От хакера секретов нет?

Чем больше секретных и критически важных данных оказывается в интернете, тем с большим интересом и вниманием тянутся к этим данным хакеры. Воры XXI века – это не только привычные нам "домушники", карманники и прочие мастера криминального жанра, а образованные и весьма неглупые молодые люди, без отмычек и монтировки вскрывающие чужие счета, глубоко личную переписку или базы данных самых разных предприятий. Ну, а имея на руках такие данные, грех не продать их за большие деньги.

И какие бы препоны ни ставились на пути у взломщиков, количество утечек данных растёт устрашающими темпами.

Для того, чтобы оценить масштаб бедствия, стоит обратить внимание на статистику, которую подготовил по результатам исследования утечек конфиденциальной информации в России Аналитический центр компании InfoWatch.

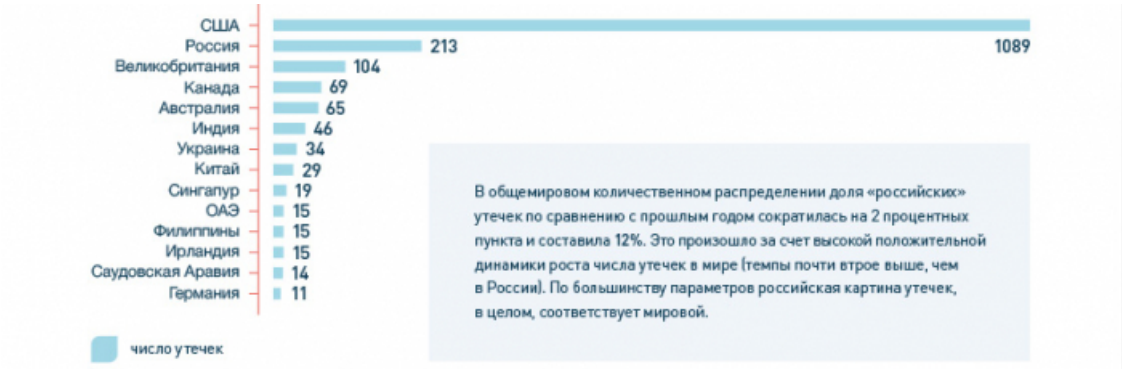
Только на основании информации, размещённой в открытых источниках, в 2017 году было зафиксировано 254 случая утечки данных - на 14 процентов больше, чем в 2016 году. В трети случаев хакеры рассчитывали воспользоваться полученной информацией в мошеннических целях, что почти втрое превышает аналогичный показатель прошлого года. Кроме того, в 4,5 раза увеличился в 2017-м году против 2016-го объём украденных финансовых данных граждан. То есть, хакеры нацелились на обогащение любым способом, начиная от шантажа, заканчивая прямым воровством. Именно поэтому в России доля утечек, в результате которых скомпрометированные данные были использованы мошенниками, увеличилась с 12 процентов в 2016 до 30 процентов в 2017-м году.

> Важно, что совокупная доля российских "квалифицированных утечек", к которым относятся случаи превышения прав доступа, в 2017 году была в два раза выше, чем доля аналогичных инцидентов в выборке по миру, – считают эксперты InfoWatch.



Количество зафиксированных утечек

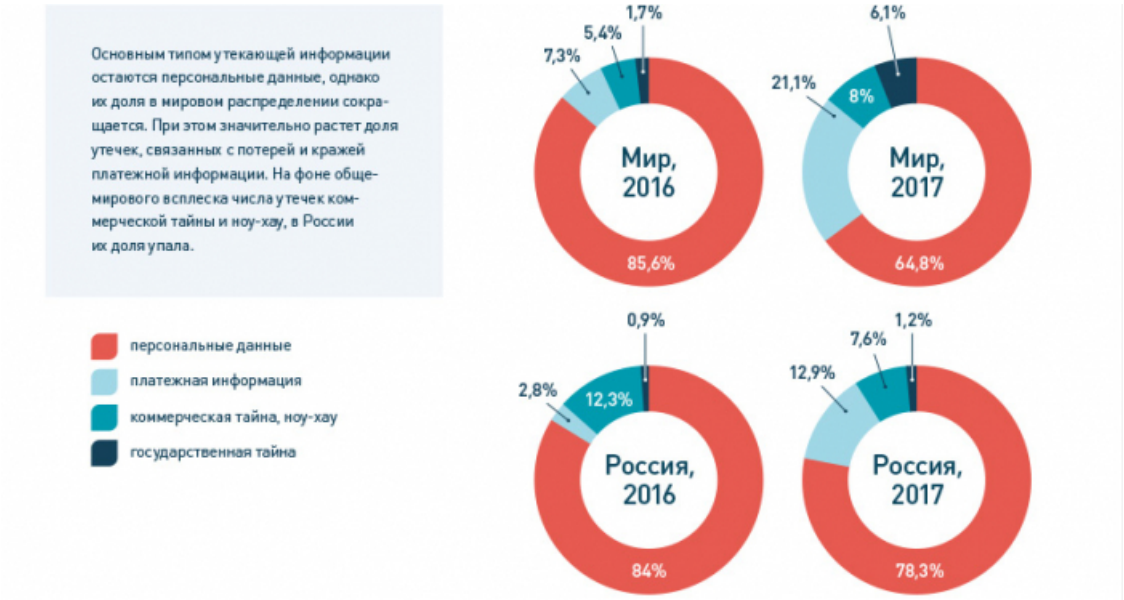
Количество утечек, как выяснили эксперты, растёт по всему миру устрашающими темпами. А вот с чем связано то, что атак на Россию совершено почти в 19 раз больше, чем на Германию, сказать, думаю, непросто. Разве что к безопасности данных там относятся настолько серьёзно, что хакеры взламывают немцев, когда точно уверены в успехе, как в случае с Deutsche Telekom. когда сотни тысяч роутеров этого гиганта были скомпрометированы, а по всей Германии начались перебои в телефонной связи и телевещании.



Распределение утечек по странам

В 2017 году основная часть скомпрометированной информации – персональные данные

пользователей, хотя их стало на шесть процентов меньше, чем в 2016 году. При этом с трёх до 16 процентов выросла доля утечек платёжной информации. По мнению авторов исследования, такое увеличение связано со стремительным развитием в нашей стране дистанционных каналов осуществления финансовых операций и появлением новых форм платежей. Но тенденция эта соответствует общемировой – во всём мире хакеры пытаются в процессе взлома сразу получить деньги, а не тратить силы и время на продажу украденных данных или шантаж и вымогательство.



В 2017 году, как и в 2016-м, лидерами по количеству умышленных утечек информации были высокотехнологичные предприятия, включая телекоммуникационные, ИТ-компании и организации банковского сектора.



Распределение утечек по вектору воздействия

Главными виновниками утечек, как и в прошлые годы, были работники компаний.

> "Как правило, в России персонал не воспринимает информационные активы организации как чужую собственность, и допускает возможность их использования в своих интересах, - отметил аналитик ГК InfoWatch Сергей Хайрук.
> Именно поэтому доля корпоративных утечек с использованием информации в личных целях в России растет год от года и уже существенно превышает среднемировые значения. Наиболее распространённый пример – мошенничество в финансовой, высокотехнологичной, социальной и других сферах с использованием доступа к данным пользователей и неправомерным копированием конфиденциальной информации. В то же время, высокий процент успешных мошеннических действий свидетельствует и о низком уровне культуры информационной безопасности в организациях при работе с данными ограниченного доступа в различных отраслях".

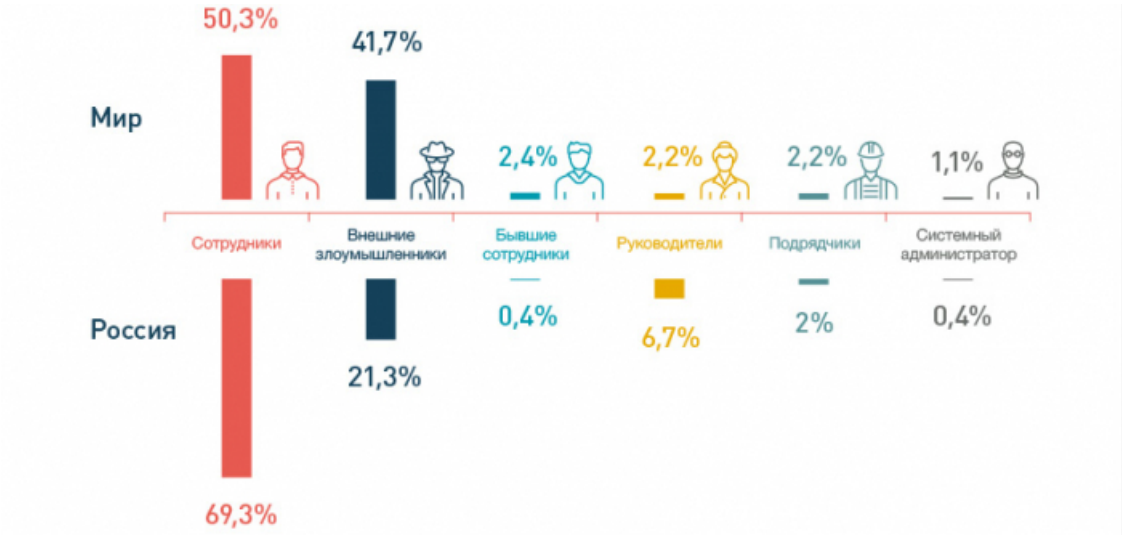
В распределении по отраслям наибольшее количество утечек данных в России было зафиксировано в муниципальных учреждениях (19,4%),организациях финансовой сферы (17,8%) и здравоохранения (13,4%). Реже всего данные утекали из образовательных учреждений (5,9%), предприятий сферы торговли (5,5%) и транспортного комплекса (4%).

Распределение утечек по вектору воздействия в России существенно отличается от мирового - внутренние нарушения в организациях стали причиной 86% случаев утечек данных в нашей стране, в то время как в мире на них пришлось 60% случаев. Таким образом, в российской выборке фактор внешних угроз влияет на картину утечек значительно в меньшей степени, чем в мировой практике.



Распределение утечек по типу инцидента

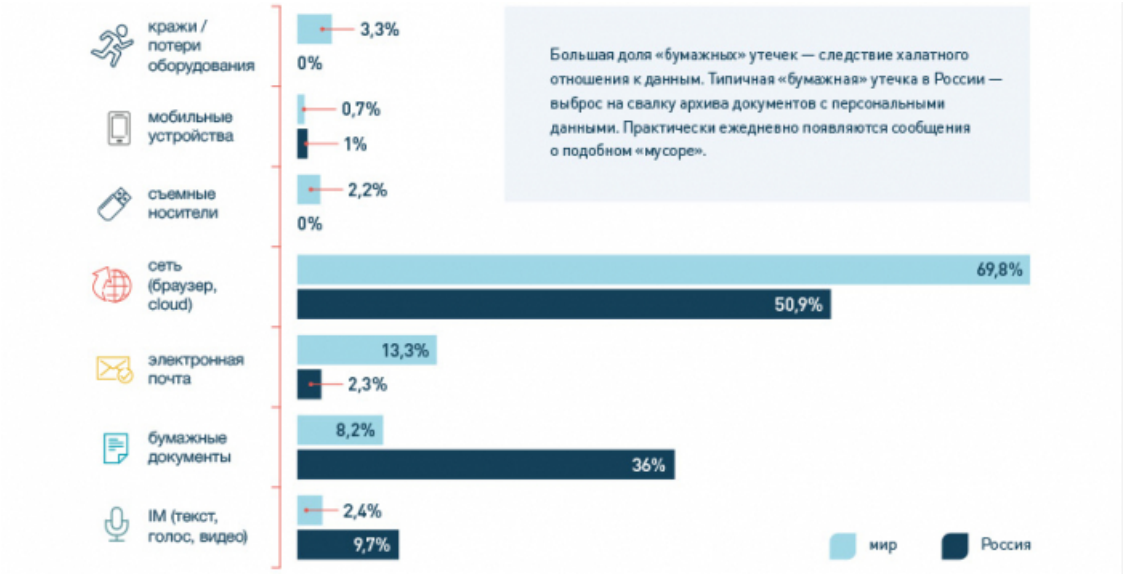
Большинство инцидентов в России пришлись на нарушения в работе рядовых сотрудников, которые составили 69% всех утечек информации в 2017 году. За год по вине высшего руководства и глав подразделений организаций произошло около 7% утечек данных. В мире намного выше влияние внешних злоумышленников, а потому значения этих показателей составляют около 50% и 2% соответственно.



Распределение утечек по виновнику

Чаще всего россияне крали данные через браузер с подключением к интернету, или просто распечатывали секретные сведения на бумаге. На эти способы в 2017 году пришлось 51 и 36 процентов от общего числа инцидентов. Кроме того, в полтора раза по сравнению с 2016 годом – до 10% – возросла доля утечек информации с использованием сервисов мгновенных сообщений.

За 2017 год в России была зафиксирована лишь одна масштабная утечка, в результате которой были скомпрометированы данные о более чем пяти миллионах пользователей. В 2016 году в нашей стране утечки были куда масштабнее. В результате четырёх инцидентов пострадали более 127 миллионов записей данных. Без учёта крупнейших утечек объем скомпрометированной информации в 2017 году изменился несущественно по сравнению с 2016 годом и составил около 200 тысяч записей.



Распределение утечек по каналам

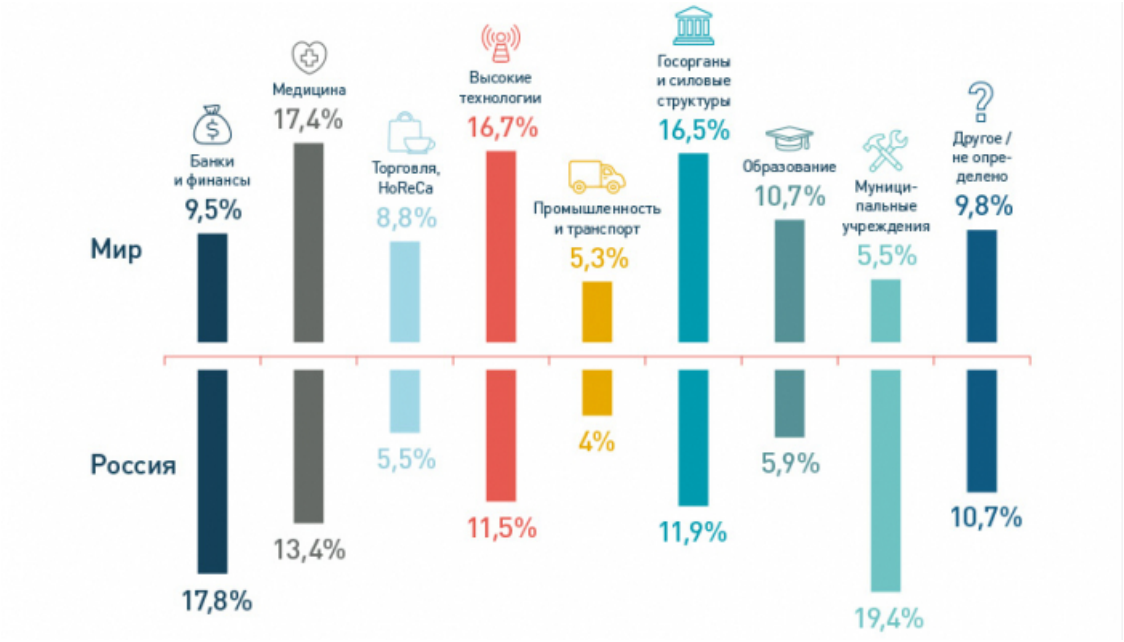
Статистику по каналам утечек спрогнозировать несложно – меньше всего данных уходит через съёмные носители и мобильные устройства, больше всего – через сети и браузеры (69,8 процента за границей, 50,9 – в России). Характерны отличия российских и мировых тенденций. У нас не зафиксировано ни одной утечки, организованной с помощью съёмных носителей, а заграничные воры данных не стесняются перекачать на флэшку конфиденциальные данные хозяина. Зато только 8,2 процента иностранцев рискуют унести их офиса распечатки, а в России на "бумажные документы" приходится 36 процентов утечек. Специалисты считают, что наряду с любовью россиян к бумаге, причина утечек – в пренебрежительном отношении к архивам. Иногда на помойке оказываются и персональные данные, и ценные для специалистов сведения о банковских операциях, и многое другое.

И ещё интересная деталь: если за границей в порядке вещей сначала украсть носитель информации – компьютер, ноутбук или диск (3,3 процента утечек), то у нас технику ради данных, похоже, не воруют.

> "Число утечек информации из организаций в России можно уменьшить только при существенном пересмотре подходов к обеспечению информационной безопасности предприятий, - отметил аналитик ГК InfoWatch Сергей Хайрук. - Будущее в этой области лежит за внедрением единых платформ управления комплексной внутренней безопасностью, работа которых строится на технологиях анализа больших данных, применении алгоритмов машинного обучения и нейронных сетей. Такие системы должны позволить организациям купировать внутренние риски уже на самой ранней стадии. При этом любая технология, даже самая передовая, не будет полновесной без соответствующих организационных мер и повышения общего уровня культуры информационной безопасности. Все это вместе должно значительно помочь стране минимизировать риски, связанные с переходом на цифровые рельсы. В противном случае следует ожидать дальнейшего роста числа квалифицированных утечек, объема украденной информации, платежных и персональных данных граждан. Очевидно, что при реализации негативного сценария, отсутствии скоординированных действий по его нейтрализации, финансовый ущерб государства, бизнеса и граждан будет расти".

Если говорить об отраслевом распределении утечек, то разница между российскими и зарубежными тенденциями тоже вполне объяснима. У нас лидеры по утечкам муниципальные учреждения, и это объяснимо. Многие муниципальные служащие просто не считают сведения особо секретными, да и архивы на помойку вынесут или сдадут в макулатуру, скорее всего, из муниципального учреждения в полной уверенности, что эти бумажки никого не заинтересуют, а уничтожить такие архивы – впустую время и деньги потратить.

Зато в краже финансовых и банковских данных мы лидеры (17,8 процента у нас, против 9,5 за границей).



Получается, что защититься от воров, нацеленных на данные, нет никакой возможности, пока остроту проблемы не поймут сами работники, и не научатся не болтать лишнего, уважать даже архивные бумаги и создавать "хитрые" пароли. Ну и конечно тем, кто отвечает за конфиденциальность на предприятии стоит постоянно совершенствоваться, чтобы всегда быть на шаг впереди хакеров.