Россия: утечки информации ограниченного доступа, 2020 год

Оглавление

Только факты

- ✓ В 2020 году Экспертно-аналитический центр InfoWatch зарегистрировал **404** случая утечки данных из коммерческих, некоммерческих (государственных, муниципальных) организаций в России. Это на **2,2%** больше, чем в 2019 году (395 утечек).
- ✓ **16,9%** - доля России в мировом распределении утечек информации за 2020 год (опубликованных на английском, русском и ряде других языков, используемых в странах с высоким уровнем цифровизации, см. Методику).
- ✓ Более **100** млн записей ПДн и платежной информации утекло за год.
- ✓ **15** – количество утечек, в результате каждой из которых было скомпрометировано от 1 млн записей.
- ✓ В общей совокупности утечек с числом утекших записей менее 1 млн каждая, в 2020 году на каждую утечку в среднем пришлось **28,1 тыс.** записей, тогда как в 2019 году на подобную утечку в среднем приходилось **19,9 тыс.** записей.
- ✓ **79%** утечек были спровоцированы внутренними нарушителями, **21%** - внешними.
- ✓ Почти **80%** всех утечек случились в результате умышленных действий.
- ✓ Доля утечек умышленного характера по вине внутренних нарушителей выросла с **38,7%** до **79,3%**.
- ✓ Доля привилегированных пользователей (руководители и системные администраторы) в общем распределении утечек в России достигла **7%**.
- ✓ Почти **20% утечек в России** происходит через канал мгновенных сообщений (мессенджеры).
- ✓ Более **40%** зарегистрированных утечек пришлись на сферы высоких технологий и финансов.

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) подготовил очередное ежегодное исследование утечек информационного доступа, случившихся в российских коммерческих компаниях, государственных органах и организациях.

В 2020 году большое влияние на реализацию многих процессов оказала пандемия новой коронавирусной инфекции. Исключением не стала и сфера защиты информации. У компаний и организаций возникли новые риски, связанные с удаленной работой, одновременно с этим давление усилили хакерские группировки. Как следствие, в 2020 году произошел резкий рост доли утечек умышленного характера, выросли проценты утечек в результате действий внешних злоумышленников и привилегированных пользователей.

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).

Результаты исследования

Динамика количества утечек и количества утекших записей

В 2020 году Экспертно-аналитическим центром InfoWatch зарегистрировано (стали известными) **404** случая утечки информации ограниченного доступа из коммерческих компаний, государственных органов и организаций, работающих на территории Российской Федерации. Это на 2,2% больше, чем в 2019 году, когда было зарегистрировано 395 утечек, и почти в 1,5 раза (на 49,6%) больше, чем в 2018 году, когда в поле исследования были включены 270 утечек (Рисунок 1).

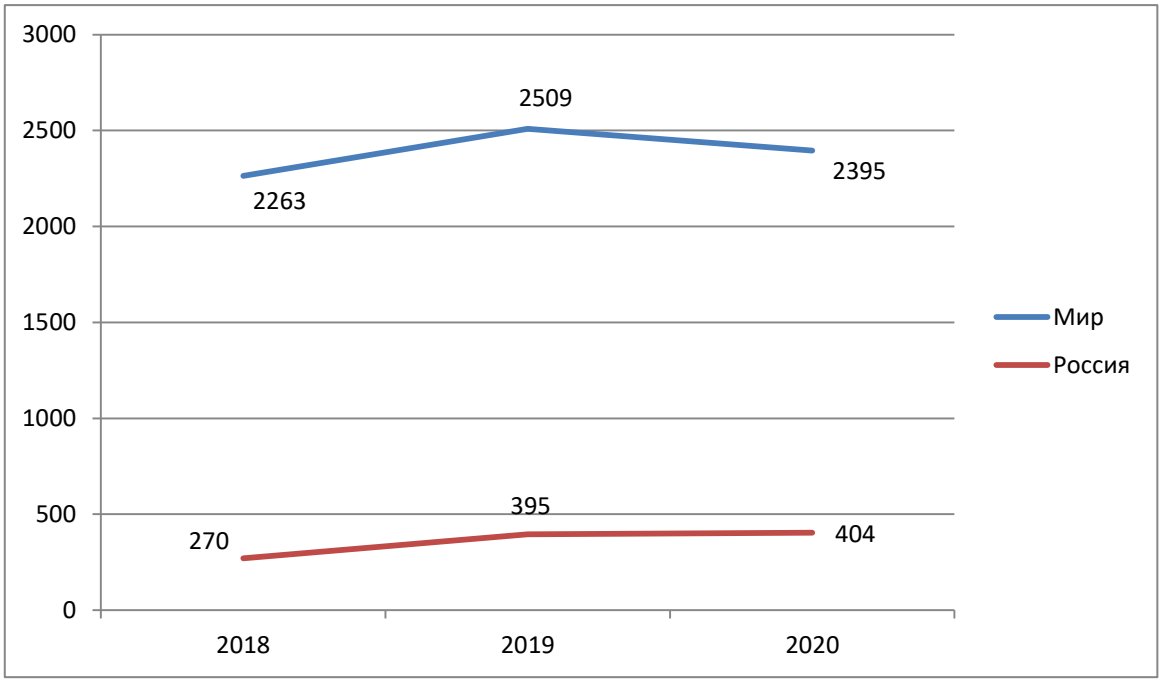

Рисунок 1. Число утечек информации, Россия - Мир, 2018 - 2020 гг.

Небольшое увеличение числа утечек в России за 2020 год - даже на фоне падениях их числа в мире – на наш взгляд, прежде всего стало следствием повышения латентности инцидентов информационной безопасности в компаниях. В период пандемии и массового перехода сотрудников на удаленную работу, когда контроль за информационными активами оказался сильно затруднен, многие случаи утечек могли остаться незамеченными. Вместе с тем, весьма скромный рост количества утечек в России за 2020 год на фоне роста почти в 1,5 раза годом ранее, может быть связан с тем, что свои плоды начали приносить корпоративные мероприятия в сфере ИБ, включая внедрение современных DLP-систем (отсюда сокращение доли утечек внутреннего характера, о чем речь пойдет ниже). Отметим, что в даркнете до сих пор распространяются базы данных, составленные из утечек прошлых лет и еще не потерявшие актуальность.

В результате утечек, информация о которых появилась в открытых источниках[1], в России было скомпрометировано 100,8 млн записей ПДн и платежной информации.

[1] см. Методику

Это на 41,4% меньше, чем в 2019 году, когда в совокупности всех зарегистрированных инцидентов «утекло» 172 млн записей (Рисунок 2). Из них 76 млн записей «утекло» в результате одного случая, когда из-за уязвимости в открытый доступ попала информация с серверов оператора фискальных данных «Дримкас». В 2020 году столь масштабной утечки не было. Наиболее значительный случай произошел в мае 2020 г., когда в открытый доступ были выложены персональные данные 26 млн подписчиков платформы LiveJournal («Живой Журнал»). А если сравнивать 2020 год с 2018 годом, общее число скомпрометированных записей выросло почти в четыре раза. Данные о количестве утечек и скомпрометированных записей отражены на рисунке 2.

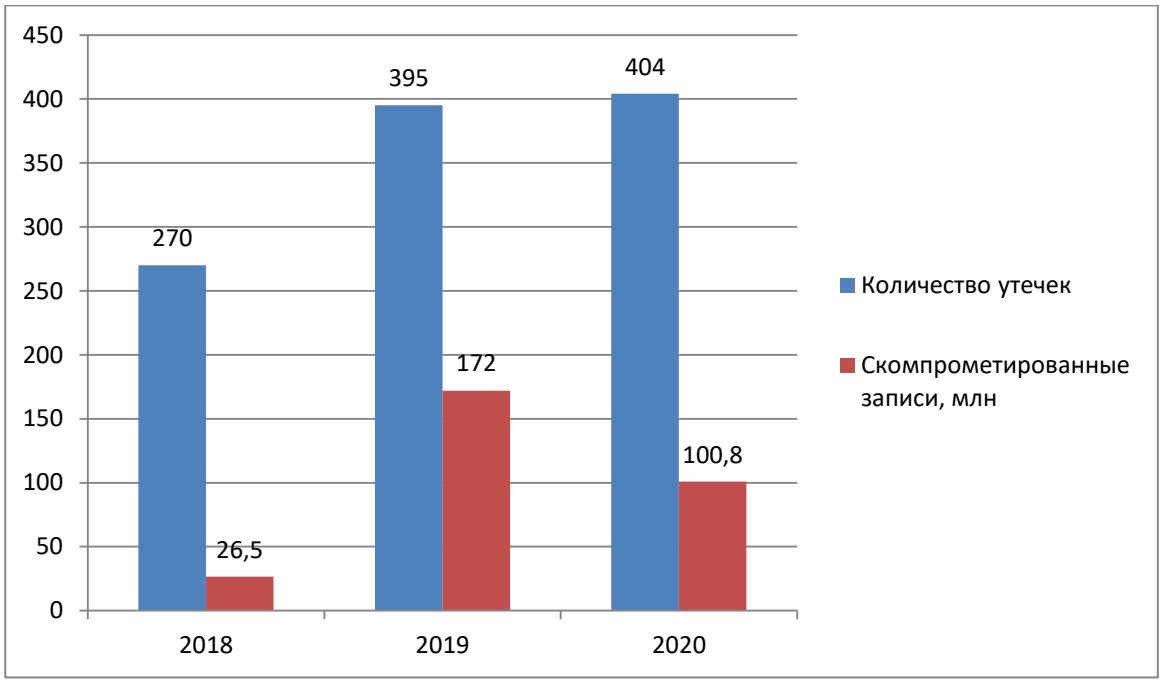

Рисунок 2. Россия: Число утечек информации и объем персональных данных, скомпрометированных в результате утечек. 2018 - 2020 гг.

> *Bleeping Computer: Порядка 26 млн учетных записей пользователей LiveJournal начали продавать в даркнете. Вероятно, платформа для ведения блогов пострадала от взлома еще в 2014 г. Кроме того, хакеры использовали старые комбинации «логин-пароль» для взлома учетных записей платформы DreamWidth, созданной на основе кода LiveJournal.*

Таким образом, в 2020 году средняя утечка составила 249,5 тыс. записей, годом ранее утекало в среднем 435,4 тыс. записей, а в 2018 году – 98,1 тыс. записей.

Крупные утечки – от 1 млн записей и более сильно влияют на общую статистику. Посмотрим срезы по утечкам в России.

Без учета утечек с количеством записей от 1 млн, **в 2020 году в срезе «случаи с числом записей менее 1 млн» средняя утечка составила 16,2 тыс. записей, в 2019 году – 23 тыс. записей, в 2018 году – менее 200 записей.** Таким образом в 2020 году произошло небольшое снижение среднего числа записей в одной утечке после скачка 2019 года. Возможно предположить, что он связан с активным развитием цифровизации и накоплением компаниями различного уровня крупных объемов

пользовательских данных. В 2020 году дальнейший рост удалось сдержать – вероятно, во многом благодаря тому, что компании провели серьезную работу по укреплению систем защиты информации в 2019 г. и их успешной адаптации в начале пандемии. , Хотя полностью продолжения неприятной тенденции избежать не удалось (см. наш отчёт по утечкам, связанным с COVID-19, в первом полугодии 2020 года).

> *КоммерсантЪ: Паспортные данные оштрафованных за нарушение самоизоляции в Москве оказались доступны на сайтах для оплаты штрафов по номеру начисления, который можно подобрать перебором с помощью простого софта. Скомпрометирована информация по меньшей мере о 35 тыс. таких штрафов.*

В 2020 году количество крупных утечек – по 1 млн записей и более – составило 15. В 2019 году таких случаев было зарегистрировано 10, а в 2018 году – 2.

При этом случаев «мега-утечек», когда было скомпрометировано от 10 млн записей, в 2020 году было 3, в 2019 году – 4, в 2018 году - 2.

Внутренние и внешние нарушители

На Рисунке 3 приведено сравнение количества утечек по вине внутреннего и внешнего нарушителя (по вектору воздействия) за 2019 и 2020 год в России (на основе уточненных данных).

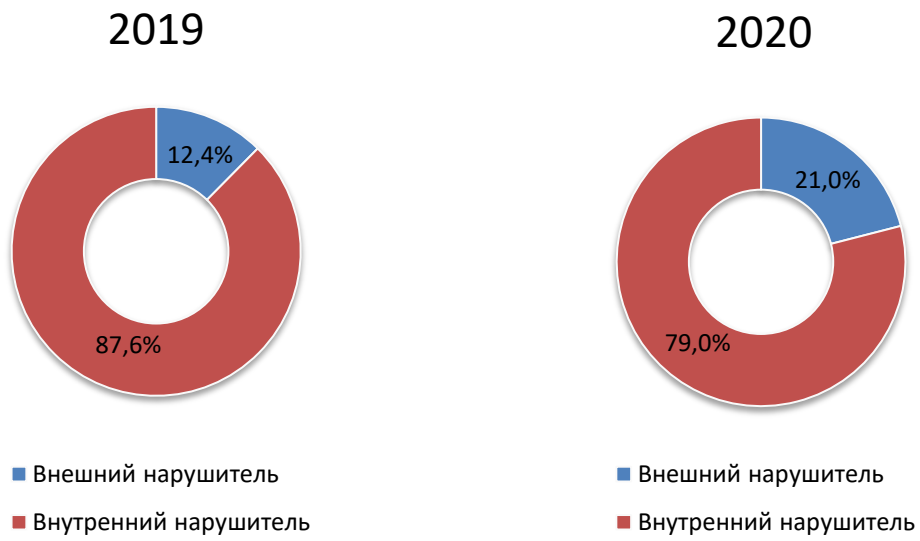

Рисунок 3. Распределение утечек по вектору воздействия, Россия, 2019-2020 гг.

В «пандемийный» 2020 год существенно выросла доля утечек в результате действий внешних нарушителей. Цифровизация привела к появлению большого количества структурированных хранилищ конфиденциальной информации, а значит, к возникновению новых рисков для информационных активов. Чтобы нивелировать эти риски, компаниям необходимо тщательно выстраивать защиту как от внутренних нарушителей, так и отхакеров, как одиночек, так и членов ОПГ, которые поняли, что в России появилось немало баз данных, которые возможно монетизировать. Судя по

всему, внешние угрозы становятся все более опасными, но в целом отечественные компании пока неплохо с ними справляются.

На Рисунке 4 представлено сравнение долей внешних нарушителей в России и в мире за последние три года. На графике легко заметить, что в обоих случаях линия неуклонно стремится вверх, но в мире доля утечек в результате внешнего воздействия по-прежнему в несколько раз выше.

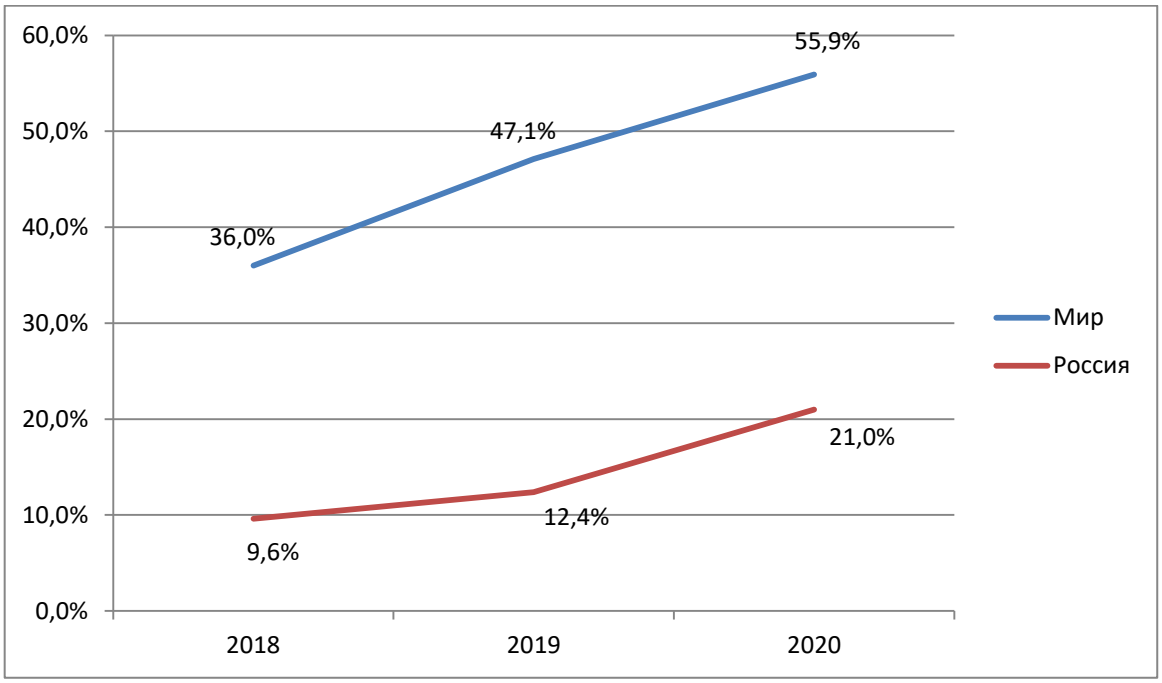

Рисунок 4. Доля внешних нарушителей в общем распределении утечек, Россия – Мир, 2018-2020 гг.

> *КоммерсантЪ: Данные 5 млн учащихся и преподавателей онлайн-школы английского языка Skyeng выставлены на продажу в интернете за 40 тыс. рублей. По словам специалистов по информационной безопасности, хакеры скачали данные с облачного сервера Mongo DB.*

Но из графиков видно, что несмотря на тенденцию роста доли внешних нарушителей, по-прежнему подавляющее большинство утечек происходит в результате действий (случайных и умышленных) внутренних нарушителей, то есть персонала. (Наш комментарий: к сожалению, это происходит несмотря на то, что есть и проверенные методики обучения пользователей, и системы контроля действий корпоративных пользователей).

Умышленные и неумышленные утечки

В 2020 году резко выросла доля утечек, к которым привели умышленные действия как персонала, так и внешних нарушителей. В России она составила почти 80% (Рисунок 5).

Мы показали, что доля утечек по вине внешнего нарушителя, которые по определению всегда умышленные, увеличилась. Соответственно, упала доля утечек по вине внутренних нарушителей. Но вот в её составе (среди внутренних) резко – почти на 60% - выросла доля умышленных утечек.

Например, недобросовестные менеджеры банков, сотрудники операторов связи и ритейлеров, пользуясь общей неразберихой в организации процессов, сознательно шли на преступления, «сливая» конфиденциальные данные заинтересованным лицам или самостоятельно используя клиентскую информацию в мошеннических целях.

> *РБК: В Башкирии сотрудница микрофинансовой компании раскрыла персональные данные 44 заемщиков. Установлено, что в августе 2020 г. женщина отправила конфиденциальную информацию своему родственнику по электронной почте.*
>
> *Сибкрай.ru: Менеджера одного из филиалов «Россельхозбанка» в Новосибирской области обвинили в мошенничестве с кредитами. По версии следствия, женщина, обманув управляющую отделения и кассира банка, от имени клиентов оформила кредиты на общую сумму более 3 млн рублей.*

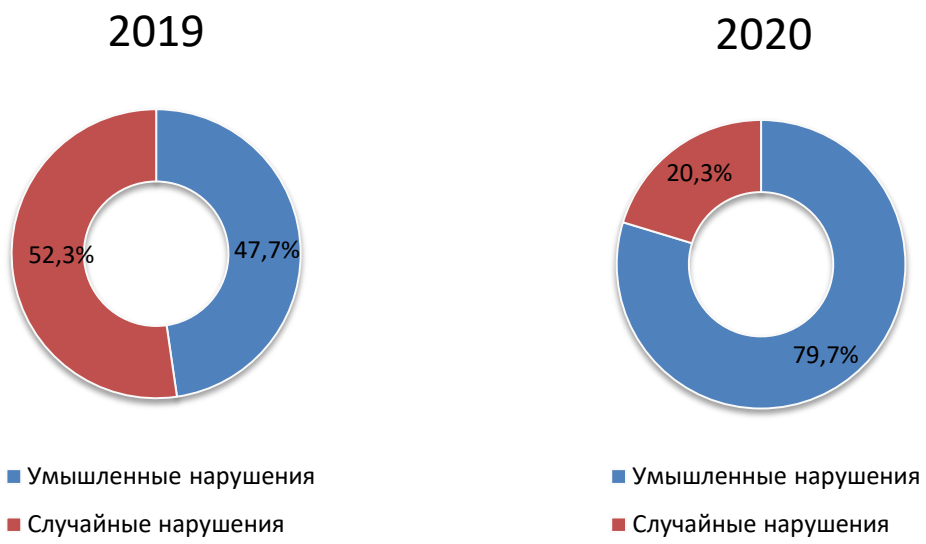

Рисунок 5. Распределение утечек по умыслу, Россия, 2019-2020 гг.

Общий тренд на увеличение процента преднамеренных утечек наметился еще несколько лет назад, когда едва ли не каждая единица конфиденциальной информации стала представлять ценность на черном рынке – цифровизация принесла

не только преимущества, но и новые риски. **В результате доля умышленных нарушений в России за 2020 год превысила мировую**[2] (Рисунок 6).

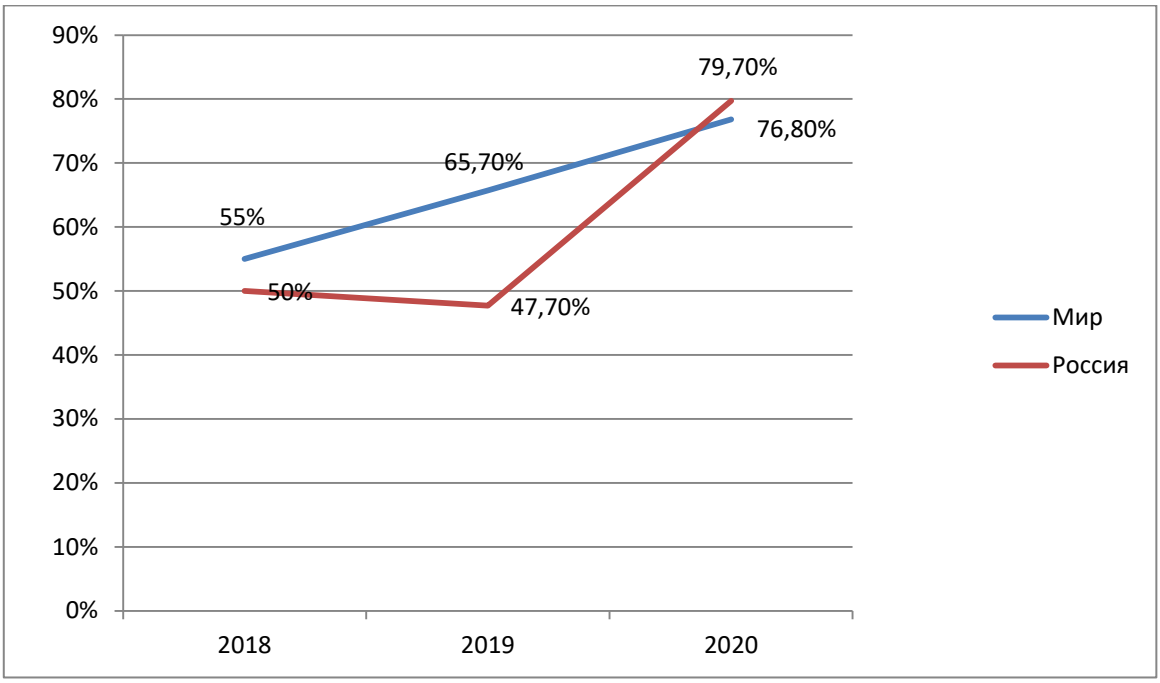

Рисунок 6. Доли утечек умышленного характера, Россия - Мир, 2018-2020 гг.

Доля умышленных утечек среди внутренних нарушителей в России достигла критического значения. **В 2020 году почти 74% случаев, когда виновниками были сотрудники компаний, носили преднамеренный характер** (Рисунок 7). При этом подобное положение может свидетельствовать о том, что компании стали намного лучше предупреждать нарушения случайного характера – эффект стал приносить переход на современные DLP-системы и их тщательная настройка в соответствии с задачами контроля различных каналов, а также мероприятия по повышению осведомленности в сфере ИБ.

[2] Применительно к утечкам, опубликованным на русском, английском и ряде других языков, используемых в странах с высоким уровнем цифровизации, см. Методику.

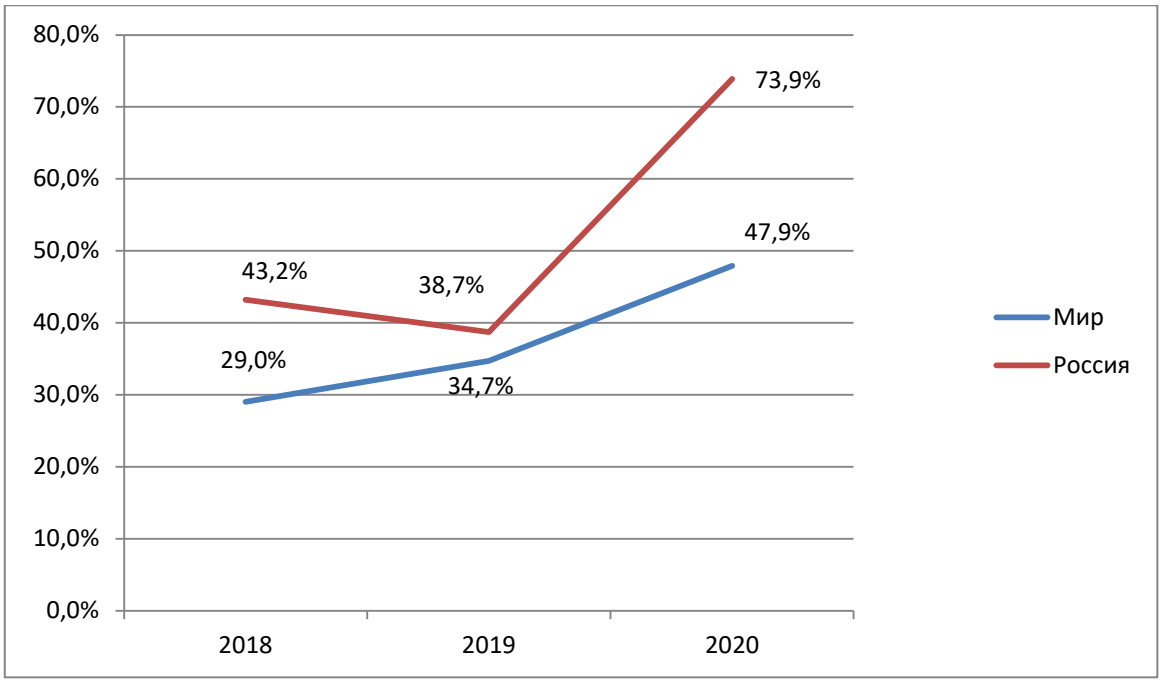

Рисунок 7. Доли утечек умышленного характера среди внутренних нарушений, Россия - Мир, 2018-2020 гг.

Рассмотрим детальную картину утечек в разрезе виновников (инициаторов) (Рисунок 8). Доля хакеров и неизвестных лиц составила почти 30%,. до 60% упала доля рядовых (непривилегированных сотрудников), остальное приходится на долю привилегированных пользователей, подрядчиков, бывших сотрудников. Отметим, что существенно больший процент нарушений по сравнению с прошлым годом совершен по вине руководителей различного уровня.

> *Свердловское областное телевидение: В центре Екатеринбурга прохожие обнаружили кредитные договоры, копии паспортов и других документов, принадлежащих клиентам одного из банков. Судя по всему, бумаги с персональными данными были потеряны при переезде банка в другой офис.*

> *Тамбовская жизнь: Руководителя частной клиники обвинили в совершении ряда преступлений. В частности, по версии следствия, женщина передавала сведения об умерших пациентах мемориальной компании. За эту услугу представители ритуального агентства переводили главе лечебного учреждения деньги на банковскую карточку. Следствию удалось доказать получение обвиняемой денежных средств в сумме около 70 тыс. рублей.*

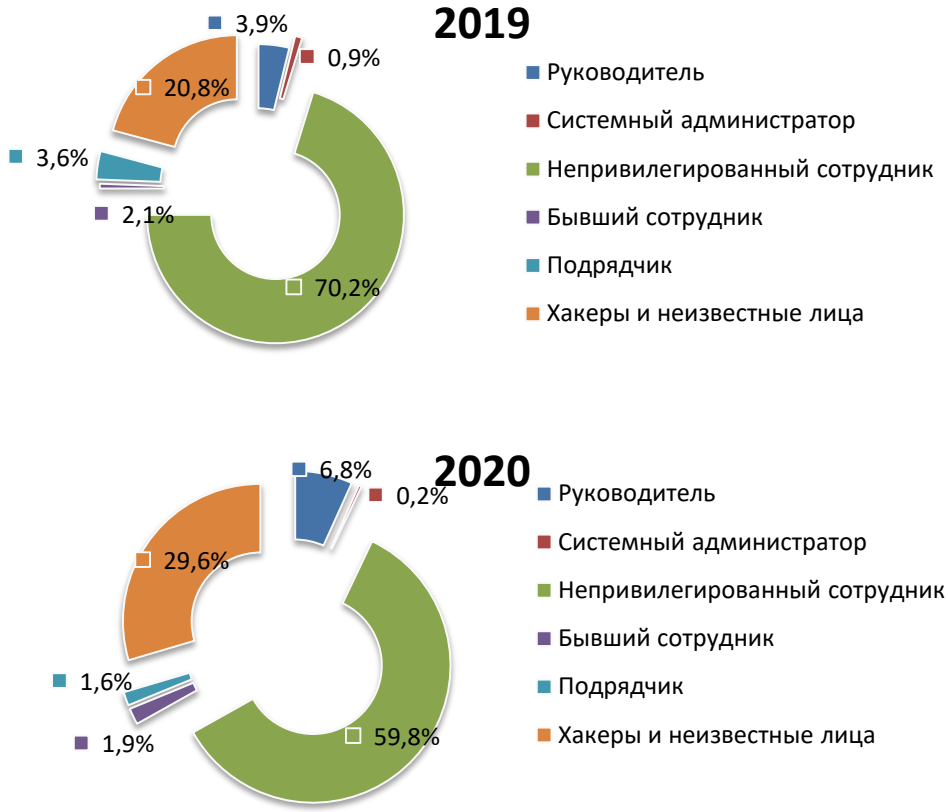

Рисунок 8. Распределение утечек по источнику (виновнику), 2019-2020 гг.

Какие данные «утекают»

В распределении зарегистрированных утечек по типам данных существенных изменений за год не произошло. Доминирующим типом данных в утечках по-прежнему остаются ПДн – доля более 86% (Рисунок 9). Возможностей монетизации личной информации о гражданах в цифровую эпоху предостаточно – от довольно безобидного электронного маркетинга до фишинговых атак и непосредственно мошеннического использования (оформление кредитов и различных выплат на имя другого человека). Вместе с тем привлекательность платежных данных для злоумышленников продолжает падать - эту информацию все сложнее использовать для извлечения денежных средств, скомпрометированные банковские карты, как правило, оперативно блокируются, к тому же, платежная инфраструктура банков достаточно надежно защищена. По данным ЦБ, в 2020 году атаки злоумышленников практически не имели успеха, а проведенные киберучения с участием 22 банков показали, что ведущие банки достойно подготовлены к отражению атак, имея все необходимые системы мониторинга, выявления и реагирования.

На этом фоне злоумышленники сохраняют большой интерес к конфиденциальной информации, составляющей коммерческую тайну, то есть к тем сведениям, которые удобно использовать в конкурентной борьбе, при шантаже, в рамках создания новых компаний (стартапов) в различных сферах бизнеса.

Томикс: 50-летний бывший сотрудник инженерной службы Ковровского электромеханического завода (Владимирская область) имел доступ к техническим документам, составляющим коммерческую тайну предприятия. За 50 тысяч рублей он продал сведения, касающиеся технологических процессов производства, заинтересованному лицу, за что в отношении работника завода возбуждено уголовное дело.

SecurityLab.ru: Специалисты по информационной безопасности раскрыли утечку персональных данных порядка 9 млн клиентов транспортно-логистической компании СДЭК. Хакер в даркнете предлагал всем желающим получить доступ к полной базе СДЭК. На полученных от автора объявления скриншотах были представлены свежие данные о заказчиках компании. Судя по всему, злоумышленник активно эксплуатировал «дыру» в системе безопасности СДЭК.

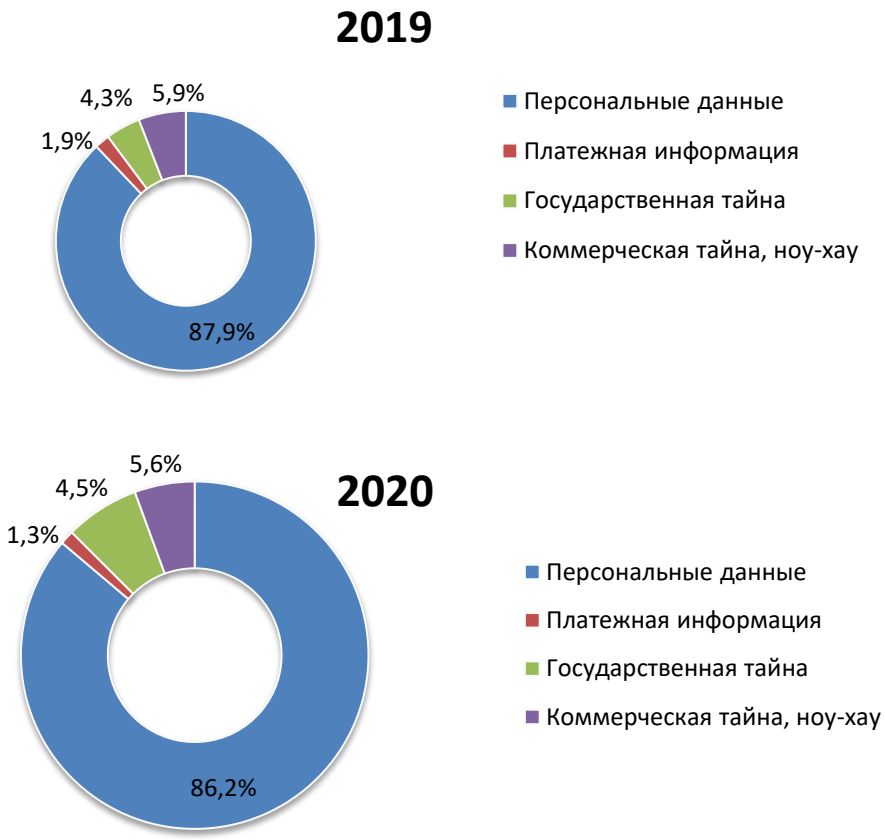

Рисунок 9. Распределение утечек по типам данных, 2019-2020 гг.

В 2020 году продолжила падать доля так называемых «квалифицированных утечек», когда нарушитель напрямую использует данные в мошеннических целях (оформление кредита, выплаты и т.д.) и (или) проникает в хранилища информации с превышением прав доступа (в основном речь идет об использовании чужих учетных данных) – см.

Рисунок 10. Совершение мошеннических действий зачастую оказывается сильно затрудненным для злоумышленника. Кроме того, в последние годы появилось намного больше возможностей для монетизации украденной информации (прежде всего персональных данных) через третьих лиц. Поэтому нарушители стараются продать полученную информацию, слить ее заинтересованным «покупателям», после чего скомпрометированные данные могут перепродаваться по фрагментам для различных целей, в том числе преступных, но не обязательно через ресурсы DarkNet-а, где о них достаточно быстро становится известно, а напрямую своим знакомым и вышедшим на них мошенникам (по заказу мошенников). Зачастую украденные базы с пользовательской информацией используются для фишинговых атак, организаторы которых пытаются выведать финансовую информацию жертв.

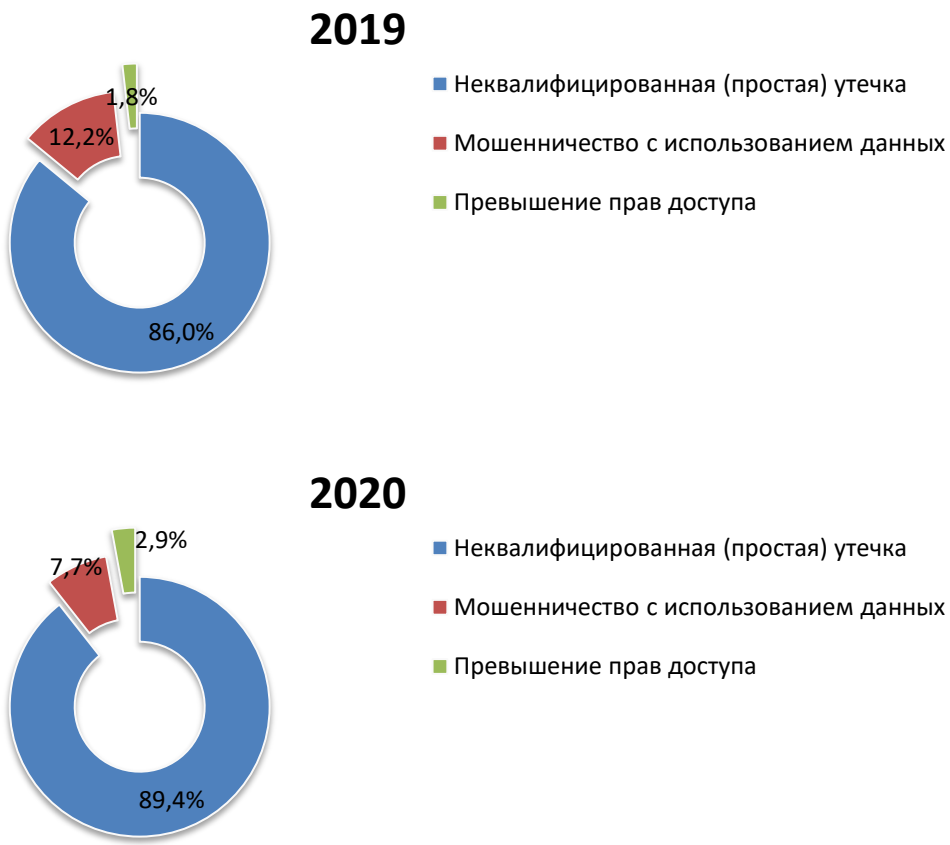

Рисунок 10. Распределение инцидентов по характеру, 2019-2020 гг.

Глас Народа: В городе Ртищево Саратовской области задержана 29-летняя сотрудница одного из салонов сотовой связи. По версии следствия, во время составления договора на покупку в кредит сотового телефона женщина предлагала клиентам дополнительно оформить на них кредитную карту. Все покупатели отказывались от подобного предложения. Однако подозреваемая, используя персональные данные клиентов, тайно оформляла на их имя кредитную карту. Таким образом, задержанная оформила четыре кредитки и потратила около 150 тысяч рублей на личные нужды. Граждане обратились в

полицию, когда им стали приходить уведомления о задолженностях на картах, о существовании которых они даже не догадывались.

SecurityLab.ru: В открытом доступе оказалась база данных пользователей сервиса online-бронирования трансферов «Киви-такси» (kiwitaxi.com). 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.

Каналы утечки данных

На Рисунке 11 представлено распределение утечек в России по каналам.

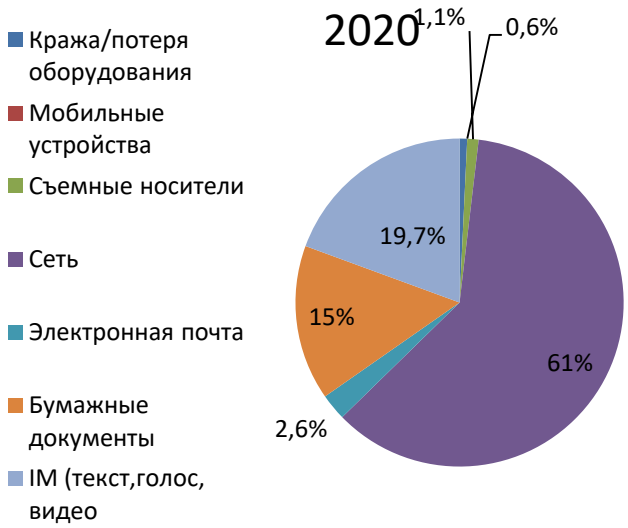

Рисунок 11. Распределение утечек по каналам, Россия, 2020 г.

Доля сетевого канала[3] за последний год немного сократилась, тогда как в мире, напротив, продолжает тенденцию роста (Рисунок 12)

[3] см. Глоссарий

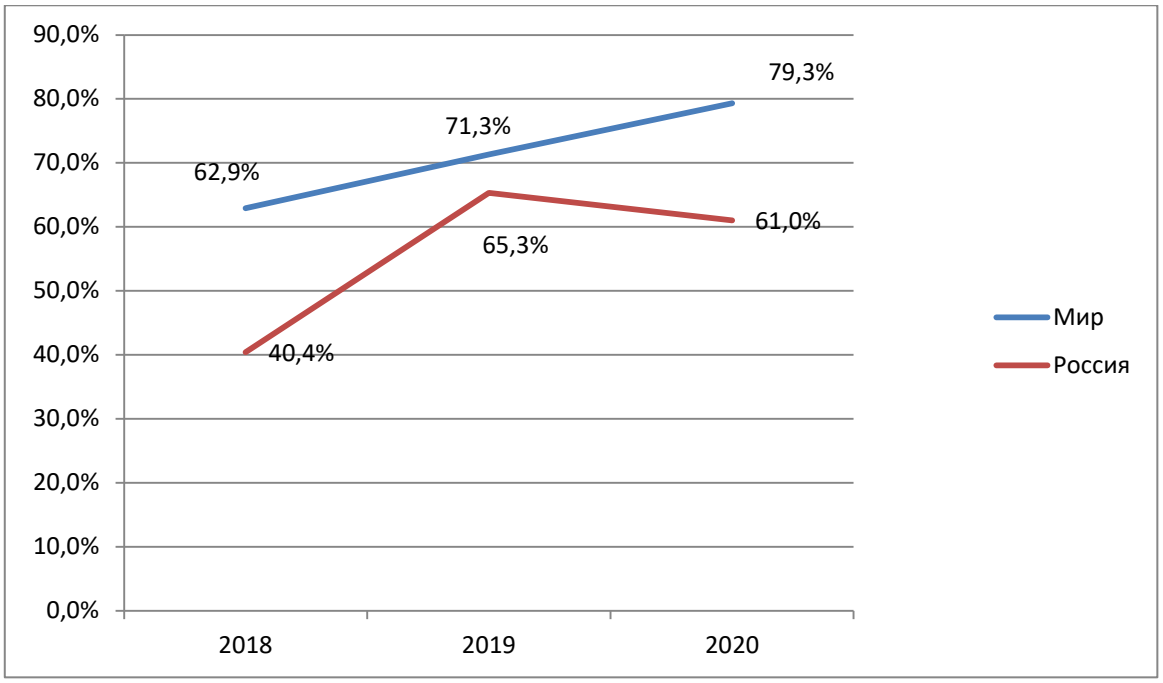

Рисунок 12. Доля сетевого канала в общем распределении утечек, Россия - Мир, 2018-2020 гг.

Более заметную роль в России стал играть канал мгновенных сообщений, связанный с передачей текстовых, голосовых и видео-сообщений (Рисунок 13). Излюбленным средством для нарушителей стали мессенджеры. Корпоративным службам безопасности следует уделить особое внимание контролю этого канала при передаче конфиденциальной информации за пределы информационного контура организации.

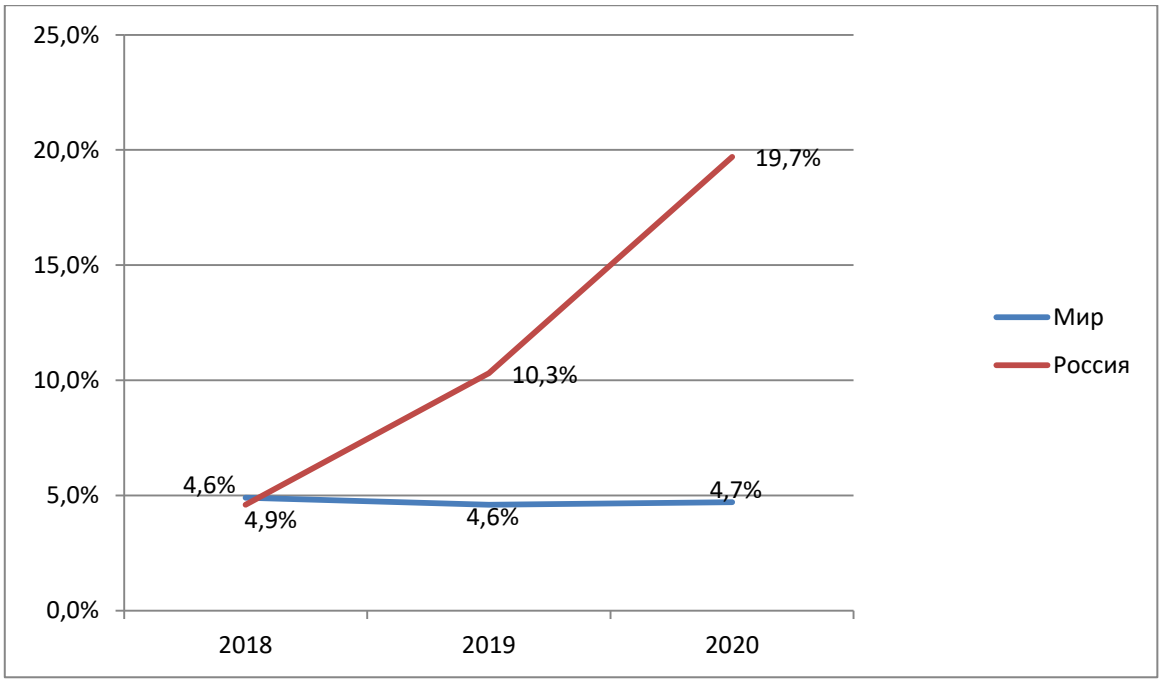

Рисунок 13. Доля канала мгновенных сообщений (IM) в общем распределении утечек, Россия - Мир, 2018-2020 гг.

Доля утечек по электронной почте в России за 2020 год незначительно выросла (попытки передачи данных по e-mail легко обнаружить, но не всегда – блокировать, не каждый поставит DLP в разрыв), тогда как в мире продолжает сокращаться (Рисунок 14).

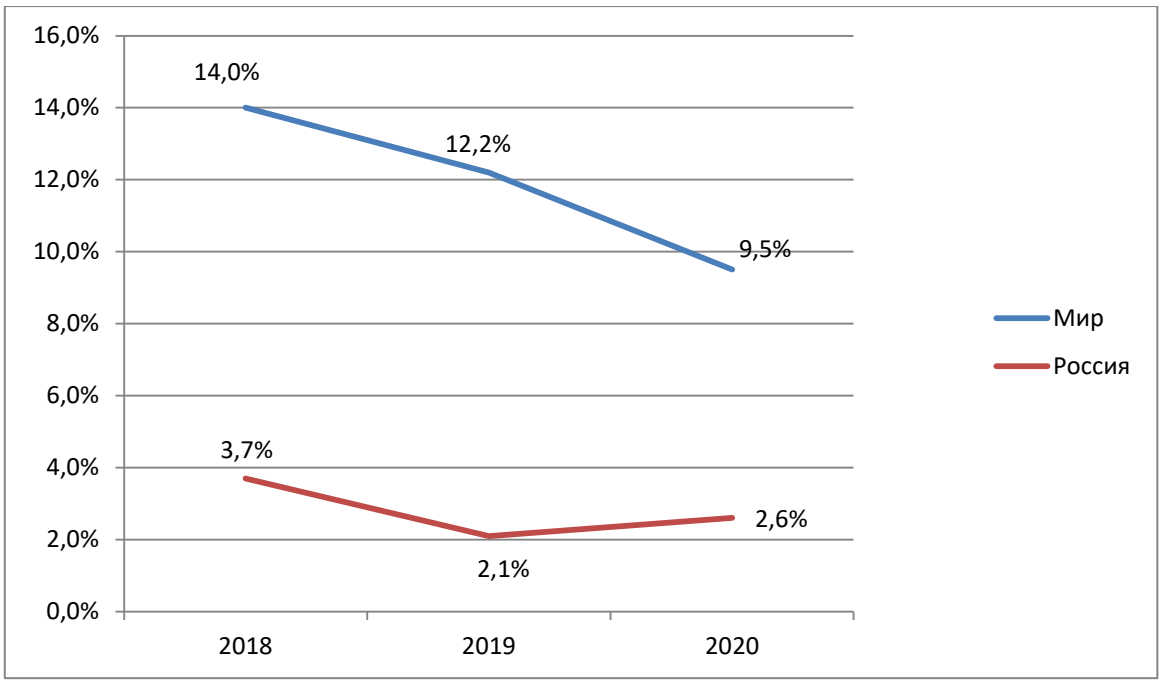

Рисунок 14. Доля канала электроной почты в общем распределении утечек, Россия - Мир, 2018-2020 гг.

Количество утечек, случившихся посредством бумажных документов, объективно снижается в цифровую эпоху, но в России все еще составляет довольно весомую долю – более 15% (Рисунок 15).

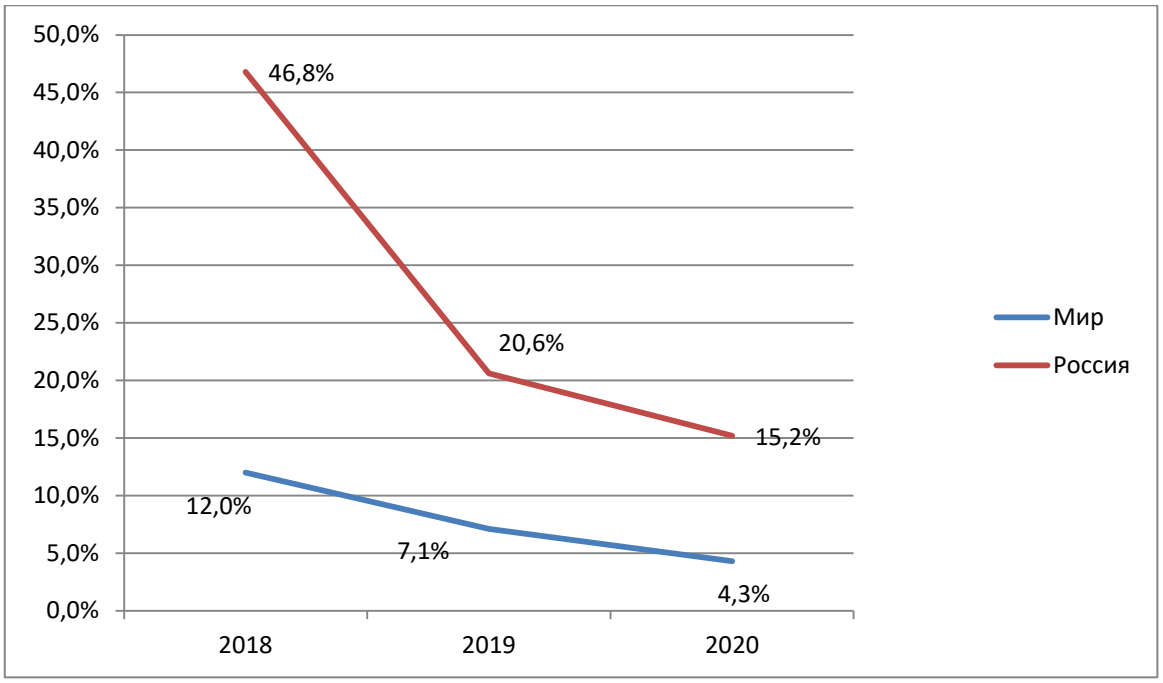

Рисунок 15. Доля канала электроной почты в общем распределении утечек, Россия - Мир, 2018-2020 гг.

В распределении по каналам не учтены неизвестные (неопределенные) случаи – традиционно таких утечек много, так как далеко не всегда авторы сообщений об утечках располагают информацией о том, каким путем были скомпрометированы утекшие данные. Авторы исследования при этом считают, что игнорировать наличие большого числа случаев с неопределенным каналом утечки методологически неправильно, поэтому решили отразить их на отдельной диаграмме.

На Рисунке 16 представлено распределение утечек по каналам с учетом доли неизвестных (неопределенных) случаев.

В 2020 году в России на неопределенные случаи утечек в распределении по каналам пришлось 14,8% случаев.

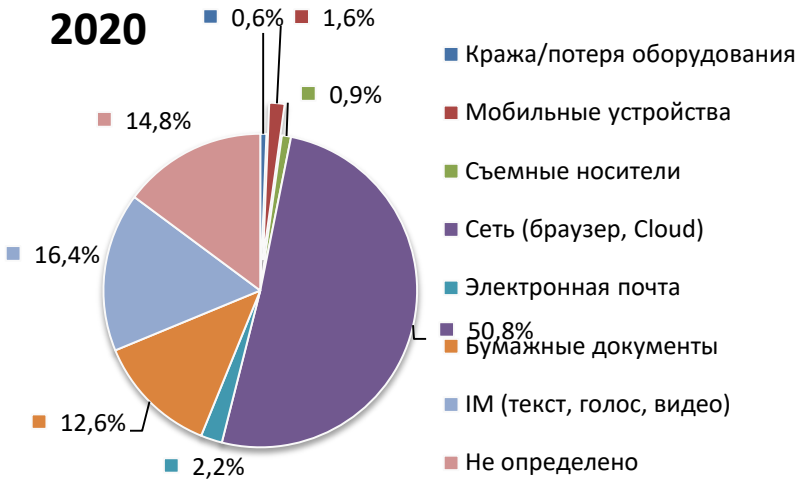

Рисунок 16. Распределение утечек по каналам с учетом доли неопределенных случаев, 2020 г.

В 2020 году в общем распределении утечек по отраслевому принципу выросли доли таких вертикалей, как финансовая сфера, высокие технологии и медицина (Рисунок 19).

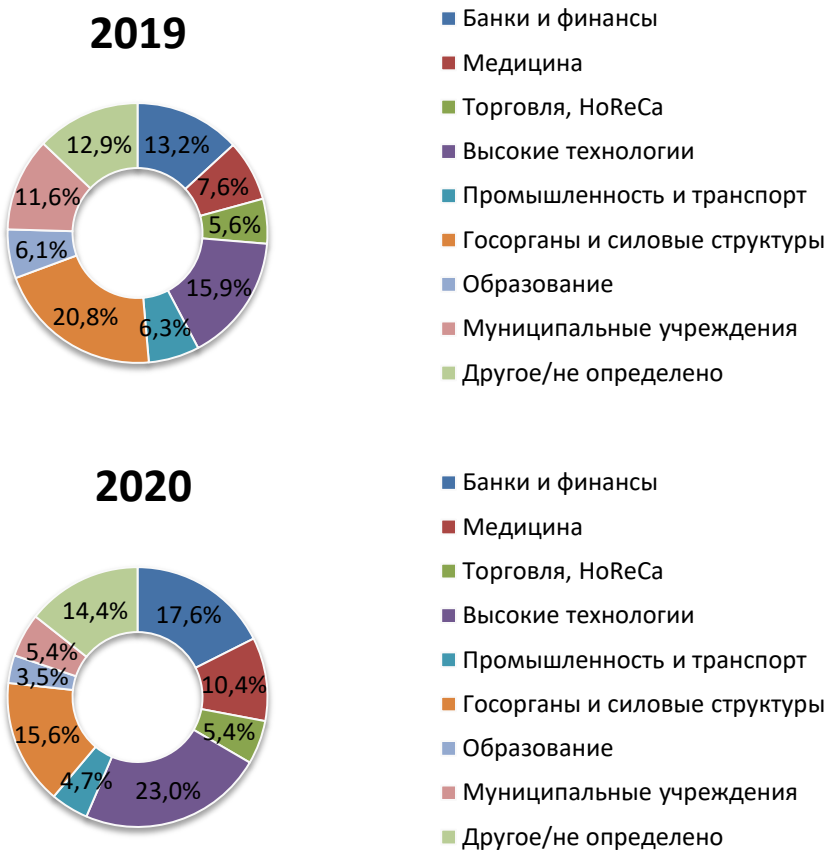

Рисунок 19. Распределение числа утечек по отраслям, Россия, 2019-2020 гг.

Заключение

Значительное влияние на формирование различных параметров утечек информации ограниченного доступа в 2020 году оказала пандемия. В процессе перевода сотрудников на удаленную работу возникли новые риски информационной безопасности, компаниям стало намного сложнее контролировать доступ к своим информационным ресурсам. Можем предположить, что вследствие этого значительно выросла латентность инцидентов ИБ, еще больше нарушений перестали попадать в «поле зрения» систем защиты. Но даже с учетом этого отмечен дальнейший рост утечек, пусть и всего на несколько процентов, по сравнению с ростом почти в 1,5 раза на фоне 2019 года.

Россия начинает постепенно «подтягиваться» к общемировым тенденциям формирования «картины утечек». Так, в прошлом году существенно, до 21%, выросла доля утечек по вине внешних нарушителей. В мире она по-прежнему намного выше (более 55% в 2020 г.), но есть все основания полагать, что «сближение» с Россией здесь продолжится. Если финансовая сфера, согласно данным ЦБ, в целом хорошо готова к отражению внешних угроз, то уровень защиты от вторжений среди других вертикалей не может не вызывать опасения.

При этом подавляющее большинство внутренних утечек происходит по вине персонала компаний (непривилегированные сотрудники, руководители различного уровня, сисадмины), хотя в России есть квалифицированные методики для борьбы с такими нарушениями и одни из лучших в мире систем для предотвращения утечек. Одновременно резко выросла доля умышленных нарушений – как в результате внешнего воздействия, так и в результате действий персонала. Почти 80% всех утечек в 2020 году совершены преднамеренно. Это свидетельствует о возросшем спросе преступного мира на конфиденциальную информацию. Вместе с тем, радикальное снижение процента утечек случайного характера может говорить об их слабой выявляемости в компаниях (на фоне повышенной латентности, о чем сказано выше).

Повышение до 7% доли утечек, связанных с действиями руководителей и системных администраторов, судя по всему, связано с тем, что в пандемию компании недостаточно внимания уделяли контролю привилегированного доступа. Если эту проблему не решить, то в ближайшие годы, скорее всего, нас ждет дальнейший рост утечек по вине пользователей с особыми полномочиями по доступу к информационным активам и назначению ролей доступа.

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

Методика

Исследование проводится на основе собственной базы утечек ЭАЦ, регулярно пополняемой специалистами ЭАЦ с 2004 года. В базу попадают публичные сообщения[4] о случаях утечек информации из учреждений, организаций, предприятий любых организационных форм и форм собственности, включая органы государственной власти и управления.

В настоящий момент количество записей в базе превышает 20 000.

Исследования ЭАЦ в основном ориентированы на анализ сообщений об утечках данных на английском и русском языках, также используется некоторое количество источников на арабском, японском, немецком, французском, испанском и итальянском языках. Выбор языков связан с высоким уровнем цифровизации в странах, их использующих.

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, где 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,

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

- дата публикации сообщения,
- название предприятия (организацит, учреждения);
- государство (страна),
- сфера деятельности обладателя информации (отрасль),
- направление деятельности (коммерческая, некоммерческая),
- примерный размер пострадавшей от утечки организации (малая, средняя, крупная)[5],
- размер причиненного в результате утечки ущерба[6],
- количество скомпрометированных записей (только для ПДн и платёжной информации),
- субъект[7], непосредственно допустивший утечку.

Выделяются следующие сферы деятельности (отрасли, отраслевые группы):

- банки, финансовые и страховые компании,
- медицина,
- торговля и HoReCa,
- высокие технологии (в основном ИТ и телекоммуникационные компании),
- промышленность, энергетика и транспорт,
- госорганы и силовые структуры,
- образование,
- муниципальные органы власти и учреждения,
- другое (некоммерческие организации, спорт, медиа, консалтинг, недвижимость и т.д.).

Далее каждое сообщение классифицируется по:

- наличию умысла[8] (если по описанию или имеющимся признакам действия лица, допустившего утечку, являются умышленными, то утечка классифицируется как умышленная; 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 (внешний, внутренний, не определено, в ряде случаев выделяем так называемый «гибридный вектор», когда утечка связана с влиянием как внешних, так и внутренних нарушителей),
- типу нарушителя.

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

[6] Данные об ущербе и количестве скомпрометированных записей взяты непосредственно из публикаций в СМИ, или на сайтах пострадавших организаций, или из отчётов органов государственной власти, экспертных организаций.

[7] Авторы классифицируют утечки по виновнику инцидента. См. Глоссарий.

[8] Утечки данных разделяются на умышленные и неумышленные (случайные) См. Глоссарий.

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 в 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, а в поле отраслевой принадлежности ставится «другое», поле «название компании» остается пустым.

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.

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

ЭАЦ регулярно отслеживает обновления по ранее зарегистрированным утечкам.
В ходе такого мониторинга в базу вносится:

- информация об утечках, которые произошли в предыдущие периоды (прошлый год, позапрошлый и ранее),

[9] Например, разрез по вектору воздействия, куда входят утечки под воздействием внешних атак и внутреннего нарушителя, не содержит утечек, для которых вектор не удалось определить. То же справедливо для распределений по виновнику, умыслу и другим критериям.

- обновлённая информация о составе (принадлежности) баз «мега-утечек»,
- уточнённые данные о дате (периоде), когда случилась ранее опубликованная утечка, об объёмах (количестве записей), векторе атаки и т.п.

То есть , при появлении новой информации, данные о количестве, а также векторах воздействия, каналах, суммах штрафов и т.п. утечек за прошлые периоды могут изменяться по сравнению с ранее опубликованными.

Но, как правило, эти данные не оказывают существенного влияния на общие показатели, отраженные в отчетах, а также на обозначенные в исследованиях тенденции.

Глоссарий

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

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

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

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

Внешняя атака – атака, совершенная внешним нарушителем.

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

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

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

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации

в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными] разведками и другими заинтересованными субъектами [ГОСТ Р 50922-2006, статья 2.3.2].

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

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

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

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

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

Примечание – Инцидентами информационной безопасности являются:

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

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

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

- «Оборудование (сервер, СХД, ноутбук, ПК)», – компрометация информации в ходе обслуживания, в результате кражи или потери оборудования.
- «Мобильные устройства» – утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.
- «Съемные носители» – потеря/кража съемных носителей (CD, USB, карты памяти и др.).

- «Сеть (сетевой канал)» – утечка, реализованная через подключение к сети связи общего пользования, в том числе Интернет, а также из облачных сервисов, например, отправка данных через веб-интерфейс в личную почту, формы ввода в браузере, через FTP, нелегитимная публикация информации в соцсетях и т.п.
- «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.