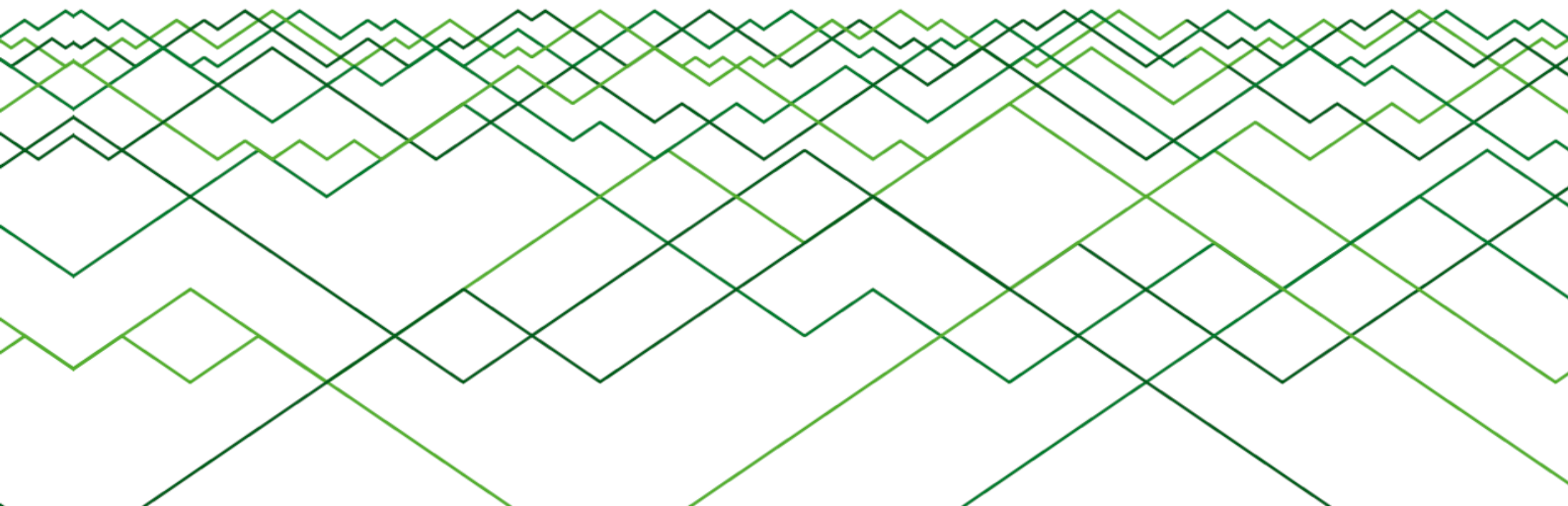
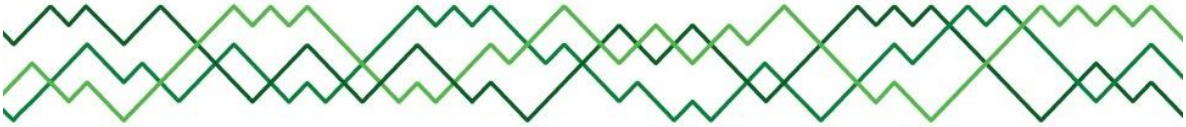
INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

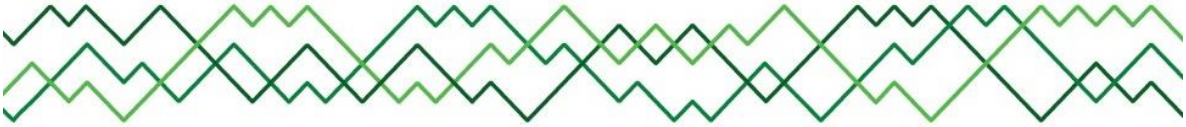
Аналитический центр InfoWatch
www.infowatch.ru/analytics

Утечки данных организаций в результате умышленных или неосторожных действий внутреннего нарушителя. Сравнительное исследование. 2013-2015 гг.





Оглавление



INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

Аннотация

Аналитический центр группы компаний InfoWatch представляет первое сравнительное исследование утечек информации ограниченного доступа, произошедших в период с 2013 по 2015 год в результате умышленных или неосторожных действий сотрудников коммерческих и некоммерческих организаций, органов государственной власти и местного самоуправления.

До 2013 года предметом наших исследований были утечки данных, произошедшие по вине или неосторожности сотрудников — «внутренние» утечки. Считалось само собою разумеющимся, что «внешние» утечки менее интересны, чем «внутренние». Конечно, хакеры и в то время взламывали системы защиты, проникали в коммуникационные сети. Однако тогда возможности хакеров по распоряжению похищенными данными были существенно ограничены. За исключением нескольких типов информации, таких как реквизиты банковских счетов и пластиковых карт, данные в цифровом виде не пользовались широким спросом.

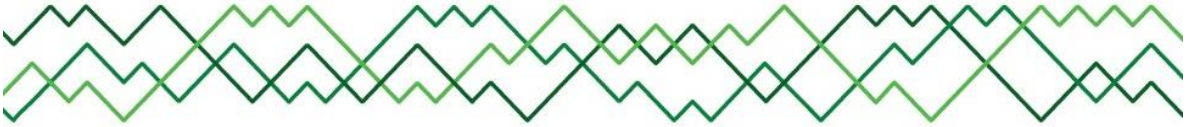
Все изменилось в тот момент, когда для идентификации личности при проведении некоторых операций, например, при подаче документов на налоговый вычет в США, отпала необходимость в использовании документов на бумажных носителях. Персональные данные превратились в чрезвычайно ценный товар, родился новый вид преступлений, получивший название «кража личности».

Сегодня массовый взлом компаний, обрабатывающих персональные данные граждан, приносит злоумышленникам ощутимую финансовую выгоду. Появилось много желающих эти данные приобрести с тем, чтобы на них «заработать». В результате количество скомпрометированных данных (записей ПДн) сравнялось с числом жителей планеты.

Тема внешних атак и утечек информации ограниченного доступа вошла в повестку и во многом предопределила итоги президентской избирательной кампании в США – уровень, немыслимый еще четыре года назад.

А что же «внутренние» утечки? Как изменилась картина нарушений применительно к этому типу инцидентов? Насколько сегодня актуальна проблема защиты от «внутренних» утечек на фоне массовых внешних атак?

В рамках данного исследования мы попытались ответить на эти вопросы, сформировать современную общую картину происшествий, связанных с внутренними» утечками, обозначить тенденции и векторы возможного развития таких угроз. Авторы уверены, что выводы исследования будут интересны практикующим специалистам в области информационной и экономической безопасности организаций, журналистам, собственникам бизнеса и высшему руководству компаний, оперирующих информацией ограниченного доступа, включая коммерческую, банковскую, налоговую тайны, а также другими ценными информационными активами.



Методология

Исследование проводится на основе собственной базы данных, пополняемой специалистами Аналитического центра InfoWatch с 2004 года. В базу попадают публичные сообщения[1] о случаях утечки[2] информации из коммерческих и некоммерческих (государственных, муниципальных) организаций, которые произошли вследствие умышленных или неосторожных действий[3] сотрудников и иных лиц[4]. База утечек InfoWatch насчитывает несколько тысяч зарегистрированных инцидентов.

В ходе наполнения базы с учетом доступности информации в открытых источниках каждая утечка классифицируется по ряду критериев, таких как размер организации[5], сфера деятельности (отрасль), размер причинённого ущерба[6], тип утечки (по умыслу), канал утечки[7], типы утекших данных.

Утечки данных, произошедшие вследствие внешнего воздействия, например, таргетированной атаки, «фишинга», взлома веб-ресурса, долгое время оставались вне поля нашего внимания. С 2014 года такие утечки также добавляются в базу наряду с утечками данных, которые связаны с действиями внутренних нарушителей. К списку критериев, по которым оцениваются утечки, добавлен вектор воздействия[8]. Утечки, зафиксированные ранее 2014 года, по умолчанию отнесены к «внутренним» - связанным с действиями внутренних нарушителей. Этим, в частности, объясняется ограничение горизонта настоящего исследования данными за три года: с 2013 года по 2015 год.

С 2014 года инциденты классифицируются по характеру действий нарушителя. Наряду с «простыми» утечками авторы исследования выделяют следующие типы «квалифицированных» утечек:

- когда сотрудник, имеющий легитимный доступ к данным, использует данные в целях мошенничества (манипуляции с платежными данными, инсайдерской информацией);
- когда сотрудник получает доступ к данным, которые не нужны ему для исполнения служебных обязанностей (превышение прав доступа).

---

[1] Сообщения об утечках данных, опубликованные официальными ведомствами, СМИ, авторами записей в блогах, интернет-форумах, иных открытых источниках.

[2] Утечка информации (данных) – утрата контроля над информацией (данными) в результате внешнего воздействия (атаки) а также действий лица, имеющего легитимный доступ к информации или действий лица, получившего неправомерный доступ к такой информации.

[3] Утечки данных разделяются на умышленные (злонамеренные) и неумышленные (случайные) в зависимости от наличия вины в действиях лица, которые привели к утечке данных. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.

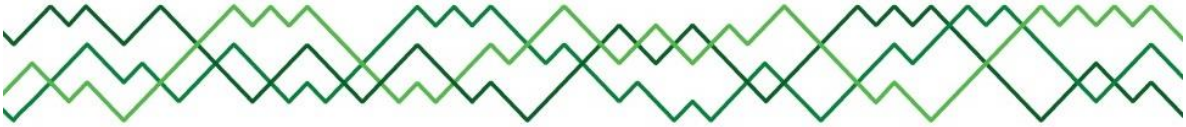
[4] Авторы классифицируют утечки по виновнику (источнику) инцидента. Наряду с внутренними нарушителями, в данную классификацию попадает внешний нарушитель.

[5] Аналитики центра InfoWatch классифицируют организации по размеру в зависимости от известного либо предполагаемого парка персональных компьютеров (ПК). Небольшие компании – до 50 ПК, средние - от 50 до 500 ПК, крупные – свыше 500 ПК.

[6] Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ.

[7] Под каналом утечки мы понимаем такой сценарий (совокупность действий пользователя корпоративной информационной системы, направленных на оборудование или программные сервисы), в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. Каналы утечек определяются только для таких утечек, которые спровоцированы действиями внутреннего нарушителя.

[8] Вектор воздействия – признак действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников, направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников, атакующих системы защиты изнутри (нелегитимный доступ к ресурсам, неправомерные действия с инсайдерской информацией и проч.).



По оценке авторов, ежегодно предметом исследования становятся не более 1% случаев предполагаемого совокупного количества утечек из-за чрезвычайно высокого уровня латентности инцидентов, связанных с компрометацией информации. Однако критерии категоризации утечек подобраны так, чтобы исследуемые множества - категории - содержали достаточное или избыточное количество элементов - фактических случаев утечки. Такой подход к формированию поля исследования позволяет считать полученную выборку теоретической, а выводы исследования и выявленные с учетом данной выборки тренды - репрезентативными для генеральной совокупности.

При формировании диаграмм по разрезам из выборки исключены утечки, классифицированные по основному критерию разреза как неопределенные. Например, разрез по вектору воздействия, куда входят утечки под воздействием внешних атак и внутреннего нарушителя, не содержит утечек, для которых вектор не удалось определить. То же справедливо для распределений по виновнику, умыслу и другим критериям.

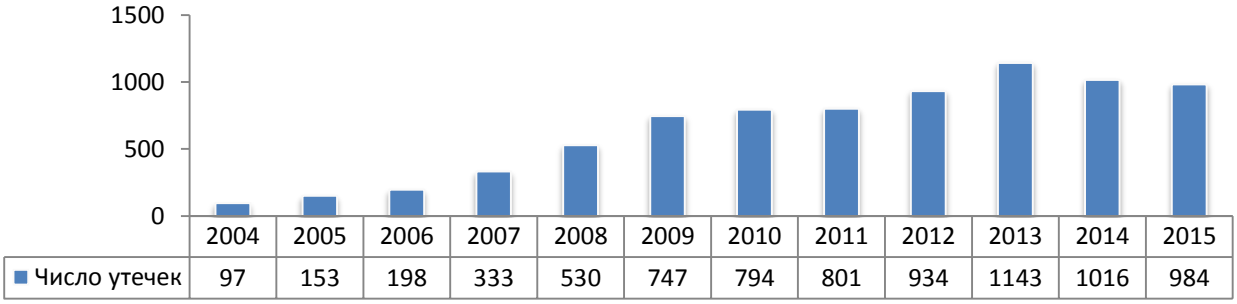
Случаи нарушения конфиденциальности информации и иные инциденты информационной безопасности (ИБ), напримерDDoS-атаки, не повлекшие утечек данных, а также утечки с неясным источником данных, когда неизвестно, какой организации принадлежали скомпрометированные данные, не включаются в выборку.

Авторы настоящего исследования не ставили перед собой задач определить точное количество произошедших утечек, оценить причинённый ими реальный или возможный ущерб организациям. Исследование направлено на выявление динамики процессов, характеризующих глобальную, отраслевую, региональную картину происшествий, связанных с утечками данных.

Результаты исследования

Анализ данных об утечках информации в результате действий внутреннего нарушителя («внутренних» утечек)[9] в 2013-2015 годах позволяет выделить несколько закономерностей.

Во-первых, число «внутренних» утечек впервые с 2004 года снижается: на 3% в 2015 году по отношению к данным за 2014 год и на 13% по отношению к данным за 2013 год. Если в 2014 году падение числа «внутренних» утечек по отношению к 2013 году можно было объяснить изменением методологии исследования[10], то в 2015 году это объяснение не выдерживает критики, так как методология не менялась.



	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Число утечек	97	153	198	333	530	747	794	801	934	1143	1016	984

Рисунок 1. Число «внутренних» утечек информации, 2004 -2015 гг.

Примечательно, что снижается не только количественный показатель числа «внутренних» утечек , но и доля утечек этого типа в распределении по «вектору воздействия»[11]. В 2015 году на внутренние утечки пришлось 65% всех утечек данных, хотя еще годом ранее доля внутренних утечек составляла 73%.

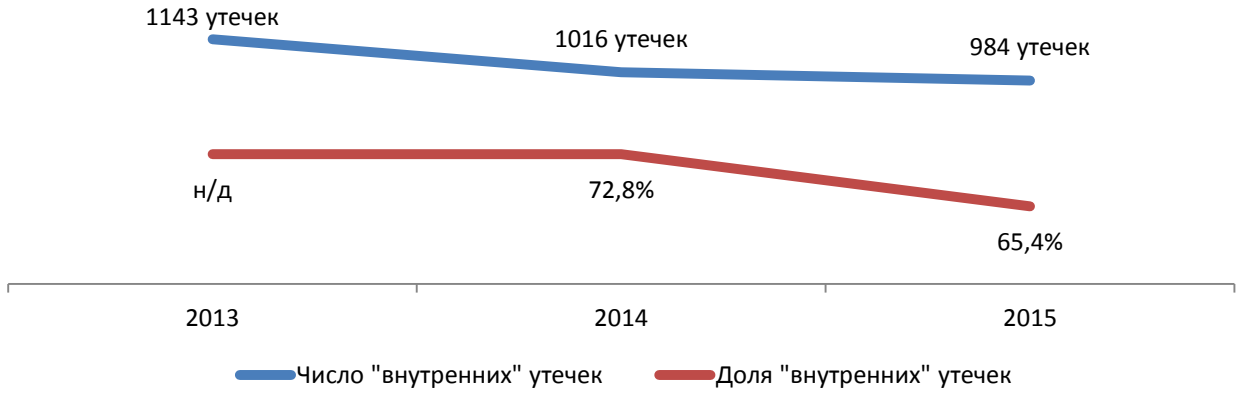


Рисунок 2. Число «внутренних» утечек информации и доля утечек этого типа, 2013 - 2015 гг.

[9] «Внутренние» утечки – утечки данных, случившиеся в результате умышленных или неосторожных действий сотрудников, имеющих легитимный доступ к информации ограниченного доступа или осуществляющих доступ к данным неправомерно.
[10] До 2014 года методология исследования не предусматривала распределение утечек на «внешние» и «внутренние».
[11] Вектор воздействия – признак действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников, направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников, атакующих системы защиты изнутри (нелегитимный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.).

Во-вторых, уменьшается объем записей ПДн и финансовой информации, скомпрометированных в результате «внутренних» утечек — 352,7 млн и 335,3 млн в 2014 и 2015 годах соответственно. Объем данных, скомпрометированных в результате одной «внутренней» утечки, составил 347 тыс. записей в 2014 году и 340 тыс. записей в 2015-м году.

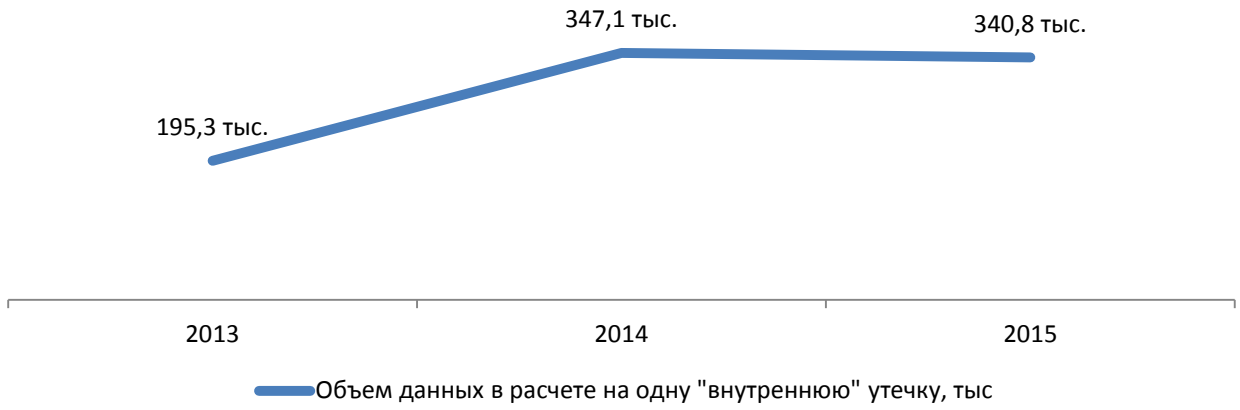


Рисунок 3. Объем данных в расчете на одну «внутреннюю» утечку, 2013 - 2015 гг.

Для сравнения, в 2015 году объем скомпрометированных данных в расчете на одну утечку превысил 640 тыс. записей.

Представленные цифры позволяют предполагать, что «внутренние» утечки потеряли в «мощности», стали менее «разрушительными». Однако интуиция и практика исследования отдельных видов утечек не позволяют сделать столь однозначный вывод. Попробуем выяснить, что же нам мешает считать «внутренние» утечки неизбежным, но небольшим злом.

«Внутренние» утечки «уходят» в сеть

С 2013 года доля «внутренних» утечек, которые произошли из-за случайных ошибок сотрудников, выросла на 34 процентных пункта (п. п.). Доля злонамеренных «внутренних» утечек, соответственно, сократилась.

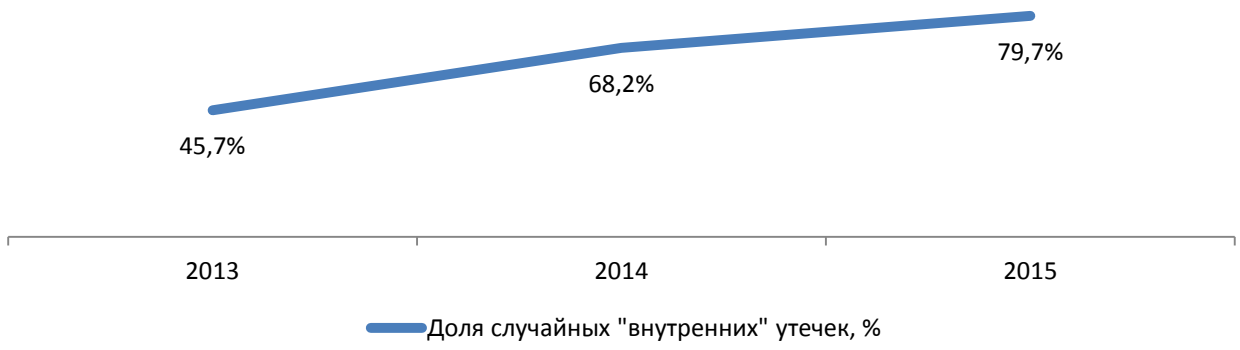


Рисунок 4. Доля случайных «внутренних» утечек, 2013 - 2015 гг.

Применительно к распределению случайных «внутренних» утечек по каналам передачи информации динамика изменений выглядит следующим образом (см. Рисунок 5).

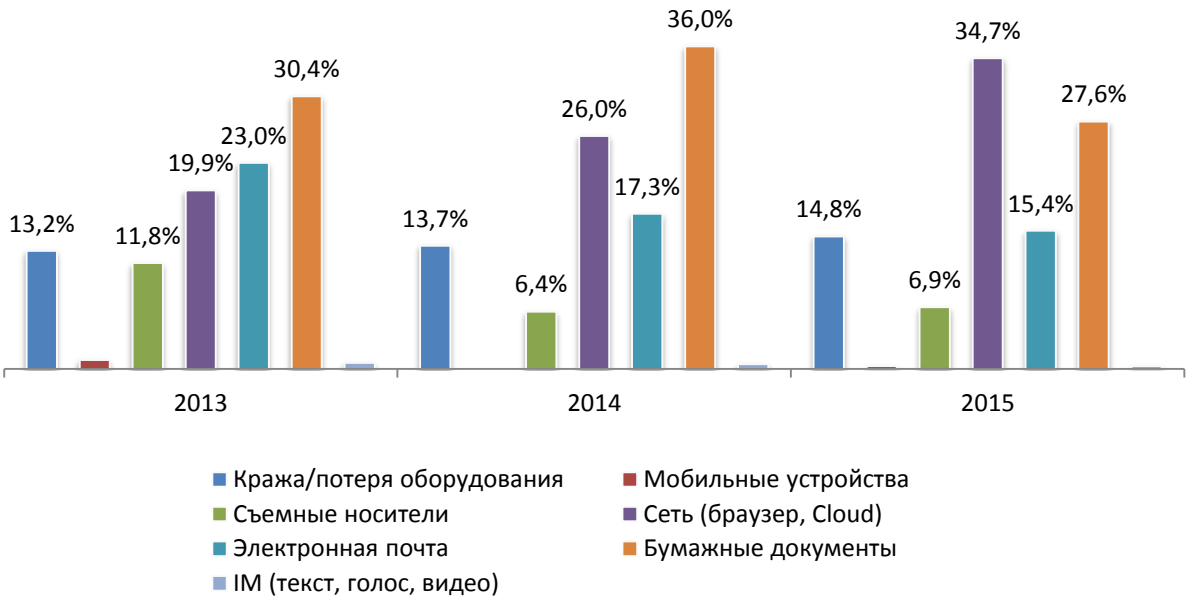


Рисунок 5. Распределение случайных «внутренних» утечек по каналам передачи информации, 2013 – 2015 гг.

Наблюдается снижение доли случайных утечек через электронную почту, бумажные и съемные носители при возрастании доли таких утечек через сетевой канал.

Распределение случайных «внутренних» утечек по каналам передачи информации подтверждает, в общем-то, понятную на уровне житейского опыта мысль – массовые ошибки при работе с информацией ограниченного доступа, ведущие к компрометации данных, связаны с наиболее «популярными», распространенными каналами. А наиболее распространенным, часто используемым каналом передачи информации в настоящее время является сетевой канал.

> securitylab.ru: *Полтора миллиона американцев стали жертвами утечки персональной информации. Полные имена, адреса, номера телефонов, данные о состоянии здоровья и прописанных медикаментах по ошибке были опубликованы в открытом виде в облачном сервисе Amazon компаниями, занимающимися медицинским страхованием и использующими программное обеспечение Systema Software. Инцидент затронул Фонд самострахования Канзаса, страховую компанию CSAC Excess Insurance Authority и базу данных округа Солт-Лейк в штате Юта. В общей сложности были опубликованы номера социального страхования 1 млн пользователей, 5 млн записей о финансовых транзакциях.*

До недавнего времени считалось, что компрометация больших объемов данных от миллиона записей и выше, если и происходит с использованием сетевого канала, то исключительно под воздействием внешнего злоумышленника. Многомиллионных

«внутренних» утечек, произошедших по неосторожности сотрудников компании, мы не фиксировали.

Теперь все иначе (см. Рисунок 6). В 2015 году в результате «внутренних» случайных утечек по сетевому каналу были скомпрометированы 295 млн записей, относящихся к категориям персональных данных и финансовой информации.

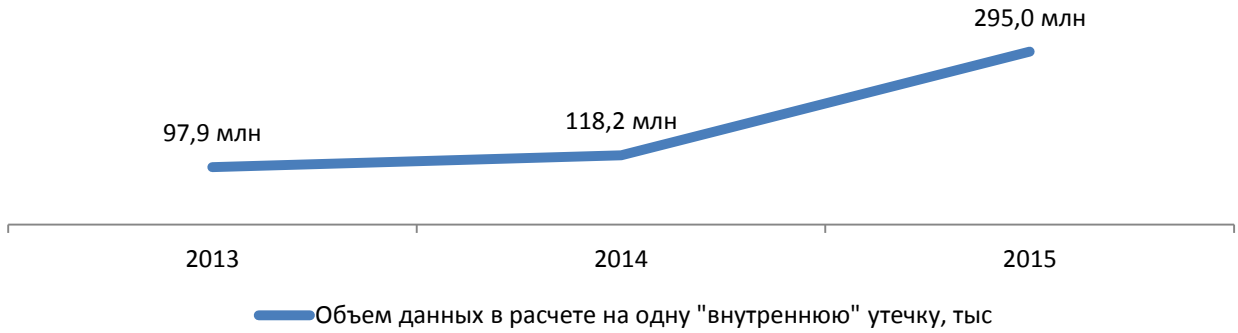


Рисунок 6. Объем записей ПДн и финансовой информации, скомпрометированных в результате «внешних» случайных утечек по сетевому каналу, 2013 - 2015 гг.

Стремительный перевод всей значимой информации в цифровой вид неизбежно приводит к росту утечек в результате ошибок персонала, обрабатывающего такую информацию, а также сбоев в автоматизированных системах.

> *eastbaytimes.com: Суд обязал компанию Comcast (американский оператор кабельного телевидения) выплатить 33 млн долл. США за разглашение персональных данных 75 тыс. непубличных клиентов. Данные оказались в глобальной сети из-за ошибки сотрудника оператора.*

Уровень ущерба вследствие случайной компрометации большого объема данных сопоставим с ущербом от злонамеренной атаки извне. Причем ущерб не ограничивается репутационными потерями. Все чаще случайные утечки приводят к коллективным искам и, как следствие, к прямым расходам в виде возмещения ущерба пострадавшим владельцам персональных данных и финансовой информации.

> ***Вывод***
>
> *Число утечек данных под воздействием внутреннего нарушителя снижается. Однако при этом наблюдается рост объема данных, скомпрометированных в результате «внутренних» случайных утечек. «Внутренние» утечки 2015 года в большинстве случаев связаны с неумышленной компрометацией данных через сетевой канал. Такие утечки отличает большая «разрушительность» - объем данных, скомпрометированных в результате случайной утечки, может достигать нескольких миллионов записей ПДн или финансовой информации.*

Критически важная информация все чаще утекает в результате ошибок внутреннего нарушителя

Распределение «внутренних» утечек по типу скомпрометированной информации за 2013 по 2015 год отражает рост доли утечек платежной информации, коммерческой тайны с одновременным снижением доли утечек персональных данных. Эти три типа информации можно назвать наиболее чувствительными для любой коммерческой компании.

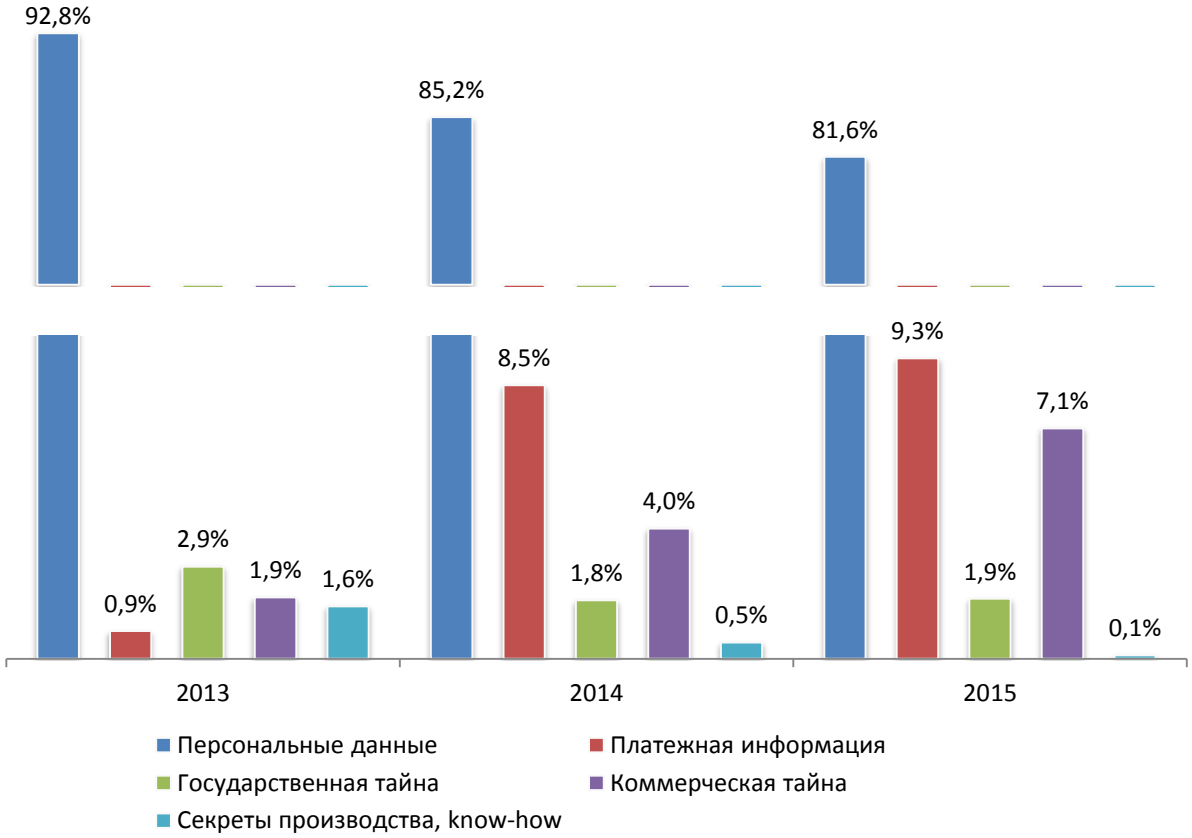


Рисунок 7. Распределение «внутренних» утечек по типу данных, 2013 – 2015 гг.

Как уже отмечалось, и персональные данные, и коммерческая тайна, и платежная информация все чаще «уходят» из компаний не в результате злонамеренных действий, а по ошибке сотрудников.

> bangordailynews.com: *Один из служащих кредитного рейтингового агентства Equifax по ошибке отправил несколько сотен кредитных историй клиентов жительнице штата Мэн. За день до этого она запросила данные о своей кредитной истории. В качестве ответа на ее почту пришло 300 писем с финансовыми данными посторонних людей. В результате утечки оказались скомпрометированы имена, даты рождения, номера социального страхования, номера банковских счетов иная чувствительная информация жителей Флориды, Нью-Джерси, Коннектикута, других штатов.*

С 2013 года по 2015 год года изменилось распределение утечек данных по типу скомпрометированной информации и умыслу (см. Рисунок 8). Если в 2013 году основная масса скомпрометированных чувствительных данных приходилась на умышленные утечки, то в 2015 году акцент сместился – теперь большая часть утечек чувствительной информации связана со случайными утечками.

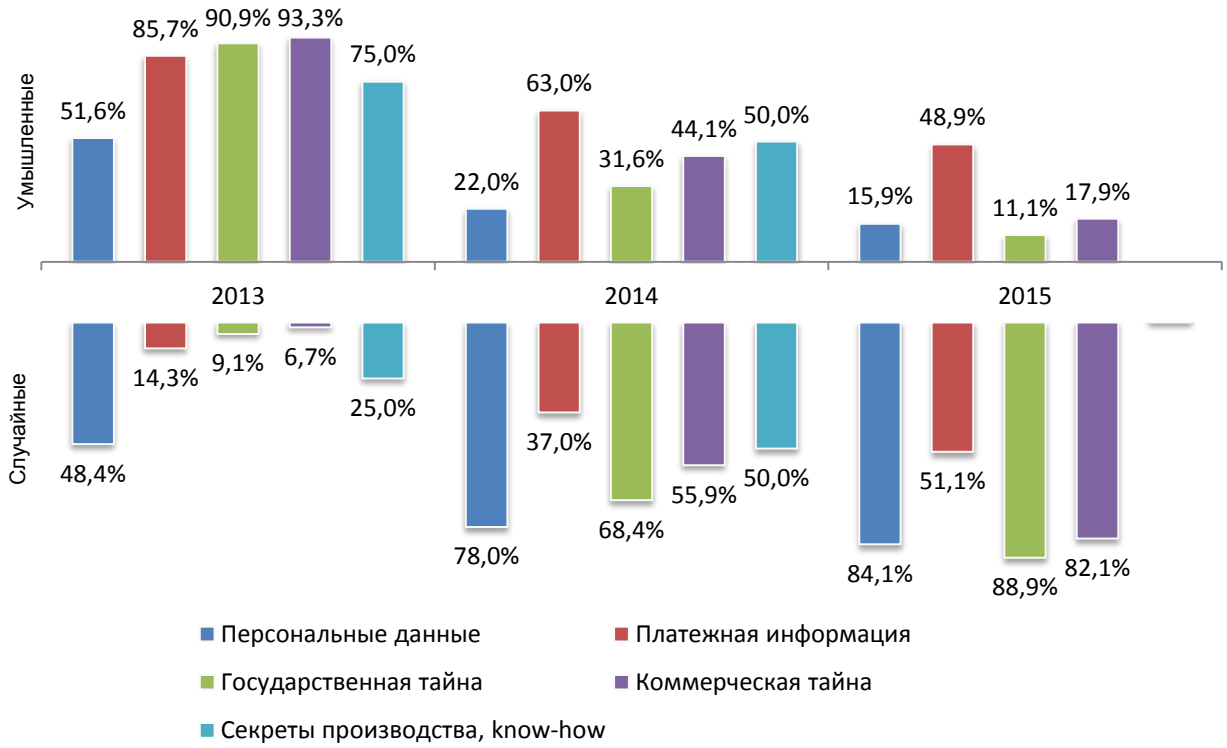


Рисунок 8. Распределение «внутренних» утечек по умыслу и типу данных, 2013 – 2015 гг.

Исключение составляет платежная информация. В 2015 году утечки данных этого типа в распределении по умыслу составили примерно равные доли.

Вывод:

Описать типичную «внутреннюю» утечку данных в 2015 году можно следующим образом: это ошибка легитимного пользователя или сбой автоматизированных систем обработки информации, результатом чего стала компрометация огромного объема данных. Случайная утечка – это прямая угроза бизнесу, поскольку утекает, как привило, критически важная информация: персональные данные, платежная информация, иные виды информации ограниченного доступа. Поэтому компания, обрабатывающая такие данные, то есть, по сути - любая компания, должна всерьез задуматься о распределении усилий между обеспечением защиты от внешних атак и от внутренних угроз. Фактически речь должна идти об ужесточении автоматизированного контроля действий сотрудников.

Количество утечек по вине привилегированных пользователей снижается

В 2013-2015 годах в распределении по умыслу произошло перераспределение долей злонамеренных и случайных утечек. На фоне падения доли злонамеренных (умышленных) утечек наблюдается еще более сильное падение доли объема данных, скомпрометированных в результате «внутренних» умышленных утечек.

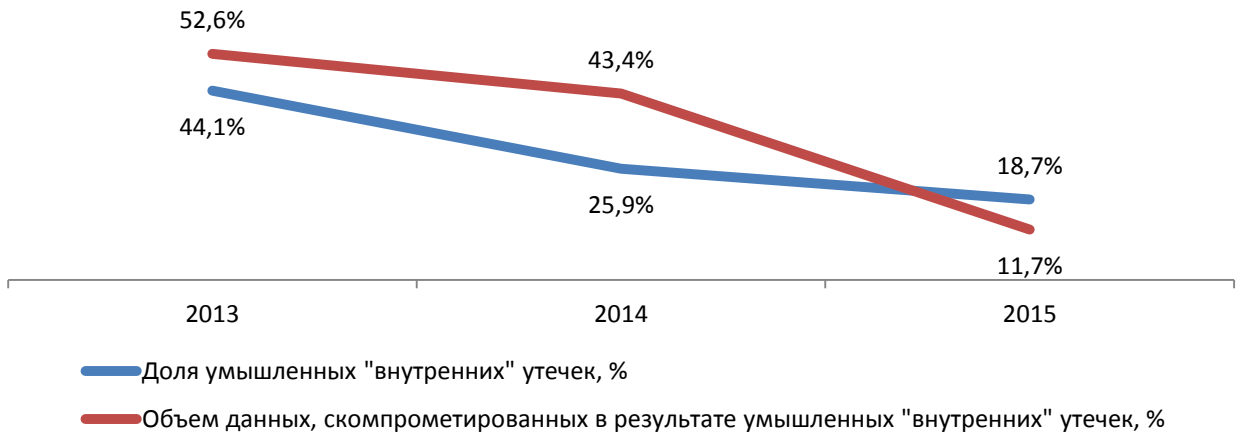


Рисунок 9. «Внутренние» умышленные утечки, число, объем скомпрометированных данных, 2013 - 2015 гг.

Столь серьезное изменение картины распределения утечек по умыслу вызвано несколькими причинами. Во-первых, это общий тренд на повсеместную цифровизацию — перевод внешнего и внутреннего (внутрикорпоративного) взаимодействия в цифровой вид. Как результат — рост объема и типов данных, которые обрабатывают компании в процессе своей деятельности. Увеличиваются и число случайных утечек, и объем данных, скомпрометированных в результате сбоев в работе персонала и информационных систем. Причем случайные утечки приводят к компрометации б**о**льшего объема данных, чем умышленные.

Во-вторых, одной из традиционных характеристик для умышленных утечек является их высокая латентность. Умышленные утечки обнаружить и предотвратить гораздо сложнее, чем случайные. Сообщения об умышленных утечках реже оказываются в центре внимания СМИ. Даже при наличии законодательно установленной обязанности сообщать о фактах утечки данных, не каждая компания готова признать умышленную утечку.

> avufa.ru: *Представители американского банка Morgan Stanley подтвердили информацию, что один из сотрудников выкрал информацию о 350 тысячах клиентов. В банке решили не разглашать имя преступника, сказав, что он передан в руки правосудия. Сообщения об утечке повлияли на стоимость акций Morgan Stanley. Теперь одна акция банка держится на уровне 37,39 долларов, что говорит о снижении цены на 3,4%.*

Латентность случайных утечек ниже, чем умышленных. Поэтому именно случайные утечки постепенно выходят на первый план.

Но есть и другая версия, на наш взгляд, более соответствующая действительности. Не секрет, что многие компании активно используют средства защиты данных для своевременного обнаружения подозрительной активности сотрудников. Также не секрет, что сведения о наличии такой системы в компании быстро распространяются в коллективе. Принципы и особенности работы систем защиты не являются тайной. В итоге «грамотные» сотрудники, решившие украсть информацию у своего работодателя, просто не используют контролируемые каналы.

Снижение доли «внутренних» умышленных утечек, таким образом, частично объясняется растущей «компьютерной грамотностью» внутреннего нарушителя.

Косвенным подтверждением такого объяснения может служить приведенное выше распределение утечек по каналам (см. Рисунок 5), где прослеживается падение доли утечек с помощью электронной почты и съемных носителей. Зная о том, что эти каналы контролируются, «грамотные» нарушители не используют их.

Распределение «внутренних» умышленных утечек по виновнику свидетельствует о снижении доли утечек по вине «привилегированных» пользователей (см. Рисунок 10).

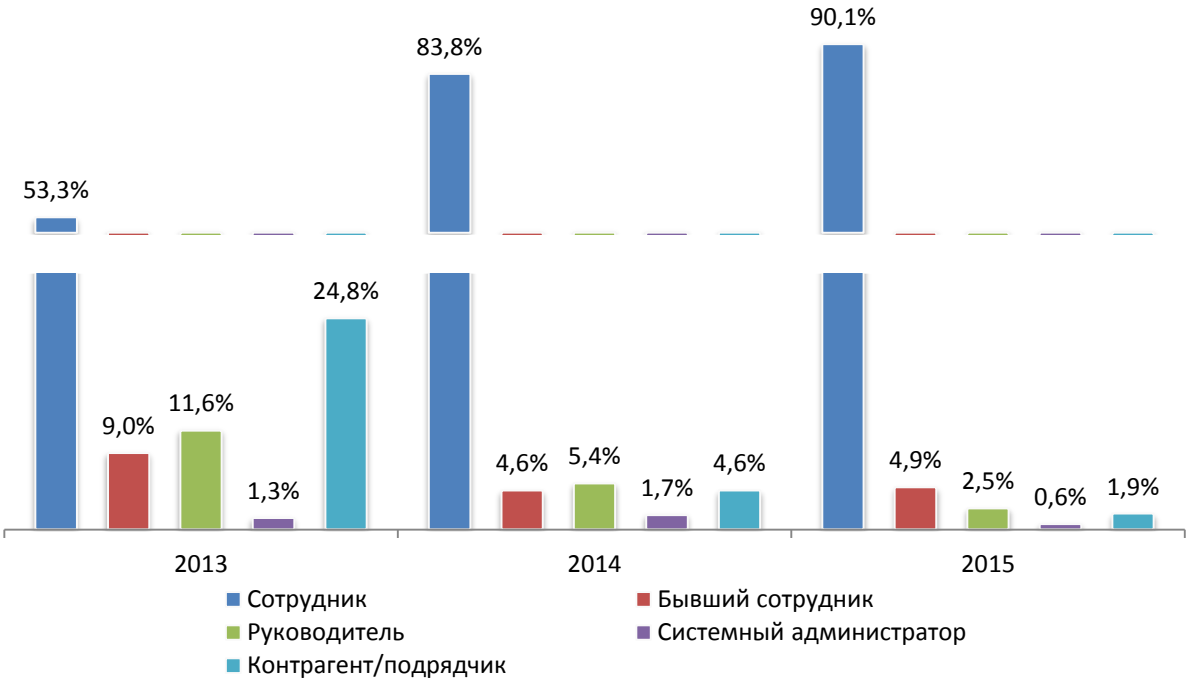
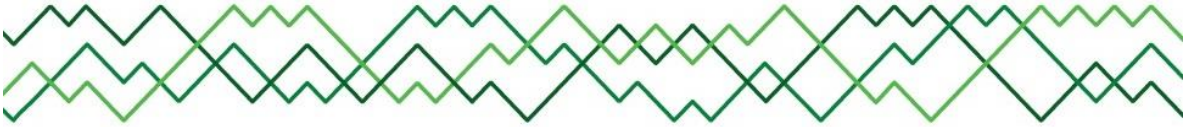


Рисунок 10. «Внутренние» умышленные утечки, распределение по виновнику, 2013 – 2015 гг.

Очевидное объяснение — привилегированные сотрудники стали меньше воровать. Но масштаб отдельных случаев воровства меньше не стал.

> *ruskorinfo.ru: Руководитель и несколько высокопоставленных сотрудников корейской компании Homeplus (подразделение британской Tesco PLC) обвиняются в сборе и продаже персональных данных 24 млн клиентов компании. По данным следствия, фигурантам удалось продать собранную*



информацию страховым компаниям. Объем выручки от незаконной сделки составил 21,14 млн долл. США.

Сообщения СМИ полны историй о нелегитимных действиях высших руководителей, причем не только в коммерческом секторе, но и в сфере государственного управления.

Центральное бюро расследований Индии: Заместитель министра и сотрудник министерства финансов Индии арестованы по подозрению в краже конфиденциальной информации. По версии следствия, чиновники передали группе лиц секретные сведения относительно инвестиционных планов иностранных корпораций в Индии. Посредником выступил консультант одной из компаний в г. Мумбаи. В ходе обысков, проведенных в Мумбаи и Дели, в офисе консультанта найдены 60 млн Шри-Ланкийских рупий наличными (около 500 тыс. долларов США). Также найдены копии конфиденциальных документов.

Напомним, что неправомерные действия привилегированных пользователей информации в среднем приводят к последствиям, гораздо более серьезным, чем действия обычных сотрудников.

Кроме того, руководство, системные администраторы по умолчанию наиболее информированные люди в вопросе использования систем защиты в компании. Напрашивается предположение, которое нельзя не привести, хотя непросто подтвердить цифрами: снижение доли привилегированных пользователей не в последнюю очередь связано с осведомленностью этой группы нарушителей о том, как работают системы защиты и задействованы ли такие системы в организации.

Не исключено, что низкая доля «привилегированных» пользователей в распределении по виновнику связана с традиционно низкой эффективностью систем защиты данных от утечек. В большинстве эти системы ориентированы на контроль каналов передачи данных, объектов защиты в большей степени, чем на контроль (анализ поведения, связей) персонала, используют технологии, позволяющие неплохо противодействовать случайным утечкам, но, зачастую, пасующие перед «продвинутым» внутренним злоумышленником.

Число «квалифицированных» утечек растет

В пользу версии о возрастающей «компьютерной грамотности» внутреннего злоумышленника и низкой эффективности систем защиты организаций от «умышленных утечек» говорит и распределение «внутренних» утечек в зависимости от сопряженности с мошенничеством или превышением прав доступа, показывающее долю так называемых «квалифицированных» утечек.

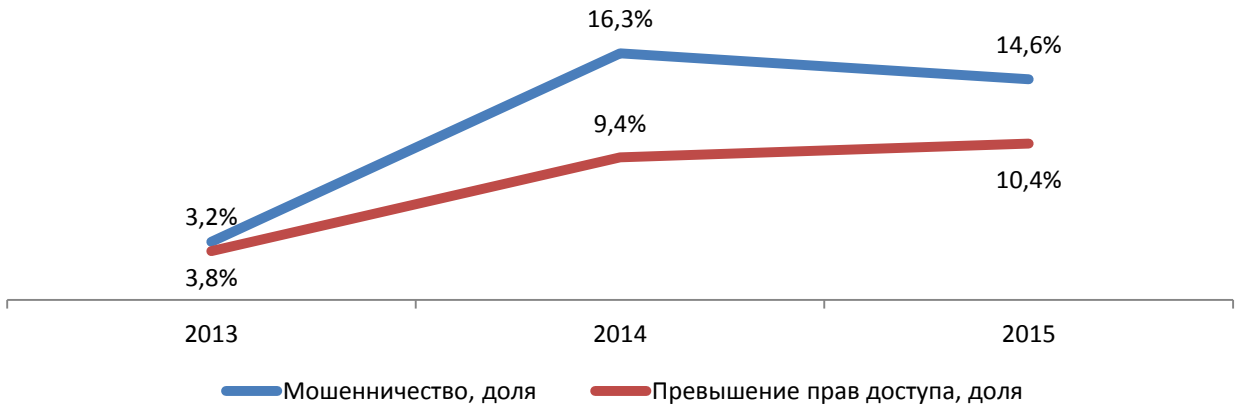


Рисунок 11. Доля «внутренних» «квалифицированных» утечек, 2013 - 2015 гг.

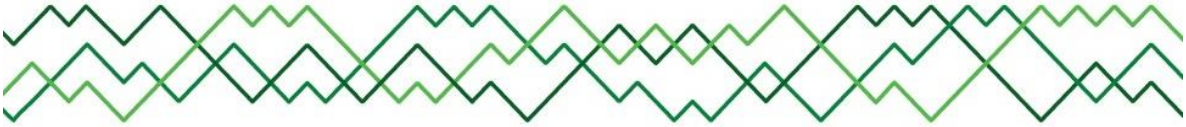
В 2015 году доля утечек данных, отягощенных последующим использованием скомпрометированной информации в целях мошенничества (как правило, банковский фрод) составила 15% (рост на 11 п. п. к данным 2013 года).

> un-sentinel.com: *24-летняя Элексис Теддис (Elexes Thaddies) пользовалась персональными данными коллег, совершая крупные покупки в магазине Nordstrom. Сумма мошенничества составила 20 тыс. долларов США. От действий мошенницы пострадали 20 человек. Многие из них работали с Элексис, некоторые знали преступницу лично. Однако это не помешало девушке открыть на имя своих коллег аккаунты в нескольких интернет-магазинах, совершить покупки и присвоить приобретенные вещи.*

10% инцидентов были классифицированы как нарушения, связанные с получением несанкционированного доступа к информации – в результате превышения прав доступа, манипуляции с информацией, которая не нужна сотруднику для исполнения служебных обязанностей. В 2015 году рост этого показателя по отношению к данным 2013 года составил 7 п. п.

> wsj.com: *Morgan Stanley уволила сотрудника за неправомерный доступ к аккаунтам 350 тыс. клиентов. Утечка данных попала в поле зрения службы безопасности финансовой компании после того, как сведения о 1200 аккаунтах оказались в сети. Разместивший эту публикацию сообщал, что у него имеется большой массив подобных данных и любой желающий может этот массив приобрести.*

Представляется, что «квалифицированные» утечки отличаются меньшей латентностью, чем «простые» умышленные утечки данных. Действия



«квалифицированного» мошенника не ограничиваются кражей данных. Эти данные еще надо использовать, что повышает риск быть обнаруженным. В случае неправомерного доступа нарушитель преодолевает системы защиты, чем также привлекает к себе внимание службы безопасности. В итоге его шансы «засветиться» повышаются.

> *nola.com: Глава программ лечения от наркозависимости в штате Луизина предстанет перед судом по обвинению в краже личности и злоупотреблении служебным положением. Шанта Барнс (Shanta Barnes) выписывал рецепты на оксикодон (опиоид, обезболивающий препарат). Однако пациенты, на чье имя выписывался препарат, его не получали. Господин Барнс продавал лекарства через систему распространителей. При этом он умудрялся получать компенсацию за выписанные и купленные препараты.*

«Квалифицированные» утечки в силу этих обстоятельств фиксируются чаще, чем «простые», доля «квалифицированных» утечек растет. Означает ли это, что в основе роста «квалифицированных» утечек лежат причины, отличные от тех, что определяют динамику роста «простых» умышленных утечек? Думается, нет.

На динамику «простых» и «квалифицированных» утечек воздействует примерно одинаковый набор факторов – ценность и ликвидность цифровых данных, низкая культура обращения с информацией ограниченного доступа, низкая эффективность корпоративных систем защиты данных применительно к умышленным утечкам, возрастающий уровень «компьютерной грамотности» внутреннего злоумышленника.

> ***Вывод:***
>
> *Опираясь на анализ сообщений об умышленных утечках и ряд вероятностных заключений, можно предположить, что именно динамика «квалифицированных» утечек лучше описывает положение дел применительно к «внутренним» умышленным утечкам в целом. Проще говоря, зафиксированное снижение количества «внутренних» умышленных утечек, доли «привилегированных» пользователей в распределении по виновнику никак не свидетельствует в пользу снижения уровня угрозы со стороны «внутренних» умышленных утечек.*

Заключение и выводы

На фоне бесконечного числа сообщений об утечках данных в результате внешних атак на информационные системы неподготовленный читатель рискует впасть в заблуждение, поддавшись «магии цифр». Действительно, многомиллионные внешние утечки, рассуждения политиков о растущей угрозе внешних атак, — все это мало способствует трезвой оценке ситуации.

Между тем «внутренние» утечки — то, с чего начинались когда-то наши исследования, — никуда не исчезли. Простые сотрудники, руководители, системные администраторы и другие привилегированные пользователи по-прежнему воруют информацию. И воруют много.

С 2013 по 2015 год число «внутренних» утечек уменьшается. Объем данных, скомпрометированных в результате «внутренних» утечек, растет не так стремительно, как в случае с «внешними» утечками. И все же авторы исследования уверены, что говорить о принципиальном снижении степени опасности «внутренних» утечек в сравнении с «внешними» преждевременно.

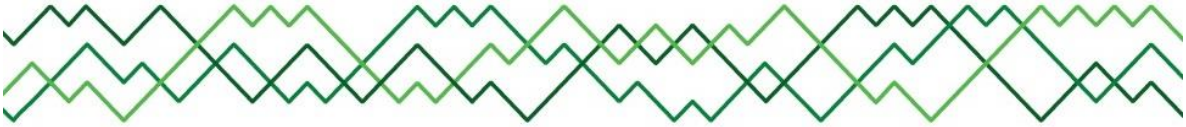
Во-первых, большая часть «внутренних» утечек пришлась на случайные утечки, которые произошли из-за ошибок персонала или сбоев информационных систем. Потенциально размер ущерба от такой утечки не ограничен. По ошибке можно скомпрометировать клиентскую базу небольшой компании или массив персональных данных всех американских избирателей – дело случая.

Во-вторых, в результате «внутренней» утечки могут быть скомпрометированы абсолютно любые данные. Даже наиболее критичные данные, такие как платежная информация и коммерческая тайна, все чаще «утекают» в результате ошибок сотрудников, и в этом есть своя логика – данных в цифровом виде стало слишком много.

Долгое время случайные утечки считались неизбежным злом. Компании исповедовали подход, согласно которому достаточно бороться с умышленной компрометацией данных путем расследования инцидентов. А в ответ на случайную отправку конфиденциальной информации достаточно проинформировать отправителя, что его действия противоречат правилам.

Сегодня такой подход не сработает. Расследования мало. Необходима блокировка даже случайной утечки, контроль сотрудников как в «зоне риска», куда относятся сотрудники с особыми правами доступа, новички или единожды «провинившиеся», так и вне ее.

В-третьих, особого внимания заслуживают «привилегированные» сотрудники. Статистически их доля снижается, но это снижение, скорее всего, не соответствует действительности. Руководители, системные администраторы и прочие «привилегированные» сотрудники, очевидно, имеют больше возможностей избежать контроля со стороны служб безопасности и систем защиты. Между тем любой «привилегированный» сотрудник по роду деятельности имеет доступ к большему объему информации, чем обычный. Эта информация, как правило, отличается высокой «чувствительностью».



Итак, у нас нет ни одного основания утверждать, что за прошедшие три года «внутренние» утечки стали менее опасны. Изменилась их природа, но это связано с увеличением объемов данных, обрабатываемых в компаниях, ростом числа каналов - способов передачи данных, а также ростом ликвидности самих данных.

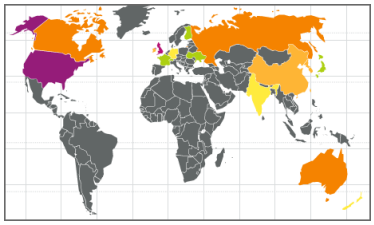
Поэтому еще раз подчеркнем — несмотря на мощный информационный фон, сопровождающий утечки данных в результате внешних атак, «внутренние» утечки были и остаются проблемой номер один для систем защиты информации, служб информационной и экономической безопасности, бизнеса в целом.

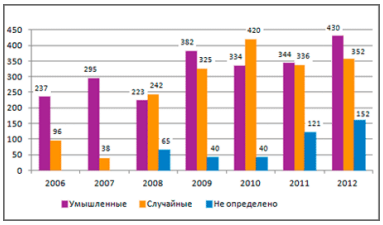
INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

Мониторинг утечек на сайте InfoWatch

На сайте Аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Кроме того на сайте представлены статистические данные по утечкам информации за прошедшие годы, оформленные в виде динамических графиков.



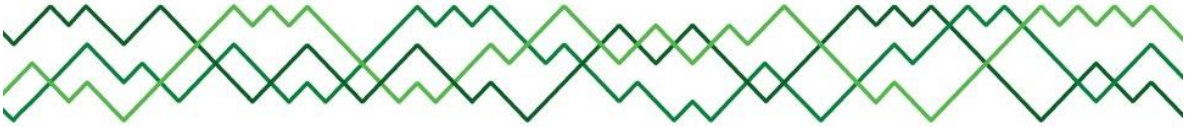


Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- Facebook
- Twitter
- RSS

Аналитический центр InfoWatch

www.infowatch.ru/analytics



INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

Глоссарий

Инциденты информационной безопасности — *в данном исследовании к этой категории авторы относят случаи компрометации информации ограниченного доступа вследствие утечек данных и/или деструктивных действий сотрудников компании.*

Утечка данных — *под утечкой мы понимаем утрату контроля над информацией (данными) в результате внешнего воздействия (атаки) а также действий лица, имеющего легитимный доступ к информации или действий лица, получившего неправомерный доступ к такой информации.*

Деструктивные действия сотрудников — *действия сотрудников, повлекшие компрометацию информации ограниченного доступа: использование информации ограниченного доступа в личных целях, сопряженное с мошенничеством; нелегитимный доступ к информации (превышение прав доступа).*

Конфиденциальная информация — *(здесь) информация, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. В данном отчете в категорию КИ мы включаем информацию, подпадающую под определение персональных данных.*

Умышленные/неумышленные утечки — *к умышленным относятся такие утечки, когда пользователь, работающий с информацией, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду. В результате создались условия для утраты контроля над информацией и/или нарушения конфиденциальности информации. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя.*

К неумышленным относятся утечки информации, когда пользователь не предполагал наступления возможных негативных последствий своих действий и не преследовал личной выгоды. При этом неважно, имели ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Термины умышленные – злонамеренные и неумышленные – случайные попарно равнозначны и употребляются здесь как синонимы.

Вектор воздействия — *критерий классификации в отношении действий лиц, спровоцировавших утечку. Различаются действия внешних злоумышленников – (Внешние атаки), направленные «внутрь» компании, воздействующие на веб-ресурсы, информационную инфраструктуру с целью компрометации информации, и действия внутренних злоумышленников – (Внутренний нарушитель), атакующих системы защиты изнутри (нелегитимный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.)*

Канал передачи данных — *сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность. На данный момент мы различаем 8 самостоятельных каналов:*

- ✓ *Кража/потеря оборудования (сервер, СХД, ноутбук, ПК), – компрометация информации в ходе обслуживания или потери оборудования.*
- ✓ *Мобильные устройства – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.*
- ✓ *Съемные носители – потеря/кража съемных носителей (CD, флеш-карты).*
- ✓ *Сеть – утечка через браузер (отправка данных в личную почту, формы ввода в браузере), нелегитимное использование внутренних ресурсов сети, FTP, облачных сервисов, нелегитимная публикация информации на веб-сервисе.*
- ✓ *Электронная почта – утечка данных через корпоративную электронную почту.*
- ✓ *Бумажные документы – утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации).*
- ✓ *IM – мессенджеры, сервисы мгновенных сообщений (утечка информации при передаче голосом, текстом, видео при использовании сервисов мгновенных сообщений).*
- ✓ *Не определено - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки».*