Финансовые последствия утечек информации, 2020 год

© Экспертно-Аналитический центр InfoWatch. 2020 г.

Оглавление

Оглавление 2

Только факты 3

Сокращения 4

Аннотация 4

Методика 5

Результаты исследования 9

Заключение 20

Мониторинг утечек на сайте InfoWatch 25

Глоссарий 26

Только факты

- ✓ На **9,3%** выросло количество штрафов и компенсационных выплат за утечки персональных данных и платежной информации в мире
- ✓ **385** млн долларов США составила общая сумма штрафов и компенсаций за утечки в 2020 г.
- ✓ Максимальная сумма выплаты составила **117,5** млн долларов США, максимальная сумма штрафа – **80** млн долларов США.
- ✓ **3,26** млн долларов США – средняя сумма штрафа за 2020 г. в мире
- ✓ Более **1/3** всех штрафов за 2020 год назначено в странах Евросоюза
- ✓ Размер среднего штрафа в странах Евросоюза снизился почти в 15 раз и составил **93 тыс.** долларов США
- ✓ **4** штрафа за утечки назначены в России в 2020 году, суммы штрафов составили от 300,0 до 10,5 тыс. рублей
- ✓ **50%** штрафов в мире пришлись на хайтек-компании, здравоохранение и ритейл
- ✓ **0,86%** - на столько в среднем падает капитализация компании в первый день после утечки

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 InfoWatch второй год подряд выпускает отчет, в основу которого ложится исследование финансовых последствий инцидентов, связанных с утечками охраняемой законом информации (персональных данных, платежных, коммерческой тайны и др. конфиденциальной информации) для юридических лиц. В исследование не входят факты применения финансовых санкций по делам, связанным с разглашением государственной тайны, незаконной продажей информации и другой практикой в рамках уголовного законодательства[1].

Первая часть исследования посвящена штрафным санкциям и решениям о компенсациях за нарушения, связанные с утечками персональных данных и платежной информации из государственных и коммерческих организаций в глобальном масштабе.

Вторая часть исследования – поиск связи и закономерностей между финансовым состоянием организации, стоимостью её активов с официальными фактами утечек информации. Она представлена в таблице с динамикой курса акций публичных компаний (обществ, акции которых свободно обращаются на фондовом рынке), допустивших утечки информации. Выборка из 17 компаний, распределенных по отраслевым группам, позволяет проследить то, как менялись консолидированные биржевые показатели непосредственно после утечек, а также спустя неделю, месяц, три месяца, полгода и год.

Особенность собранных исходных данных в том, что мы видим только официально опубликованные факты и показатели, но не всегда есть сведения, позволяющие однозначно определить размер ущерба – часто они содержатся в составе разделов финансовой отчётности, включающих несколько показателей; также на курс акций влияют и другие факторы, которые одновременно могут повысить их стоимость, так что возможно говорить только о трендах, но не о точных расчётах.

В исследовании, в основном, рассмотрены европейские и американские компании в связи с тем, что рынки, на которых котируются их акции, довольно развиты и открыты. Применительно к российским компаниям задумано отдельное исследование. В связи с

[1] Планируем выпустить отдельное исследование

чем, данное исследование не претендует на исчерпывающий характер, однако позволяет получить представление о развитии практики регуляторного финансового воздействия на компании, допустившие нарушения в области защиты от утечек охраняемой законом информации, а также проследить влияние этих утечек на биржевые показатели.

Исследование, прежде всего, предназначено специалистам в области информационной безопасности, топ-менеджерам, собственникам бизнеса, финансистам, юристам в сфере защиты информации, специалистам по compliance-контролю, а также журналистам и лицам, интересующимся темами утечек информации, их последствий и влияния на финансовые показатели компаний.

Методика

Исследование проводится на основе собственной базы утечек ЭАЦ, регулярно пополняемой специалистами ЭАЦ с 2004 года. В базу попадают публичные сообщения[2] о случаях утечки информации из коммерческих, некоммерческих (государственных, муниципальных) организаций, госорганов.

В настоящий момент количество записей в базе превышает 19 800.

Исследования ЭАЦ в основном ориентированы на анализ сообщений об утечках данных на английском и русском языках, 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.

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[3] (если его оценила сама компания, допустившая утечку, или аналитические агентства),
- количество скомпрометированных записей (только для ПДн и платёжной информации),
- государство (страна),

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

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

- сфера деятельности обладателя информации (отрасль)[4],
- примерный размер пострадавшей от утечки организации (малая, средняя, крупная)[5],
- направление деятельности (коммерческая, некоммерческая),
- субъект[6], непосредственно допустивший утечку.

Далее каждое сообщение классифицируется по:

- наличию умысла[7] (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 неполная или противоречивая. При невозможности классифицировать сообщение (нельзя выявить вариант признака и отразить в базе, если в сообщении об утечке прямо или косвенно нет указания признака), в соответствующем поле проставляется значение «неизвестно». 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

---

[4] 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.

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

[6] 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.

[7] 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.

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.

В случаях, когда тип нарушителя неизвестен, и удельный вес таких неизвестных в выборке незначителен (как правило, менее 3%), авторы исследования также добавляют их к внешним нарушителям, т.к. подобная выборка соответствует данным, полученным при изучении аналогичных случаев.

Сообщения об утечках (единицы совокупности или элементы выборки) в базе ЭАЦ далее именуются 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 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 которой было скомпрометировано 10 млн и более записей. Отдельно могут исследоваться и 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.

В абсолютных показателях также представлены данные в виде так называемой «отраслевой карты утечек» — 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.[8] 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.

[8] 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

За 2020 г. Экспертно-аналитический центр ГК InfoWatch (ЭАЦ) на основе изучения открытых источников (сайты регуляторов, сайты компаний, сообщения СМИ и т.д.) выявил в мире 118 случаев назначения штрафов и компенсационных выплат за нарушения, связанные с утечками конфиденциальной информации из коммерческих компаний, некоммерческих организаций и органов власти.

По сравнению с 2019 г. количество выявленных штрафов и компенсаций выросло на 10 единиц (+9,3%).

Общая сумма штрафов и компенсаций составила около $385 млн. Это более чем в 15 раз меньше, чем в 2019 г., когда компании за утечки были оштрафованы в общей сложности на $5,913 млрд.

Здесь надо сделать важное отступление. В отчете о финансовых последствиях утечек за 2019 г. общая сумма штрафов составила $6,224 млрд. Во-первых, тогда мы подчеркивали, что она предварительная, так как включает штрафы, которые оспаривались компаниями-нарушителями. Речь шла об авиакомпании British Airways и сети отелей Marriott – обе структуры подали апелляции на решения британского информационного регулятора ICO. Осенью 2020 г. он вынес окончательный вердикт: сумма штрафа компании Marriott была сокращена более чем в 6 раз – с 99 млн до 14,4 млн британских фунтов, а British Airways удалось добиться снижения штрафа в 9 с лишним раз – со 184 млн до 20 млн британских фунтов. Во-вторых, в отчете отмечалось, что в предварительной сумме основную часть составил штраф компании Facebook - $5 млрд.

Таким образом, за вычетом оспоренных штрафов сумма за 2019 год составила 5,913 млрд долларов США, включая «мега-штраф» компании Facebook.

Общие суммы штрафов за утечки в 2018-2020 гг. (с учетом апелляций) представлены на Рисунке 1.

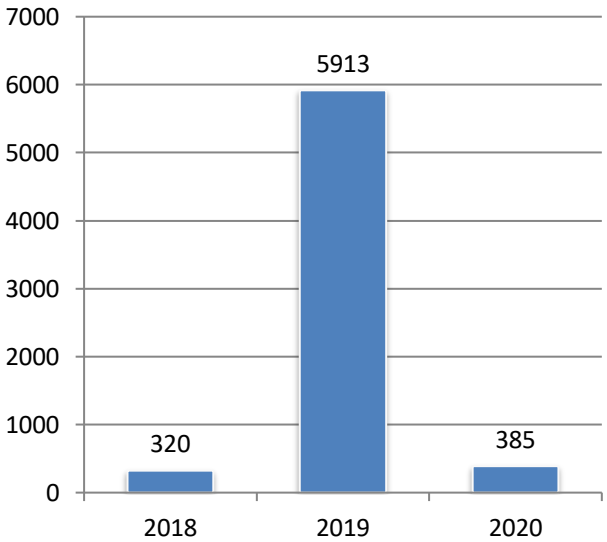


Рисунок 1. Общие суммы штрафов за утечки в 2018-2020 гг., млн $

Без учета «мега-штрафа» компании Facebook общая сумма штрафов уменьшилась в 2,37 раза.

По предварительным данным ЭАЦ InfoWatch, в 2020 г. общее число утечек в мире сократилось примерно на 5%, но на наш взгляд, это практически никак не отражается на динамике количества штрафов. К тому же, стоит отметить, что штрафы и компенсационные выплаты регуляторы за рубежом назначают не по «горячим следам», а после длительных расследований и судебных разбирательств, порой спустя несколько лет после появления информации об утечках.

Крупнейшие штрафы и компенсационные выплаты за утечки в 2020 году

- ✓ *$117,5 млн заплатит компания Yahoo! в рамках урегулирования претензий по коллективному иску 194 млн клиентов. Интернет-компания несет ответственность за серию потерь конфиденциальной информации пользователей в 2012-2016 гг.*
- ✓ *$80 млн – такой штраф наложен на финансовую компанию Capital One Управлением контролера денежного обращения – регулирующим органом министерства финансов США. В результате хакерской атаки на Capital One произошла утечка персональных данных около 106 млн клиентов.*
- ✓ *$39,5 млн – такую сумму выплатит американская страховая компания Anthem, чтобы удовлетворить требования по иску от ряда штатов. В конце 2014 – начале 2015 гг. страховщики потеряли медицинскую информацию и персональные данные примерно 79 млн клиентов.*
- ✓ *$30,5 млн потратит бюро кредитных историй Equifax в рамках удовлетворения требований по иску, поданному в суд штата Джорджия. Из этой суммы $5,5 млн будет направлено на компенсации, а $25 млн компании придется потратить на укрепление своей системы безопасности. Так Equifax расплачивается за утечку персональных данных более 140 млн американцев.*
- ✓ *$19,5 млн – столько Equifax выплатит за утечку по иску штата Индиана.*

Полный список крупных штрафов и компенсаций (в размере от 1 млн долларов США) смотрите в Приложении к отчету.

Более трети мировых штрафов выписали регуляторы стран Евросоюза

В 2020 г. ЭАЦ выявил сообщения о штрафах за утечки конфиденциальной информации из коммерческих компаний и государственных организаций **в 24 странах**: Великобритания, Венгрия, Гибралтар, Греция, Дания, Ирландия, Исландия, Испания, Италия, Канада, Кипр, Нидерланды (Голландия), Новая Зеландия, Норвегия,

Перу, Польша, Россия, Румыния, Сингапур, США, Турция, Франция, Швеция, Южная Корея.

В 2019 году количество стран, где были зафиксированы штрафы за утечки, составило **23**: Австралия, Австрия, Бельгия, Болгария, Бразилия, Великобритания, Венгрия, Германия, Нидерланды (Голландия), Греция, Испания, Италия, Мальта, Новая Зеландия, Норвегия, Польша, Россия, Румыния, Сингапур, США, Турция, Франция, Швеция.

Как и годом ранее, в 2020 г. лидерами по числу штрафов стали США и Сингапур –28 и 23 финансовых взыскания соответственно (Рисунок 2). В первую пятерку также вошли Румыния (11 штрафов), Италия (9 штрафов) и Соединенное Королевство Великобритании и Северной Ирландии (5 штрафов).

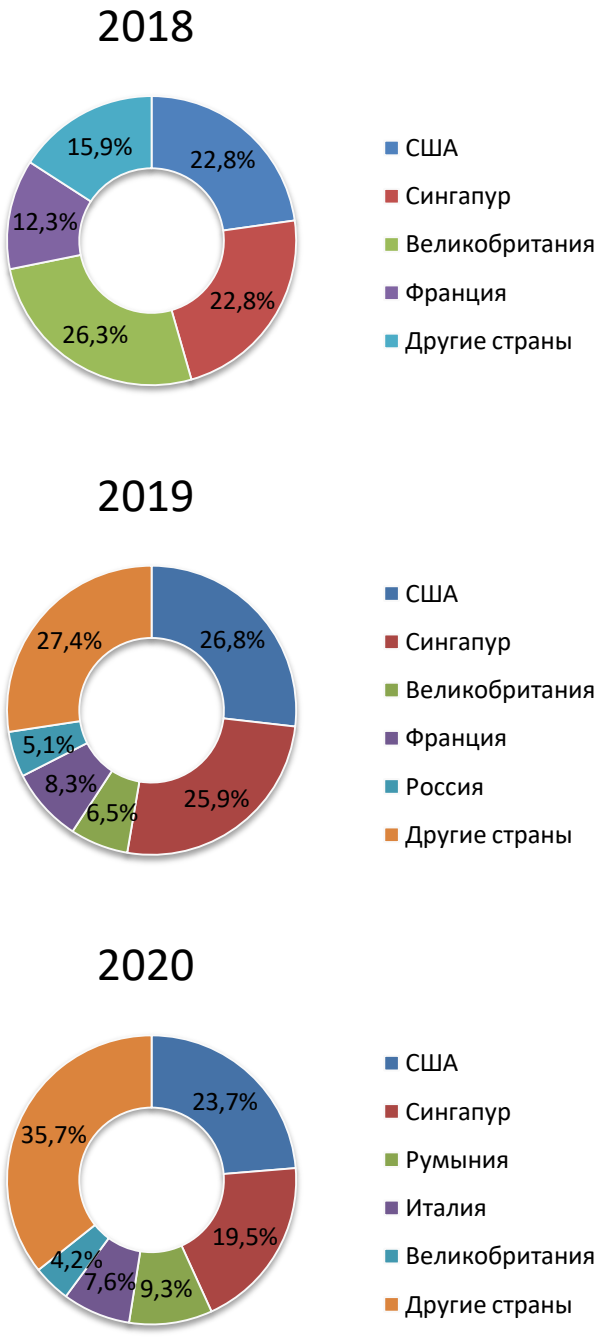


Рисунок 2. Распределение штрафов по странам 2018-2020 гг.

BBC: Британское Управление комиссара по информации (ICO) оштрафовало компанию Ticketmaster (занимается продажей билетов на мероприятия) на 1,25 млн фунтов (примерно $1,65 млн). Компания понесла наказание за то, что не смогла обеспечить безопасность данных своих клиентов. По данным ICO, были украдены персональные данные и платежная информация до 9 млн клиентов Ticketmaster из Европы.

DataGuidance: В Румынии национальный надзорный орган по обработке данных (ANSPDCP) объявил о решении оштрафовать автомобильного дилера Proleasing Motors более чем на 72 тыс. леев (15 тыс. евро). В результате

халатности компании был отмечен несанкционированный доступ к персональным данным 436 клиентов. Кроме того, ANSPDCP подчеркивает, что Proleasing Motors не смогла принять адекватные организационно-технические меры по защите данных.

Число штрафов, вынесенных регуляторами стран Евросоюза за утечки, составило 42 (35,6% от всех штрафов). Это на 6 штрафов больше, чем в 2019 г.

Самые высокие штрафы по-прежнему в США

Как и в предыдущие два года, первое место по размеру среднего штрафа занимают США. Если в 2018 г. он составил $23,3 млн, в 2019 г. уже $201,3 млн (а без учета мега-штрафа компании Facebook только $29,8 млн), то по итогам 2020 г. размер среднего штрафа «полегчал» примерно до $13 млн.

В мире средняя сумма штрафа в 2020 г. составила $3,26 млн. Это в 16,8 раза меньше, чем в 2019 г. (с учётом апелляций по штрафам British Airways и Marriott, а также с учетом мега-штрафа Facebook).

Если считать без учета мега-штрафа Facebook, но с учетом апелляций по штрафам British Airways и Marriott, то средняя сумма штрафа в 2020 г. по сравнению с 2019 г. снизилась в 2,6 раза (на 62%) – см. Рисунок 3.

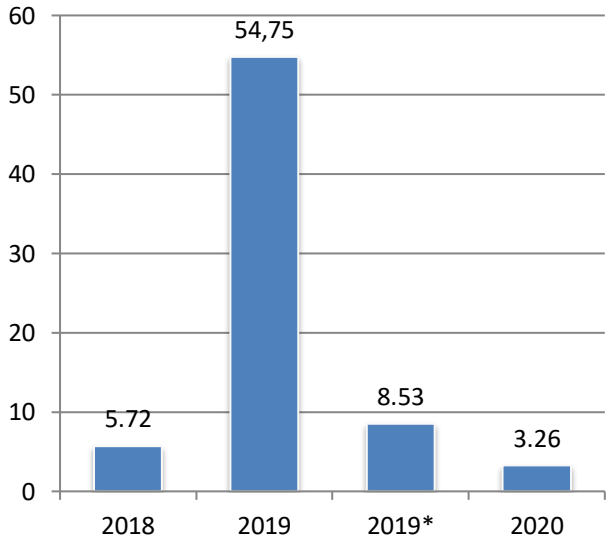


Рисунок 3. Средняя сумма штрафов за утечки в 2018-2020 гг., млн $

**Без учета штрафа компании Facebook в размере $5 млрд.*

Размеры средних штрафов и компенсаций по ряду стран представлены на Рисунке 4.

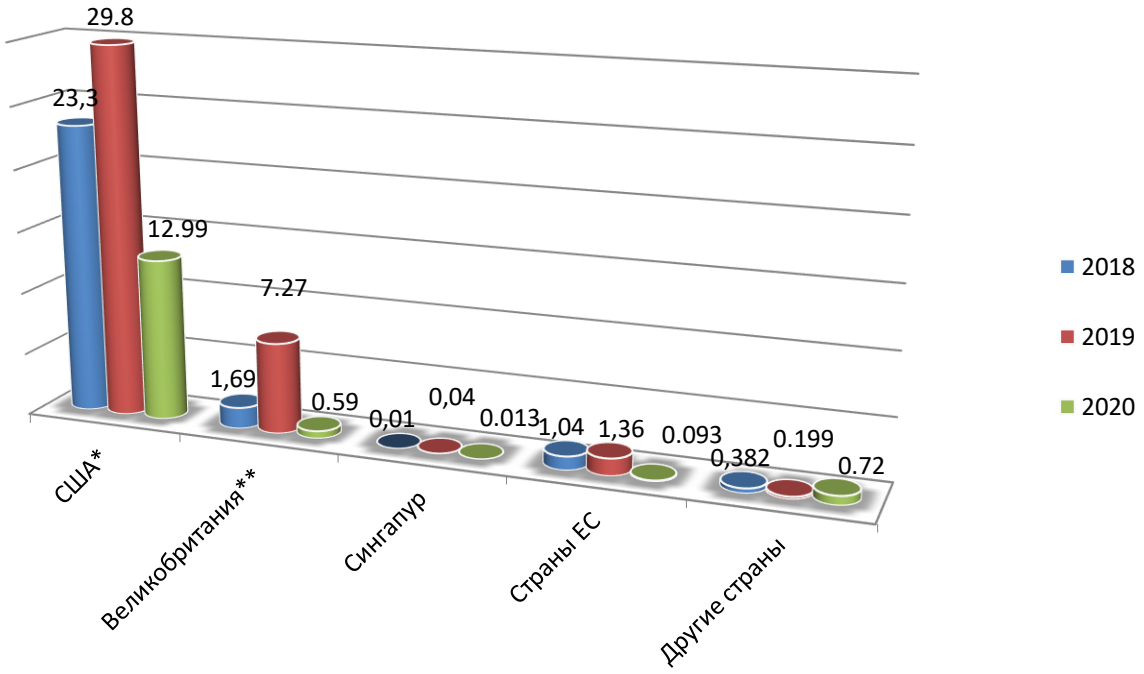


Рисунок 4. Средняя сумма штрафов в отдельных странах, млн $, 2020 г.

**Средний размер штрафа в США за 2019 г. без учета наказания Facebook ($5 млрд).*

***Средняя сумма штрафа в Великобритании за 2019 г. пересчитана с учетом принятых апелляций по делам British Airways и Marriott. Хотя официальный выход Великобритании из Евросоюза состоялся 1 февраля 2020 г., статистика по этой стране дана не в структуре ЕС, а отдельно за все три года.*

> *Health IT Security: Управление по гражданским правам министерства здравоохранения и социальных служб США (HHS OCR) решило на $2,3 млн оштрафовать медицинскую организацию CHSPSC. В ходе расследования выяснилось, что инцидент затронул в общей сложности 237 медицинских учреждений, входящих в состав CHSPSC. Хакерам удалось похитить данные 6,12 млн пациентов, включая такую информацию, как номера социального страхования (SSN), пол, даты рождения, контакты, этническая принадлежность и контакты в экстренных случаях.*

Размер среднего штрафа, выписанного надзорными органами Великобритании, снизился более чем в 12 раз и составил около $0,6 млн. В 2020 г. национальный информационный регулятор ICO не выписывал столь крупных штрафов, как годом ранее авиакомпании British Airways и сети отелей Marriott, что отразилось на снижении размера среднего штрафа.

В странах Евросоюза в 2020 г. средний штраф стал ниже почти в 15 раз и составил $93 тыс. Вероятно, регуляторы ЕС в период пандемии решили применять власть весьма деликатно и дозированно, полагая, что в сложные времена важен сам факт наказания, а не размер штрафа.

Более чем в три раза в прошлом году упал размер типичного штрафа в Сингапуре – до $13 тыс.

> *The Straits Times: Сингапурская бухгалтерская комиссия (SAC) оштрафована на 5 тыс. сингапурских долларов (около $3700). Сотрудник по ошибке вложил файл с персональными данными более 6500 участников программы повышения квалификации бухгалтеров в письмо, которое было отправлено 41 адресату.*
>
> *DataGuidance: Итальянский уполномоченный орган по защите данных (Garante) в июне 2020 г. принял решение наложить штраф в размере 600 тыс. евро (порядка $720 тыс.) на финансовую компанию UniCredit. В период с апреля 2016 г. по июль 2017 г. она допустила утечку персональных данных более 700 тыс. клиентов.*

Россия: четыре штрафа за утечки персональных данных

В ходе исследования в открытых источниках найдена информация о четырех штрафах российским компаниям и организациям за нарушения, которые можно отнести к утечкам персональных данных. Общая сумма штрафов составила 510,5 тыс. (примерно $6900).

В 2019 году было выявлено шесть штрафов за подобные нарушения на общую сумму 180,5 тыс. рублей (около $2800). То есть сумма штрафов выросла в 2,83 раза.

В 2018 году в России не было выявлено штрафов за утечку пользовательских данных.

В 2020 году российские суды вынесли решения о назначении штрафов по делам, возбужденным в отношении таких организаций, как одно из коллекторских агентств в Новосибирской области, ООО «Национальная служба взыскания», Центр немецкого языка при Волгоградском Социально-Педагогическом Университете, а также Центральная районная больница города Николаевск-на-Амуре. Посмотрим на каждую из них.

Таблица 1. Штрафы за утечки данных, выписанные в России в 2020 году

Нарушитель	Сфера деятельности	Истец Проверяющий	Суд	Нарушение (кратко)	Сумма штрафа, тыс. руб.	Сумма штрафа, долларов США[9]
Коллекторское агентство, г. Новосибирск	Финансы	ФССП	Арбитражный суд Кемеровской области	Нарушение правил сбора просроченной задолженности (повторно, 230-ФЗ)	300,0	4160,0
Национальная служба взыскания, г. Москва	Финансы	ФССП	Арбитражный суд Омской области	Нарушение требований 230-ФЗ (кредитор не вправе разглашать персональные	150,0	2080,0

[9] по средневзвешенному курсу за 2020 год – 72,14 рубля

				данные должника и информацию о его долге)		
Директор Центра немецкого языка при ВГСПУ, г. Волгоград	Образование	Роскомнадзор Прокуратор	мировой суд Центрального судебного района Волгоградской области	Трансграничная передача персональных данных (152-ФЗ)	50,0	690,0
Главный врач и Центральная районная больница, г. Николаевск-на-Амуре	Здравоохранение	Прокуратура	Прокуратура	Условия для неограниченного доступа неопределенного круга лиц к персональным данным (152-ФЗ)	10,5	150,0

«..., в феврале жительница Анжеро-Судженска взяла деньги в одной из микрофинансовых организаций, однако не смогла вовремя вернуть долг. К возврату компания привлекла коллекторское агентство. Спустя несколько дней женщина начала получать текстовые сообщения с угрозами: ей пообещали, что «начнут работать с её окружением», а звонки в течение дня будут получать абсолютно все друзья и знакомые, включая работодателя и его семью.

Впоследствии угрозы и жалобы действительно начали поступать друзьям и работодателю должницы — при том, что согласия на использование персональных данных никто из них не давал. Сама женщина получала до 25 звонков в день. Примечательно, что один из телефонных номеров, с которого поступали звонки и сообщения, был зарегистрирован на имя человека, скончавшегося ещё в 2016 году».

https://gazeta.a42.ru/lenta/news/99137-sud-oshtrafoval-kollektorov-ugrozhavshikh-zhitelnitse-kuzbassa-i-ee

«... коллекторы позвонили жене должника и сообщили ей имя и отчество мужчины, информацию о его долге, времени получения микрозайма, сумме просроченной задолженности. Действовали они по договору с микрофинансовой компанией «Займ Онлайн».

В итоге омские приставы составили на «Национальную службы взыскания» протокол о нарушении прав мужчины. Арбитражный суд Омской области на основании этого протокола оштрафовал компанию на 150 тыс. рублей. Коллекторы пытались оспорить это решение, упирая на то, что жена должника не возражала против телефонного разговора с представителями фирмы, однако этого довода для отмены решения было недостаточно».

https://www.omskinform.ru/news/140034

«Директор Центра немецкого языка … оштрафована на 50 тысяч рублей за нарушение правил обработки, хранения и передачи персональных данных. …
Поводом для судебного разбирательства послужило дело об административном нарушении, возбужденное Роскомнадзором по материалам проверки, проведенной Прокуратурой Центрального района Волгограда. По данным ведомства, Центр немецкого языка при Волгоградском Социально-Педагогическом Университете систематически собирал персональные данные волгоградцев – слушателей Центра и вопреки нормам действующего законодательства передавал их Немецкому культурному центру имени Гёте при германском посольстве, а также Гёте Институту в Мюнхене.
Переданные данные содержали фамилии, имена, даты и места рождения, адреса проживания, личные телефоны слушателей, а также их уровень языковой подготовки. Примечательно, что в большей части анкет, изъятых Прокуратурой в ходе проверочных мероприятий, целью изучения языка является переезд на постоянное место жительства в Германию.
В судебном заседании было установлено, что Центр не является самостоятельным юридическим лицом, а входит в структуру «ВГСПУ», которое в свою очередь, согласно уведомлению в Роскомнадзор, не занималось и не занимается трансграничной передачей персональных данных.
Суд, изучив все доводы, принял решение не применять максимальных санкций, ограничившись назначением штрафа в отношении директора Центра немецкого языка[10] *…».*

https://volgasib.ru/virtual/skandali-4p/tsentr-nemetskogo-yazyka-oshtrafovan-za-peredachu-personalnyh-dannyh-volgogradtsev-v-germaniyu/

«Установлено, что в феврале 2020 года экспертной комиссией Николаевской-на-Амуре центральной районной больницы принято решение об уничтожении медицинских карт, срок хранения которых истек. Вопреки требованиям федеральных законов "Об отходах производства и потребления", "О персональных данных" карты вынесли на контейнерную площадку по сбору мусора вблизи одного из жилых домов, доступ к картам был неограничен. …
Отмечается, что ранее прокурор вынес главврачу больницы представление. По результатам его рассмотрения нарушения устранены, виновные должностные лица привлечены к дисциплинарной ответственности.
… главврач и больница оштрафованы на общую сумму 10,5 тысячи рублей, три сотрудника получили выговор и предупреждение. Медицинские карты утилизированы.

https://ria.ru/20200629/1573605285.html

[10] Здесь штраф в итоге вынесли в отношении руководителя, но случай включен в исследование в связи с тем, касается функционирования организации в целом (системы), а не разового нарушения, которое могло быть и неумышленным, случайным.

То есть фактически мы видим, что первые две «утечки» - это переданная знакомым и родственникам пострадавших информация о том, что те взяли кредит и не выплачивают его. Фамилии и контакты знакомых могли быть получены из документов, заполненных при получении кредита (поручители), из открытых источников (социальные сети), с «чёрного рынка информации».

Из других сообщений, из обзоров судебной практики мы знаем, что коллекторов часто штрафуют за нарушение прав должника – за отправку сообщений и звонки чаще, чем разрешено законодательством. Но два примера из Сибирского региона показали, что коллекторские агентства могут быть привлечены к ответственности и за нарушение порядка обработки персональных данных, причём указанных в 230-ФЗ, не только на базе 152-ФЗ.

Другие две «утечки» совершены сотрудниками организаций, легально обрабатывавших персональные данные. В первом случае передача информации проводилась сознательно, как часть рабочего процесса Центра немецкого языка, и не важно в какой форме «утекли» данные (анкеты в бумажном виде, или в электронном - их сканы или данные в виде выгрузки из базы данных), так как мы понимаем, что она не связана с утерей контроля над обращением с информацией. Проблема лежит в юридической плоскости – руководство центра не изучило требования законодательства по защите персональных данных и не построило процессы соответствующим образом.

Во-втором случае сотрудники пренебрегли своими обязанностями и не утилизировали носители информации как положено.

В трёх из четырех случаев непосредственными виновными являются рядовые сотрудники, в одном руководитель.

Также в трех из четырех примерах налицо умышленные действия.

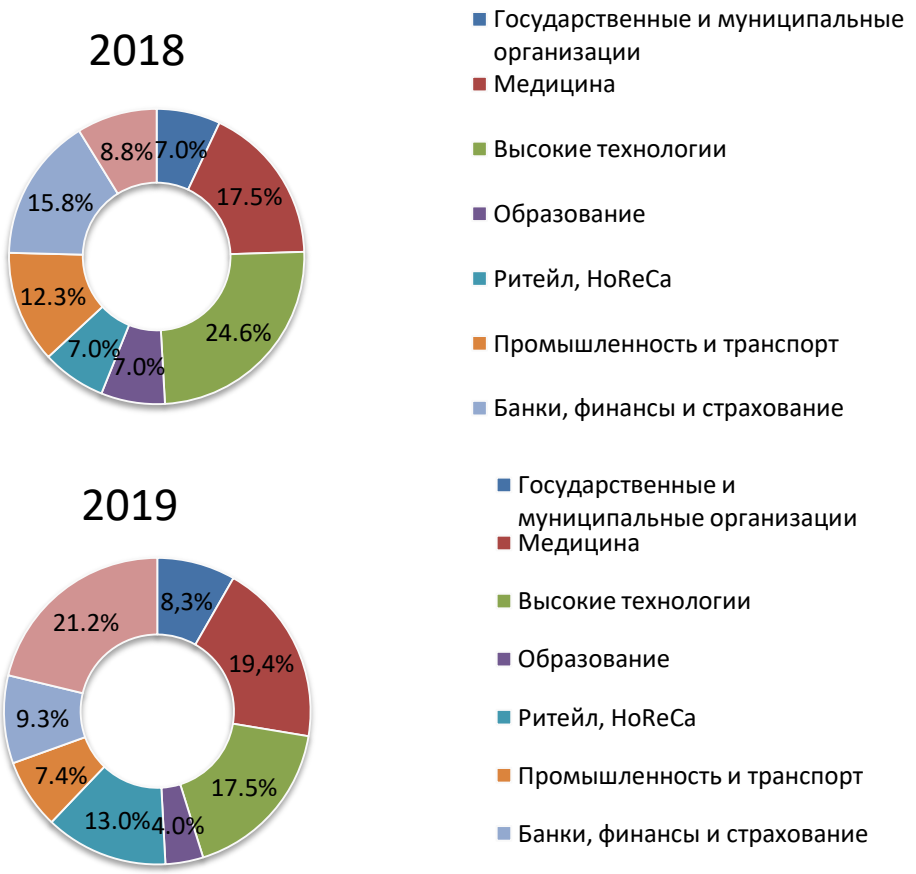
Интересно, что ни одна из «штрафных утечек» 2020 года не была компьютерной, хотя фактов утечек информации из организаций, находящихся в российской юрисдикции, известно довольно много, мы приводили в своих отчётах как статистику, так и примеры.

Когда текст этого отчета готовился к публикации, стало известно о первом штрафе в России за 2021 год. На этот раз наказана микрокредитная организация, умышленно разместившая в Сети данные клиента, допустившего просрочку платежей.

> *Ugra-News.ru: Сотрудники МФО «Хорошая история» из Югры прибегли к сомнительным методам, чтобы заставить клиента вернуть задолженность. Они выложили историю клиента с долгом и его персональные данные в Сеть. Рассмотрев материалы дела, Нижневартовский районный суд оштрафовал компанию «Хорошая история» на 20 тысяч рублей.*

В мире половина штрафов пришлись на сферы хайтека, здравоохранения и ритейла

Серьезных изменений в отраслевом распределении штрафов за 2020 год по сравнению с предыдущим годом не произошло, за исключением смены «лидера»: сфера медицины (включая медицинское страхование) уступила первенство по числу штрафов высокотехнологичной отрасли (хайтек, рисунок 5), которая вернулась на первое место после 2018 года.



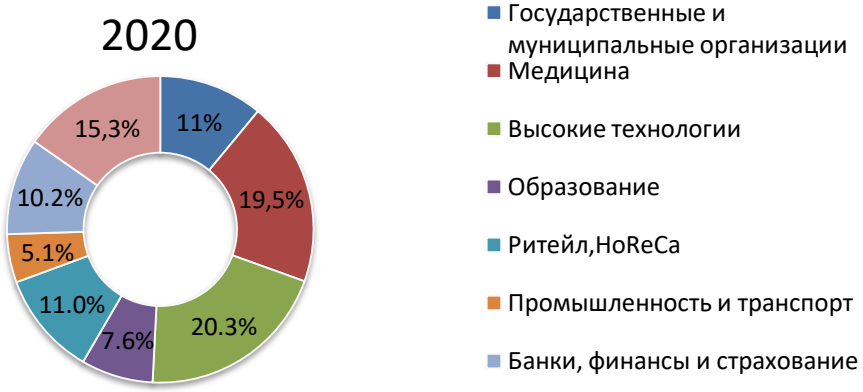


Рисунок 5. Распределение назначенных штрафов по отраслям, 2018-2020 гг.

CNBC: Ирландская комиссия по защите данных (DPC) 15 декабря решила оштрафовать сервис микроблогов Twitter на 450 тыс. евро (примерно $547 тыс.). Это первый случай, когда американская технологическая компания наказана за нарушение общеевропейского регламента по защите данных GDPR, действующего с 25 мая 2018 г. DPC пришла к выводу, что компания Twitter, европейская штаб-квартира которой располагается в ирландском Дублине, нарушила статью 33 (пункты 1 и 5) регламента, несвоевременно оповестив уполномоченные органы об утечке и не приняв должных мер для того, чтобы правильно задокументировать нарушение. Речь идет о проблеме с настройками аккаунтов пользователей с устройствами на базе ОС Android: некоторые закрытые твиты могли отображаться в открытом доступе.

DataBreaches.net: Клиника Athens Orthopedic согласилась выплатить $1,5 млн управлению по гражданским правам (OCR) Министерства здравоохранения и социальных сервисов США и принять план корректирующих действий для своей системы безопасности. Еще в 2016 г. хакер, используя учетные данные одного из подрядчиков, смог на протяжении месяца выкачивать персональные данные пациентов. Всего пострадали более 208 тыс. человек. Украдены такие данные, как имена пациентов, даты рождения, даты рождения, номера социального страхования, результаты медицинских исследований, а также информация о медстраховании.

Курс акций: после утечки компании в среднем теряют около 1% капитализации

В рамках подготовки отчета о финансовых последствиях утечек конфиденциальной информации отдельное исследование было посвящено влиянию утечек на формирование курса акций компаний. Для публичной компании любой инцидент, ставший достоянием общественности, чреват серьезными потерями на бирже. Настроение игроков на бирже может испортить как сам факт утечки, так и ее масштаб. Кроме того, важное значение для игроков на рынке акций имеет поведение самой компании, то, какие меры она принимает для ликвидации последствий инцидента.

Из базы InfoWatch были выбраны 17 утечек из крупных публичных компаний, случившихся в 2019 г. В результате каждой из этих утечек были скомпрометированы персональные и (или) платежные данные объемом от 1000 записей. В исследовании прослежена динамика курса акций компаний непосредственно после утечки (публичного сообщения об утечке со стороны компании, отраженного в СМИ), а также спустя неделю, месяц, три месяца, полгода и год после утечки (см. Таблицу 1).

Выяснилось, что в течение первого дня после появления информации об утечке курс акций в среднем падал на 0,86%. Но в течение недели компании не только отыгрывали падение, но и возвращались в плюс. Средний рост курса акций через 7 дней составлял более 1%. К концу первого месяца после утечки курс акций немного проседал по сравнению с котировками первой недели (+0,87% по сравнению с позициями до оглашения утечки). За три месяца допустившие утечку компании, в целом, укрепляли свои позиции, и консолидированный показатель роста достигал 3,16%. На протяжении следующих трех месяцев наблюдалось падение, в результате курс акций практически откатывался к исходным значениям. К концу первого года после обнародования факта утечки общее падение курса акций превышало 4%. Почти во всех рассмотренных случаях конец первого года после утечки пришелся на период пандемии, так что наиболее мощным фактором корректировки капитализации компаний стоит признать именно влияние на экономику распространения коронавирусной инфекции. Поэтому «гнет» утечек на этот период стал второстепенным фактором.

В целом, утечка конфиденциальных данных довольно негативно сказывается на биржевых котировках. В среднем в первые часы после объявления об инциденте падение выглядит небольшим, в пределах 1%, но нельзя забывать, что за этой цифрой для крупной компании стоит потеря многих десятков, а то и сотен миллионов долларов. В дальнейшем утечка, как правило, не лежит тяжким гнетом, и на формирование курса акций оказывают влияние другие факторы.

Посмотрим на динамику курса акций в отдельных отраслевых группах.

Наибольшее падение биржевых показателей сразу после утечек отмечено среди компаний сегментов «Ритейл&HoReCa», а также «Высокие технологии» (хайтек - телеком, ИТ) –на 2,29% и 2,02% соответственно.

Наименее восприимчива к утечкам сфера промышленности и транспорта – здесь даже после инцидента, связанного с компрометацией данных, акции в среднем выросли на 0,56%. Относительно устойчивой также можно признать финансовую сферу, потери участников которой в первые часы после утечки оказались довольно невелики – менее четверти процента.

В течение недели после утечки усугублялось положение только промышленности и транспорта. Три другие отраслевые группы демонстрировали рост, правда, участникам группы «Ритейл&HoReCa» не удалось выйти в плюс. А вот финансовые компании в целом демонстрировали рост почти на 4%, хайтек прибавлял 1,78%.

К концу первого месяца группа «Высокие технологии» еще немного подрастала на биржах, «Ритейл&HoReCa» практически полностью отыгрывала падение, а

«Промышленность и Транспорт» выходила в уверенный плюс. В то же время «Финансы и страхование» резко падали, общее снижение котировок в этой группе составляло 3,46%.

На горизонте трех месяцев финансовая сфера возвращалась к положительным значениям, хайтек падал, но удерживался в плюсе по сравнению с исходным курсом, промышленность демонстрировала рост на 6,58%. Однако по итогам трех месяцев существенно падала группа «Ритейл&HoReCa» - минус 2,58%.

Посмотрев на консолидированные отраслевые значения через полгода после утечек, отметим, что финансовая сфера демонстрировала огромное падение биржевых показателей (на 16,5% по сравнению с курсом, который предшествовал объявлению об утечке), сфера высоких технологий немного падала и уходила в минус. При этом ритейл существенно рос.

К концу первого года после сообщения об утечке падение курса акций финансовых компаний отражалось в целом драматически – их капитализация снижалась более чем на треть. Ритейл и промышленность также были в сильном минусе. Однако курс акций высокотехнологичных компаний вырастал на 13,31%.

Таблица 2. Динамика биржевого курса компаний после утечек

	Прошедшее после утечки время					
	1 день	**1 неделя**	**1 месяц**	**3 месяца**	**6 месяцев**	**1 год**
Консолидированное значение, %	**-0,86%**	**+1,05%**	**+0,87%**	**+3,16**	**+0,18%**	**-4,07%**
Финансы и страхование	-0,24%	+3,99%	-3,46%	+2,20%	-16,50%	-37,46%
Высокие технологии	-2,02%	+1,78%	+2,00%	+0,53%	-0,21%	+13,31%
Ритейл&HoReCa	-2,29%	-0,43%	-0,10%	-2,58%	+9,51%	-7,99%
Промышленность и транспорт	+0,56%	-1,47%	+0,60%	+6,58%	+3,85%	-3,58%

Заключение

Как мы и ожидали, в 2020 г. в мире выросло общее число штрафов и выплат по различным искам, связанным с утечками пользовательских данных. Традиционно самыми высокими штрафы за утечки остаются в США, хотя размер этих взысканий в прошлом году существенно упал.

Регуляторы стран ЕС, опираясь на положения вступившего в силу в 2018 г. регламента GDPR, в 2020 г. большая часть которого была связана с экономическими трудностями вследствие объявленной пандемии, продолжили методично штрафовать компании, допустившие утечки. Также напомним, что GDPR включает широкий спектр положений, связанных со сбором, обработкой, хранением и передачей персональных данных. По данным ЭАЦ InfoWatch, за различные нарушения регламента регуляторами стран ЕС в 2020 г. были наложены 327 штрафов, причем только 42 из них (менее 13%), как было отмечено выше, выписаны за нарушения, связанные с утечками ПДн. При этом, судя по размерам выписанных штрафов, в период распространения COVID-19, регуляторы решили, что в такое время важен сам факт наказания за допущенное нарушение, а не размер взыскания.

На наш взгляд, в ближайшее время мега-штрафы (в размере десятков и сотен миллионов долларов) в основном будут выписываться регуляторами США и только за резонансные утечки, то есть те, при которых могут быть потеряны миллионы записей пользовательских данных, при этом отягчающими факторами будут выступать длительное сокрытие фактов утечек и недостаточное внимание компаний к контуру кибербезопасности.

В России опубликованы данные только о четырёх штрафах за утечки (3,4% от общего количества), причём все они назначены не за компьютерные преступления, а связаны с неправомерным обращением с персональными данными.

В 2021 году, прежде всего, стоит ожидать расширения географии штрафов за утечки. Это связано с тем, что регуляторы в сфере защиты информации во многих странах постепенно совершенствуют законодательство, исходя из новых реалий, и встают на путь методичной защиты пользовательских данных как основного компонента цифровой личности.

В России следует ожидать появления штрафов, связанных с обеспечением безопасности значимых объектов критической информационной инфраструктуры (не утечки). Также будет интересно рассмотреть правоприменительную практику и её влияние на финансовое состояние организаций.

Утечка конфиденциальной информации, прежде всего большого объема пользовательских данных, - важный катализатор для формирования курса акций компании. Капитализация крупной компании, допустившей утечку, может упасть на десятки, а то и сотни миллионов долларов в первый день после сообщения об инциденте.

На сегодня можно достаточно уверенно говорить о том, что утечка оказывает сильное влияние на уровень капитализации компании в краткосрочной перспективе, то есть в

первые дни после сообщения об инциденте. В дальнейшем на формирование курса акций влияют другие факторы. Полагаем, что выявление фактов утечек со временем станет оказывать еще большее влияние на курс акций компаний, причем не только в краткосрочной перспективе. Для биржевых игроков значение будет иметь то, как компания реагирует на утечку, что она предпринимает для смягчения ее последствий, как она укрепляет свою систему безопасности и каким образом выстраивает отношения с пострадавшими клиентами. Для получения новых выводов необходимо провести исследование на основе более широкой выборки, когда накопятся дополнительные данные.

Приложение

Таблица 3. Компенсационные выплаты и штрафы за утечки, в размере от 1 млн долларов США, 2020 г.

№	Компания	В какой стране оштрафована	Сумма штрафа или выплаты, в млн $
1	Yahoo	США	117,5
2	Capital One	США	80
3	Anthem	США	39,5
4	Equifax	США (Джорджия)	30,5
5	Equfax	США (Индиана)	19,5
6	Equifax	США (Массачусетс)	18,2
7	Home Depot	США	17,5
8	Google	США	7,5
9	Premera Blue Cross	США	6,85
10	Facebook	Канада	6,5
11	Facebook	Южная Корея	6
12	Community Health System	США	5
13	Kalispell Regional Healthcare	США	4,2

14	UnityPoint	США	2,8
15	Sabre	США	2,4
16	SHSPSC	США	2,3
17	CafePress	США	2
18	Ticketmaster	Великобритания	1,65
19	Intercontinental	США	1,5
20	Athens Orthopedic Clinic	США	1,5
21	Lifespan	США	1,04
22	American Home Patient	США	1
23	Aetna	США	1

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 неизвестных) – 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.