ЗИ

АКАДЕМИЯ
СОВРЕМЕННЫХ
ИНФОКОММУНИКАЦИОННЫХ
ТЕХНОЛОГИЙ

ЗИ **Защита информации**

ЗИ.3 Отчет об утечках корпоративной информации и персональных данных за 2010 год
(количество частей – 1, число страниц - 32)

ЗИ.3

Оглавление

Аннотация

Аналитический центр SECURIT Analytics представляет результаты отчета об утечках конфиденциальной информации, обнародованных в 2010 году. Теме утечек информации не зря уделяется повышенное внимание, ведь в 2009 году только в результате обнародованных инцидентов пострадало более 300 млн граждан, а убытки допустивших утечки организаций составили более 1,5 млрд долларов США. Всего же с начала ведения статистики пострадало более 1 млрд граждан различных стран мира, и только прямые убытки организаций составили более 10 млрд долларов.

Цель отчета SECURIT Analytics — еще раз обратить внимание на проблему незащищенности персональных данных и конфиденциальной информации в подавляющем большинстве организаций. В отчете приведена статистика всех обнаруженных инцидентов, проанализированы наиболее крупные и интересные утечки и дан прогноз развития ситуации. Целевая аудитория отчета — топ-менеджеры и специалисты по информационной безопасности коммерческих и государственных организаций, законодатели и журналисты.

Под утечкой информации в данном отчете понимаются инциденты, в результате которых доступ к конфиденциальным данным получили люди, изначально не имеющие на это прав. Виновниками инцидента могут быть сотрудники, подрядчики или никак не связанные с организацией злоумышленники, а каналом утечки могут служить USB-устройства, электронная почта, интернет-пейджеры, публичные веб-сервисы, ноутбуки или резервные копии данных. Классическим примером утечки можно назвать ситуацию с WikiLeaks, которой будет посвящена отдельная глава. В результате работы WikiLeaks фактически любой житель планеты получил возможность прочитать множество секретных документов.

По оценкам SECURIT Analytics реально в СМИ появляется информация лишь о небольшой части инцидентов, в лучшем случае 0,1% от реального количества утечек. Это связано с двумя основными причинами. Первая — несовершенство законодательства, которое лишь в нескольких государствах требует от организации обнародовать факт утечки данных сразу после ее обнаружения. Вторая — несовершенство применяемых мер защиты и, как следствие, техническая невозможность обнаружить утечку. Использование же специализированных DLP-систем пока еще довольно редко.

Мы надеемся, что подготовленные SECURIT Analytics результаты стимулируют организации обратить большее внимание на угрозы, связанные с возможной утечкой их конфиденциальной информации, и будут способствовать повышению общего уровня информационной безопасности в российских компаниях.

Ключевые факты

- В 2010 году зафиксировано 1014 утечек, что на 15,6% больше показателя 2009 года.
- Каждый рабочий день 2010 года происходило в среднем 4 утечки данных.
- Наибольшее количество инцидентов (924) зафиксировано в США. Это на 18,9% (147 утечек) больше, чем в 2009 году, однако в общей статистике доля США сократилась (–0,8%).
- В России зафиксировано 37 инцидентов, что на 60,9% больше, чем в 2009 году.
- Основными виновниками утечек (суммарно 76%) являются государственные организации, медицинские и образовательные учреждения, финансовые и торговые компании.
- От утечек страдают не только допустившие кражу или потерю данных организации, но и их сотрудники, клиенты, партнеры и подрядчики.
- Главными каналами утечек по-прежнему остаются электронная почта (17,8%) и потерянные или украденные ноутбуки (22,5%), хотя доля последних в общей массе в прошедшем году существенно снизилась (–6,5%).
- В 2010 году произошел значительный рост доли утечек через мобильные накопители (+4,4%) и веб-сервисы (+3,2%).
- В основном утекают персональные данные (63,6%) клиентов и сотрудников.
- Средний ущерб от одной утечки в 2010 году составил 3 793 725 долларов США, что на 49,3% ниже показателей 2009 года.
- Средняя утечка включала в себя более 250 тыс. персональных данных, что на 50,8% меньше, чем в 2009 году.

Методология

Основой для проведения исследования служит постоянно обновляемая SECURIT Analytics база данных утечек конфиденциальной информации. Для сбора сведений об инцидентах используются публикации СМИ, специализированные базы данных и собственные источники аналитического центра. Под утечками понимаются инциденты, в результате которых была потеряна или украдена действительно конфиденциальная информация. Обязательным требованием для попадания в базу SECURIT Analytics является достоверность информации, которая дополнительно перепроверяется в случае малейших сомнений.

Как было отмечено в аннотации, количество обнародованных утечек по оценкам SECURIT Analytics составляет в лучшем случае 0,1% от их фактического количества. Это связано с двумя основными причинами: отсутствием законодательно закрепленных требований обнародовать инцидент в подавляющем большинстве стран и несовершенством применяемых для защиты данных мер, которые просто не позволяют обнаружить факт утечки. Тем не менее, даже сравнительно небольшое количество обнародованных утечек, по оценкам SECURIT Analytics, позволяет получить реалистичные статистические данные.

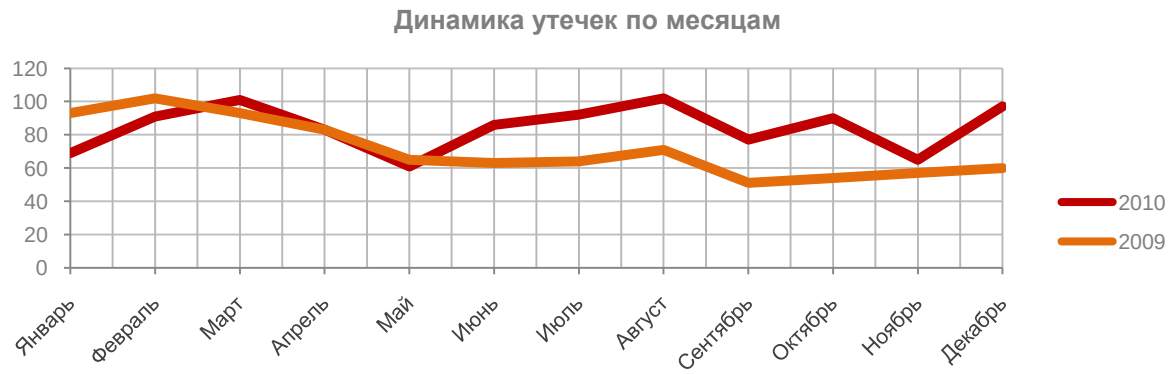
Подсчет ущерба от утечек производится по специальной методике, разработанной аналитиками SECURIT на основе российских и международных практик, с которыми приходится сталкиваться организациям, допустившим утечку. Величина ущерба в первую очередь зависит от масштаба утечки, действий организаций после обнаружения, внимания со стороны СМИ (индекса цитируемости и окраски сюжетов), действий регулирующих органов и характера самих данных. Так как не всегда удается оценить реальные затраты организаций, в некоторых инцидентах уровень ущерба занижается до минимума, связанного с очевидными расходами на работу со СМИ, внутренними расследованиями и компенсациями пострадавшим (в случаях с утечками персональных данных).

Статистика утечек

Анализируя динамику утечек информации в 2010 году по всему миру, в первую очередь хотелось бы отметить, что общее количество случаев по сравнению с 2009 годом демонстрирует тенденцию к увеличению. Всего за год было зафиксировано 1014 утечек, годом ранее их количество составляло 856. При этом мы видим, что в первом полугодии 2010 года наблюдалось уменьшение числа утечек по сравнению с аналогичным периодом 2009 года. Впрочем, достигнув самой низкой отметки в мае, количество обнаруженных утечек начало расти, дойдя до пика в августе и декабре 2010 года.

Увеличение числа обнаруженных утечек можно объяснить влиянием целого ряда факторов. Так, немаловажную роль играет рост интереса СМИ к этой проблеме и общее усиление внимания к утечкам со стороны общественности. Также можно отметить, что проблема утечек по-прежнему сохраняет свою актуальность в США, а внимание к таким случаям в других странах становится все более серьезным. Это подтверждают и данные по географии утечек, согласно которым в 2010 году доля инцидентов в США среди общего числа несколько снизилась.

Впрочем, хотелось бы обратить внимание и на то, что, несмотря на рост общего количества случаев в 2010 году, значительно уменьшился общий ущерб от всех утечек, а также средний показатель ущерба от каждого из инцидентов. Кроме того, заметно сократилось и число утерянных записей. Этот факт можно объяснить массовым внедрением DLP-систем и общей активизацией мер, направленных на борьбу с утечками, особенно в США, где все чаще компании сталкиваются со штрафами и прочими негативными последствиями допущенных утечек.



География

Географические данные на сегодняшний день наглядно показывают, насколько подходы к проблеме защиты от утечек конфиденциальной информации разнятся в зависимости от страны и действующих там законов. Так, большая часть из обнародованных утечек по-прежнему относится к США, в то время как в России ставшие достоянием гласности инциденты можно пересчитать по пальцам, однако даже они смогли затронуть интересы огромной части населения. Кроме того, несмотря на формальную принадлежность Google, Facebook, Gawker Media и других крупных организаций к США, связанные с ними утечки коснулись интересов людей во всем мире, в том числе и российских пользователей.

Перекос данных в сторону США объясняется действующим там законодательством, согласно которому организация обязана сразу же уведомить всех пострадавших, а в ряде случаев и компенсировать их реальные и потенциальные убытки. Данные требования не распространяются на утечки корпоративной информации, от которых страдает как сама компания-виновник утечки, так и сторонние юридические лица, например, клиенты или партнеры. В отличие от российских нормативно-правовых актов, в законодательстве США практически отсутствуют требования к техническим параметрам защиты, оставляя выбор инструментов на усмотрение менеджмента организаций. При этом предусматриваются крайне жесткие меры, которые часто включают финансовую и уголовную ответственность для должностных лиц, что существенно повышает внимание к проблеме утечек со стороны руководства компаний.

Тем не менее, большая часть утечек данных остается не только не обнародованной, но и просто неизвестной самим компаниям. Так, согласно данным опроса Harris Interactive, опубликованным в августе 2010 года, конфиденциальную информацию крадет каждый пятый сотрудник. Наибольшей опасности, по итогам опроса, подвержены данные о клиентах, а также корпоративные планы компаний и зарплатные ведомости. В случае увольнения риски утечки увеличиваются в 2,5 раза — те или иные конфиденциальные документы с бывшего места работы уносит почти половина опрошенных.

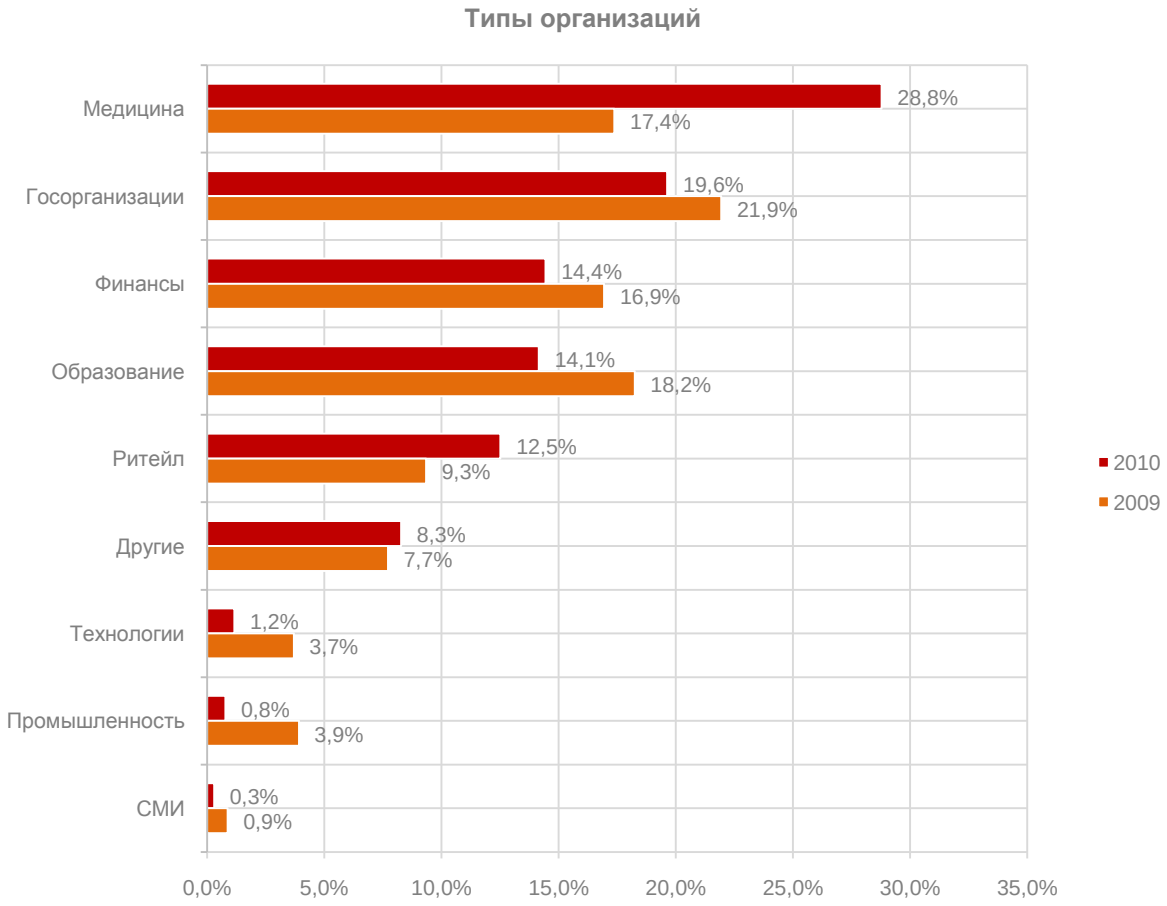
Типы организаций

Что касается распределения утечек по типам организаций, то, как мы видим, показатели прошлого года значительно изменились по сравнению с данными за 2009 год. Так, в 2010 году наблюдался рост доли инцидентов в медицинских организациях за счет снижения показателей других категорий.

Доля случаев в медицинских организациях выросла сразу на 11,4%, переместившись с третьего места по итогам 2009 года на первое. Государственные организации, лидировавшие по этому показателю годом ранее, теперь оказались на втором месте с долей в размере 19,6%. Снизились также доли образовательного и финансового секторов.

Такую тенденцию, как рост утечек в медицинской сфере, можно объяснить тем, что личные данные клиентов медицинских организаций зачастую представляют немалый интерес для злоумышленников, тогда как охраняется такая информация, как правило, значительно хуже, чем данные финансовых и государственных компаний.

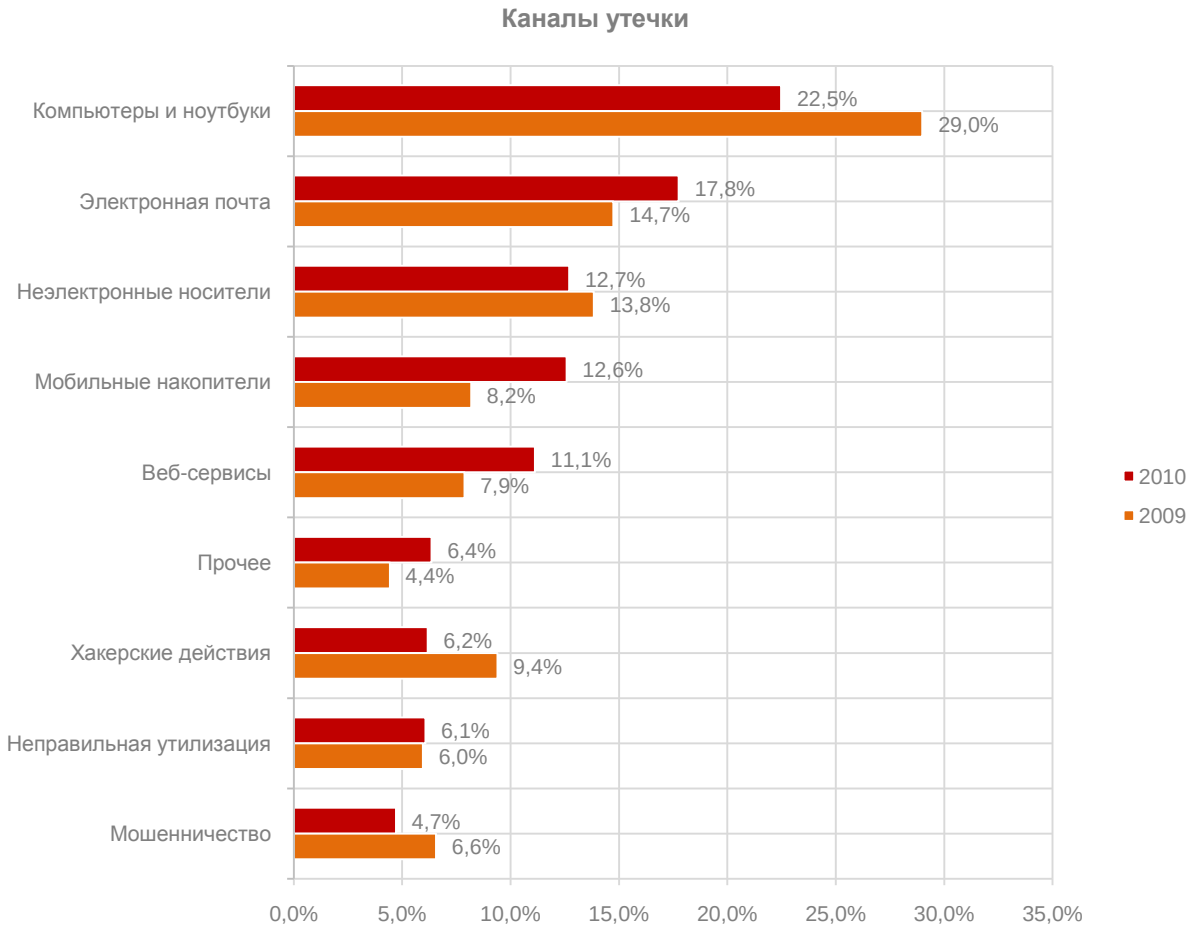
Между тем доля утечек в двух вышеуказанных секторах все еще остается достаточно высокой по вполне понятным причинам — данные таких организаций могут быть весьма ценными для преступников, а компании, работающие в этих секторах, часто имеют большой штат сотрудников, что увеличивает риск потери конфиденциальной информации.



Каналы утечки

В первую очередь можно обратить внимание на то, что заметно снизилась доля компьютеров и ноутбуков в качестве канала утечки, хотя их доля по-прежнему высока. В случае мобильных и стационарных (в меньшей степени) компьютеров утечка, как правило, происходит вследствие потери или кражи самого устройства. При этом зачастую ценность для злоумышленников, крадущих компьютер, представляет как раз само устройство, а не записанная на нем информация. Утечки же происходят из-за того, что владельцы компьютеров не шифруют конфиденциальную информацию на жестком диске — в этом случае при утрате она оказывается скомпрометированной. Таким образом, можно предположить, что снижение доли этого канала утечки связано как раз с более широким распространением среди пользователей различных DLP-систем или более простых программ для шифрования данных.

В то же время выросла доля утечек через Интернет и электронную почту. Причиной данной тенденции в значительной степени является недооценка многими организациями веб-сервисов, интернет-пейджеров и корпоративной почты как потенциального канала утечки данных. В свою очередь рост доли мобильных накопителей информации можно объяснить сложностью контроля использования флешек, CD, DVD и других носителей в крупной организации.

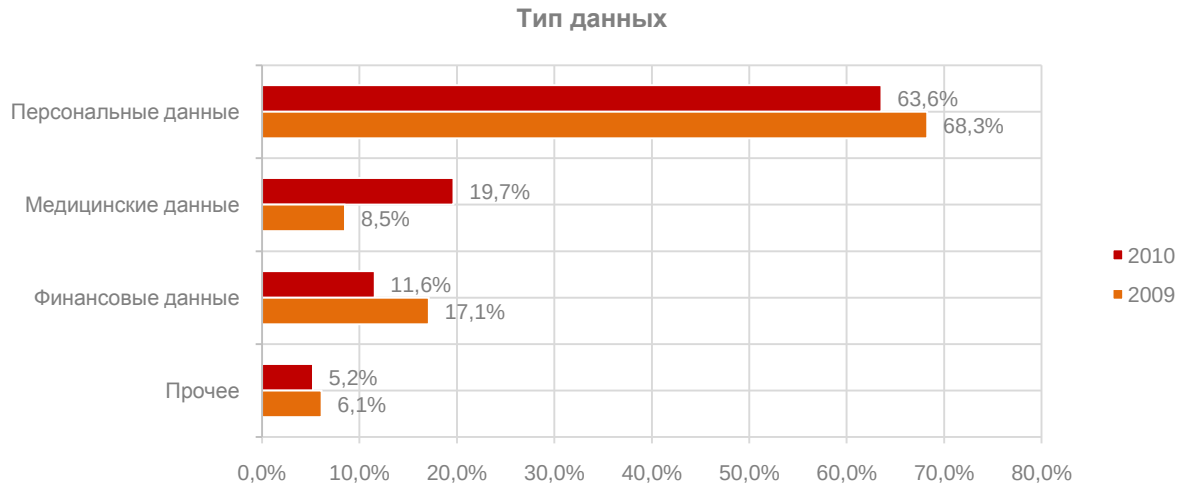


Типы данных

Утечки персональных данных по-прежнему составляют львиную долю всех обнародованных в прошлом году инцидентов. Что вполне ожидаемо, так как персональные данные активно используются различными организациями в повседневной работе, из-за чего и подвергаются риску компрометации.

Впрочем, следует отметить, что зачастую посторонние лица получают доступ к личной информации о человеке, неправомерное использование которой может принести ему лишь незначительные неудобства. Например, во многих из случаев в 2010 году скомпрометированы были лишь адреса электронной почты граждан, их номера мобильных телефонов или полные имена, что, разумеется, не представляет слишком серьезной опасности для пострадавшего.

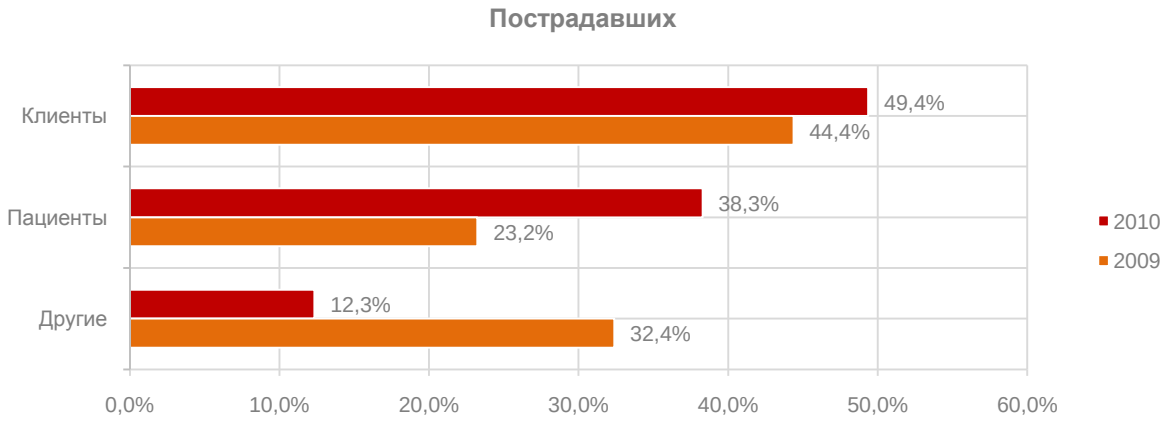
Утечки корпоративной информации входят в группу «Прочее», так как их доля в общей статистике крайне мала. Такая ситуация связана с особенностями современного законодательства и отраслевых стандартов, которые требуют обнародования факта утечки лишь в исключительных случаях. Сами же компании редко обнародуют данные об утечках корпоративной информации, так как это может не только негативно сказаться на их имидже в глазах клиентов, партнеров и сотрудников, но и повлечь за собой снижение котировок акций. Как уже отмечалось, по оценкам SECURIT Analytics в открытом доступе появляется информация максимум о 0,1% от реального числа утечек, и утечки корпоративной информации составляют большую часть всех необнародованных инцидентов.



Пострадавшие

В разделе «Пострадавшие» наряду с сокращением категории «Другие» мы видим увеличение долей клиентов компаний и пациентов медицинских учреждений, от утечек информации в 2010 году. Значительный рост доли пострадавших пациентов в 2010 году по сравнению с аналогичным периодом годом ранее прямо соотносится с увеличением числа утечек в медицинском секторе.

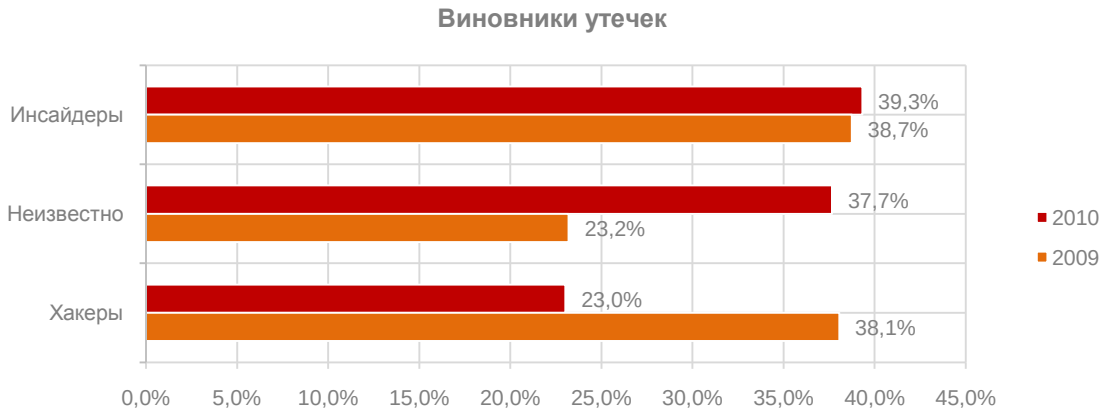
В то же время в категорию «Другие», доля которой среди общего количества пострадавших в 2010 году сократилась, вошли сотрудники различных организаций, а также другие частные лица, имеющие прямое отношение к компании, допустившей утечку. На основании этих данных можно заключить, что организации, возможно наученные горьким опытом громких утечек, произошедших в предыдущие годы, стали более внимательно относиться к персональной информации собственных сотрудников.



Виновники

Как и в прошлом году, на первом месте среди виновников утечек оказались инсайдеры — показатели этой категории остались примерно на том же уровне, что и в 2009 году. При этом значительно сократилась доля хакеров (–15,1%), но выросла доля случаев, когда виновники утечки остались неизвестны. Существенное сокращение доли хакеров, вероятно, связано с тем, что многие компании после ряда громких инцидентов усилили защиту своих сетей против внешних угроз, однако не смогли предотвратить внутренние утечки, обезопасить себя от которых в разы сложнее.

Очень часто организации не предоставляют общественности данных о виновниках утечек, а во многих случаях они и сами не имеют такой информации, тогда как результаты последующего за обнаружением инцидента внутреннего расследования не раскрываются. По этой же причине сложно судить о том, была ли утечка случайной или умышленной.



Ущерб от утечек

Что касается ущерба от утечек в 2010 году, то мы видим: общий ущерб сократился по сравнению с 2009 годом, и уменьшились средние потери организаций в каждом из инцидентов. В 2009 году самый большой всплеск по размеру потерь пришелся на октябрь, тогда как в 2010 году — на ноябрь. В течение же большей части и того, и другого года показатели оставались примерно на одном уровне.

Общее количество потерянных записей в 2010 году составило 254 627 497, что на 41,8% меньше показателей 2009 года. В среднем за одну утечку снижение и вовсе составило 50,8% или 251 112 записей.

Крупнейшие мировые утечки

WikiLeaks

Пожалуй, не будет преувеличением сказать, что утечки информации через WikiLeaks стали не только наиболее крупными в 2010 году, но и самыми громкими в истории утечек секретных сведений вообще.

Историю этого весьма популярного сейчас ресурса принято отсчитывать с 4 октября 2006 года, когда было зарегистрировано соответствующее доменное имя. Официальный запуск сайта, вместе с появлением на нем первых утечек, состоялся уже в декабре того же года. На сайте говорилось, что основан он «китайскими диссидентами, журналистами, математиками и создателями ИТ-стартапов из США, Тайваня, Европы, Австралии и ЮАР».

С именем Джулиана Ассанжа WikiLeaks стали связывать в январе 2007 года, когда тот заявил о себе в качестве публичного представителя сайта. Позже в прессе неоднократно отмечалось, что именно Ассанж является основателем ресурса, его философом, организатором и даже создателем кода, а также обеспечивает финансирование данного проекта.

В прессе о WikiLeaks впервые широко заговорили тогда же, в январе 2007-го, когда Ассанж сообщил, что у него имеется более чем 1,2 млн документов, которые будут опубликованы. Документы якобы были получены одним из источников WikiLeaks, имевшим отношение к сети серверов-анонимайзеров Tor. Этот человек заметил, что данную сеть часто используют китайские хакеры для сбора информации зарубежных правительств, после чего стал записывать этот трафик и позже передал его редакторам WikiLeaks. Впрочем, на WikiLeaks так и не был опубликован весь архив документов, лишь небольшая его часть. Однако именно эта утечка помогла сайту добиться популярности и первых упоминаний в СМИ.

До 2010 года сайт опубликовал ряд сравнительно интересных утечек, которые, впрочем, не вызвали громких скандалов. В конце декабря 2009 года представитель WikiLeaks также сообщал о проблемах с финансированием ресурса, из-за которых он на некоторое время прекращал свою работу.

Во второй половине 2010 года через сайт WikiLeaks, а также сотрудничающую с ним прессу по всему миру, было опубликовано сразу три крупных архива секретных документов властей США. Благодаря публикациям во всех крупнейших СМИ мира, эти утечки стали достоянием широкой общественности и привели к огромному росту популярности ресурса WikiLeaks и появлению армии его сторонников.

Первая из трех крупнейших в истории утечек произошла 25 июля 2010 года, когда администрация WikiLeaks предоставила трем авторитетным изданиям — британскому The Guardian, американскому The New York Times и немецкому Der Spiegel — доступ к архиву из более чем 92 тыс. документов с информацией, относящейся к военным действиям в Афганистане в период с 2004 по конец 2009 года. Позже этот архив выложили в свободный доступ на сайте.

Документы в значительной степени были составлены из отчетов различных военных подразделений армии США и союзников. Большинство из них написаны солдатами или офице-

рами разведки. Утечку назвали самой масштабной на тот момент в истории США. Она нанесла серьезный ущерб репутации американской администрации и вызвала гнев представителей Белого дома, который, в свою очередь, стал причиной начала преследований создателя WikiLeaks Джулиана Ассанжа, а также кампании властей США, направленной на прекращение работы скандального сайта.

В опубликованных о войне в Афганистане документах содержались, в частности, ранее не сообщавшиеся данные о гибели мирных жителей в результате операций войск НАТО, реальных потерях британских и американских военных, стратегических неудачах этой военной кампании, возможной поддержке афганских талибов Ираном и Пакистаном и т. д. Несколько документов относятся и к Усаме Бен Ладену, хотя представители властей США ранее заявляли, что не получали о нем никакой достоверной информации уже несколько лет.

Уже 23 октября 2010 года состоялась вторая крупная утечка — администрация WikiLeaks опубликовала в свободном доступе «Иракское досье». В Сети выложили почти 400 тыс. документов, посвященных войне в Ираке, относящихся к периоду с 1 января 2004 года по 31 декабря 2009 года.

Первым о содержании нового архива рассказал телеканал «Аль-Джазира». В иракском архиве WikiLeaks содержится огромное количество различных сведений о войне в этой стране, которые ранее не были известны широкой общественности. В частности, в документах архива сказано, что всего в ходе военных действий пострадали 285 тыс. иракцев, среди которых 109 тыс. человек были убиты. Около 63% из них были мирными жителями. Кроме того, в архиве содержится информация о многочисленных случаях, когда бойцы американской фирмы Blackwater (охранная фирма, которую называют самой большой в мире «частной армией») открывали огонь по мирным жителям.

Если в случае с утечкой афганского досье властям не удалось предъявить кому-либо обвинения в распространении секретных сведений, несмотря на все старания найти анонимные источники WikiLeaks, то в случае с публикацией документов по военной кампании в Ираке виновного все же нашли. В утечке обвиняют военнослужащего разведподразделения армии США Брэдли Меннинга. Он являлся специалистом по анализу разведывательных данных при батальоне поддержки 2-й бригады 10-й горнострелковой дивизии быстрого реагирования, входящей в американский контингент в Ираке.

Меннинга арестовали еще в мае 2010 года, тогда как обвинение предъявили только через два месяца — в июле. По информации американских военных, именно он передал сотрудникам WikiLeaks значительную часть «Иракского досье» — около 250 тыс. документов. Кроме того, специалист по анализу разведданных опубликовал в Сети оперативную видеозапись, сделанную с борта вертолета, который в 2007 году расстрелял группу мирных жителей Ирака с детьми. Меннинг все еще ожидает суда в тюрьме, а вина его не доказана.

Завершила же 2010 год третья крупная утечка, которая привела к масштабному скандалу, так как затронула дипломатические отношения США с большинством других стран мира. 28 ноября 2010 года WikiLeaks через собственный сайт, а также ряд значительных СМИ начал раскрывать крупный архив секретных дипломатических телеграмм США, в которых подробно освещается взаимодействие Государственного департамента США с американскими посольствами по всему миру.

Всего в свободный доступ планируется выложить архив из 251 287 документов. Первую 291 дипломатическую депешу опубликовали 28 ноября, предоставив доступ к ним международной прессе. Все депеши в архиве датируются 1966–2010 годами и отправлялись из 274 посольств США по всему миру. В них содержится огромное количество разной информации — дипломатический анализ политики различных стран и их лидеров, слова и действия политических лидеров, которые, по мнению американских дипломатов, имеют важность для США или характеризуют ситуацию в стране, обсуждение многих международных и локальных вопросов и многое другое.

Поскольку опубликованные депеши так или иначе затрагивают большинство государств мира, эта утечка вызвала бурную реакцию как со стороны властей, так и в СМИ. Так, правительство США подвергло WikiLeaks жесткой критике за публикацию архива, заявив, что данная утечка может представлять существенную угрозу для международных отношений и глобальной безопасности.

Документы из архива дипломатических депеш США публикуются на сайте частями. По словам представителей WikiLeaks, весь архив планируется выложить в течение примерно 7 месяцев.

Власти США, между тем, изо всех сил пытаются прекратить поток утечек секретных данных разными способами. Так, в декабре Пентагон именно с целью борьбы с утечками официально запретил всем представителям вооруженных сил США использовать любые переносные носители данных, включая CD, DVD и USB-накопители, несмотря на то, что такое нововведение может значительно осложнить для военных повседневную работу.

Результатом масштабной кампании против WikiLeaks, начатой американскими властями, стали многочисленные проблемы с хостингом этого ресурса, а также другими услугами, которые обычно оказывают для подобных некоммерческих организаций сторонние компании. Так, после совершения целого ряда DDoS-атак на WikiLeaks во второй половине 2010 года его было решено перенести на хостинг компании Amazon. Через некоторое время Amazon отказался предоставлять сайту такие услуги под давлением властей США. После этого WikiLeaks был вынужден пользоваться услугами хостинга OVH во Франции, что, в свою очередь, привело к требованиям французского правительства отключить этот сайт. Согласно последней информации, сейчас WikiLeaks размещается на серверах шведской компании PRQ. Впрочем, после многочисленных отключений сайта его сторонники создали в Сети множество зеркал WikiLeaks, чтобы помешать противникам идеи распространения секретных сведений остановить этот процесс.

Целый ряд зеркал WikiLeaks запустили и в Рунете. Российская «Пиратская партия» создала копию WikiLeaks в доменной зоне «.рф» под названием «Викислив.рф». «Пиратские партии будут только поддерживать доступность сайта в случае последующих атак на него. Российские пираты играют для WikiLeaks такую же роль, как и пираты из других стран: строят и поддерживают инфраструктуру, разрабатывают механизмы распределения трафика между зеркалами наподобие p2p-сети», — отметил председатель российской «Пиратской партии» Павел Рассудов.

23 декабря 2010 года газета The Washington Post сообщила, что Центральное разведывательное управление (ЦРУ) США создало подразделение WikiLeaks Task Force — WTF, которое займется оценкой ущерба американскому аппарату и другим службам от публикаций дипломатических депеш и документов американских военных сайтом WikiLeaks. Стоит отме-

тить, ЦРУ меньше других ведомств пострадало от утечек — бывшие сотрудники разведки рассказали The Washington Post, что в Управлении действуют строгие правила безопасности, сотрудникам запрещено записывать информацию на переносные диски. Новый отдел главным образом будет реагировать на последние утечки свежих документов, сообщил представитель ЦРУ.

Подводя итоги, можно отметить, что утечки на WikiLeaks не только стали самыми масштабными и наиболее резонансными в истории, но и, судя по всему, оказали весьма заметное влияние на политику многих стран, и США в первую очередь. В связи с широким резонансом последней утечки в прессе, армия фанатов WikiLeaks по всему миру быстро растет, а значит, увеличивается и число людей, которые, имея доступ к разного рода секретным сведениям, захотят поделиться ими со всем миром.

Facebook

Еще одна крупная утечка в 2010 году связана с самой популярной в мире социальной сетью Facebook, аудитория которой превышает 500 млн зарегистрированных пользователей по всему миру.

Как обнаружило в сентябре издание Wall Street Journal, соцсеть предоставляла более чем двум десяткам сторонних организаций сведения о зарегистрированных посетителях своего сайта, передавая им уникальные номера-идентификаторы пользователей. Делалось это даже в том случае, если пользователь установил максимальный уровень защиты. Данные пользователей передавались приложениями к Facebook — эта утечка затронула десятки миллионов человек, а информация поступала как минимум в 25 рекламных агентств и организаций, занимающихся статистикой.

Среди уличенных в передаче данных было популярнейшее игровое приложение, в котором пользователю предлагается вести собственное фермерское хозяйство, — FarmVille от компании Zynga Game Network, насчитывающее 59 млн пользователей, а также Texas HoldEm Poker и FrontierVille. Причем многие приложения отправляли сторонним компаниям данные не только непосредственно своих пользователей, но и их друзей.

Впрочем, следует сказать, что, несмотря на большое количество скомпрометированных в результате этой утечки данных (их точное число все еще неизвестно, но, как уже упоминалось, счет идет на десятки, а то и сотни миллионов), сторонним организациям передавались только ID (идентификаторы) пользователей социальной сети. Как отмечали аналитики, идентификаторы не относятся к разряду личной информации, а их утечка не может стать причиной серьезных проблем для пользователей — это ведь не номера социального страхования или финансовые данные, а выяснить по ID имя пользователя социальной сети, в принципе, может любой желающий.

Однако идентификаторы применялись рекламными агентствами и фирмами для сбора сведений о пользователях соцсети, что и вызвало значительное негодование как со стороны обычных людей, так и правозащитников, недовольных тем, как администрация Facebook относится к таким данным.

С помощью идентификационных номеров пользователей компании составляли их профили в собственных базах данных и отслеживали каждое их действие в Сети. Среди фирм, которые получали от приложений ID пользователей, например, была компания RapLeaf, которая специализируется на составлении баз данных с информацией о людях для их дальнейшей продажи сторонним фирмам.

После появления информации об утечках администрация Facebook постаралась успокоить общественность, сообщив о том, что примет меры для усиления конфиденциальности данных. Некоторые приложения, замеченные за передачей ID на сторону, действительно через некоторое время были закрыты, однако далеко не все.

Также представители Facebook отмечали, что в некоторых случаях разработчики приложений могут сами не знать о том, что их программа снабжает кого-либо данными о пользователях, так как приложения пишутся на основе технологий, скрытые возможности которых и применяются для получения информации.

Таким образом, мы видим, что даже не слишком важная, на первый взгляд, информация, такая, как идентификатор в социальной сети, при желании может привести к раскрытию достаточно большого объема конфиденциальных сведений о человеке. А если учесть, что ID пользователей передавались сторонним фирмам в течение достаточно долгого времени (сколько точно — неизвестно и подсчету не поддается), можно заключить, что эта утечка тоже была весьма и весьма серьезной.

В последнее время как обычные люди, так и эксперты по всему миру стали все чаще отмечать социальные сети в качестве потенциально опасного источника заражений вредоносным ПО, утечек конфиденциальной информации и финансовых потерь для компаний. И самой опасной и вредоносной соцсетью, конечно, является Facebook, ввиду своей массовости. Так, по данным исследования Panda Security, 73,2% американских компаний сталкивались с утечками секретных данных через названную сеть. Другие опасные с этой точки зрения сервисы — Twitter, YouTube и LinkedIn.

ECMC Group

Американская компания ECMC (Educational Credit Management Corp) Group, гарант по кредитам на обучение, в марте 2010 года потеряла личные данные более чем 3,3 млн человек в результате кражи портативного устройства (его тип отказались называть в интересах следствия) из штаб-квартиры организации в Миннесоте.

Скомпрометированные данные включали в себя полные имена заемщиков средств на образование, их адреса, даты рождения и номера социального страхования, за исключением финансовой информации разного рода. Всем пострадавшим должны были предоставить помощь по защите конфиденциальности и мониторингу счетов на предмет незаконного доступа к ним. Также всем людям, данные которых находились на украденном носителе, разослали письменные предупреждения.

Впервые об утечке стало известно 27 марта, когда работники ECMC Group уведомили о краже правоохранительные органы Миннесоты и получили от них разрешение на обнародование информации об этом инциденте.

Через некоторое время после появления новостей об утечке стало известно, что правоохранительным органам удалось найти преступника, укравшего портативное устройство у компании, — он был арестован и осужден. По словам представителей ECMC, они так и не выявили случаев использования скомпрометированных злоумышленником данных.

Как зачастую бывает с корпоративными утечками такого рода, широкой общественности не стали раскрывать все подробности и сообщать о ходе расследования, поэтому известно не так много. Компания принесла пострадавшим стандартные извинения с сожалениями о случившемся и заверениями о том, что она сделает все возможное, чтобы защитить пострадавших и не допустить повторения подобных инцидентов в будущем.

ECMC Group является подрядчиком департамента образования США по сбору и управлению информацией, связанной с кредитами на обучение в рамках федеральной программы кредитования семьи, а также предоставляет другие услуги в этой сфере. Принимая во внимание количество потерянных личных данных и их важность (злоумышленники получили доступ в том числе к номерам социального страхования), несложно подсчитать, что на устранение последствий этой утечки компании пришлось потратить немалые средства — по нашим оценкам, более 16 млн долларов США. В то же время, злоумышленник мог заработать на продаже конфиденциальных данных (в первую очередь, именно номеров соцстрахования) даже больше — около 20–30 млн долларов США. Впрочем, общественность уверяют, что он не успел продать эти данные.

Google

Утечка данных о бюджетах пользователей сервиса контекстной рекламы Google AdWords стала одной из самых интересных в прошедшем году. В начале сентября издание Advertising Age опубликовало внутренний документ с расходами крупнейших рекламодателей AdWords за июнь 2010 года, согласно которому 47 компаний ежемесячно тратят на контекстную рекламу в Google AdWords более 1 млн долларов США, 71 компания — от 0,5 до 1 млн долларов, 357 имеют бюджет в размере 100–500 тыс. долларов США, а остальные 1356 присутствующих в обнародованном списке организаций выделяют на контекст от 10 до 100 тыс. долларов США.

Крупнейшим рекламодателем в июне стал оператор связи AT&T Mobile, который за отчетный месяц потратил на продвижение в AdWords более 8 млн долларов США. На втором месте по расходам на рекламу оказалась компания Apollo Group, вложившая в контекст 6,67 млн долларов США. На третьем — крупнейшая в мире система онлайн-бронирования отелей и перелетов Expedia с показателем в размере 5,95 млн долларов США. Другими очень крупными клиентами сервиса контекстной рекламы Google стали известные площадки для интернет-торговли Amazon.com и eBay, рекламные бюджеты которых составили 5,85 и 4,25

млн долларов США соответственно, нефтяной гигант BP с бюджетом в размере 3,69 млн долларов США, а также система онлайн-бронирования отелей Hotels.com — 3,3 млн долларов США. Apple ежемесячно выделяет на контекстную рекламу в Google почти миллион долларов. Столько же тратит и производитель процессоров Intel. Киностудия Disney, крупнейшим акционером в которой является глава Apple Стив Джобс, потратила в июне на рекламу в AdWords менее 500 тыс. долларов США.

Особенно интересной оказалась ситуация с нефтяной корпорацией BP, которая после катастрофы в Мексиканском заливе выделила значительные средства из своего маркетингового бюджета на то, чтобы выкупить в поисковиках Google и Yahoo рекламу по запросам «oil spill» и «gulf oil spill» с целью противостояния волне критики, обрушившейся на компанию после трагедии. Сразу после катастрофы бюджет BP на контекстную рекламу только в системе Google подскочил с 57 тыс. до 3,69 млн долларов США в месяц. Этот факт также стал причиной негативных отзывов о компании и обвинений в попытках скрыть от общественности реальные сведения о масштабах трагедии.

Кроме того, в документе упоминаются такие известные компании, как General Motors, BMW, Eastman Kodak и многие другие — расходы трех вышеупомянутых фирм составили менее 500 тыс. долларов США.

Сразу же после публикации данного документа в Интернете Google отказалась как-либо комментировать эти цифры, заявив, что в настоящий момент проводит расследование относительно обнародования конфиденциальной информации, и пообещав наказать виновных.

О результатах своего расследования компания не сообщала. Многочисленные аналитики высказывали свое удивление тем, что интернет-гигант впервые допустил такую серьезную утечку. Некоторые эксперты даже предполагали, что утечка могла быть умышленной, хотя никаких доказательств такой версии предоставлено не было.

Gawker Media

Одной из крупнейших утечек 2010 года стал взлом баз данных крупной интернет-компании Gawker Media, в результате которого злоумышленники получили доступ к аккаунтам более чем 1,3 млн человек. Об инциденте стало известно 12 декабря.

Из-за взлома баз данных хакеры получили доступ к аккаунтам зарегистрированных пользователей таких ресурсов Gawker Media, как Gawker, Gizmodo, Jezebel и некоторых других популярных сайтов. Об утечке стало известно после того, как представители Gawker Media сообщили пользователям о необходимости изменения паролей к их аккаунтам.

Вскоре после взлома хакеры опубликовали в свободном доступе в Сети пароли к профилям некоторых сотрудников Gawker Media, а также логины тех пользователей, которые в качестве пароля использовали слово «password». По неподтвержденным официально данным, хакерам удалось получить в свои руки части кода собственной системы управления контентом, которая применялась на всех сайтах Gawker Media, благодаря чему они и смогли взломать базу данных.

Хакеры, которые взяли на себя ответственность за этот взлом, заявили, что сделали это из-за того, что авторы ресурса Gawker ранее нехорошо отзывались о хакерском форуме

4chan, который является главным сайтом для группы хакеров-активистов Anonymous, осуществляющей атаки на многие ресурсы по всему миру. В частности, они провели DDoS-атаки на сайты организаций, выступающих против пиратства в Сети и известного ресурса The Pirate Bay, а также сайты компаний, которых они считают врагами WikiLeaks.

«Нам казалось, что такой сайт, как Gawker, который любит издеваться над людьми, лучше позаботится о своей безопасности, а его сотрудники будут понимать, что они делают. Но мы доказали, что они не смогли защитить свои системы, хотя и думали, что находятся вне досягаемости от нас», — говорится в заявлении хакеров.

Приблизительно через неделю после утечки ряд экспертов отметили, что утечка данных Gawker Media окажет негативное влияние не только на саму компанию и принадлежащие ей ресурсы, но и на всю Сеть, а особенно крупные популярные сервисы. Как отмечают аналитики, многие пользователи вполне могли применять скомпрометированные логины и пароли на других ресурсах в Интернете, что является обычной практикой для большинства. А из-за этого хакеры вполне могут взломать аккаунты этих людей и на многих других сайтах, от социальных сетей и блог-платформ до интернет-банкинга и электронной почты.

Одними из первых всю опасность новой утечки оценили компании Google, Yahoo и Twitter, которые начали постепенно менять пароли некоторых своих пользователей, сообщая им об этом. Так как взломанная база данных долгое время находилась в свободном доступе в Сети (хотя и не полностью — как мы помним, хакеры выложили данные только тех аккаунтов, владельцы которых были настолько беспечны, что использовали в качестве пароля слово «password»), представители других крупных интернет-компаний имели возможность сравнить логины и пароли ресурсов Gawker Media с аккаунтами на собственных сайтах, предупредив тех пользователей, данные которых оказались в обеих базах.

Однако сам факт появления проблем такого рода напомнил всем о фундаментальной проблеме с паролями в Сети — пользователи применяют их на множестве сайтов сразу, что в случае утечки ставит под угрозу не только сервис, который непосредственно допустил ее, но и многие другие компании. Особенно это актуально для развлекательных ресурсов и социальных сетей.

Также следует отметить, что число различных сайтов и сервисов в Интернете продолжает быстро расти, а значит, и увеличивается количество аккаунтов, где используются стандартные для пользователя логин и пароль. При этом зачастую те же логины с паролями могут применяться не только в соцсетях, блогах и прочих сервисах развлекательного характера, но и, например, для доступа к корпоративной сети компании, в которой работает человек. А это уже, в свою очередь, является очень серьезной угрозой безопасности.

Другие

В середине февраля 2010 года Латвийское телевидение сообщило о крупнейшей в истории страны утечке конфиденциальных документов. По данным телеканала, к неизвестным попал архив 7,4 млн документов с конфиденциальной информацией о высших должностных лицах Латвии, коммерческих компаниях и физических лицах, а также о сотрудниках канцелярии президента Латвии и других госструктур.

Об утечке журналистам программы De Facto сообщили люди, которые называют себя «Народной армией четвертой Атмоды (Возрождения)» (4ATA). О «дыре» в системе они узнали еще весной 2009 года. В разговоре с человеком, трудившимся над разработкой системы электронного декларирования, они поняли, что «дыра» не случайна, а была сделана по указанию кого-то из самой верхушки СГД. По признанию представителей 4ATA, получить доступ к документам было очень просто, и в течение трех месяцев они беспрепятственно скачивали данные, итоговый объем которых составил порядка 120 Гб.

Ранее член 4ATA, называющий себя Нео, уже опубликовал в Интернете данные о зарплатах сотрудников рижского муниципального предприятия Rigas Satiksme («Рижское сообщение»), которое отвечает за общественный транспорт, и Rigas Siltums, которое обеспечивает город теплом. Руководители организаций подтвердили, что опубликованные Нео данные являются подлинными.

В феврале 2010 года стало известно об утечке личных данных более чем 170 тыс. работников и подрядчиков крупной нефтяной компании Shell. Скомпрометированная информация включала в себя полные имена сотрудников и подрядчиков Shell, их рабочие телефонные номера, домашние почтовые индексы, а также в некоторых случаях другие данные, такие, как домашние телефоны.

Копии скомпрометированной базы данных разослали по электронной почте представителям различных некоммерческих организаций по защите прав человека. Предполагается, что утечка произошла по вине кого-то из сотрудников нефтяного гиганта, недовольных политикой своего работодателя. Представители Shell заявили, что проведут тщательное расследование данного инцидента, но о его результатах общественности не сообщили.

В последних числах декабря 2010 года в СМИ появилась информация об утечке личных данных более чем 2,2 млн покупателей автомобилей Honda в США. С помощью компьютерного взлома злоумышленники получили доступ к полным именам владельцев автомобилей Honda, идентификационным номерам машин, а также логинам и паролям пользователей сайта Owner Link, созданного компанией Honda для владельцев своих автомобилей. Кроме того, хакеры завладели архивом в 2,7 млн адресов электронной почты премиального подразделения Honda в США.

По словам представителей Honda, утечка произошла по вине одной из фирм-партнеров производителя автомобилей. Всем пострадавшим разослали по электронной почте письма с уведомлением об инциденте и ссылкой на специальный сайт с мерами защиты против потенциальных угроз из-за утечки.

В августе 2010 года страховая компания Zurich была оштрафована Британским независимым управлением по финансовым услугам на 3,5 млн долларов США за утечку персональных данных 46 тыс. клиентов компании. Сама утечка произошла еще в 2008 году по вине представительства компании Zurich в ЮАР и была обнаружена в 2009 г. Штраф в размере 3,5 млн долларов США за потерю личных данных стал самым крупным в истории Великобритании.

BKK Health, крупнейшая компания, которая занимается страхованием здоровья в Германии, потеряла медицинские данные более чем 1,5 млн своих клиентов.

Американская компания Lincoln National допустила уязвимость в безопасности своей системы управления аккаунтами, в результате которой были скомпрометированы личные данные около 1,2 млн человек.

Страховая компания AvMed Health Plans допустила утечку личных данных около 1,2 млн своих клиентов в результате кражи двух ноутбуков с конфиденциальной информацией из офиса компании.

В результате ошибки на публичном веб-сайте округа Меса (штат Колорадо) около 7 месяцев в свободном доступе находились огромные объемы конфиденциальных данных, среди которых — имена информаторов полиции и домашние адреса помощников шерифа.

Крупнейшие российские утечки

Один из интернет-ресурсов для поиска работы

Одной из самых заметных российских утечек этого года стало появление в продаже на «черном рынке» кадровой базы данных с личной информацией более чем 847 тыс. людей, разместивших в Сети свои резюме для поиска работы.

Впервые о появлении на раскладках продавцов нелегальных баз данных подобного архива сообщила газета «Ведомости» в конце июня 2010 года. На диске, который пираты продавали по 1500 руб., содержались адреса электронной почты, номера мобильных телефонов, информация об образовании, семейном положении, местах работы и другие сведения о людях, разместивших свои резюме в Интернете.

В основном в базе данных были жители Москвы, однако встречались также сведения о соискателях из Томска, Ульяновска и ряда других городов. Большая часть резюме размещалась в сентябре 2009 года, однако были там данные и за прошлые годы.

Несмотря на то, что продавцы не раскрывали источники своих данных, эту утечку аналитики связали с HeadHunter — крупнейшим игроком рынка онлайн-рекрутмента в Рунете. Многие люди, чьи данные были в базе, утверждали, что размещали свои резюме именно на этом ресурсе примерно в те же даты.

Представители HeadHunter, впрочем, не подтвердили факта утечки, категорически опровергнув возможность взлома сайта. По их словам, данные для такой базы можно было получить открытыми способами, так как зарегистрированным пользователям HeadHunter была доступна информация о многих людях на сайте. Таким образом, хакеры могли выкачать резюме и вполне легальными способами.

По словам экспертов, в случае признания утечки, репутация HeadHunter могла весьма серьезно пострадать, ведь из-за этого компании перестали бы доверять многие люди. Сама же база данных такого рода может пригодиться в первую очередь не рекрутерам, так как информация из нее устаревает очень быстро, а спамерам и телемаркетологам.

Кроме того, база «Резюме-2009» стала первой в своем роде по двум параметрам: во-первых, это вообще первая в России нелегальная база данных соискателей, которая открыто распространялась, а во-вторых, она стала первой, которая позволяет искать электронную почту человека по номеру его телефона и наоборот. Это является дополнительным плюсом именно для спамеров и телемаркетологов, так как потенциальным клиентам можно предлагать одни и те же товары или услуги сразу по двум каналам одновременно.

«Молоток.Ру»

Пострадал из-за утечки и крупнейший в Рунете онлайн-аукцион «Молоток.Ру», хотя надо признать, что эту утечку очень крупной и резонансной все-таки не назовешь.

1 декабря администрация «Молоток.Ру» попросила своих пользователей сменить пароли, сообщив, что «в ходе тестирования была выявлена ошибка, которая могла привести к потере личных данных». При этом представители онлайн-аукциона подчеркнули, что проблема коснулась только небольшой части зарегистрированных пользователей сайта.

«23 ноября проводилось тестирование новых методов работы WebAPI. В ходе тестирования была выявлена ошибка, которая могла привести к потере личных данных. Проблема была решена, но пользователям, которых она затронула, в целях повышения безопасности необходимо изменить пароль для входа на «Молоток.Ру». Информационное письмо об этом было отправлено по электронной почте. Кроме того, форма изменения пароля доступна при попытке авторизации. Если вы продаете или покупаете на других платформах, используя тот же самый пароль, также измените его на каждой из них. Мы полностью проанализировали данное происшествие, чтобы избежать подобного в будущем. Случаи мошенничества, связанные с этой ошибкой, пока не наблюдались, но мы непрерывно отслеживаем работу сайта и попытки незаконного использования личных данных», — было сказано в сообщении администрации популярного ресурса.

Позже текст этого сообщения изменили, убрав из него упоминания о потере личных данных и смены паролей на других сервисах. Как отметил Александр Кудасов, глава департамента маркетинга «Молоток.Ру», в комментарии для издания «Маркер», смена паролей была неправильно аргументирована, так как на самом деле риск утечки имел место лишь для нескольких тыс. пользователей — не более 2% от их общего числа.

Сам факт утраты паролей подтверждения не получил — объявлено было лишь об уязвимости, способствующей доступу к ним. Впрочем, некоторые эксперты отмечали, что, если судить по рекомендации поменять пароли также и на других сайтах, «Молоток.Ру» не использовал стойкое шифрование паролей.

В контексте этой утечки уместно вспомнить и о куда более крупном по объему скомпрометированных данных инциденте с Gawker Media, а точнее, о проблеме паролей, которые часто используются на многих сайтах одновременно, — потеря базы данных одним из лидирующих сервисов Рунета в любой из категорий вполне может стать причиной проблем для всех остальных.

«Дальсвязь» (Группа «Связьинвест»)

Одной из крупнейших российских утечек в 2010 году стал недавний инцидент с компанией «Дальсвязь», которая скомпрометировала личные данные как минимум об 11 тыс. своих текущих и бывших клиентов.

8 декабря 2010 года было обнаружено, что на публичном FTP-сервере «Дальсвязи» выложены файлы со служебными и личными данными около 11 тыс. клиентов компании. Файлы содержали в себе такую информацию, как паспортные данные текущих и бывших клиентов, состояние абонента, последние платежи, используемый тарифный план, общую сумму начислений, указание на компанию-дилера, осуществившую подключение, и другое.

Судя по датам создания файлов, они находились в открытом доступе как минимум с июля 2010 года. Некоторые файлы датировались январем 2010 года. Таким образом, оказалось, что клиентская база филиала «Дальсвязь» была доступна всем желающим для свободного

скачивания на протяжении многих месяцев. К утру 9 декабря доступ к скомпрометированному каталогу был закрыт.

Кроме файлов со служебными и личными данными клиентов компании, на FTP-сервере был открыт доступ также к видео- и аудиоконтенту, некоторым пиратским программам. Судя по размещенным на сервере файлам, материал был выложен в открытый доступ одним из работников для личных нужд.

Представители «Дальсвязи» заявили, что не несут ответственности за утечку, обвинив во всем сотового оператора «Беспроводные информационные технологии» (БИТ), работающего на острове Сахалин. «Клиентская база, опубликованная на FTP-сервере, принадлежит сотовому оператору «Беспроводные информационные технологии». FTP-сервер, на котором был выложен файл с персональными данными, используется как файлообменник среди интернет-пользователей Сахалинской области. Согласно Регламенту предоставления услуг сетей передачи данных и электронной почты, клиент-пользователь FTP-сервера несет персональную ответственность за размещенную в его разделе информацию», — говорится в официальном комментарии компании.

Понес ли кто-либо из сотрудников БИТ или «Дальсвязи» персональную ответственность за произошедшую утечку, так и осталось неясным. Ничего не известно и о мерах, предпринятых компаниями для того, чтобы предотвратить появление подобных инцидентов в будущем.

Компании даже не принесли официальных извинений пострадавшим от утечки, несмотря на то, что она была весьма серьезной, не говоря уже о помощи в виде мониторинга финансовых счетов, широко распространенной в таких случаях в США.

Следует также отметить, что подобная утечка представляет опасность не только для людей, данные которых находились в скомпрометированных файлах, но и для самих компаний — ведь база может быть использована в том числе конкурентами для переманивания клиентов.

ChronoPay

Еще один заметный инцидент произошел уже в последние дни 2010 года. 27 декабря издание «Лента.Ру» написало о взломе базы данных популярного платежного сервиса chronopay.com со ссылкой на официальное заявление администрации ChronoPay, размещенное на сайте сервиса и подписанное генеральным директором ЗАО «Хронопей» Павлом Врублевским.

В заявлении сообщалось о том, что взлом базы данных ChronoPay привел «к полной утечке всех имеющихся персональных данных пользователей за 2009—2010 годы, включая полные номера кредитных карт и cvv-кодов». Пользователям посоветовали немедленно позвонить в свой банк и заблокировать кредитную карту «для предотвращения массового списания злоумышленниками денег в период новогодних и рождественских праздников» и сообщить об этой утечке всем знакомым, использующим сервис ChronoPay.

Впрочем, очень скоро администрация ChronoPay опровергла все сообщения о масштабной утечке, заявив, что информация о взломе была опубликована на сайте злоумышленниками, укравшими доменное имя ChronoPay.com. «Злоумышленники перевели домен нашей

компании, ChronoPay.com, с нашего регистратора (DirectNic) на другого (Network Solutions), после чего связали домен со своим сервером, где и разместили компрометирующий нас текст, — объяснили инцидент представители ChronoPay. — При этом непосредственно пользовательские данные скомпрометированы не были».

По словам администрации ChronoPay, взлом сайта и сообщение об утечке стали очередной волной «черного пиара» в адрес ChronoPay, осуществляемой «с целью дискредитации сервисов компании». «В октябре мы проходили сертификацию Payment Card Industry Data Security Standard, утечек с нашей стороны не было», — отметили в ChronoPay.

При этом злоумышленники даже создали специальный блог на платформе «Живой журнал» под названием chronofail, где опубликовали якобы часть информации, полученной в ходе взлома. В частности, в блоге выложили реальный номер кредитной карточки Юрия Синодова, основателя и главного редактора популярного среди деятелей Рунета новостного сайта Roem.ru. Представители ChronoPay заявили, что опубликованные номера кредиток были получены хакерами не в результате взлома базы данных процессинговой системы, а с помощью поддельного сайта на домене ChronoPay.com. Многие эксперты подтвердили данную версию. Кроме того, хакеры опубликовали набор SSL-ключей якобы из числа использующихся в ChronoPay на момент публикации.

ChronoPay является международной процессинговой компанией со штаб-квартирой в Амстердаме. Компания специализируется в области обработки платежей по банковским картам и иным платежным инструментам в Сети, являясь связующим звеном между банками-эквайрами и интернет-торговцами.

Принимая во внимание высокую популярность системы ChronoPay у российских пользователей, можно отметить, что в случае реальной утечки персональных данных пользователей последствия могли быть очень серьезными как для самих людей, так и для компаний, ведь для устранения всех рисков потребовалось бы срочно заблокировать значительное количество кредитных карт. Впрочем, представители компании утверждают, что система безопасности ChronoPay «содержит около 50 фильтров 100 базовых настроек и около 200 комбинированных», что обеспечивает надежную защиту конфиденциальной информации.

«Альфа-банк»

В декабре 2010 года также стало известно о крупной утечка в финансовом секторе, ставшая самой масштабной в истории российской банковской системы. 7 декабря в прессе появились сообщения о том, что «Альфа-банк» с целью предотвращения массового хищения денежных средств со счетов принял беспрецедентное решение о блокировании 7 тыс. пластиковых банковских карт.

Как позже объявили представители банка, утечка конфиденциальной информации произошла через сеть банкоматов в Краснодаре. Через сеть банкоматов одного из краснодарских банков злоумышленникам удалось завладеть данными о PIN-кодах пластиковых карт клиентов «Альфа-банка».

Служба безопасности банка не смогла установить, каким именно образом преступники получили доступ к PIN-кодам. Предполагается, что имел место взлом компьютерной системы сети банкоматов, хотя не исключена возможность утечки с помощью сотрудников банка.

Впрочем, эксперты отмечают, что мошенничество сотрудников банка все же маловероятно, так как в этом случае злоумышленники, скорее всего, смогли бы вывести со счетов деньги раньше, чем факт утечки был бы обнаружен.

В результате блокировки пластиковой карты клиенты «Альфа-банка» лишились возможности удаленных операций со своим банковским счетом. При этом они по-прежнему могли продолжать совершать операции со счетом в отделениях банка.

По словам представителей «Альфа-банка», обычно замена пластиковой карты клиента занимает срок от 2 до 5 дней, однако в данном случае из-за очень большого числа пострадавших сроки замены несколько увеличились.

Эксперты отмечают, что данная утечка стала первым инцидентом такого рода в России, хотя в мире подобные взломы происходили неоднократно. В частности, в Германии в 2009 году банки были вынуждены провести замены сразу более 100 тыс. пластиковых банковских карт Visa и MasterCard в результате утечки данных кредиток немецких туристов в Испании. Пострадали все банки Германии, среди которых Raiffeisenbank и Volksbank, а также австрийские, шведские и финские банки.

После вышеупомянутой утечки под угрозой компрометации оказались и личные данные клиентов ряда российских банков — в группе риска были более 2,5 тыс. российских туристов, пользовавшихся кредитными картами в гостиницах Германии, Австрии, Бельгии и Швейцарии. Тогда банки не стали раскрывать причины замены карт, объяснив лишь, что это связано с безопасностью счетов.

«Альфа-банк» первым открыто заявил о массовой утечке и своих действиях, направленных на устранение последствий данного инцидента. Представители банка пока не сообщали новых сведений о результатах расследования.

Другие

В декабре произошла утечка, в результате которой в Сеть попали фрагменты записи новогоднего концерта на телеканале «Культура». Фрагменты записи были опубликованы в социальных сетях, блогах и на некоторых других сайтах. По факту утечки было начато служебное расследование.

Департамент труда и занятости населения города Москвы в ноябре 2010 года опубликовал в открытом доступе на своем сайте данные о заработной плате за 2010–2011 гг. более чем 47 тыс. легальных мигрантов, работающих в Москве. При этом люди, данные которых фигурируют в опубликованном архиве, не были оповещены о планах ведомства.

В результате утечки внутренних документов сервиса ICQ в декабре 2010 года стало известно о том, что за год число подключений к ICQ упало почти на треть (согласно внутренней статистике компании), а также о планах по перевозу серверов этой службы мгновенных сообщений в Москву.

В феврале Роскомнадзор сообщил о том, что сотрудники инспекции ФНС в Пензе допустили нарушения правил обработки персональных данных налогоплательщиков. Они рассылали по почтовым ящикам незапечатанные в конверты налоговые извещения. По выявленным фактам нарушений было направлено заявление в прокуратуру.

Прогнозы

Законодательные требования, внимание со стороны СМИ, экономическая ситуация, действия конкурентов, отношение общественности будут оказывать все большее давление на менеджмент организаций в теме защиты от утечек информации. Основной движущей силой снижения числа утечек в ближайшее время, как и раньше, могут стать нормативно-правовые акты, необходимость разработки, принятия и исполнения которых назревает уже как минимум несколько лет. Главная проблема существующего законодательства почти во всех странах — практически полное отсутствие ответственности организаций за сам факт утечки, если ими соблюдаются все формальные требования по защите данных. На практике отсутствие ответственности не создает никаких предпосылок и стимулов для развития системы безопасности и защиты от новых угроз.

Внимание со стороны СМИ и общественности оказывает давление на менеджмент организаций, который все больше задумывается о необходимости защиты от утечек. Немалую роль в привлечении внимания к проблеме сыграл интернет-ресурс WikiLeaks, хотя, конечно, еще нельзя говорить о каких-то коренных изменениях в сознании руководства большинства компаний. По прогнозам SECURIT Analytics, в ближайшие годы важную роль в вопросе защиты от утечек должен сыграть рынок. Система безопасности будет рассматриваться как весомое конкурентное преимущество, ведь клиенты, бизнес-партнеры, поставщики и работники просто не захотят иметь дело с организациями, которые могут в любой момент допустить утечку их персональных данных или другой конфиденциальной информации.

При этом не стоит забывать и о сдерживающих факторах, основным из которых является сопротивление изменениям в организации. Этой проблеме посвящено множество научных трудов и публикаций, где были определены причины такой поведенческой стратегии. В большинстве случаев ни рядовые сотрудники, ни топ-менеджмент не видят явной выгоды от принятия специальных мер внутреннего контроля и опасаются, что изменения могут навредить им лично или просто поменять привычный уклад работы, например, вынудить существенно уменьшить объем личной переписки через корпоративные каналы коммуникаций. Не стоит забывать и о финансовой составляющей, ведь посчитать эффективность инвестиций в специализированные решения довольно трудно, что добавляет сложности при обосновании бюджетов в средних и крупных организациях.

Количество обнародованных утечек напрямую зависит от приведенных выше факторов и, по прогнозам SECURIT Analytics, в ближайший год вырастет на 20–30%. Такой прогноз обусловлен динамикой последних лет, когда количество утечек постоянно росло, и высоким вниманием к проблеме со стороны СМИ, субъектов персональных данных, отраслевых аналитиков, конкурирующих организаций, которые играют все большую роль в снижении количества незамеченных утечек.

DLP-решения для защиты данных

DLP (Data Loss Prevention) — основное обозначение ИТ-решений, помогающих организациям минимизировать риски утечки конфиденциальных данных. DLP-системы перехватывают и анализируют основные информационные потоки (каналы утечек) данных, которые пересекают периметр защищаемой информационной сети. При обнаружении запрещенной к пересылке или просто подозрительной информации DLP может заблокировать данные или просто уведомить администратора безопасности. В большинстве DLP также существует возможность архивирования всей перехваченной информации, что в будущем существенно облегчает расследование инцидентов информационной безопасности.

Zgate

Zgate является сетевым DLP-решением и минимизирует риски утечек информации через корпоративную электронную почту, интернет-пейджеры, веб-почту, социальные сети, блоги, форумы, файлообменные сети, торренты и другие потенциально опасные каналы коммуникаций. Zgate анализирует все данные, передаваемые сотрудниками за пределы локальной сети организации, и блокирует передачу запрещенной или подозрительной информации. В Zgate используются современные технологии, которые безошибочно определяют уровень конфиденциальности передаваемой информации и категорию документов с учетом особенностей бизнеса, требований отраслевых стандартов и законодательства России, в том числе закона 152-ФЗ «О персональных данных». Подробная информация.

Zlock

Zlock является DLP-решением для защиты конечных точек сети и минимизирует риски утечек информации, связанных с использованием ноутбуков, мобильных телефонов, USB-накопителей, фото- и видеокамер, Wi-Fi- и Bluetooth-устройств, локальных и сетевых принтеров. Zlock работает по сходным с Zgate принципам и блокирует запись и печать конфиденциальной или подозрительной информации. Подробная информация.

Zserver Suite

Zserver Suite является DLP-решением для защиты данных, которые хранятся на серверах, магнитных лентах, оптических дисках, в системах хранения и на любых внешних площадках. Zserver Suite защищает данные в процессе использования, хранения, транспортировки и даже в случае попадания физических носителей в руки злоумышленников. Надежность защиты обеспечивают специализированные алгоритмы шифрования с длиной ключа до 512 бит. Подробная информация.

О компании SECURIT

Компания SECURIT — ведущий разработчик систем для защиты информации от внутренних угроз. SECURIT основана в 2001 году и является инновационной компанией и первым российским разработчиком гибридных DLP-систем. Продукты компании позволяют минимизировать риски умышленной и случайной утечек корпоративной информации и персональных данных.

Линейка продуктов компании SECURIT включает в себя полный спектр средств защиты информации от инсайдеров. Продукты SECURIT контролируют все потенциальные каналы утечки, ведут архив действий сотрудников, защищают данные в процессе использования и хранения, а также управляют доступом пользователей к корпоративной сети, приложениям и конфиденциальной информации. Использование DLP-решений компании обеспечит защиту информации от утечек на протяжении всего ее жизненного цикла — от создания до записи в архив или удаления.

SECURIT с 2001 года является лидером в области шифрования данных при хранении, а с 2006 года — в области разработки DLP-систем. Благодаря инновационным подходам и ориентированности решений на требования бизнеса комплексные системы SECURIT на текущий момент защищают данные в более чем 8 тыс. организаций. Компанию SECURIT поддерживают более 50 бизнес-партнеров из различных регионов Российской Федерации и СНГ, стран Азии и Тихоокеанского региона, Европы и США.

Контактная информация

Александр Ковалев
Директор по маркетингу SECURIT
market@securit.ru, kovalev@securit.ru

109316, Российская Федерация, Москва
Волгоградский просп., дом 42 корпус 8

Телефон +7 495 221-21-60
Факс +7 495 221-21-60

www.securit.ru