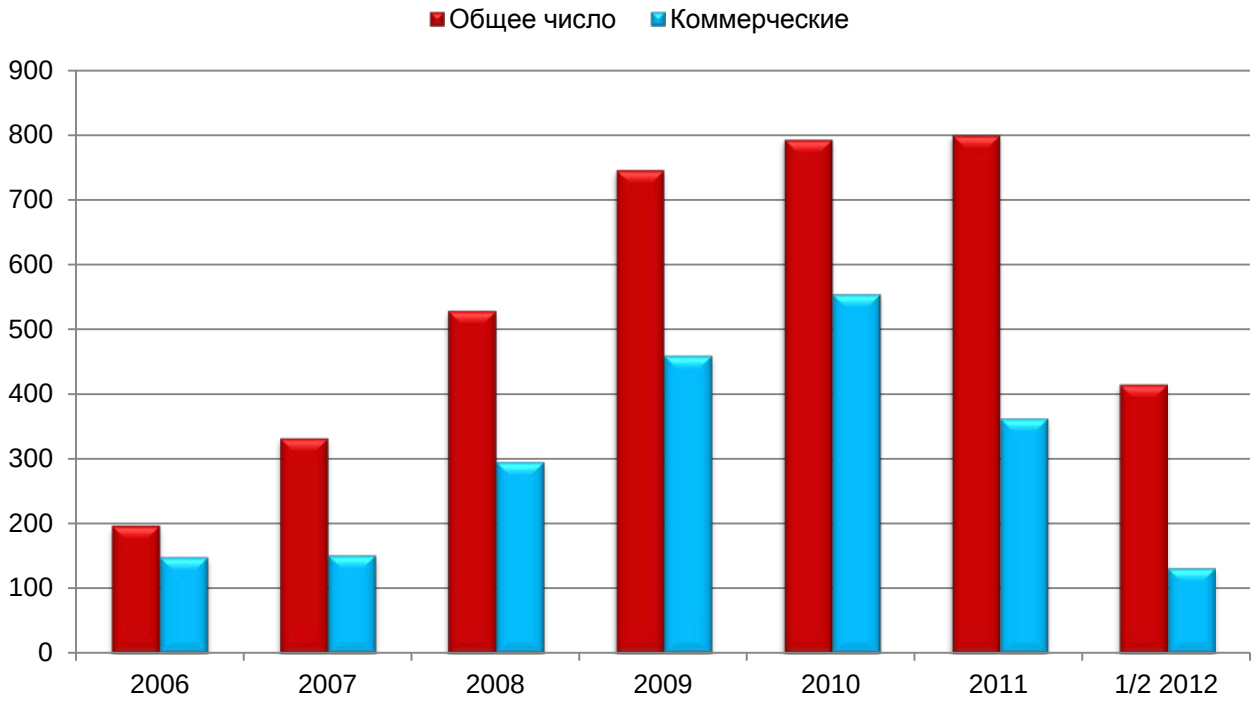


Рис. 2. Снижение доли коммерческих утечек в общей картине

Умысел

Соотношение случайных и умышленных утечек в финансово-кредитных учреждениях серьезно отличается от общей картины. На злонамеренные утечки приходится до **68%** утечек, в то время, как доля случайных составляет всего **20%**.

Это легко объяснить, исходя из имеющейся на рынке тенденции (наблюдаемой с 2007 года) к сокращению доли неумышленных утечек. Дело в том, что системы защиты корпоративной информации намного успешнее противодействуют именно случайным утечкам. Вспомним, что банковский сегмент – один из наиболее зрелых в плане информационной безопасности, и использование DLP-систем здесь скорее норма, чем исключение.

Очевидно, что благодаря продуктивной работе DLP-решений тренд на снижение доли случайных утечек проявляется в банковской отрасли наиболее ярко. Остальные отрасли идут с запаздыванием.

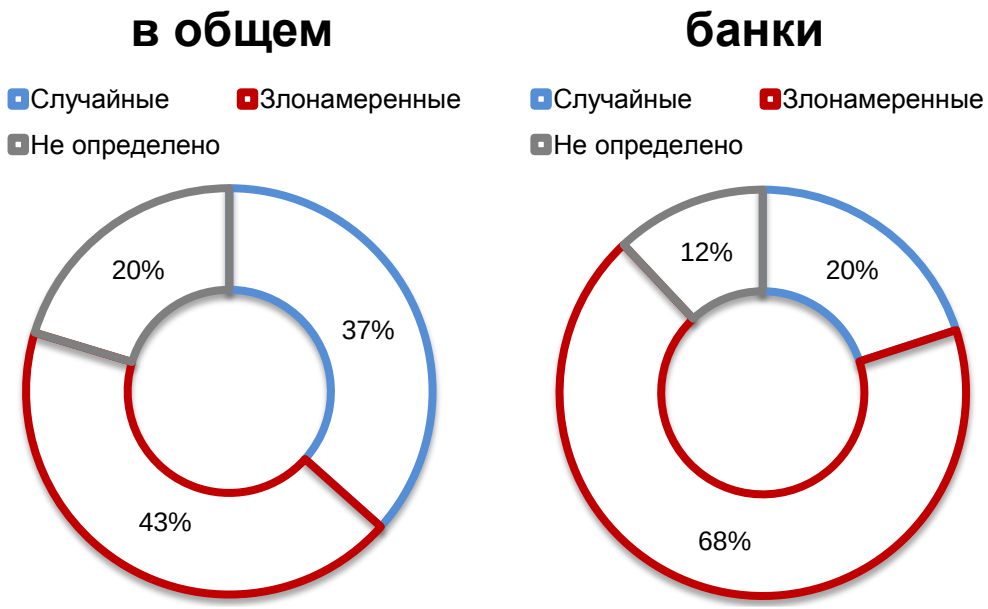


Рис.3. Соотношение случайных и умышленных утечек

Каналы утечек

С небольшой (по сравнению с общей картиной утечек) долей случайных утечек хорошо перекликаются данные по наиболее популярным каналам, через которые информация уходит из банков. Легко видеть, что такие популярные каналы утечек, как электронная почта и веб, полностью отсутствуют в картине банковских утечек. Это не означает, что в банках нет электронной почты и выхода в интернет. Скорее, **утечки на данных каналах отсутствуют как раз потому, что банковское сообщество активно использует технические средства для контроля перемещения информации**.

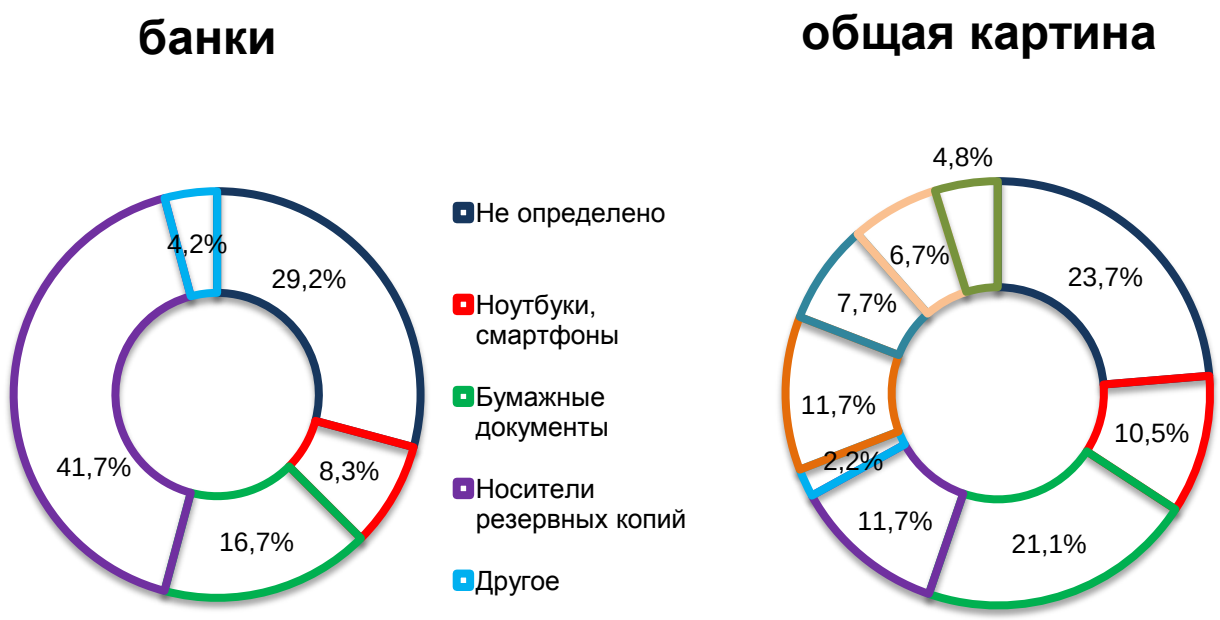


Рис.4. Каналы утечек. Утечки в банках и общая картина

С другой стороны, довольно высокий процент утечек через «нетрадиционные» для технических средств каналы – бумажные документы (**16,7%**), носители резервных копий (**41.7%**) показывает, что контролировать каналы недостаточно. Необходимо знать, где конкретно хранится или перемещается информация, и каков уровень ее конфиденциальности. Для решения этой задачи больше подходят контент-ориентированные, сложные DLP-решения. **Очевидно, что эти решения банки пока применяют далеко не повсеместно**.

Высокий (по сравнению с общей картиной) процент утечек через носители резервных копий также может быть связан, с одной стороны, с повышенным интересом злоумышленников к этой информации, а с другой - с недостаточностью организационных мер по контролю доступа к данным носителям, с низкой культурой информационной безопасности в ИТ-отделах банков.

Что утекает

Характер информации, которая уходит из банков, дает лишнее подтверждение тому, что банковский сегмент – совершенно особая сфера информационной безопасности. Если в общей картине утечек превалируют персональные данные **- 87,8%,** то в банках лидирующий тип утечек – финансовая информация - до **60%**. Персональные данные также уходят, но в меньших количествах - всего **8%**

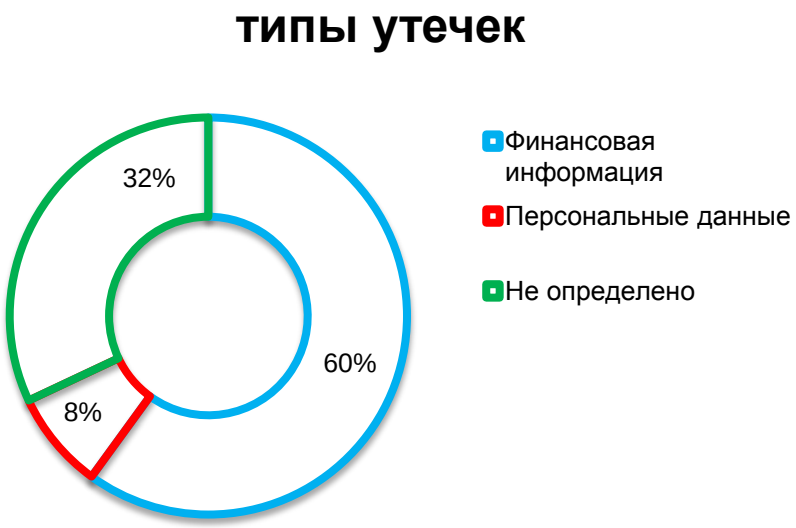


Рис.5. Распределение утечек по типам данных, 2012г.

Справедливости ради, в ряде случаев разграничить финансовую информацию и персональные данные не всегда возможно. Так утечка персонализированной базы данных клиентов с детализацией счетов относится и к финансовой информации, и к персональным данным. Однако столь значительная доля финансовой информации в сочетании с высоким показателем по намеренным утечкам позволяет сделать вывод о существующей корреляции данных. Очевидно, что финансовая информация банков представляет интерес, как для внешних, так и для внутренних нарушителей. Также очевидно, что утечка такого рода информации, ставшая достоянием общественности, долго не сходит с первых полос газет.

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Российские особенности

Следует отметить непропорционально большое количество случаев утечек конфиденциальной информации из российских банков. В то время как доля российских утечек в общемировой картине незначительна, отечественные банковские утечки составляют до четверти - **24,7%** (!) - процентов от совокупного количества утечек по всему миру.

Правда, в отличие от мировой практики, для российских утечек ущерб можно определить лишь на основе экспертной оценки (а это всегда дискуссионная цифра). Добавим также, что все утечки, зарегистрированные в российских банках, относятся к числу умышленных. Это не означает, впрочем, что случайных утечек не было совсем. Скорее, нужно говорить о том, что случайные утечки в силу слабости медийного повода практически не интересуют российские СМИ и блоггеров.

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Тенденции

На примере банковского сегмента можно увидеть, какой будет картина утечек в случае, если все компании начнут столь же внимательно относиться к вопросам информационной безопасности. Известно, что в кредитно-финансовых учреждениях интерес к теме ИБ повышенный. Приведенные в исследовании факты можно рассматривать как иллюстрацию эффективности (или недостаточной эффективности) организационных и технических мер, направленных на борьбу с утечками.

Очевидно, что **разительное отличие данных по утечкам в банковском сегменте от положения дел в целом по миру говорит о принципиальной особенности банковской отрасли**. Данное исследование дает нам уникальную возможность проанализировать последствия ужесточения регулирования и массового применения ИБ-систем в отдельно взятой отрасли.

- ✓ Снижение доли случайных утечек несомненно является следствием поголовного «увлечения» информационной безопасностью в банковской среде.
- ✓ Утечки «мигрируют» в незащищенные и неконтролируемые технически каналы. Так, утечки резервных копий – чистой воды разгильдяйство и несоблюдение установленных правил. Еще раз подтвержден тезис о том, что за техническими мерами неуклонно должны следовать организационные, повышение ИБ-культуры и пр.
- ✓ С ростом регуляционной нагрузки на отрасль повышается ее открытость (увеличение внимания регуляторов к банковской деятельности привело к возрастанию доли российских банков в отраслевой картине утечек). Поскольку все факты утечек получены из публичных источников, можно констатировать рост интереса населения (клиентов) к проблеме безопасности собственных финансовых данных.

Заключение

Аналитический Центр InfoWatch отслеживает сообщения о нарушении конфиденциальности информации с 2006 года. На протяжении всего периода наблюдений мы заметили, что доля коммерческих компаний, ставших жертвой утечек, неуклонно снижается (с **70%** в 2010 году до **32%** за первые полгода 2012). Однако доля банков - **17-20%** - от общего числа коммерческих компаний) за это время практически не менялась.

Тезис о том, что банковская отрасль более дисциплинированна, чем другие вертикали, оказался на поверку несостоятельным. Соотношение умышленных и случайных утечек (**68%** на **20%**) в банках несопоставимо с положением в целом по рынку (там **43%** на **37%**). Львиная доля (**90%**) инцидентов связана с потерей персональных данных и финансовой информации. Причем, речь идет не только о платежной (номера счетов, карточек - что было бы объяснимо), но и о внутренней банковской информации (например, зафиксированы случаи, когда из банков уходили данные о задолженности клиентов).

В некоторых случаях утечки информации повлекли за собой не только репутационные потери, но и прямые финансовые убытки. Наибольший ущерб (**2 млрд долл.** и падение акций на **17%**) своему работодателю нанес бывший менеджер американского банка, предавший огласке планы финансового развития компании.

Отметим, однако, что западные банки чаще несут прямые убытки не вследствие мошенничества (системы безопасности достигли определенного уровня надежности), а из-за неправомерных действий персонала – неправильной утилизации бумажной документации, неверно выстроенных политик безопасности, халатного отношения к хранению резервных копий и пр. Как результат – повышенное внимание со стороны регулирующих органов и штрафы за невыполнение требований законов и нормативных актов.

Очевидно, что в случае ужесточения требований к банковским системам информационной безопасности в нашей стране (что ожидается в скором времени), прямые убытки российских банков, связанные с нарушениями требований регуляторов и, как следствие, с утечками данных, «подтянутся» к мировым показателям.

Типичные банковские утечки 1-2Q 2012

Скомпрометированы данные 7 тыс. клиентов Credit Suisse

Сотрудник швейцарского банка Credit Suisse передал властям Германии данные о гражданах, уклоняющихся от налогов. Размер сокрытого капитала оценивается в несколько миллиардов евро.

По сообщению Handelsblatt, речь идет примерно о 7 тыс. клиентов, большинство из которых являются гражданами Германии. Размер же скрытого от налоговой инспекции капитала составляет несколько миллиардов евро. По данным немецких следователей, попавший в их распоряжение перечень клиентских данных позволяет почти со 100-процентной гарантией находить уведенные от налогообложения в ФРГ громадные суммы. В среднем речь идет о вкладах примерно в 500 тыс. евро, но в отдельных случаях встречаются депозиты в 12 млн евро и даже больше.

Служба финансового надзора оштрафовала сотрудника JP Morgan на $450 тыс

Служба финансового надзора оштрафовала сотрудника JP Morgan на 450 тыс. фунтов за разглашение конфиденциальной информации своих клиентов.

Сотрудник банка JP Morgan Йен Чарльз Ханнам передавал инсайдерскую информацию о предстоящих сделках и других активностях клиентов третьим лицам. Службе финансового надзора стало известно о двух инцидентах, произошедших еще в сентябре и октябре 2008 года. Г-н Ханнам пересылал конфиденциальные сведения, которые он получал от клиентов, по электронной почте. Максимальный штраф, который назначала за подобные действия Служба финансового надзора, составил 7,2 млн фунтов.

Сотрудница Bank of America воспользовалась персданными клиентов, заработав 180 тыс. долл.

36-летняя Люсиана Альварадо призналась в краже 180 тыс. долл. с клиентских счетов банка. Как сотрудник отдела претензий, она имела доступ к личной информации клиентов, чем и смогла воспользоваться. Путем подмены данных об адресах клиентов, кредитной информации, ей за несколько лет удалось перевести чуть менее 200 тыс. долл. с клиентских аккаунтов на личные счета и счета своей семьи. После увольнения из банка, Люсиана продолжала «трудиться» на ниве электронных переводов, используя логины и пароли, оставшиеся у нее со времени работы в банке. Интересно, что мошенница творчески подходила к выбору жертв и облегчала электронные счета тех клиентов, чьи имена и фамилии были схожи по звучанию с ее собственными.

За первое полугодие 2012 года в банках по всему миру скомпрометировано более 2 млн. записей, в том числе финансовые и персональные данные. Размер прямых убытков, понесенных банками вследствие утечек – более 2 млрд долл.