Утечки данных. Россия. 2019 год

Оглавление

Только факты

- ✓ В 2019 году Экспертно-аналитическим центром InfoWatch зафиксировано **395** случаев утечки данных из российских компаний и государственных органов, что составляет 15,7% от числа утечек данных по всему миру. В результате утечек оказались скомпрометированы[1] более **172 млн** записей персональных данных и платежной информации.
- ✓ В 2019 году по сравнению с данными 2018 года число утечек увеличилось на **46%**, объем скомпрометированной пользовательской информации вырос более чем **в 6 раз.**
- ✓ По числу утечек Россия седьмой год подряд занимает второе место в мировом распределении (после США). Чаще всего в России «утекают» персональные данные и платежная информация — на эти типы данных приходится **87,3%** утечек, случившихся в 2019 году.
- ✓ В **72,1%** случаев виновными в утечке информации оказались рядовые сотрудники компаний, в **4,6%** случаев — топ-менеджмент организаций, в **18,4%** – хакеры и неизвестные лица.
- ✓ В 2019 году доля утечек, случившихся под воздействием внутреннего нарушителя, составила **88,2%.** По вине или неосторожности внутренних нарушителей было скомпрометировано **117 млн** записей персональных данных и платежной информации — 68,1% от совокупного количества записей, скомпрометированных в 2019 году. В 2019 году в России наибольшие доли утечек пришлись на сетевой канал и на бумажную документацию — **53,4%** и **17,5%** соответственно[2].

[1] Компрометация данных — нарушение состояния защищенности, последствие утечки данных.

[2] Данные приведены с учётом того, что на момент публикации в каждом седьмом случае канал утечки еще не был установлен (14,4%).

Сокращения

GDPR	General Data Protection Regulation (Регламент Евросоюза о персональных данных от 27.04.2016 г., вступил в силу 25.05.2018 г.)
ИБ	Информационная безопасность
ИС	Информационная система
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
ЭАЦ	Экспертно-аналитический центр ГК ИнфоВотч

Аннотация

Экспертно-аналитический центр группы компаний InfoWatch представляет ежегодное исследование утечек информации ограниченного доступа, зафиксированных в российских (работающих в России) коммерческих и некоммерческих компаниях, государственных органах и организациях в 2019 году.

В отличие от США, Европы, некоторых стран Азии, в России не наблюдается последовательного ужесточения регуляторной политики, ответственность за утечку данных (на примере персональных данных) остается номинальной, хотя законопроекты об увеличении штрафов обсуждаются более 6 лет. Например, выявлено шесть штрафов за утечки, назначенных по представлениям Роскомнадзора, на общую сумму 180,5 тыс. рублей.

На практике авторам не удалось найти ни одного публичного случая, когда база данных, отнесенная самой компанией к коммерческой тайне, была бы оценена и принята на баланс как нематериальный актив. Это означает, что за разговорами о ценности данных не стоит реальной оценки актива, то есть, если нет оценки, то нет и ущерба, как потенциального (для обоснования стоимости системы ИБ), так и реального (для возмещения ущерба через суд или страховку).

Статистика инцидентов (утечек) дает наглядное представление, например, о том, какой канал утечки чаще используется в настоящее время и какую отрасль злоумышленники считают наиболее привлекательной с точки зрения ценности содержащихся в её системах данных.

Авторы отчета уверены, что результаты исследования будут интересны специалистам в области информационной и экономической безопасности, журналистам, собственникам и высшему менеджменту компаний, которые оперируют информацией ограниченного доступа (коммерческая, банковская, налоговая тайна, персональные данные), иными ценными информационными активами.

Методика

Исследование проводится на основе собственной базы утечек ЭАЦ, регулярно пополняемой специалистами ЭАЦ с 2004 года. В базу попадают публичные сообщения[3] о случаях утечки информации из коммерческих, некоммерческих (государственных, муниципальных) организаций, госорганов.

В настоящий момент количество записей в базе превышает 18 000.

Исследования ЭАЦ в основном ориентированы на анализ сообщений об утечках данных на английском и русском языке, также используется некоторое количество источников на арабском, немецком, французском, испанском и итальянском языках. Во многом с этим связана большая доля информации о российских утечках, сообщений об утечках из компаний англосаксонских стран и Европы.

При этом была найдена информация об утечках, произошедших в более чем 50 странах на всех пяти континентах за 2019 год.

В ходе наполнения базы утечек ЭАЦ каждое сообщение об утечке классифицируется по закрытому списку признаков. Каждый признак обладает ограниченной вариативностью. К примеру, при классификации по страновой принадлежности, как было указано выше, каждому сообщению ставится в соответствие один из вариантов (название страны, на территории которой работает обладатель информации и где, предположительно, произошла утечка информации).

В базу вносятся:

- текст заголовка и сообщения об утечке,
- ссылка на источник сообщения,
- дата публикации сообщения,
- размер причиненного в результате утечки ущерба[4] (если его оценила сама компания, допустившая утечку, или аналитические агентства),
- количество скомпрометированных записей (только для ПДн и платёжной информации),
- государство (страна),
- сфера деятельности обладателя информации (отрасль)[5],
- примерный размер пострадавшей от утечки организации (малая, средняя, крупная)[6],
- направление деятельности (коммерческая, некоммерческая),

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

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

[5] Выделяются следующие отрасли (отраслевые группы): банки и финансы, медицина, торговля и HoReCa, высокие технологии (в основном ИТ и телекоммуникационные компании), промышленность и транспорт, госорганы и силовые структуры, образование, муниципальные учреждения, другое.

[6] По предполагаемому количеству персональных компьютеров в компании. Малые – до 50 ПК, средние – от 50 до 500 ПК, крупные – более 500 ПК.

- субъект[7], непосредственно допустивший утечку.

Далее каждое сообщение классифицируется по:

- наличию умысла[8] (если действия лица, допустившего утечку, являются умышленными, утечка классифицируется как умышленная / злонамеренная; в обратном случае как неумышленная / случайная);
- каналу утечки,
- типам данных (относятся ли скомпрометированные сведения к персональным данным, платежной информации, государственной или коммерческой тайне, ноу-хау и т.п.),
- вектору воздействия,
- типу нарушителя.

Все перечисленные признаки (конкретные варианты признаков) вносятся при наличии информации, определяются методом экспертной оценки, носят вероятностный характер, если информация не полная или противоречивая. При невозможности классифицировать сообщение (выявить вариант признака и отразить в базе), в соответствующем поле проставляется значение «не известно». Иных признаков (категорий для классификации) база утечек ЭАЦ не содержит.

Также базу попадают случаи, когда невозможно установить обладателя скомпрометированной информации, но совершенно точно известно, что утекшая информация не является скомпилированным набором данных на основе других утечек. Такие случаи при добавлении в базу классифицируются по всем известным параметрам.

В базу вносится только количество записей, содержащих ПДн и/или платёжную информацию, т.к. в остальных случаях количественные характеристики обычно отсутствуют.

Важно отметить, что наряду с неквалифицированными «простыми» утечками авторы исследования выделяют «квалифицированные» утечки — случаи, когда деструктивное поведение сотрудников выражается в использовании легитимного (правомерного, санкционированного) доступа к данным в мошеннических целях (манипуляции с платежными данными, инсайдерской информацией); случаи превышения прав доступа, когда сотрудник знакомится, копирует, передает данные, к которым не должен иметь доступа по роду службы или работы. Указанные признаки также устанавливаются на основе экспертной оценки.

Также в случаях, когда тип нарушителя неизвестен, и удельный вес таких неизвестных в выборке незначителен (как правило, менее, 3%), авторы исследования добавляют их к

---

[7] Авторы классифицируют утечки по виновнику инцидента. Используются следующие категории: внешний нарушитель - хакер/неизвестное лицо, рядовой сотрудник, топ-менеджер (руководитель), системный администратор, подрядчик: сторонний исполнитель работ по заказу компании, партнер и внештатный сотрудник; бывший сотрудник. См. Глоссарий.

[8] 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. См. Глоссарий.

внешним нарушителям, т.к. соответствует данным, полученным при изучении аналогичных случаев.

Сообщения об утечках (единицы совокупности или элементы выборки) в базе ЭАЦ далее именуется утечками. Т.е. каждая запись в базе ЭАЦ содержит сведения об одном событии, которое полностью соответствует приведенному выше определению утечки данных (информации).

Авторы считают, что большие шансы стать известными имеют случаи утечки данных, ставшие следствием:

- кражи в целях продажи неопределенному кругу лиц;
- действий хактивистов для достижения общественных и политических целей;

а также утечки из наиболее крупных и широко известных компаний, организаций, учреждений.

Кроме того, крупные утечки (объемом более 1 млн записей) и утечки из известных компаний с известными брендами чаще попадают в сферу внимания СМИ, блогеров, надзорных органов. Для анализа и корректного расчета среднего числа записей в одной публичной утечке выделена отдельная категория - «мега-утечка», то есть утечка, в результате которых было скомпрометировано 10 млн и более записей. Также отдельно могут исследоваться все утечки с числом скомпрометированных записей от 1 млн, а также вся совокупность утечек с числом записей до 1 млн.

Сведения об утечках представлены с использованием исторических данных — количественных показателей предыдущих лет.

Для повышения качества выводов использованы следующие подходы: исследования проводятся ежегодно на основе выборки, сформированной по единой методике (случайный поиск исходных сообщений об утечках, классификация сообщений по единому списку признаков). При формировании выводов авторы опираются на динамические показатели. Все данные в сравнительных исследованиях (сравнения с аналогичными показателями предыдущего периода) представляются в процентном виде. Исключение: сведения о совокупном количестве утечек, включенных в базу ЭАЦ, объеме записей, скомпрометированных в результате этих утечек, объеме скомпрометированных записей в расчете на одну утечку (только ПДн и платежная информация).

Указанные данные носят иллюстративный характер, дают представление, например, об изменении объемов определенных типов данных, хранимых и обрабатываемых обладателями информации.

Также в абсолютных показателях представлены данные в виде так называемой «отраслевой карты утечек» — данная карта показывает фактическое распределение объема скомпрометированных персональных данных по отраслям (наглядно показывает зависимость объема ПДн в отрасли от размера компании-обладателя информации, числа утечек ПДн).

При анализе выборки по определенному признаку и построении сравнительных диаграмм (такие диаграммы авторы именуют разрезами или распределениями) все

утечки, классифицированные по исследуемому признаку как «неизвестные» и с долей менее 5%, исключаются из выборки, после чего совокупность оставшихся утечек принимается за 100% для распределения по вариантам выбранного признака и последующего представления в диаграммах.[9] Такой подход позволяет проиллюстрировать динамические изменения отдельных показателей (долей, приходящихся на утечки, обладающие определенным признаком) более ярко, т.е. решает исключительно презентационные задачи. Но в случаях, когда доля утечек с признаком, классифицированным как «неизвестный», превышает 5%, представляются отдельные диаграммы.

[9] 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.

Результаты исследования

В 2019 году Экспертно-аналитическим центром InfoWatch зарегистрировано 395 случаев утечки информации ограниченного доступа из коммерческих компаний, некоммерческих организаций, государственных органов и других организаций, работающих в России. В результате утечек оказались скомпрометированы более 172 млн записей персональных данных и платежной информации (далее – пользовательская информация), в частности имена и фамилии, адреса электронной почты и сведения о постоянном месте проживания, номера полисов социального страхования, реквизиты пластиковых карт и данные о банковских счетах жителей Российской Федерации.

В 2018 году было зафиксировано 270 утечек, оказались скомпрометированы 26 млн записей. Таким образом, в 2019 году число утечек увеличилось на 46%, объем скомпрометированной пользовательской информации вырос более, чем в 6 раз (см. **Ошибка! Источник ссылки не найден.**).

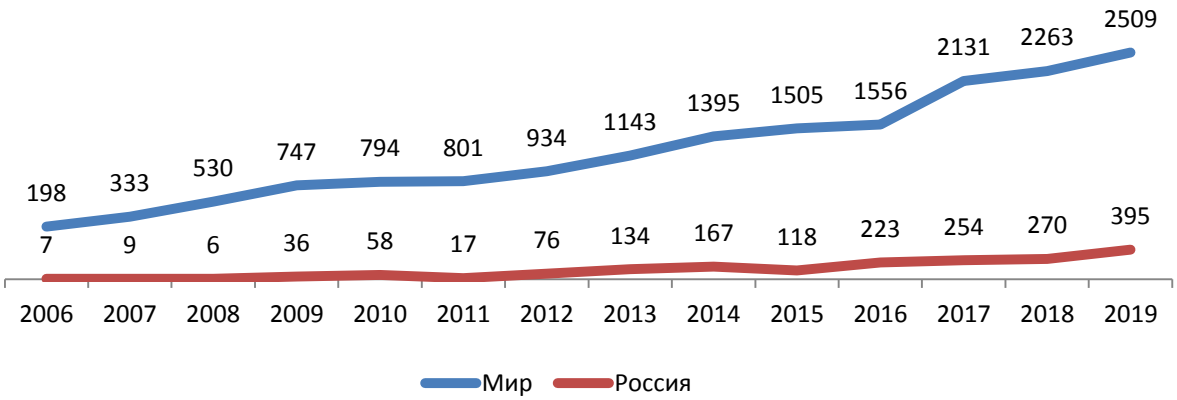

Рисунок 1. Число зафиксированных утечек, Россия – мир, 2006-2019 гг.

В 2019 году в мировом «рейтинге» стран, пострадавших от утечек, Россия заняла второе место — сразу вслед за США. В общемировом распределении доля «российских» утечек составила 15,7%. Объем скомпрометированных данных, который пришелся на российские компании и государственные организации, не превысил 1,1% от совокупного объема данных, скомпрометированных по всему миру (см. Рисунок 2).

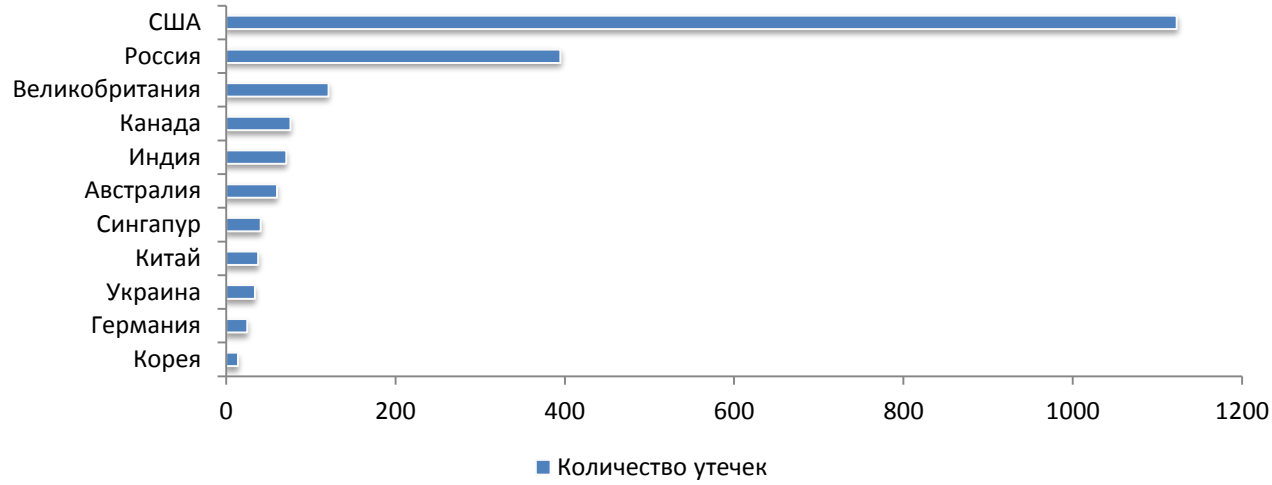

Рисунок 2. Распределение утечек по странам, 2019 г.

При этом более половины объема данных, скомпрометированных в России в 2019 году, приходится на один инцидент, когда свыше 90 млн записей, содержащих сведения о юридических и физических лицах, оказались в открытом доступе из-за ошибки в настройках сервера оператора фискальных данных «Дримкас».

За 2019 год в России зафиксировано 9 утечек, в результате каждой из которых объем скомпрометированных данных превысил 1 млн записей.

В среднем на одну утечку приходится 0,435 млн записей (для сравнения – в 2019 году в мире на одну утечку приходится в среднем 5,92 млн записей). Без учета утечек объемом свыше 1 млн записей на одну утечку в России в среднем приходится 22,9 тыс. записей, в мире 19,9 тыс. записей.

Практически все российские утечки объемом свыше 1 млн записей связаны с попаданием в открытый доступ крупных баз данных, предположительно, из-за ошибок технического персонала при настройке удаленного доступа к хранилищам информации.

> safe.cnews.ru: *В течение нескольких месяцев в свободном доступе находились данные о кредитных историях россиян. Утекшая в интернет база данных предположительно принадлежала микрофинансовой организации «ГринМани» и содержала сведения, предоставленные бюро кредитных историй «Эквифакс» и «Объединенным кредитным бюро». База насчитывает более 1 млн записей о персональных данных жителей России.*

При этом типичные, наиболее распространенные «российские» утечки представляют собой инциденты, в ходе которых компрометации подвергаются единичные записи. Чаще всего в СМИ и иных источниках описываются следующие сценарии: неправомерное предоставление за плату сотрудниками медучреждений и правоохранительных органов сведений об умерших гражданах (в пользу ритуальных агентств); неправомерные действия сотрудников организаций в сфере ЖКХ, допустивших распространение персональных данных (вывешивание списков жильцов, не оплативших коммунальные услуги); компрометация персональных данных граждан

из-за ошибок системных администраторов действующих или приостановленных веб-проектов (как правило, необеспечение парольной защиты баз данных с персональными данными граждан).

Распределение утечек по типам данных свидетельствует о небольшом (по сравнению с мировой картиной) количестве случаев компрометации платежных данных. При этом доли утечек информации, составляющей государственную и коммерческую тайну, в России и в мире практически равны (см. Рисунок 3).

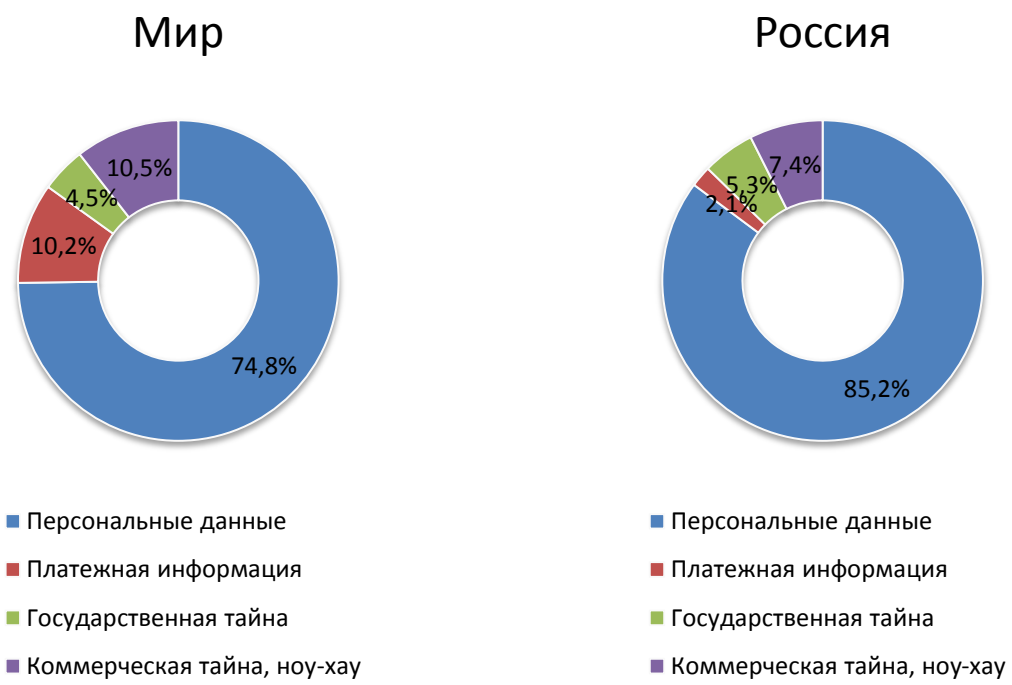

Рисунок 3. Распределение утечек по типам данных, Россия – мир, 2019 г.

Вероятно, небольшая доля платежной информации (по сравнению с мировым показателем) объясняется тем, что основными операторами платежной информации в России остаются финансовые учреждения, которые не зря считаются лидерами в сфере информационной безопасности. Следствием относительно высокого уровня ИБ в российских банках, иных финансовых учреждениях, по-видимому, и является незначительное число утечек такой информации. Кроме того, банковская сфера остается высококонкурентной, любая утечка данных грозит оттоком клиентов, что также вынуждает банки со всей серьезностью относиться к обеспечению безопасности информации.

Впрочем, все вышесказанное не означает, что финансовая отрасль представляет собой этакий «островок безопасности», не отменяет действие «человеческого» фактора. Сотрудники банков и иных финансовых компаний, имеющие легитимный доступ к персональным данным клиентов, зачастую не обладают элементарными знаниями о правилах безопасного обращения с информацией ограниченного доступа либо умышленно игнорируют запреты и политики безопасности.

> *letnews.ru: В Саратовской области местная жительница, имея доступ к персональным данным, оформила шесть кредитов на граждан без их согласия.*

Сообщается, что подозреваемая была сотрудником одного из финансовых учреждений г. Энгельса и имела свободный доступ к персональным данным клиентов.

Как следствие, число утечек информации по вине или неосторожности рядовых (непривилегированных) сотрудников, и без того немалое, имеет тенденцию к дальнейшему росту. В 2019 году в России на долю сотрудников пришлось 72,1% утечек. При этом общемировой показатель составляет лишь 41,0%.

Кроме того, в России вдвое выше доля утечек по вине руководства компаний (топ-менеджеров и линейных руководителей), чем по миру в целом — 4,6% против 2,3% (см. Рисунок 4).

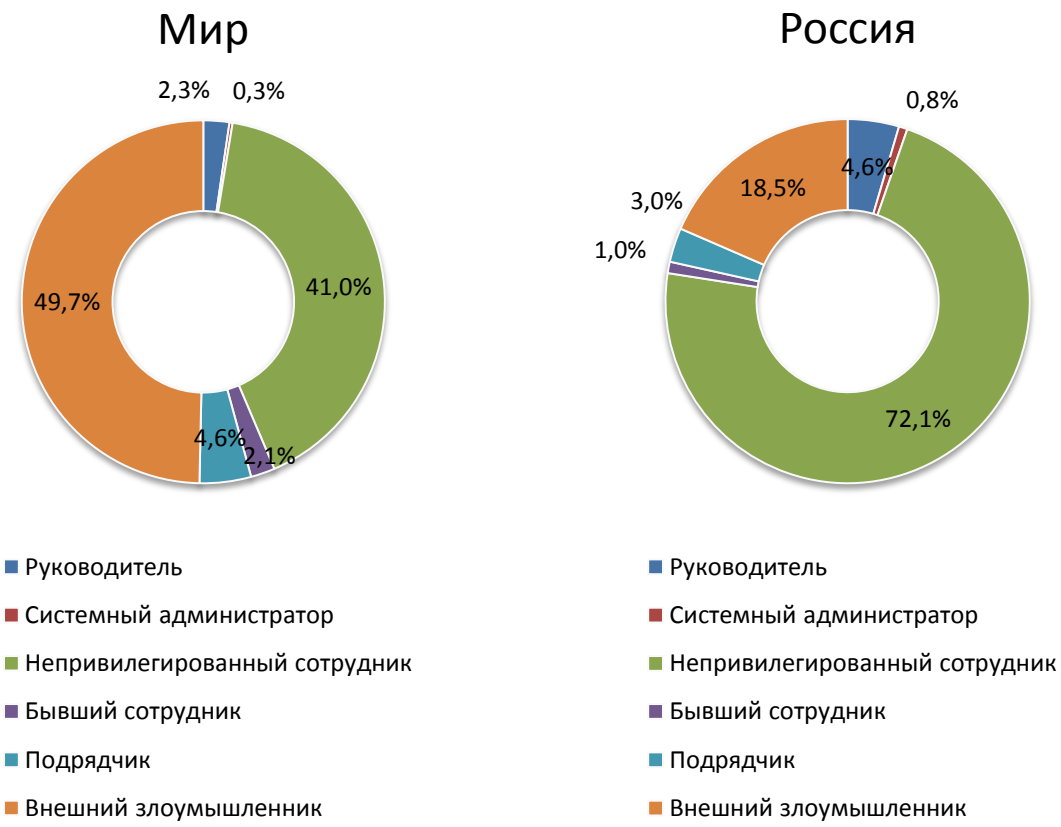

Рисунок 4. Распределение утечек по виновнику, Россия – мир, 2019 г.

В силу традиций, берущих начало еще в советское время, руководители отечественных компаний практически неподконтрольны службам безопасности, имеют множество привилегий в том, что касается доступа к информации. К примеру, расследование инцидента в одной крупной российской компании показало, что интерфейсы для подключения сторонних устройств хранения, заблокированные по умолчанию, были открыты для руководителей подразделений и высшего управленческого звена. Воспользовавшись этим, один из руководителей незадолго до своего увольнения скопировал несколько тысяч документов на внешний носитель информации.

И этот случай нельзя назвать единичным. Складывается парадоксальная ситуация, когда привилегированные пользователи обладают доступом к огромному массиву информации ограниченного доступа, но при этом риск утечки такой информации по

вине или неосторожности привилегированных пользователей берется в расчет по остаточному принципу, сценарии возможных утечек по вине топ-менеджеров либо вовсе не рассматриваются, либо имеют более низкий приоритет по сравнению со сценарием умышленных или случайных утечек из-за действий рядовых сотрудников.

Впрочем, следует сказать, что в 2019 году (по сравнению с данными 2018 года) доля утечек по вине или неосторожности сотрудников практически не изменилась (77,9% в 2018 году), в то время как аналогичный показатель для руководства компаний уменьшился на 3,7 п. п. (8,8% в 2018 году). По-видимому, на пути решения проблемы привилегированного пользователя наметились некоторые успехи. Тем более, что средства для контроля их действий существуют на рынке довольно давно (более 10 лет).

Сравнительно небольшая доля утечек по вине внешнего нарушителя (хакеры и неизвестные лица) в России - 18,5% против 49,7% в мире - имеет свое объяснение. Значительное количество случаев компрометации данных по вине внешнего нарушителя, зафиксированы в странах, установивших значительные штрафы за утечку данных (прежде всего США и страны Европы), а также за не информирование о таких случаях.

Впрочем, следует также учитывать, что персональные данные жителей России (которые составляют основную долю российских утечек) в целом менее ликвидны, чем персональные данные, скажем, граждан США. Возможное применение украденных данных россиян пока сводится к спам-рассылкам, телефонному мошенничеству, фишингу. В последнее время к этому списку добавились услуги каршеринга. Получение кредитов на чужие персональные данные уже требует наличия соучастника в кредитном учреждении — сотрудника, который оформит кредит без участия владельца данных. Получить электронную подпись без личного участия человека с паспортом также не получится (случаи незаконного получения такой подписи без присутствия заявителя были, но их все же нельзя назвать массовыми, к тому же, эту «лазейку» для мошенников государство недавно закрыло).

> *securitylab.ru: Мошенники смогли украсть квартиру, использовав чужую электронную подпись. Сделка по передаче жилплощади мошенникам была осуществлена через интернет-портал Росреестра.*

В России, в отличие от тех же США, у гражданина пока нет цифрового эквивалента личности, практически нет финансово значимых услуг, которые он мог бы получить полностью онлайн, только по цифровому идентификатору. Поэтому «кража личности» и ее последствия — к примеру, получение налогового вычета от имени другого человека, — в России практически не распространены.

Изучение баз данных, предлагаемых к продаже в «темном» сегменте интернета, позволяет сделать вывод, что криминальный оборот персональных данных граждан России ограничен. Несмотря на безусловные успехи цифровизации, число простых сценариев использования персональных данных (включая изображения владельца с паспортом в руках) исчисляется единицами, требует от преступников существенных усилий (то же использование каршеринга под чужим аккаунтом предполагает наличие

доступа к телефону владельца аккаунта при возникновении любых нештатных ситуаций). Это при том, что базы данных, содержащие фотографии (селфи) граждан с паспортами в руках в интернете периодически появляются.

> *tgstat.ru: В открытом доступе была обнаружена база данных MongoDB с персональными данными заемщиков из Южного, Уральского и Приволжского федеральных округов. В обнаруженной базе данных содержалось: записи об именах, датах и местах рождения, телефонных номерах, иных данных 294 заемщиков, 893 тыс. отсканированных документов, более 246 тыс. фотографий людей, сделанных на веб-камеру в точках продаж. Общий размер данных в базе превышал 157 Гб.*

По-настоящему массовыми, типовыми сценариями «заработка» на чужих пользовательских данных можно признать лишь криминальную деятельность сотрудников кредитных организаций (оформление кредитов, микрозаймов на чужие данные) и сотрудников сотовых операторов (предоставление за плату детализаций — сведений о соединениях).

«Черный» рынок персональных данных в России остается рынком покупателя. Т.е. даже получив в свое распоряжение достаточно подробную базу данных какой-либо компании, организации, злоумышленнику предстоит серьезно потрудиться, чтобы ее продать или найти «украденным» данным иное применение. Чуть проще обстоит дело, когда сотрудник пытается продать базу данных клиентов своего работодателя прямому конкуренту. Тут покупатель известен заранее, но и в этом случае не все просто — большинство рыночных ниш в России относительно небольшие, поэтому у конкурента (потенциального покупателя), скорее всего, есть своя база со схожим набором сведений. Исключение – закрытый оборот баз данных, используемых службами безопасности банков и корпораций.

Пример попытки создать «бизнес» путём сбора данных граждан приведен ниже, чаще всего именно такие «энтузиасты» и становятся героями криминальных новостей в сфере ИБ и ПДн.

> *ura.news: Бывший сотрудник администрации Кургана Александр Грибанов продавал сведения о частной жизни жителей города и области коллекторам и банкам. Обвиняемый создал подробную программно-информационную систему, содержащую адреса, прописку, данные ИНН, СНИЛС, наличия кредитов в банках, водительских удостоверений, паспортов, задолженности в сфере ЖКХ.*

Таким образом, массового «свободного спроса» («свободного рынка») на персональные данные в России пока нет. Как следствие, нет и заметной активности внешних нарушителей (злоумышленников) в попытках получить эти данные. Отсюда сравнительно небольшая (на фоне мирового показателя) доля утечек, произошедших под воздействием внешнего нарушителя (злоумышленника) (см. Рисунок 5[10]).

[10] Соотношение приведено без учёта случаев, когда неизвестен тип нарушителя, которые применительно к данной выборке составляют менее 5%.

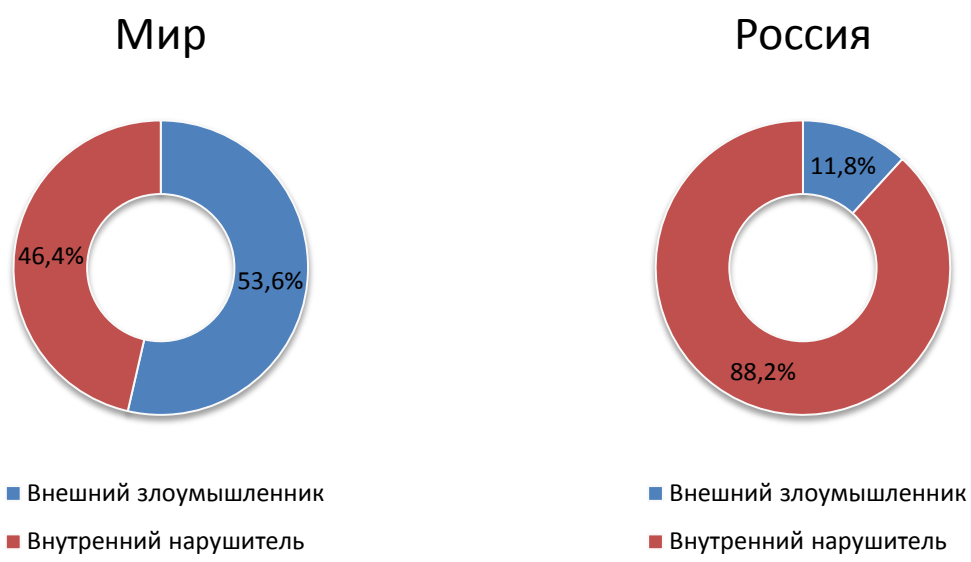

Рисунок 5. Распределение утечек по вектору воздействия, Россия – мир, 2019 г.

Еще одно отличие, характерное для России — более высокая (на фоне мирового показателя) доля так называемых «квалифицированных» утечек данных, то есть таких случаев, когда злоумышленник осознанно использует украденную им информацию для достижения личной выгоды (мошенничество с данными, банковский фрод), или получает доступ к информации, заведомо не нужной ему для выполнения трудовой функции (превышение прав доступа).

Так в 2019 году на долю утечек, сопряженных с последующим мошенническим использованием скомпрометированной информации, пришлось 17,8%. Доля утечек, связанных с превышением прав доступа, то есть с получением доступа к информации, которая была не нужна виновнику утечки по роду работы или службы, составила 1,8% (см. Рисунок 6).

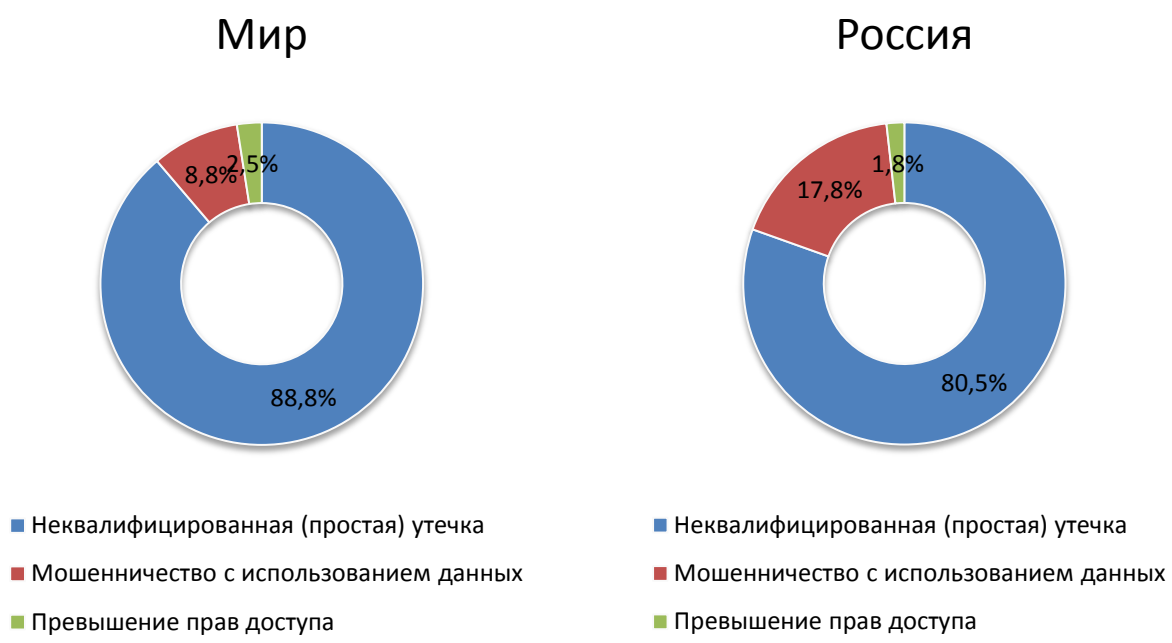

Рисунок 6. Распределение утечек по типу инцидентов, Россия – мир, 2019 г.

Годом ранее на долю утечек, связанных с мошенничеством, пришлось 23,7%. Доля утечек с превышением прав доступа составила 5,2%. Заметное снижение доли «квалифицированных» утечек налицо. Вместе с тем доля мошеннического использования данных все еще значительно превышает среднемировые показатели.

Большое число подобных утечек в России можно объяснить тем, что сотрудники не принимают в расчёт то (сознательно или «забыв»), что информация организации, в т.ч. созданная ими, принадлежит работодателю. Результат - многочисленные случаи известные продажи баз данных, содержащих сведения о клиентах и контрагентах организации-работодателя, скачивания всей доступной информации с рабочего ПК перед увольнением, получить не только заработную плату, но и самостоятельно заработать некий «бонус» на основе информационных активов работодателя.

> *vladimirnews.ru: В Муроме сотрудник офиса продаж салона сотовой связи, пользуясь служебным положением, незаконно получил доступ к персональным данным абонентов. После этого от их имени подписывал заявления на получение детализации звонков. Полученную информацию он планировал продавать сторонним лицам.*

Как и годом ранее, в 2019 году в России наибольшие доли утечек пришлись на сетевой канал и на бумажную документацию — 65,3% и 19,2% соответственно. При этом доля утечек через бумажную документацию сократилась на 25,4 п. п., т. е. более, чем вдвое.

И наоборот, почти вдвое (на 5,4 п. п.) выросла доля утечек данных с использованием сервисов мгновенных сообщений (IM) — в эту категорию относятся утечки с применением смартфонов (фотографирование экрана, отправка полученных изображений через WhatsApp, Telegram и пр.). Как видим, популярность мессенджеров среди пользователей находит отражение и в структуре утечек – данные каналы все чаще используются для передачи конфиденциальной информации. Контроль сервисов

мгновенных сообщений станет одной из актуальных задач для офицеров безопасности.

Незначительны доли утечек, связанных с использованием электронной почты — 1,2%, потерей или кражей оборудования (ПК, ноутбуки, серверы) — менее 1%, утечек через съемные носители информации — 1,7%.

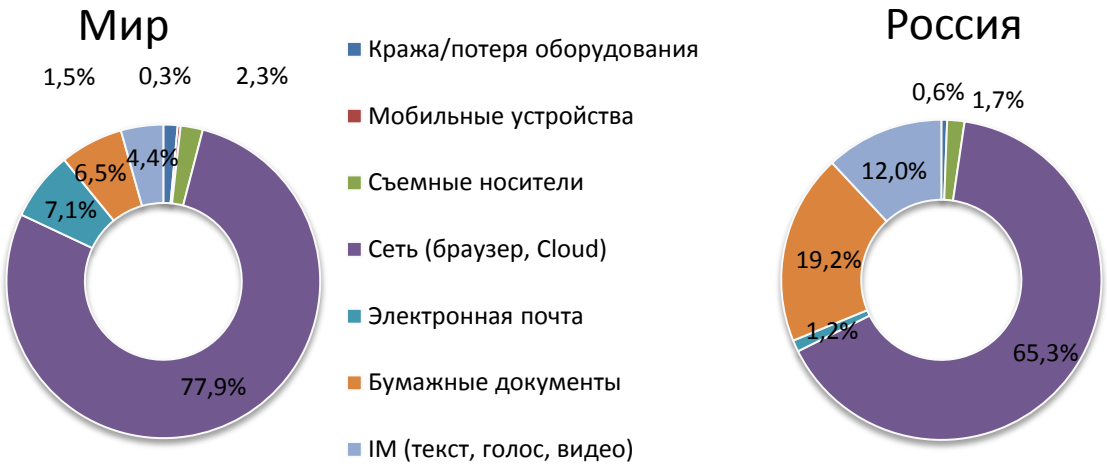

Рисунок 7. Распределение утечек по каналам, Россия – мир, 2019 г.

На рисунке 8 представлены доли утечек по каналам с учетом доли каналов утечки, неопределенных на момент публикации.

Рисунок 8. Распределение утечек по каналам с учетом неопределенных, Россия – мир, 2019 г.

Несмотря на отмеченную выше тенденцию снижения доли каналов утечки компьютерной информации, по-прежнему типичными для нашей страны являются сценарии утечек через «бумажную документацию». Как правило, крупные компании

нанимают подрядчиков для утилизации архивной документации. При этом надлежащий контроль за результатом работы отсутствует. СМИ полны сообщениями о найденных свалках документации, включая материалы уголовных дел, копии паспортов, результаты медицинских исследований. Особенно интересны случаи, когда компании таким образом «утилизируют» подписанные согласия на обработку персональных данных.

Утечки из государственных органов и организаций занимают в России более заметное место, чем в целом по миру — на долю государственных и муниципальных органов приходится в совокупности 32,4% от всех случаев компрометации информации, зафиксированных в 2019 году (см. Рисунок).

Рисунок 9. Отраслевое распределение утечек, Россия – мир, 2019 г.

Далее по убыванию идут утечки из организаций сферы высоких технологий (15,9%), финансового сегмента (13,2%). Небольшая доля «медицинских» утечек (данных о здоровье пациентов) — 7,6% на фоне 18,3% доли в мировом распределении — объясняется относительно низким уровнем «цифровизации» российской медицины, особенностями развития российского медицинского страхования, относительно низкой ликвидностью медицинских записей на черном рынке. Даже имея на руках

чужие персональные данные, мошенник в России вряд ли получит дорогостоящее лечение от страховой компании.

Приведенная диаграмма дает фактическую картину, общее представление об утечках информации в различных отраслях экономики. Но для решения практических вопросов информационной безопасности важно выяснить, какие из отраслей в настоящий момент являются наиболее «привлекательными» для злоумышленников, следовательно, более других подверженными утечкам информации.

«Привлекательность» отрасли прямо обусловлена ликвидностью данных, которые обрабатывают компании этого сектора, т. е. чем проще конвертировать украденную информацию в деньги, тем «привлекательнее» сегмент. Представление злоумышленников об уровне защиты данных в отрасли влияет на «привлекательность» обратно пропорционально.

Одним из индикаторов «привлекательности» можно считать число умышленных утечек в конкретной отрасли. Отраслевое распределение умышленных утечек одного типа данных даст нам ответ на вопрос, какие сегменты наиболее «привлекательны» для злоумышленника (и наиболее уязвимы). Проиллюстрируем это графически:

$$\text{Доля умышленных утечек} \leftarrow \frac{\text{Ликвидность данных}}{\text{Представление об уровне защищенности информации}}$$

В 2019 году наиболее «привлекательными» для злоумышленников оказались банковские, страховые компании, организации сферы торговли и гостеприимства, высоких технологий. В этих отраслях более половины утечек, сопровождавшихся компрометацией персональных данных, носили умышленный характер (см. Рисунок).

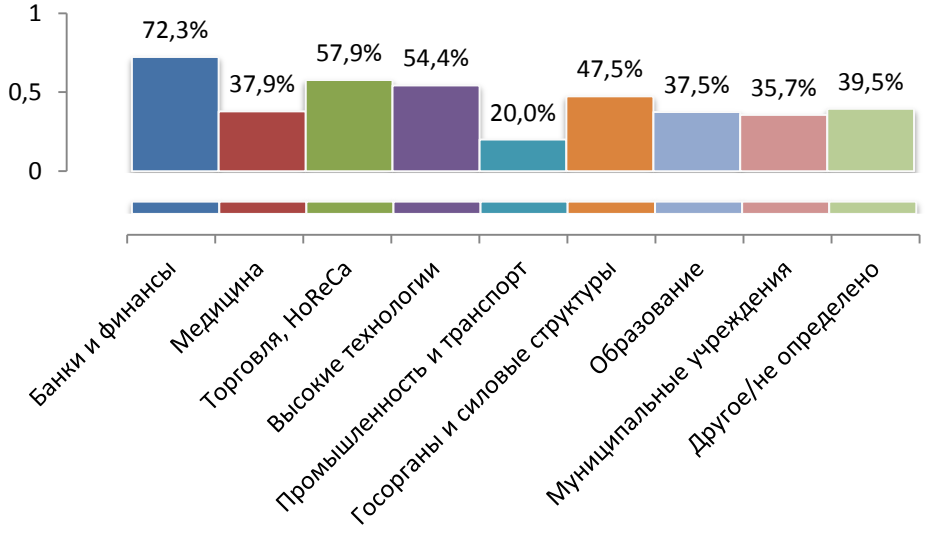

Рисунок 10. Доля умышленных утечек ПДн по отраслям, 2019 г.

Заключение

По сравнению с общемировой картиной в России:

- динамика роста утечек меньше;
- структура утечек по типам данных фактически одинакова, в т.ч. по утечкам ПДн, но практически в 5 раз меньше утечек платежной информации;
- структура утечек по виновнику – почти в 3 раза меньше утечек по результатам «работы» внешних нарушителей, в 2 раза меньше по вине бывших или непривилегированных работников, но практически в 2 раза выше по вине руководителей и системных администраторов;
- основным каналов утечки является сетевой, практически в 6 раз меньше утечек через электронную почту, и в 3 раза больше через сервисы мгновенных сообщений и на бумажных носителях;
- по структуре утечек из различных отраслей картина также похожа, но на четверть больше утечек из государственных структур, в полтора раза больше в торговле и практически в 2 раза меньше в сфере здравоохранения.

Таким образом, на основании приведенных в отчёте данных, можно сделать вывод, что в России, несмотря на ряд особенностей (минимальные санкции за утечку данных, ограниченное использование «цифровой» личности для получения финансовых услуг, совершения юридически значимых действий), в сфере безопасности информации наблюдаются тенденции, аналогичные общемировым, но с учётом принятых весной 2020 года поправок в нормативно-правовые акты, связанные с дистанционным предоставлением услуг, а также скачкообразным ростом количества удалённо работающих сотрудников следует ожидать роста утечек через электронные каналы, снижения доли бумажного документооборота.

Мониторинг утечек на сайте InfoWatch

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

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

- Почтовая рассылка
- Facebook
- Telegram

Экспертно-аналитический центр InfoWatch

www.infowatch.ru/analytics

Глоссарий

Атака – см. компьютерная атака, сетевая атака, вторжение.

Вторжение (атака) – действие, целью которого является осуществление несанкционированного доступа к информационным ресурсам [Методический документ ФСТЭК России. Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ. Утвержден ФСТЭК России. 3 февраля 2012 г.].

Вектор воздействия – критерий классификации в отношении действий лиц, спровоцировавших утечку (в рамках данного отчета InfoWatch).

Различаются действия внешних нарушителей (нарушителей - хакеров и других лиц, как известных, так и не известных) – внешние атаки, направленные против компании, воздействующие на веб-ресурсы, информационную инфраструктуру, носители корпоративной информации с целью компрометации информации, и действия внутренних нарушителей, (сотрудники компании и подрядчики, получившие права доступа к ресурсам компании) атакующих системы защиты изнутри (неправомерный доступ к закрытым ресурсам, неправомерные действия с инсайдерской информацией и проч.), а также допускающих утечки данных своими случайными действиями (бездействием).

Внешняя атака – атака, совершенная внешним нарушителем.

Внутренний нарушитель – см. Нарушитель информационной безопасности организации (нарушитель).

Внешний нарушитель – см. Нарушитель информационной безопасности организации (нарушитель).

Деструктивные действия сотрудников – в рамках данного отчета об утечках информации аналитики InfoWatch к таким действиям относят действия сотрудников, повлекшие компрометацию информации ограниченного доступа: использование информации ограниченного доступа в личных целях, в том числе сопряженное с мошенничеством; нелегитимный доступ к информации (превышение прав доступа).

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными] разведками и другими заинтересованными субъектами [ГОСТ Р 50922-2006, статья 2.3.2].

Примечание – Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Инцидент – см. инцидент безопасности, инцидент информационной безопасности, компьютерный инцидент.

Инцидент безопасности (Security incident) – неблагоприятное событие в системе или сети, а также угроза такого события.

Примечание – Иногда используется термин ≪несостоявшийся инцидент≫ для описания события, которое могло обернуться инцидентом при несколько других обстоятельствах [ГОСТ 56205-2014, статья 3.2.106]

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность [ГОСТ Р 53114-2008, статья 3.2.7. ГОСТ Р ИСО/МЭК 27001-2006, статья 3.6].

Примечание – Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Канал утечки информации – способ утечки информации; предполагает сценарий, в результате выполнения которого потерян контроль над информацией, нарушена ее конфиденциальность.

На данный момент аналитики InfoWatch выделяют 8 самостоятельных каналов утечки (далее - классификаторы):

- «Оборудование (сервер, СХД, ноутбук, ПК)», – компрометация информации в ходе обслуживания, в результате кражи 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, USB, карты памяти и др.).
- «Сеть (сетевой канал)» – утечка через браузер (отправка данных через веб-интерфейс 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 на бумаге).
- «IM –сервисы мгновенных сообщений» - утечка информации при передаче ее голосом, в текстовом виде, а также через видео - при использовании мессенджеров.

- «Не определено» - категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].

Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки [Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»].

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, п.7 ст.2].

Конфиденциальная информация – сведения конфиденциального характера, в соответствии с Указом Президента РФ от 6 марта 1997 г. №188.

В данном отчете (исследовании) авторы относят к таким сведениям информацию, доступ к которой осуществляется строго ограниченным и известным кругом лиц с условием, что информация не будет передана третьим лицам без согласия владельца информации. Помимо персональных данных, это платежная информация, коммерческие секреты и ноу-хау, а также государственные и военные секреты. В некоторых случаях при анализе полученных сведений определить тип конфиденциальной информации не представляется возможным, поэтому она относится в категории «не определено».

Нарушитель информационной безопасности организации (нарушитель) – физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации [ГОСТ Р 53114-2008, статья 3.3.5].

В БДУ ФСТЭК России bdu.fstec.ru приведены следующие виды нарушителей/ источников угроз:

- внутренний нарушитель (потенциал низкий, средний, высокий);
- внешний нарушитель (потенциал низкий, средний, высокий).

В данном отчете (исследовании) к категории «нарушитель» авторы относят лицо, которое по ошибке или осознанно (с умыслом – злоумышленник) совершило определенные запрещенные действия, повлекшие утечку информации.

InfoWatch различает два вида нарушителей – «внешний нарушитель» и «внутренний нарушитель», а также шесть категорий нарушителей:

- Внешний нарушитель – Хакер/неизвестное лицо: взломщики компьютерных сетей, в том числе представляющие организованную киберпреступность; владельцы хакерского инструментария (библиотек); взломщики, действующие в политических и социальных целях, - хактивисты; сотрудники иностранных разведок и армий; похитители оборудования с конфиденциальной информацией.
- Рядовой сотрудник.
- Топ-менеджер (руководитель).
- Системный администратор.
- Подрядчик: сторонние исполнители работ по заказу компании, партнеры и внештатные сотрудники.
- Бывший сотрудник.

В рамках исследования топ-менеджеров, системных администраторов, а в отдельных случаях и подрядчиков авторы включают в категорию привилегированных пользователей, то есть пользователей, наделенных повышенными правами доступа к информации. Как правило, действия таких пользователей в информационной системе службами информационной безопасности контролируются слабо либо не контролируются.

Иных пользователей корпоративной информационной системы (рядовых сотрудников) авторы относят к непривилегированным, обычным пользователям.

Неправомерный доступ – см. несанкционированный доступ.

Несанкционированный доступ – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа [ГОСТ Р 53114-2008, статья 3.3.6].

Примечания:

1. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.
2. Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них.

В данном отчете (исследовании) авторы используют также словосочетание «нелегитимный доступ».

Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [ГОСТ Р 50922-2006, статья 2.6.6]

Правонарушение – неправомерное поведение, запрещенное законом под угрозой наступления ответственности общественно вредное или опасное деяние.

Выделяют: преступление (в рамках УК РФ и УПК РФ), административное правонарушение (в рамках КОАП РФ), налоговое правонарушение (в рамках НК РФ).

В отчетах (исследованиях) авторы используют понятие «правонарушение» как родовое (общее) по отношению к преступлению и административному правонарушению.

Привилегированный пользователь – к таким пользователям InfoWatch относит категории лиц, имеющие расширенные права доступа в информационные системы, полномочия по изменению конфигураций и назначения прав администраторов другим пользователям. К привилегированным пользователям относятся руководители различного уровня, системные администраторы, в некоторых случаях подрядчики и другие категории.

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации [ГОСТ Р 53114-2008, статья 3.3.11].

Разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору [98-ФЗ «О коммерческой тайне» п.9 ст.3]

Событие: Возникновение или наличие определенной совокупности обстоятельств [ГОСТ Р 53114-2008, статья 3.2.8].

Примечания:

1. Характер, вероятность и последствия события могут быть не полностью известны.
2. Событие может возникать один или несколько раз.
3. Вероятность, связанная с событием, может быть оценена.
4. Событие может состоять из невозникновения одного или нескольких обстоятельств.
5. Непредсказуемое событие иногда называют «инцидентом».
6. Событие, при котором не происходит никаких потерь, иногда называют предпосылкой к происшествию [инциденту], опасным состоянием, опасным стечением обстоятельств и т.д.

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками [ГОСТ Р 53114-2008, статья 3.3.10].

В данном отчете (исследовании) InfoWatch к категории «утечка информации» относится событие, когда в результате умышленных или неумышленных действий внутреннего или внешнего нарушителя обладатель информации ограниченного доступа (компания) утрачивает контроль над этой информацией.

Умышленная (злонамеренная) утечка информации – InfoWatch понимает под ней такую утечку, когда пользователь, работающий с информацией ограниченного доступа, предполагал возможные негативные последствия своих действий, осознавал их противоправный характер, был предупрежден об ответственности и действовал из корыстных побуждений, преследуя личную выгоду, или руководствовался иными мотивами (месть, зависть, личная неприязнь и т.д.). При этом в результате таких действий контроль над информацией со стороны ее обладателя был утрачен. При этом неважно, повлекли ли действия пользователя негативные последствия в действительности, равно как и то, понесла ли компания убытки, связанные с действиями пользователя. Также к умышленным утечкам относятся все утечки, спровоцированные хакерскими атаками или физическим доступом извне к носителям информации ограниченного доступа, принадлежащей компании.