Утечки информации ограниченного доступа:
отчет за 9 месяцев 2020 г.

Оглавление

Только факты

- ✓ За 9 месяцев 2020 года в мире зарегистрировано на **7,4%** меньше утечек, чем за аналогичный период прошлого года. В России за тот же период число утечек, наоборот, выросло на **5,6%**.
- ✓ В январе-сентябре 2020 г. в мире «утекло» **9,93** млрд записей ПДн и платежной информации , из них **96,5** млн - в России.
- ✓ В сумме более **15%** утечек в глобальном масштабе связаны с компрометацией платежных данных и коммерческой тайны. В России эта доля вдвое ниже.
- ✓ В мире **52,6%** случаев утечек спровоцированы внешним воздействием, но в России – в пределах **21%**, так как более **79%** утечек случились в результате внутренних нарушений.
- ✓ Если в мире чуть больше половины нарушений внутреннего характера признаны умышленными, то в России таких нарушений более **3/4**.
- ✓ В России доля утечек по вине сотрудников вдвое выше, чем в мире, - более **72%**.
- ✓ Доля утечек, сопряженных с мошенническими действиями, в России превышает **10%**, в мире она втрое ниже.
- ✓ Каждый **шестой** случай компрометации конфиденциальных данных в России происходит через мессенджеры.
- ✓ Более **40%** зарегистрированных утечек в России приходится на хайтек-индустрию и финансовый сектор – **21,9%** и **18,9%** случаев соответственно.
- ✓ В глобальном распределении по отраслям на первом месте находится сектор высоких технологий (хайтек) с долей **19,4%**, на втором месте здравоохранение – **16,4%**.

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 (далее ЭАЦ) представляет исследование случаев утечек информации ограниченного доступа, зарегистрированных в течение I-III кварталов 2020 г. Значительная часть утечек имеет временной лаг: информация о них стала достоянием общественности спустя несколько месяцев, а то и год-два после самих инцидентов, однако с полной уверенностью можно сказать, что на общий ландшафт нарушений большое воздействие оказала пандемия COVID-19. Она спровоцировала целый ряд изменений в самых разных сферах, в том числе в сфере безопасности информации.

Напомним, что по утечкам в первом полугодии 2020 г., связанным с данными о больных COVID-19, был подготовлен отдельный отчёт. Цель данного исследования – представить предварительную картину по утечкам, включенным в базу инцидентов ЭАЦ InfoWatch за исследуемый период.

Авторы отчета уверены, что результаты исследования будут интересны специалистам в области информационной и экономической безопасности, журналистам, собственникам и высшему менеджменту компаний, которые работают с информацией ограниченного доступа (например, сведениями, составляющими коммерческую, банковскую, налоговую тайну), а также всем, кто активно пользуется услугами в этой сфере, особенно с учётом ряда изменений, начиная с этого года.

Методика

Исследование проводится на основе собственной базы утечек ЭАЦ, регулярно пополняемой специалистами ЭАЦ с 2004 года. В базу попадают публичные сообщения[1] о случаях утечки информации из коммерческих, некоммерческих (государственных, муниципальных) организаций, госорганов.

В настоящий момент количество записей в базе превышает 19 000.

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.

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[2] (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)[3],
- примерный размер пострадавшей от утечки организации (малая, средняя, крупная)[4],
- направление деятельности (коммерческая, некоммерческая),
- субъект[5], непосредственно допустивший утечку.

---

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

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

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

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

Далее каждое сообщение классифицируется по:

- наличию умысла[6] (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 (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.

В базу также попадают случаи, когда невозможно установить обладателя скомпрометированной информации, но 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

---

[5] 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.

[6] 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. это 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 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. Отдельно также 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.

В абсолютных показателях также 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.[7] Такой подход позволяет проиллюстрировать динамические изменения отдельных показателей , приходящихся на утечки и обладающих определенным признаком (признаками) более ярко, т.е. решает исключительно презентационные задачи. Но в случаях, когда доля утечек с признаком, классифицированным как «неизвестный», превышает 5%, представляются отдельные диаграммы.

[7] 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 первые 9 месяцев 2020 года в базу Экспертно-аналитического центра InfoWatch внесено 1773 случая утечки информации ограниченного доступа из коммерческих компаний, государственных организаций и органов власти во всем мире.

В результате зарегистрированных случаев «утекло» 9,93 млрд записей персональных (ПДн) и платежных данных. По сравнению с аналогичным периодом 2019 г. в целом (в мире) число утечек снизилось на 7,4%, а число скомпрометированных записей – на 1,4%.

За тот же период в России зафиксировано 302 утечки, что на 5,6% больше, чем за 9 месяцев 2019 г. Но количество «утекших» записей ПДн и платёжной информации уменьшилось на 29,2% по сравнению с аналогичным периодом 2019 года (69,5 млн. записей).

Изменение числа утечек и скомпрометированных записей отражено на Рисунках 1-2.

Снижение числа зарегистрированных (ставших известными) утечек в мире главным образом можно объяснить влиянием пандемии коронавируса на бизнес и госсектор: в результате спешной перестройки процессов и перевода значительной доли сотрудников на удаленную работу контроль над информационными активами во многих компаниях мог быть ослаблен, а значительная часть инцидентов перестала фиксироваться.

В то же время в России рост числа выявляемых утечек продолжился даже несмотря на пандемию, что возможно сопоставить со скачкообразным ростом числа заявок на приобретение или «пилотирование» продуктов для контроля утечек и мониторинга действий работников.

Существенное, более чем на четверть, снижение числа скомпрометированных записей в России также не должно вводить в заблуждение – в 2019 г. львиная доля записей – порядка 90 млн – утекла из хранилищ оператора фискальных данных «Дримкас». За 9 месяцев 2020 г. столь масштабных утечек не выявлено. В то же время стало намного больше относительно крупных инцидентов, в результате каждого из которых утекало от 1 млн записей ПДн и платежной информации. Если в январе-сентябре 2019 г. их было зафиксировано шесть, то за 9 месяцев 2020 г. - пятнадцать.

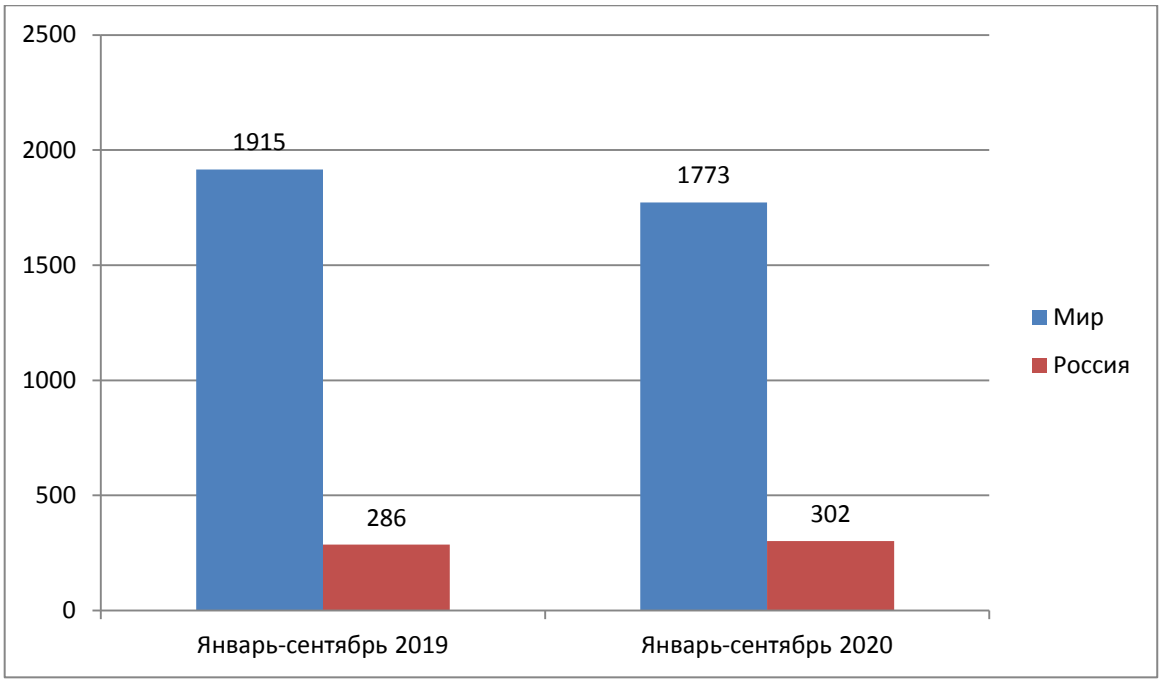

Рисунок 1. Число зарегистрированных утечек: Россия-Мир, январь-сентябрь 2019 г. и январь-сентябрь 2020 г.

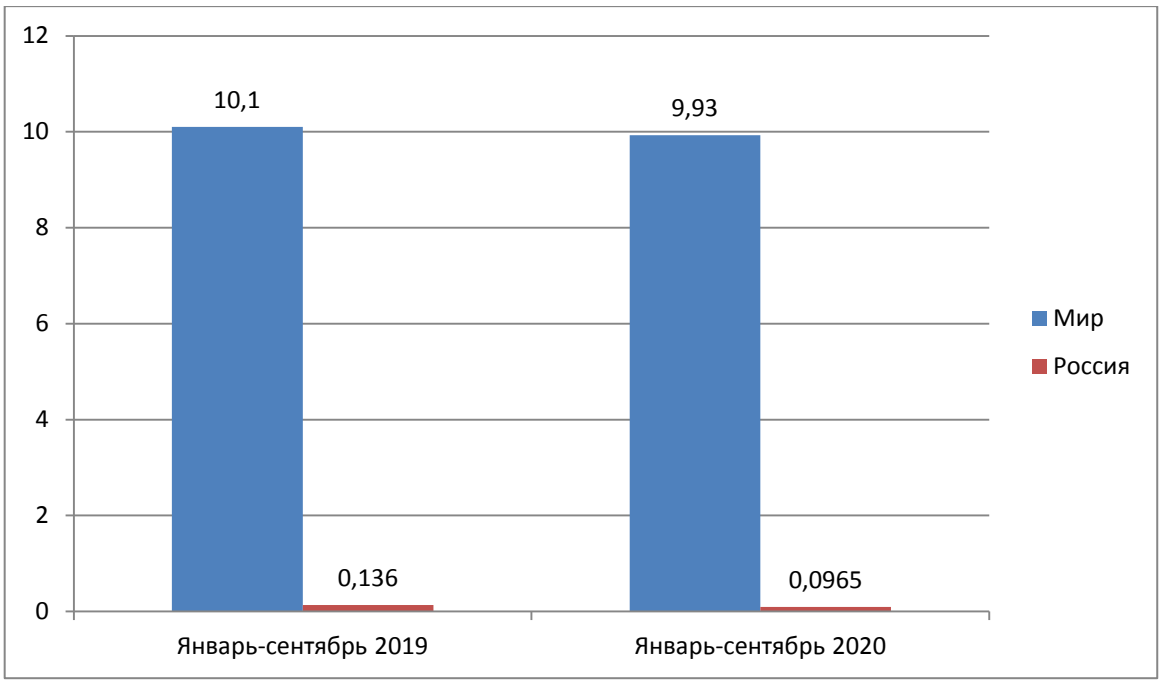

Рисунок 2. Число скомпрометированных записей ПДн и платежной информации в результате утечек: Россия-Мир, январь-сентябрь 2019 г. и январь-сентябрь 2020 г., млрд

Bleeping Computer: Киберпреступники из группировки ShinyHunters взломали популярное сообщество Wattpad, объединяющее авторов и любителей книг. По данным компании Cyble, сведения более 270 млн подписчиков Wattpad предлагались в Даркнете за 10 биткойнов (почти $100 тыс.), но через некоторое время стали распространяться бесплатно. Образцы данных

содержали имена пользователей, реальные имена, хэшированные пароли, адреса электронной почты и географические координаты.

Ведомости: В интернет утекла база программы лояльности сети «Красное и белое». В документе содержатся записи о 17 млн человек, якобы имеющих карты лояльности этой сети. В базе есть их фамилия, имя, отчество, дата рождения и номер телефона.

Таким образом, средняя «мощность» одной утечки (число утекших записей на один зарегистрированный инцидент в среднем) по итогам 9 месяцев 2020 г. составила 5,7 млн записей в глобальном масштабе и 0,32 млн в России. Разрыв почти в 18 раз, во-первых, обусловлен тем, что в нашей стране пока не так много компаний и государственных служб, которые оперируют огромными базами, с десятками миллионов записей ПДн. Во-вторых, в России пока лишь формируется рынок больших данных, который практически неизбежно будет сопровождаться теневой частью. Как следствие, в ходу у преступников пока лишь действительно ликвидная информация – те данные, из которых можно извлечь быструю выгоду (например, оформив кредит), а это всегда отдельные записи, но не дампы мегахранилищ. В-третьих, крупнейшие банки, телеком, ритейл, госорганы, – то есть, те, кто накопил обширные базы данных клиентов и граждан, – вероятно, обладают достаточно устойчивыми системами защиты от кибератак и в ряде случаев не подключены к сети Интернет.

В мире сложился перевес в пользу внешних злоумышленников, в России же подавляющее большинство утечек имеют внутренний вектор (Рисунок 3). При этом стоит отметить, что доля нарушений внешнего характера в нашей стране растет второй год подряд и впервые превысила 20%.

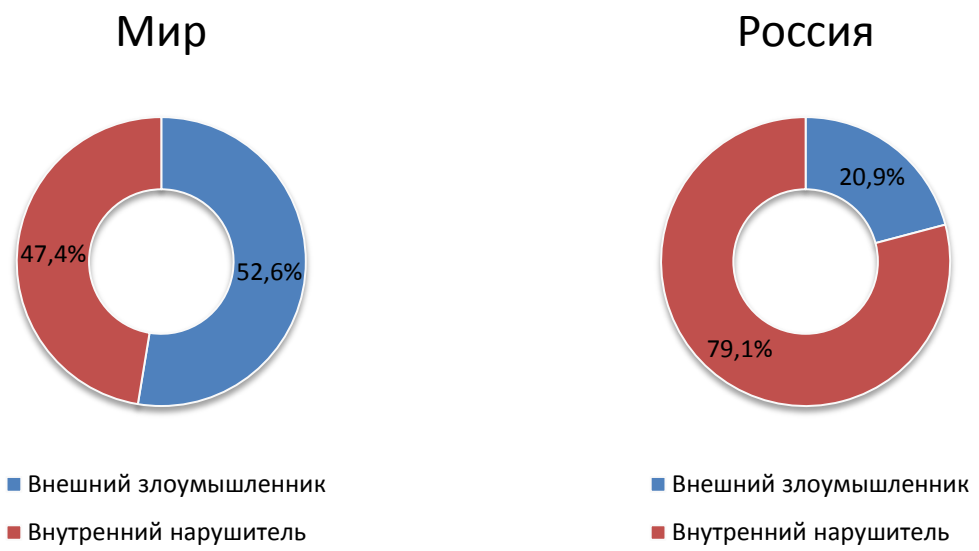

Рисунок 3. Распределение утечек по вектору воздействия: Россия - Мир, январь-сентябрь 2020 г.

IT Web: Южноафриканский Postbank сообщил, что заменит карты 12 миллионам получателей социальных выплат и владельцев счетов,

пострадавшим в результате серьезного нарушения. Инцидент носил внутренний характер. Неназванные сотрудники смогли скопировать мастер-ключ – основной электронный идентификатор. Известно, что мастер-ключ, содержащий 36-значный код, позволяет любому открыть беспрепятственный доступ к банковским системам и получать информацию об остатках на счетах, осуществлять списания денежных средств, а также изменять данные на любой из 12 млн действующих карт, эмитированных Postbank.

tkgorod.ru: В Братске осудили сотрудника банка, который похищал средства со счетов клиентов. Мужчину обвиняли в незаконном получении и разглашении сведений, представляющих банковскую тайну, а также в мошенничестве с причинением значительного ущерба и кражах средств с банковских счетов. Всего обвиняемому инкриминировалось больше десятка преступлений. Суд признал обвиняемого виновным и приговорил его к лишению свободы сроком на 3 года и 6 месяцев. Наказание назначено условно с испытательным сроком 4 года.

Традиционно уровень ликвидности данных для внутреннего нарушителя мы определяем по уровню умышленных утечек конфиденциальных данных: чем больше ценность данных, ради которых инсайдеры готовы пойти на преступления, тем более высоким оказывается процент инцидентов умышленного характера. При этом ни в коем случае нельзя забывать об опасности, которую несут случайные нарушения, вызванные некорректно настроенными серверами с базами данных, отправкой информации по неправильным адресам, потерей оборудования с данными, неправильной утилизацией бумажных документов и т.д. В ряде случаев подобные утечки могут представлять б**о**льшую угрозу для бизнеса компании и конфиденциальности ее клиентов, чем хакерские атаки и другие действия извне в отношении информационных активов. На Рисунке 4 представлено распределение утечек внутреннего характера по умыслу.

В мире доля умышленных нарушений, совершенных персоналом и руководителями компаний, составляет немногим более половины от всех случаев внутренних утечек, тогда как в России 77%. Такое соотношение, предположительно, связано с высоким уровнем выявления фактов внутренних утечек и попыток кражи конфиденциальных данных в России, прежде всего в банках и в госорганах, в том числе за счёт наличия средств контроля. В то же время во многих странах, прежде всего на Западе, DLP-системы имеют ряд ограничений по контролю каналов передачи информации, корпоративные политики ИБ «заточены» на противодействие внешним угрозам, а регуляторы строго наказывают компании за сокрытие фактов утечек в результате хакерских атак. Но даже при таком положении в некоторых случаях утечки по вине внутренних нарушителей зарубежным компаниям проще списать на вторжение извне. Это может быть выгоднее с точки зрения имиджа и позволяет избежать пристального внимания правоохранительных органов.

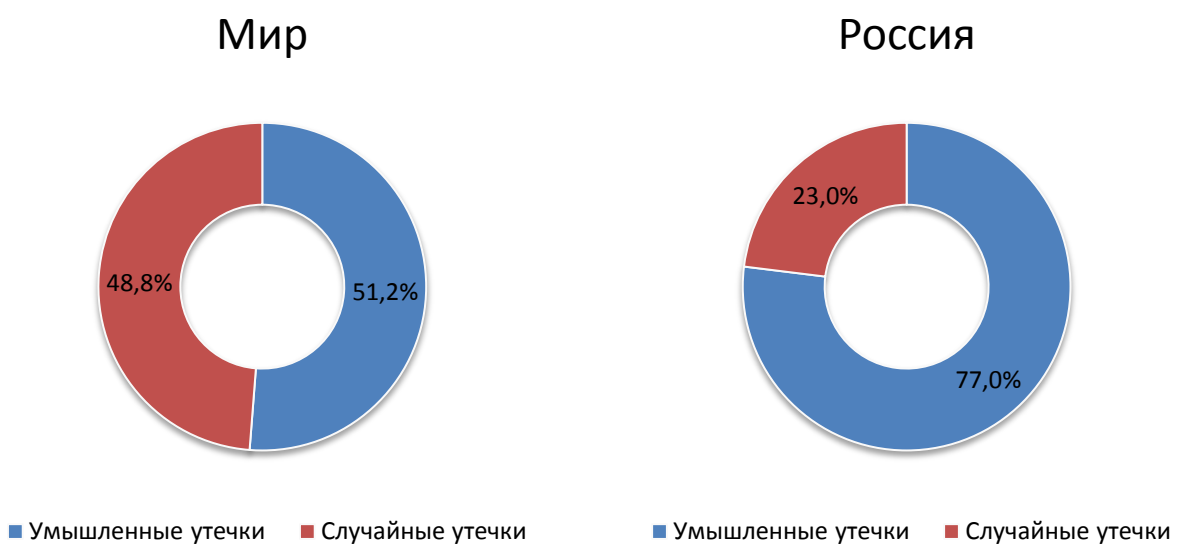

Рисунок 4. Распределение утечек внутреннего характера по умыслу: Россия - Мир, январь-сентябрь 2020 г.

> *The Washington Post: Еврейская федерация агломерации Вашингтона (The Jewish Federation of Greater Washington) сообщила о взломе, в результате которого благотворительный фонд лишился крупной денежной суммы – порядка $7,5 млн. Первоначальный вектор хакерской атаки был направлен на сотрудника, работающего удаленно.*[8]
>
> *56orb: Сотрудник оренбургского офиса одного из крупных операторов мобильной связи скопировал для личного пользования персональные данные абонентов. Позже, оставшись без стабильного заработка, оренбуржец решил использовать эту конфиденциальную информацию в корыстных целях. Он отправлял сообщения на номер обслуживания клиентов одного из банков и узнавал о состоянии счетов потерпевших. Если сумма оказывалась внушительной, он переводил чужие деньги на подконтрольные ему абонентские номера, зарегистрированные на вымышленных людей. Все похищенные деньги он конвертировал в криптовалюту. В результате оренбуржец обокрал 58 человек на общую сумму свыше 450 тысяч рублей.*

Как в мире, так и в России более 80% случаев утечки конфиденциальной информации связаны с кражами или непредумышленным раскрытием персональных данных (Рисунок 5). При этом в мире существенно выше доля утечек коммерческой тайны, что связано с критически важным значением этого типа информации для многих компаний, прежде всего на Западе, и новым витком конкурентной войны Китая и США. Также в мире выявлена более высокая доля утечек платежных данных, чем в России. Полагаем, что такой разрыв связан с успехами нашей страны в развитии финансовых

[8] В результате взлома почты злоумышленник получает доступ к корпоративным и персональным данным, содержащимся в переписке, которые затем использует для проведения атак на другие ресурсы.

сервисов за последние годы. Судя по всему, рост направления подкрепляется мероприятиями по защите платежной инфраструктуры.

Рисунок 5. Распределение утечек по типам данных: Россия – Мир, январь-сентябрь 2020 г.

> *ZDNet: На хакерском форуме Joker Stash выставлена на продажу база платежной информации, украденная из компании Wawa, крупной сети магазинов и автозаправочных станций на восточном побережье США. Скомпрометированы такие данные, как номера карт, сроки истечения действия. Анализ утекшего набора данных показал, что в руках хакеров оказалась информация о картах 30 млн граждан США из порядка 40 штатов, а также порядка миллиона карточных сведений иностранцев, представляющих более 100 стран.*
>
> *SecurutyLab.ru: В открытом доступе оказалась база данных пользователей сервиса online-бронирования трансферов «Киви-такси». База данных содержит более 330 тыс. записей с информацией о клиентах и сотрудниках службы, включая имена и фамилии, адреса электронной почты, номера телефонов, должность (для сотрудников сервиса и некоторых других записей), а также хеши паролей (SHA2-512 и SHA1) и соль для хеширования. Вероятно, неизвестные скопировали эти данные с сервера MongoDB, оставленного службой такси без защиты.*

Интересное распределение получилось среди виновников утечек. В мире вдвое выше, чем в России, доля утечек по вине хакеров и неизвестных лиц (внешний нарушитель). Соответственно, в нашей стране превалируют нарушения в результате действий

персонала (непривилегированных пользователей, относящихся к внутренним нарушителям) - см. Рисунок 6.

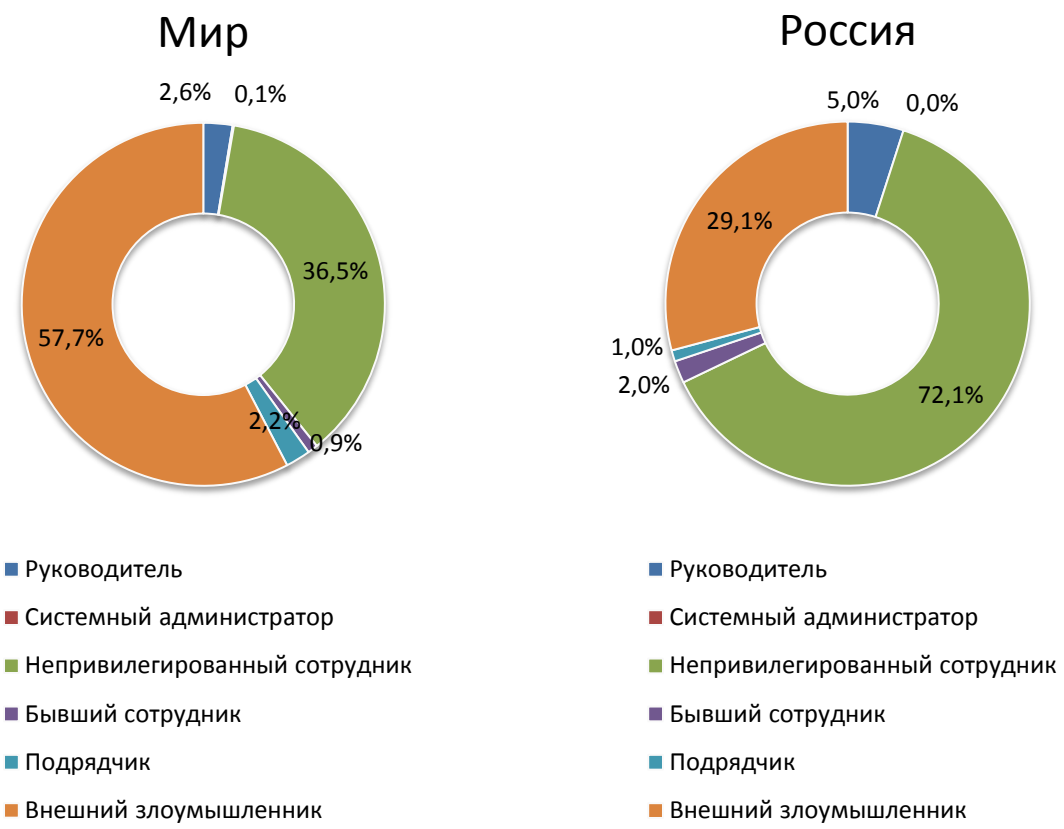

Рисунок 6. Распределение утечек по виновнику, Россия – Мир, январь-сентябрь 2020 г.

Bleeping Computer: Известный учебный центр SANS Institute пострадал от утечки. В SANS подчеркивают, что вектором атаки стало фишинговое письмо, открытое одним из менеджеров. Известно, что злоумышленник, получив доступ к аккаунту сотрудника SANS, поменял настройки, в результате чего вся электронная почта стала автоматически перенаправляться на неизвестный внешний адрес e-mail. Кроме того, хакер установил вредоносное расширение программы Office 365. В общей сложности киберпреступнику удалось перенаправить на внешний адрес 513 электронных писем, в которых содержались персональные данные более 28 тыс. участников SANS. В частности, похищены электронные адреса, полные имена, номера телефонов, должности, названия компаний и адреса.

КоммерсантЪ: В Москве возбуждено уголовное дело в отношении полицейских, которые, по версии следствия, незаконно распространяли сведения о гражданах, полученные из системы распознавания лиц. Интересно, что одной из предполагаемых жертв преступления стала волонтер «Роскомсвободы» Анна Кузнецова, которая ранее подавала иск к столичному главку МВД и Департаменту информационных технологий Москвы с требованием остановить работу уличной системы распознавания.

В России втрое выше доля утечек, сопряженных с мошенническими действиями (см. Рисунок 7). Это значит, что нарушители, прежде всего внутренние, по-прежнему имеют много лазеек, чтобы воспользоваться похищенной из корпоративного контура информацией для извлечения прямой выгоды.

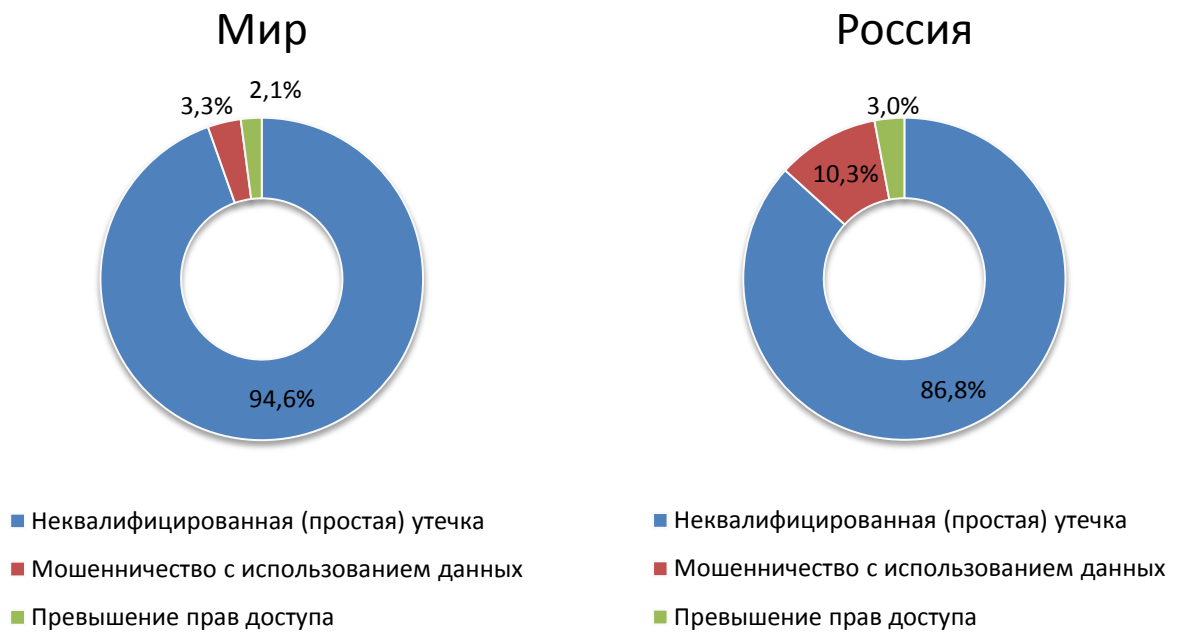

Рисунок 7. Распределение инцидентов по характеру: Россия - Мир, январь-сентябрь 2020 г.

> *TechTheLead: Хакеры взломали правительственную базу Тайваня и похитили персональные данные более 20 млн граждан. Добычей хакеров стал полный реестр прописки резидентов Тайваня – всего более 20 млн записей. Размер предлагаемого на подпольном форуме архива составляет 3,5 ГБ. В него включены полные имена, домашние адреса, идентификационные номера, даты рождения и номера телефонов граждан.*
>
> *ТАСС: Столичные полицейские задержали четверых мужчин, которые подозреваются в мошенничестве в сфере страхования. Незаконно завладев персональными данными клиентов одной из страховых компаний, они проводили фиктивные экспертизы и оформляли документы на возмещение ущерба. Установлено, что подозреваемые оформили более 500 выплат по поддельным документам на общую сумму более 100 млн рублей.*

Основным каналом утечек остается Сеть (Рисунок 8). На диаграмме обращает на себя внимание то, что в России популярным каналом в период пандемии стали популярные мессенджеры и другие сервисы мгновенных сообщений. Очевидно, что контроль IM-приложений требует повышенного внимания со стороны служб безопасности. Также в России довольно высокой остается доля утечек через бумажную документацию – несмотря на бурное развитие электронного документооборота в последнее время, значительная часть данных по-прежнему хранится и передается на бумажных носителях. Многие российские компании при этом пренебрегают правилами

утилизации бумажных носителей информации. В то же время в нашей стране стало исчезающе мало утечек по электронной почте. Судя по всему, этот канал довольно хорошо контролируется коммерческим сектором и государственными органами, а злонамеренные нарушители, зная об установленных системах защиты e-mail, ищут другие способы слива информации.

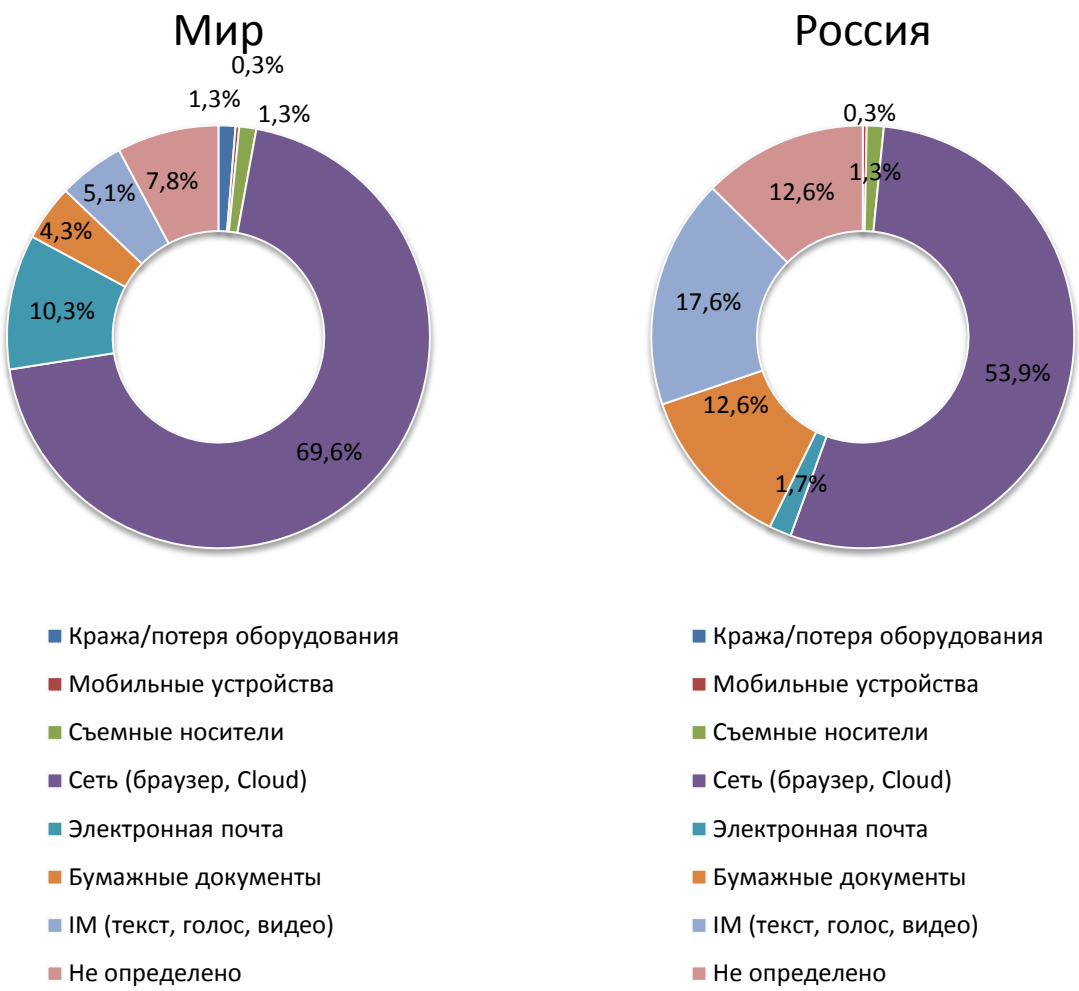

Рисунок 8. Распределение утечек по каналам:, Россия - Мир, январь-сентябрь 2020 г.

На рисунке 9 представлено распределение зарегистрированных утечек за 9 месяцев по отраслям. Как в мире, так и в России на первом месте по числу нарушений находится хайтек-индустрия. В России вторую по величине утечек долю занимает финансовый сектор. Это весьма тревожное положение, которое может свидетельствовать о том, что банки, финансовые и страховые компании в период пандемии испытывают повышенное давление со стороны нарушителей. Вместе с тем в мире второе место по утечкам занимает медицинская сфера, где пандемия обнажила многие проблемы защиты информации, прежде всего связанные с отражением кибератак. В частности, здравоохранение США стало сильно страдать от программ-вымогателей, операторы которых требуют у медицинских учреждений выкуп за удерживаемые данные.

Рисунок 9. Отраслевое распределение утечек, Россия – Мир, январь-сентябрь 2020 г.

Заключение и выводы

Несмотря на небольшое снижение числа зарегистрированных случаев компрометации данных ограниченного доступа в мире за 9 месяцев 2020 г. по сравнению с аналогичным периодом прошлого года, на наш взгляд, не приходится говорить о каком-либо переломе в борьбе с утечками информации.

Наиболее вероятно, что пандемия, вызвав значительные изменения в технологии реализации многих процессов, стала большой помехой для выявления инцидентов ИБ. Значительная часть сотрудников была отправлена на удаленную работу, в результате чего корпоративный периметр еще больше размылся, контроль над информационными активами оказался ослаблен.

Масштабы дистанционной работы дают как киберпреступникам, так и инсайдерам намного больше возможностей для кражи информации. Огромные риски могут быть связаны с использованием в компаниях так называемых «теневых ИТ» (Shadow IT), то есть информационных сервисов, развернутых на внешних, не корпоративных ресурсах, владельцы которых не несут никакой ответственности за обрабатываемые на них данные.

Уровень как внешних, так и внутренних угроз на «удаленке» также повышается в связи с использованием незащищенных домашних Wi-Fi-сетей, проблемами контроля личных устройств, используемых для работы с корпоративной информацией, отсутствием во многих компаниях адекватной инфраструктуры по управлению доступом, игнорированием решений для анализа поведенческих характеристик пользователей информационных систем. Только треть участников опроса на BIS Summit–2020 ответила, что для них (по их мнению) уровень угроз не изменился.

Таким образом, пандемия только усугубила и без того сложную ситуацию с защитой данных.

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 пр.), 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. К умышленным утечкам также относятся все утечки, спровоцированные хакерскими атаками или физическим доступом извне к носителям информации ограниченного доступа, принадлежащей компании.