Аналитический отчет

Россия: утечки информации ограниченного доступа в 2022 г.

Оглавление

Только факты

- → Количество утечек информации в России выросло более чем в 2,1 раза.
- → За год утекло более 667 млн записей ПДн и платежной информации — в 2,67 раза больше, чем в 2021 году.
- → Количество утекших записей в 4,5 раза превысило население России.
- → На одну утечку в среднем пришлось на 25% больше записей, чем в 2021 году.
- → Порядка 80% имеют гибридный вектор воздействия, когда в краже информации могли участвовать как внешние, так и внутренние нарушители.
- → Вдвое выросла доля утечек информации категории «коммерческая тайна».
- → Заметнее всего выросла доля утечек среди организаций отраслевой группы «Ритейл & HoReCa» — практически в пять раз, среди промышленных, транспортных и энергетических компаний — почти в три раза.
- → На малый бизнес пришлось более 20% утечек — доля вдвое больше, чем в 2021 г.

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
ИТ	Информационные технологии
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
ЭАЦ	Экспертно-аналитический центр ГК ИнфоВотч

Аннотация

Экспертно-аналитический центр ГК InfoWatch подготовил отчет по результатам ежегодного исследования утечек конфиденциальной информации в России. По итогам 2022 года традиционно приведены данные о количестве утечек информации, количестве скомпрометированных записей ПДн и платежной информации, представлены графики и диаграммы, иллюстрирующие распределение утечек по характеру умысла. Также приведено соотношение утечек в разных отраслевых группах. Впервые, в связи с их значительным ростом, аналитики оценили долю утечек с неопределенным вектором воздействия.

Результаты исследования

Утечек стало вдвое больше

Количество утекших записей в 4,5 раза превысило число жителей России

После стабильного роста количества зарегистрированных утечек информации в 2017–2019 годы и их падения в разгар пандемии, вызванного прежде всего увеличением латентности инцидентов, в 2022 году произошел скачок. По сравнению с предыдущим годом количество утечек выросло более чем в 2,1 раза (на 112,6%) — см. Рисунок 1.

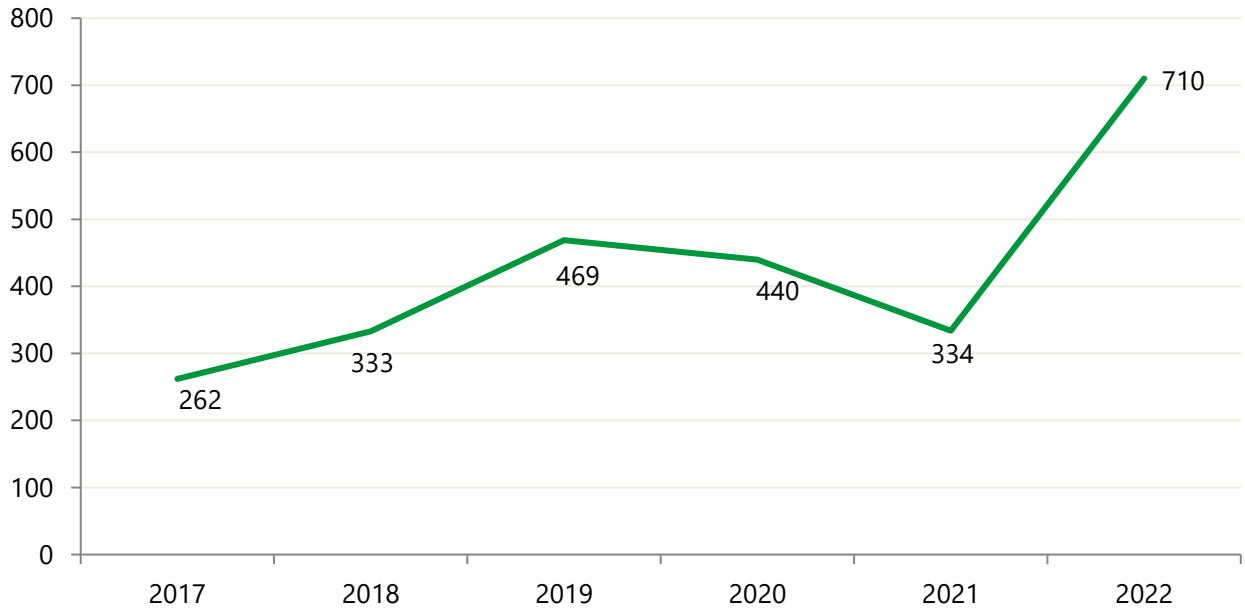

Рис 1. Количество утечек данных: Россия, 2017–2022 гг.

Ведомости: Хакеры выставили на продажу в даркнете данные пользователей российского сервиса аренды электросамокатов Whoosh. По информации Data1eaks, лот стоимостью $4200 содержит файл с промокодами сервиса и два файла с данными о пользователях. В нем содержатся имена, 7,2 млн уникальных номеров, 6,9 млн уникальных e-mail-адресов, частичные (шесть первых и четыре последних цифры) номера банковских карт, имена/фамилии латиницей, типы карт, дата создания записи и последней аутентификации, а также отметки GPS-навигации.

Такой значительный рост обусловлен повышением хакерской активности в результате накалившейся международной обстановки с начала проведения Специальной военной операции. Связанные с ней события вскрыли проблемы в сфере информационной безопасности в разных странах, в результате в ряде стран количеств утечек за год выросло в 10–18 раз(!) — см. отчет по утечкам информации в мире за 2022 год.

В России рост количества утекших записей ПДн и платежной информации за 2022 год был внушительным. Всего за год утекло 667,6 млн записей (Рисунок 2). Это в 2,67 раза (на 167%) больше, чем в 2021 году.

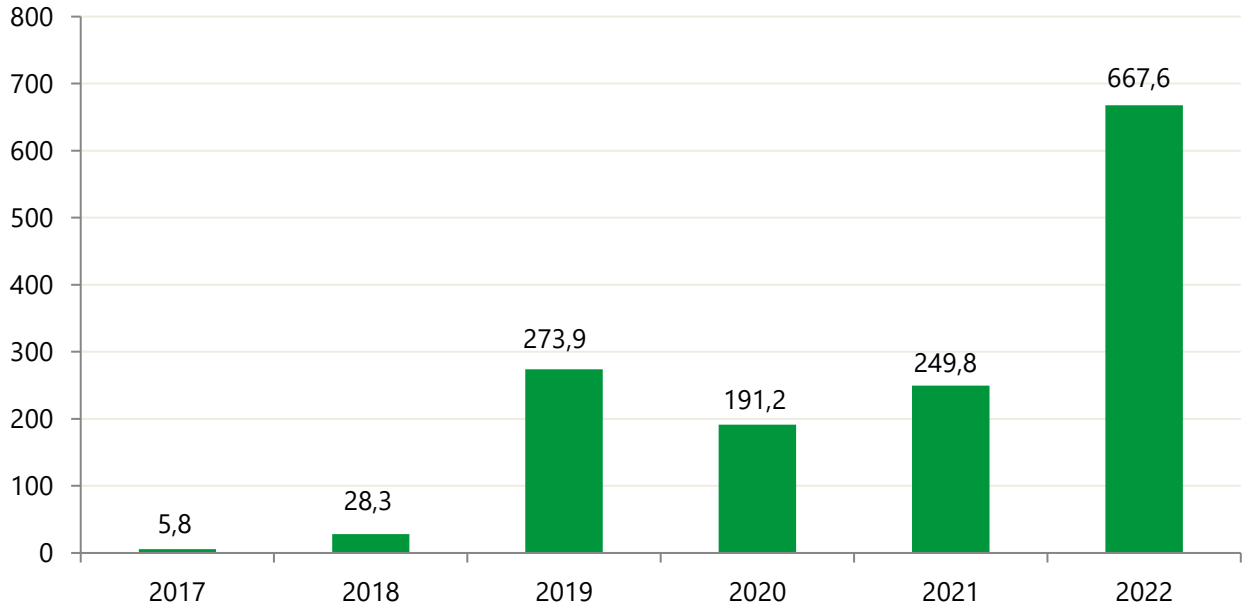

Рис 2. Количество утекших записей ПДн и платежной информации, млн: Россия, 2017–2022 гг.

РБК: В открытый доступ попали данные почти 44 млн пользователей онлайн-кинотеатра Start. В базе содержатся имена и фамилии, адреса электронной почты, хэшированные пароли, IP-адреса и названия стран пользователей, а также даты начала и окончания подписки.

В 2019–2021 гг. количество известных скомпрометированных записей персональных и платежных данных за каждый год неизменно превышало население России. Всего за три года утекло около 715 млн записей. Но в 2022 году только за один год украдено или случайно раскрыто почти столько же данных. Количество скомпрометированных записей в прошлом году более чем в 4,5 раза превысило число жителей России.

Средняя утечка стала больше на 25%.

На Рисунке 3 представлена диаграмма, которая отражает количество скомпрометированных записей ПДн и платежной информации в расчете на одну утечку[1]. **По сравнению с 2021 годом средняя утечка «потяжелела» на четверть и составила более 940 тыс. записей. Крупными базами уже оперируют даже небольшие региональные компании, и утечка подобной информации может затронуть многие тысячи людей**.

[1] Для тех утечек, когда известно количество записей, содержащихся в них.

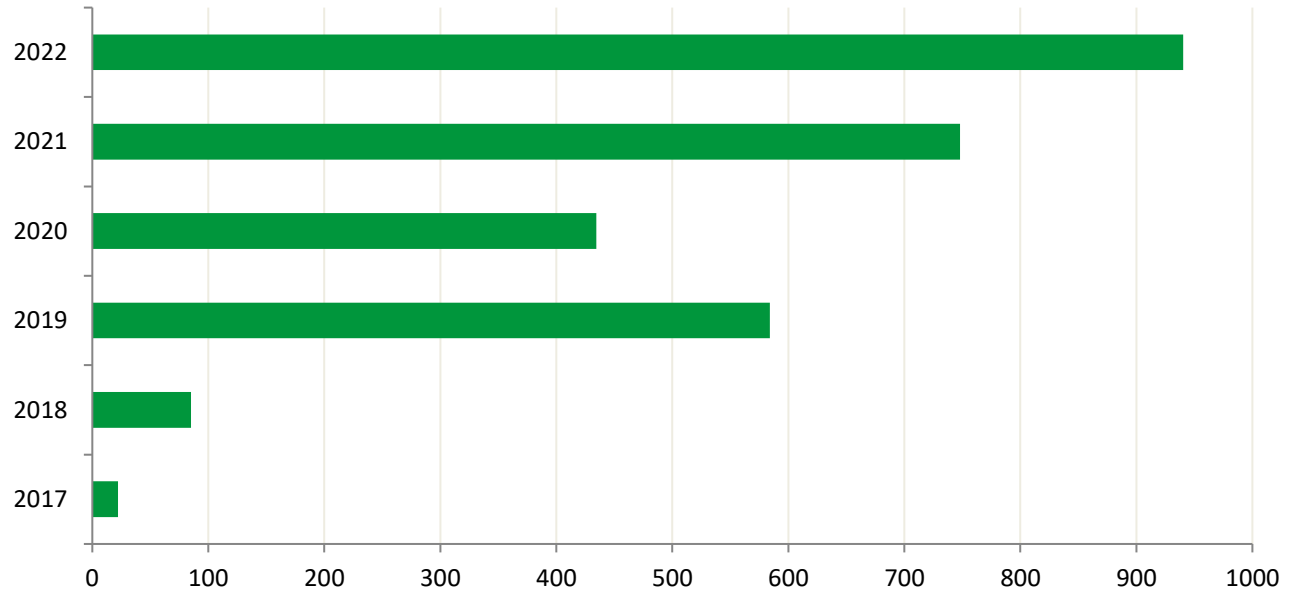

Рис 3. Среднее количество записей на одну утечку данных, тыс.: Россия, 2017–2022 гг.

Гибридный вектор воздействия

Более 80% утечек имеют внешний или гибридный вектор воздействия

С 2018 года в России неуклонно растет доля утечек информации по вине внешних нарушителей (хакеров и других злоумышленников). Вместе с тем, некоторое время назад исследование утечек по вектору воздействия все сложнее проводить по общепринятым критериям — внешний/внутренний. Появилось все больше утечек, где на основе найденных сведений (чаще всего крайне скупых) определить вектор было затруднительно, **за 2021–22 гг. значительно уменьшилось количество сведений, позволяющих идентифицировать утечки**. В ряде случаев имеющиеся сведения указывали на то, что на конфиденциальные данные той или иной организации нарушители воздействовали как изнутри, так и снаружи информационного контура, то есть находясь в сговоре. **Это привело к решению ввести в исследованиях новый термин — «гибридный вектор утечки».** Зарубежные исследования подтверждают тезис о том, что объявления о продаже данных и другие публикации о произошедших утечках информации содержат все меньшее количество сведений, позволяющих идентифицировать эти утечки информации[2]. Кроме того, при подготовке отчета по итогам исследования 2022 года мы отказались от упрощенного деления рассматриваемых инцидентов на утечки внешнего и внутреннего характера, приведя долю случаев, где вектор определить не удалось (Рисунок 4). Доля таких утечек за год составила более 80%. Во многом это связано с большим количеством распространяемых данных на «теневых площадках» (закрытых ресурсах в ДаркВеб и т.д.). Проследить источник их утечки зачастую не представляется возможным. Вероятно,

[2] Отчет Identity Theft Resource Center «2022 Data Breach Report». Дата публикации: 25.01.2023 г.

значительная их часть так или иначе связана с действиями хакеров, но предполагаем, что во многих случаях возможно участие персонала компаний.

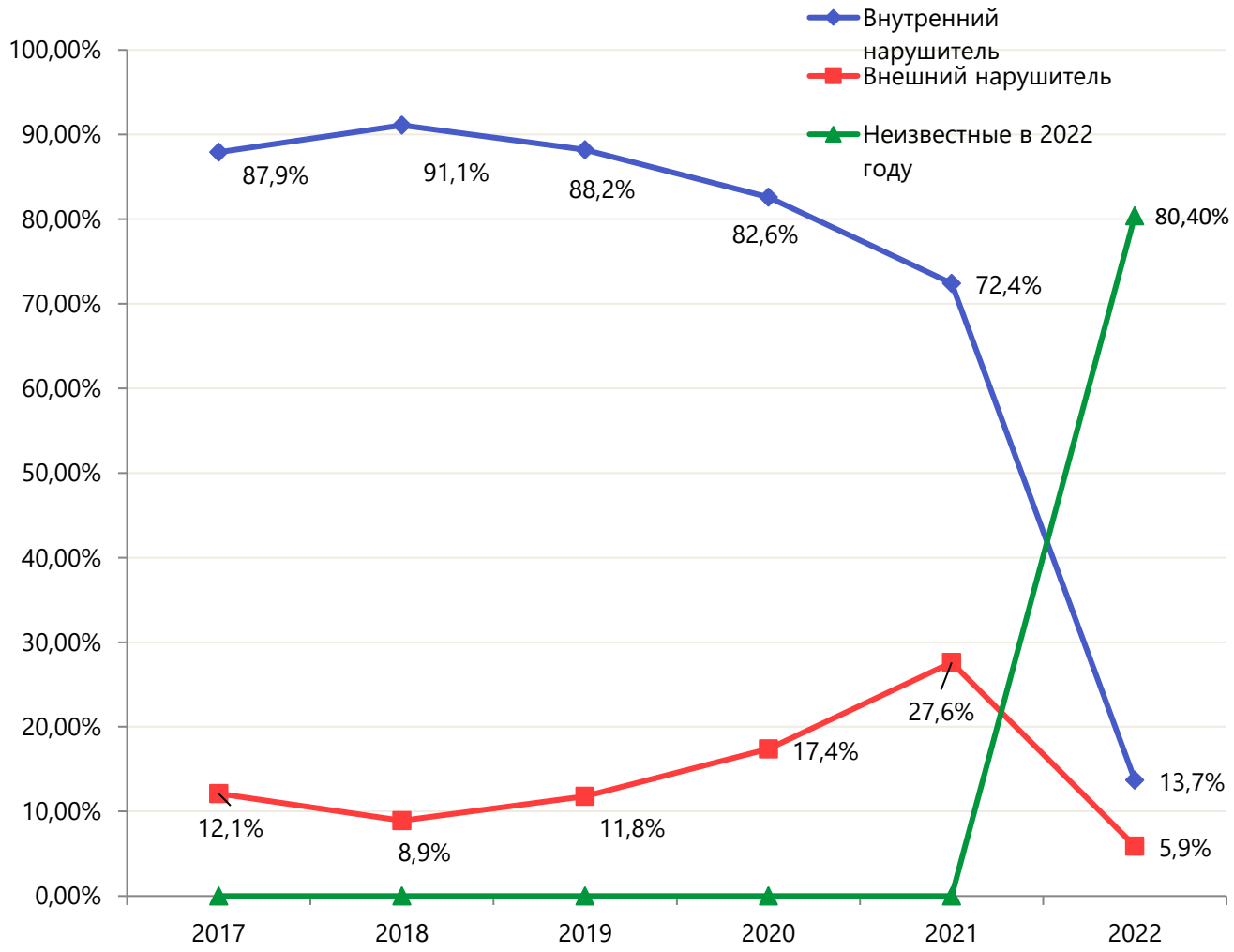

Рис 4. Распределение утечек информации по вектору воздействия (внешний/внутренний),%: Россия, 2017–2022 гг.

В 2017–2021 гг. доля неопределенных случаев утечек не превышала 5%.

РБК: У российского оператора экспресс-доставки документов и грузов СДЭК произошла новая утечка данных пользователей. Скомпрометированная информация включает Ф.И.О, адреса электронной почты, телефоны, почтовые адреса, сведения о юрлицах. По оценкам Infosecurity, вместе с предыдущей утечкой у СДЭК в сумме утекли данные десятков миллионов клиентов.

Рост доли утечек умышленного характера

Как и в глобальном масштабе, **в России с 2019 года постоянно растет доля утечек информации умышленного характера** (как по вине внешних, так и внутренних нарушителей, Рисунок 5). С одной стороны, это отражает бурное развитие цифровой

экономики, с другой — связанные с этим в целом позитивным трендом побочные эффекты (больше цифровых данных — больше потенциальных утечек, например). Каждая единица конфиденциальной информации имеет денежный эквивалент на черном рынке, а значит, является желанным объектом для злоумышленников. С другой стороны, **существенное снижение утечек случайного характера может говорить о росте латентности инцидентов внутреннего характера, а во многих случаях — об успехах организаций в практике использования DLP-систем, спрос на которые резко вырос в пандемийные годы**. Современные корректно настроенные системы предотвращения утечек надежно выявляют случайные утечки и позволяют предотвращать их.

При этом стоит отметить, что в отдельные годы зафиксирована высокая (свыше 5%) доля инцидентов, когда характер умысла установить не удалось.

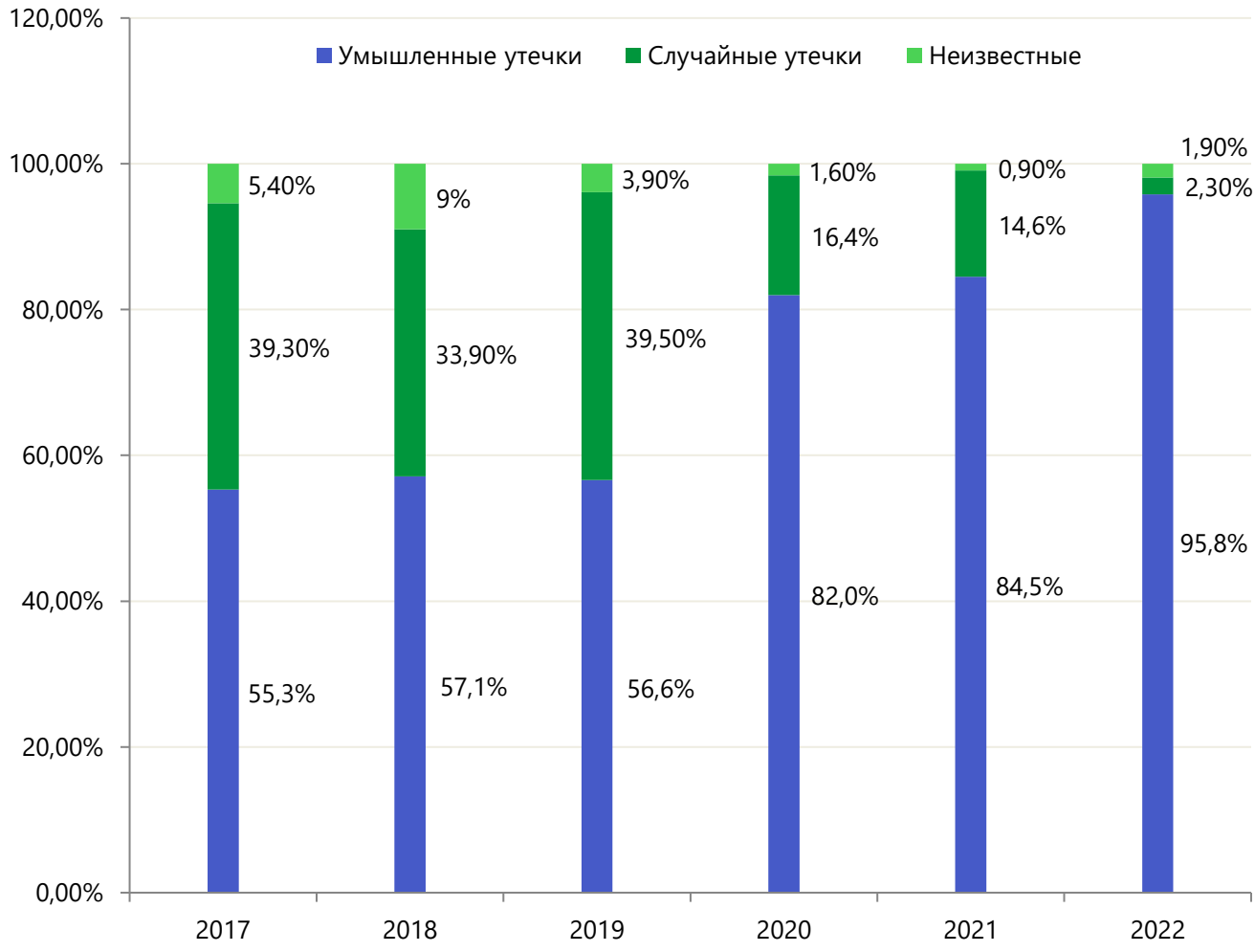

Рис 5. Распределение утечек информации по характеру умысла (умышленные и случайные, за счёт как внешнего, так и внутреннего нарушителя),%: Россия, 2017–2022 гг.

Интерфакс: «Яндекс.Еда» в конце 2022 года сообщила, что февральская утечка данных ее клиентов произошла в результате хакерской атаки на внешнюю

инфраструктуру. По факту атаки возбуждено уголовное дело. Первоначально «Яндекс.Еда» заявляла, что информация пользователей (телефонные номера и сведения о заказах) была опубликована «в результате недобросовестных действий одного из сотрудников».

Среди утечек внутреннего характера около 80% отнесены к умышленным

Наиболее показательным является **соотношение случайных и умышленных утечек информации среди нарушений внутреннего характера**, то есть случившихся по вине сотрудников компаний. Оно служит неким индикатором востребованности конфиденциальной информации среди персонала. Если установлено, что утечка внутренняя, практически всегда известен виновник, канал и наличие или отсутствие умысла. **В 2022 году почти 80% нарушений внутреннего характера отнесены к категории умышленных** (Рисунок 6).

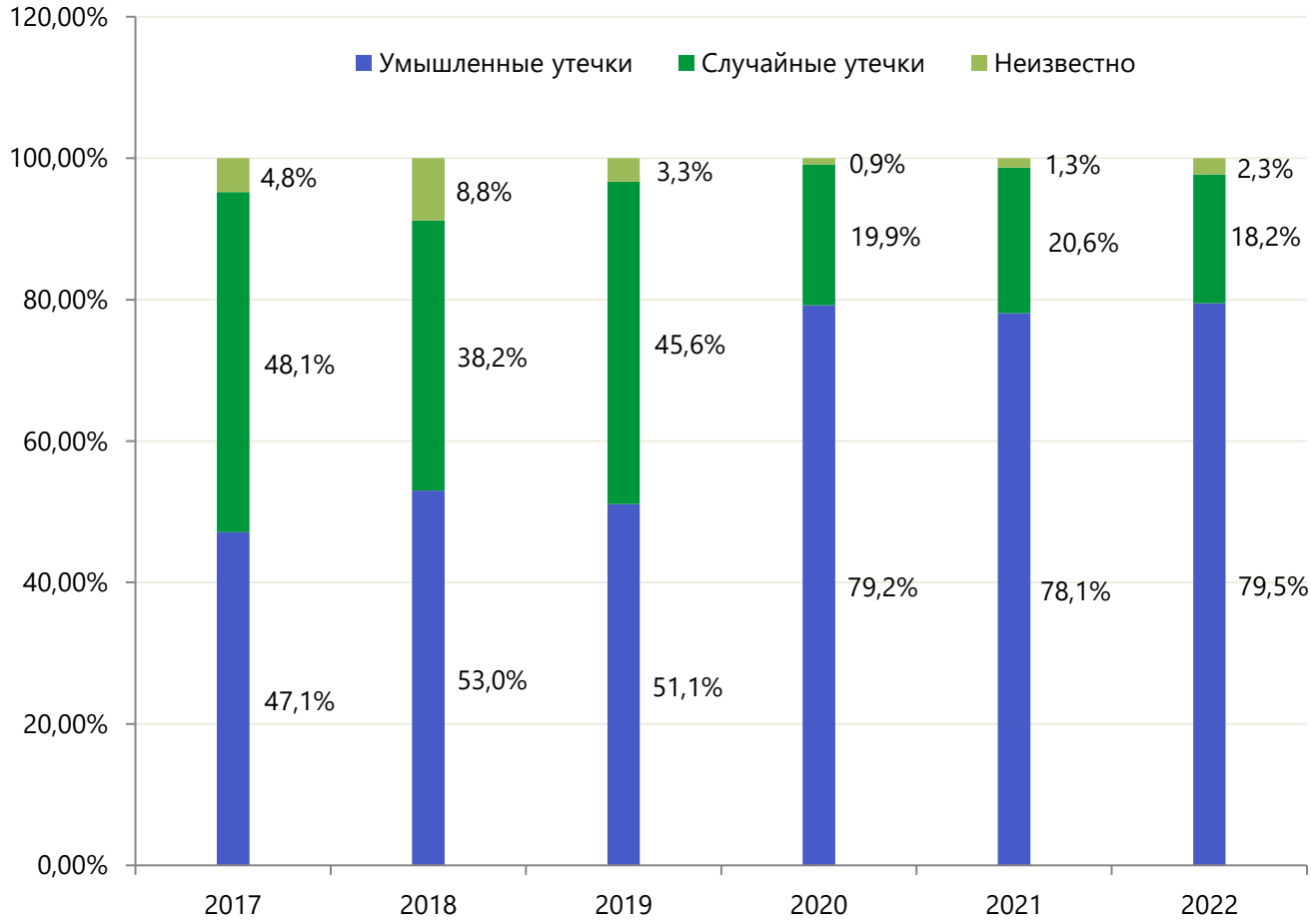

Рис 6. Распределение по умыслу (умышленные/случайные) утечек внутреннего вектора воздействия: Россия, 2017–2022 гг.

CNews: Бывший сотрудник «Ростелекома» выложил в Сеть персональные данные более 100 тыс. коллег. В дарквебе оказались Ф.И.О, должности, адреса корпоративной почты, логины и телефонные номера.

76.ru: В Переславле-Залесском Ярославской области на городской мусорке оказались ксерокопии паспортов. Источник утечки персональных данных людей установить не удалось. Расположенные неподалеку от места свалки ксерокопий налоговая инспекция и страховая компании от причастности к нарушению открестились.

Коммерческая тайна стала утекать вдвое чаще

На Рисунке 7 приведено распределение утечек по типам данных. В 2022 году вдвое выросла доля компрометации сведений, составляющих коммерческую тайну. Полагаем, что это связано с интенсификацией кибервойн в связи с СВО. Злоумышленники усиленно атаковали российские компании, причем порой не с целью продажи украденных данных, а для того, чтобы вызвать общественный резонанс и привлечь внимание широких масс к теме СВО. Тем не менее, в США количество утечек также выросло в два с лишним раза, а во многих других «недружественных стран» в 5–10 раз.

По прежнему основным типом утекших данных остаются персональные данные.

Также почти в 3 раза в 2022 году стало меньше сообщений об утечке сведений, составляющих государственную тайну, что связываем с закрытостью этой информации, в том числе в связи с проведением СВО. Полагаем, что реальную картину сможем увидеть через 2–2,5 года.

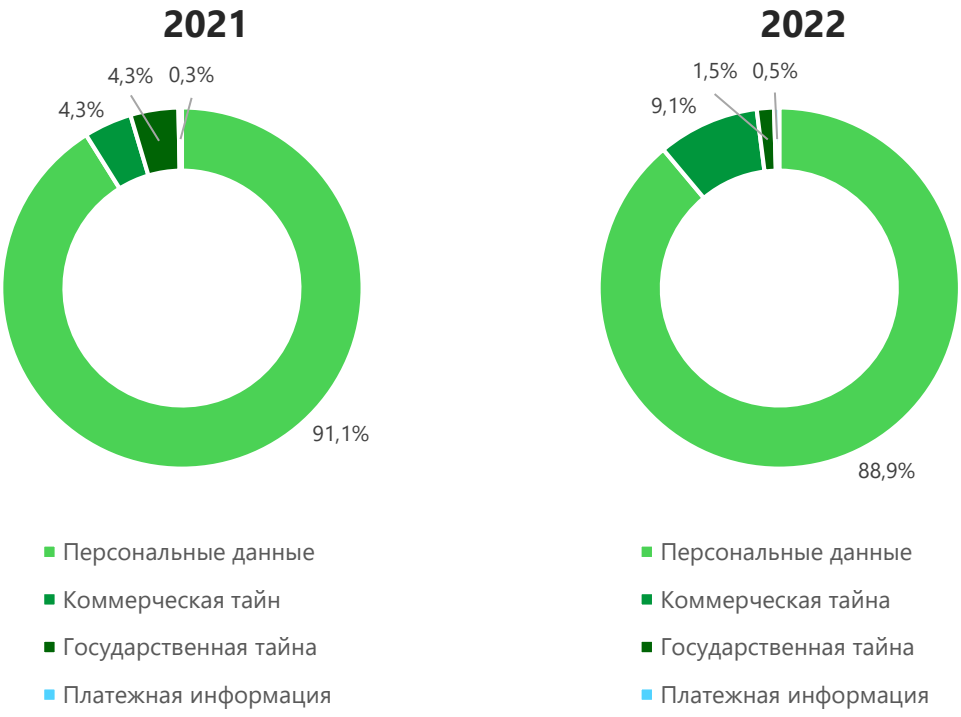

Рис 7. Распределение утечек по типам данных: Россия, 2021–2022 г.

News.ru: Помощник брокера похитил базу данных компании «Сколково-Недвижимость», содержащую информацию об объектах недвижимости, застройщиках и собственниках, накопленную за долгие годы. Похититель продал базу конкурирующей компании за 100 тысяч рублей. Возбуждено уголовное дело.

Утечки информации по отраслям

Хакеры активно взламывают торговые и производственные организации

Существенное перераспределение долей произошло на отраслевой карте утечек (Рисунок 8). Почти в пять раз выросла доля утечек в группе «Ритейл&HoReCa», что, скорее всего, свидетельствует о низком уровне защиты информационных активов среди ряда розничных сетей, в общепите и службах доставки. При этом в базах предприятий из данной группы содержится значительное количество ПДн и платежной информации, объемы этих данных сильно выросли во время пандемии.

Также значительно чаще данные стали утекать из организаций отраслей промышленности, транспорта и энергетики. Это говорит о назревшей необходимости перехода на современные средства защиты объектов критической инфраструктуры.

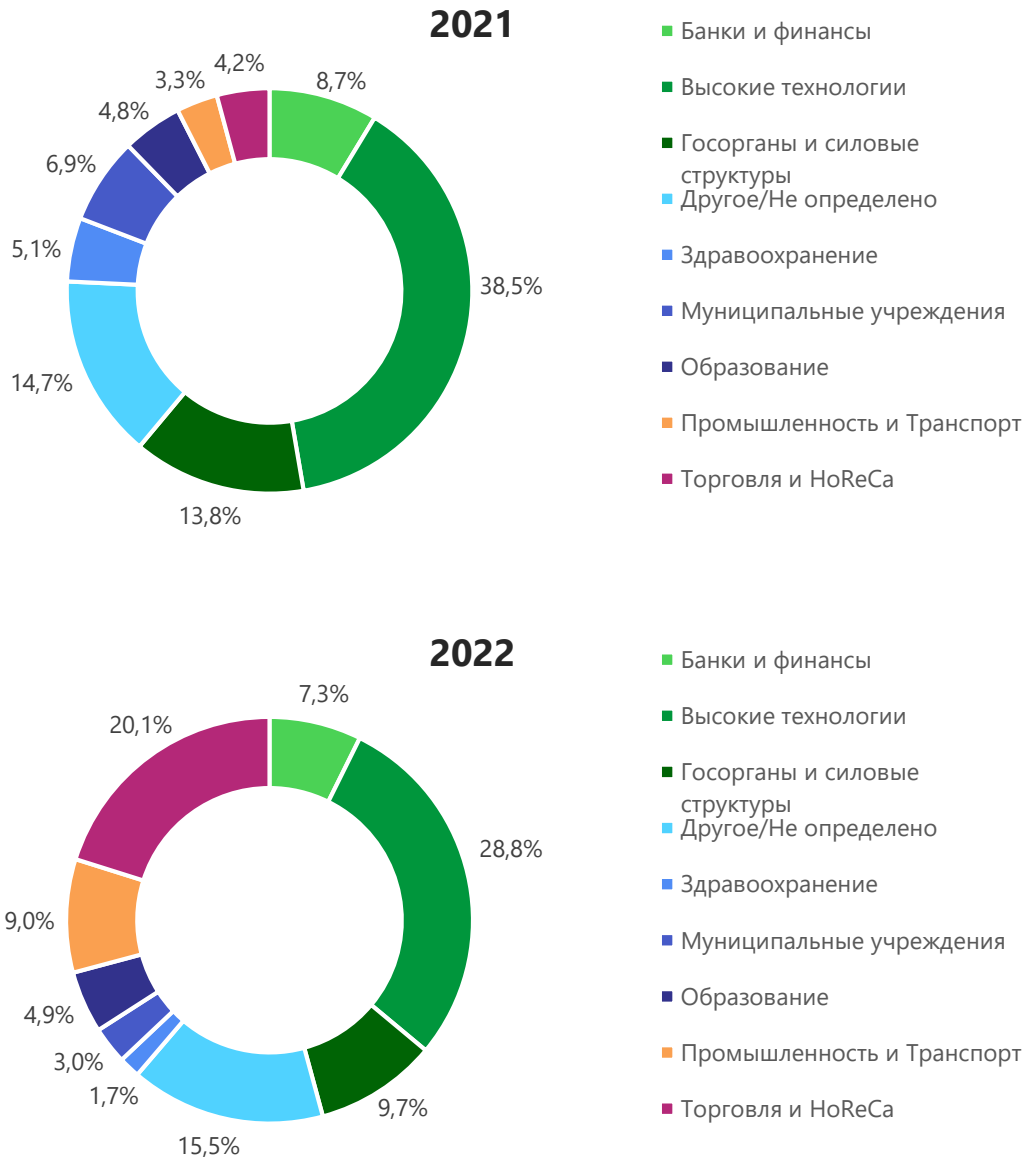

Рис 8. Отраслевое распределение утечек информации: Россия, 2021–2022 г.

От утечек намного чаще стал страдать малый бизнес

Выше мы отмечали, что даже небольшие компании все чаще обрабатывают конфиденциальную информацию большого объема. Их хранилища могут содержать миллионы записей. На Рисунке 9 представлено распределение утечек данных по размеру пострадавших организаций. **Из малых компаний конфиденциальная информация стала утекать вдвое чаще**, выросла доля и средних компаний. **Отсюда можно сделать вывод, что время, когда малый бизнес мог относительно спокойно себя чувствовать, уже прошло**. В условиях массовой цифровизации каждая компания обладает ценными информационными активами, защита которых требует принятия стратегии ИБ и реализации целого комплекса организационно-технических мероприятий.

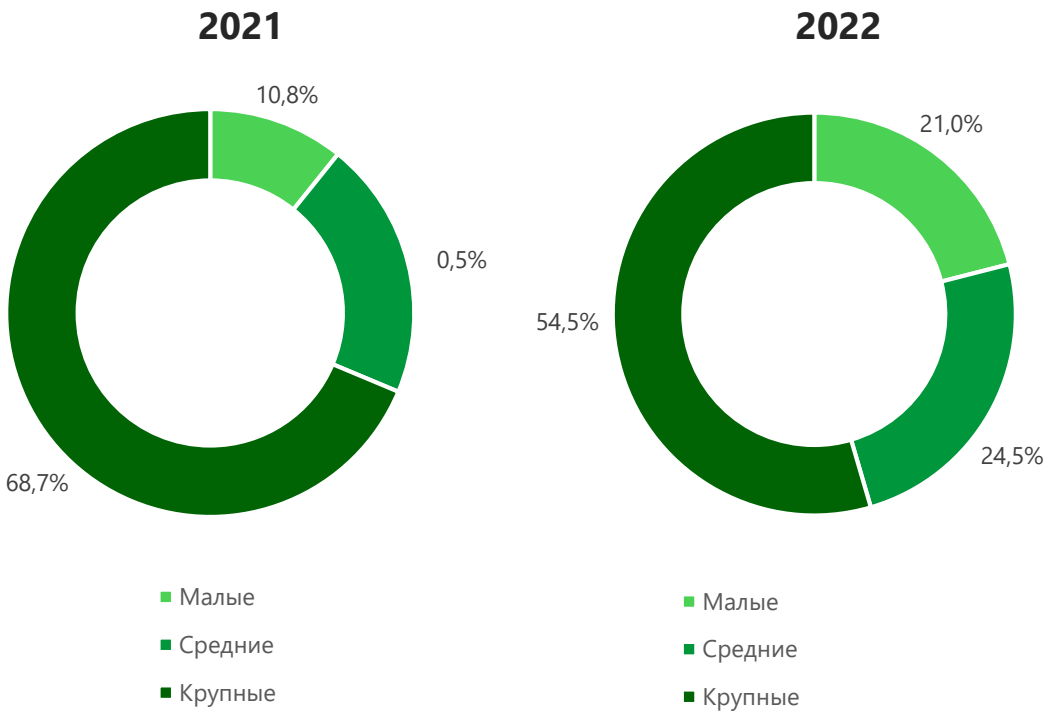

Рис 9. Распределение утечек данных по размеру пострадавших организаций: Россия, 2021–2022 г.

Заключение и выводы

Еще в конце 2010-х годов эксперты по кибербезопасности отмечали, что ландшафт угроз очень быстро меняется, и адаптировать под него системы защиты становится все сложнее. События последних трех лет, прежде всего, связанные с пандемией и СВО, еще больше усложнили работу по выявлению инцидентов и ликвидации (смягчению) их последствий. Кибератаки все чаще носят изощренный и целевой характер, причем если раньше хакеры в качестве мишеней выбирали крупные компании, то в последнее время от действий киберпреступников также регулярно страдает средний и малый бизнес.

Идентификацию нарушений, связанных с утечками информации, затрудняет сложность современной ИТ-инфраструктуры, развитие практики удаленной работы сотрудников, скрытный характер многих атак и нарушений, постоянная адаптация приемов фишинга и социальной инженерии. В свою очередь, многообразие зарегистрированных утечек и лавинообразный характер их роста в 2022 году затрудняет идентификацию виновников этих нарушений, вектора воздействия (внутренний, внешний или гибридный) и каналов утечки. Поэтому вопрос о том, кто стоит за той или иной утечкой — внешние нарушители (хакеры), сотрудники (по своей инициативе или в сговоре с хакерами), подрядчики, — все чаще не находит однозначного ответа.

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:

- Рассылка InfoWatch
- ВКонтакте
- Telegram

Методика (версия от 28.02.2023 г.)

Исследование проводится на основе собственной базы утечек информации (данных) ЭАЦ, регулярно пополняемой специалистами ЭАЦ с 2004 года.

Источником сведений для этой базы являются публичные сообщения[3] (преимущественно в электронном виде, размещенные в сети Интернет, в других сетях и системах общего пользования) о случаях утечек охраняемой законом информации из учреждений, организаций, предприятий любых организационных форм и форм собственности, включая органы государственной власти и управления, ведущих деятельность во всех странах мира, а также данные из закрытых и условно-закрытых электронных источников информации (Интернет-форумы, чаты и каналы в мессенджерах, группы в мессенджерах и социальных сетях, в том числе доступ к которым осуществляется только с разрешения модераторов и/или с применением специализированного программного обеспечения).

В качестве сообщений об утечках информации также рассматриваются аналитические отчёты, бюллетени и другие публикации в случае, если указаны сведения об утечке информации, достаточные для внесения в базу утечек.

Сведения об утечках собираются путём мониторинга и просмотра источников информации (преимущественно в электронном виде), поиска по ключевым словам на различных языках с применением поисковых Интернет-систем.

По состоянию на 28.02.2023 г. количество записей в базе утечек превышает 30 тысяч.

Исследования ЭАЦ, в основном, ориентированы на анализ сообщений об утечках данных на английском и русском языках. Для обеспечения и увеличения полноты охвата используются источники на арабском, японском, немецком, французском, испанском, итальянском языках, в том числе с применением программного обеспечения, предназначенного для перевода, но с проверкой того, отражает ли полученный перевод особенности существующих информационных и производственных (операционных) технологий (IT, OT), в том числе путём поиска дополнительной информации об организации-источнике утечки, применяемых в ней информационных системах, соответствует ли принятой в предметной области терминологии (корректность перевода терминов) и т.д.

В ходе наполнения базы утечек ЭАЦ каждое сообщение об утечке классифицируется по признакам из сформированных списков (разработаны соответствующие классификаторы). Каждый классификатор имеет ограниченное количество вариантов.

Например, при классификации по принадлежности утечки информации к государству каждому сообщению присваивается одна характеристика по классификатору (название страны, на территории которой работает обладатель информации и где, предположительно, произошла утечка информации). Например, если утечка информации произошла в филиале, ЦОД или структурном подразделении организации, которое находится на территории государства, отличного от государства, в котором расположена головная организация, то вносится название государства, в котором расположен этот филиал или структурное подразделение.

Если прямо не указана страна или филиал (обособленное подразделение) организации, из которой произошла утечка, то в записи об утечке информации указывается государство, где расположен головной офис организации или холдинга (штаб-квартира).

В базу утечек информации вносятся сведения, идентифицирующие утечку (обязательный минимум):

- текст заголовка и сообщения об утечке в СМИ или другом источнике информации;
- интернет-ссылка на источник сообщения (или другая ссылка, позволяющая найти данное сообщение);
- дата публикации сообщения;
- дата или год утечки.

Если в сообщении не указан год произошедшей утечки, то сначала проводится проверка того, не относится ли данное сообщение к ранее известной утечке, уже внесенной в базу. Затем, в случае если данная утечка информации ранее не была зарегистрирована, сведения о годе утечки устанавливаются путем их поиска в других источниках информации.

Если в ходе этого поиска обнаружено, что сведения относятся к ранее известной утечке, то в запись об утечке информации в базе вносятся дополнения. Если сведения о дате утечки установить не удалось, то в качестве года утечки вносится год обнаруженного сообщения об утечке. В случае поступления новой информации год утечки и дата утечки изменяются.

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

К дополнительным данным об утечке информации, которые вносятся при их наличии, относятся:

- название организации (предприятия, компании, учреждения);
- государство (страна), на территории которого произошла утечка (где находится филиал или обособленное структурное подразделение, или ЦОД компании);
- сфера деятельности организации, из которой произошла утечка (отрасль);
- примерный размер организации (малая, средняя, крупная)[4];
- размер причиненного в результате утечки ущерба[5];
- тип скомпрометированной («утекшей») информации (данных);
- количество скомпрометированных записей (только для ПДн и платёжной информации);
- тип канала, через который произошла утечка информации;
- субъект, непосредственно допустивший утечку информации (виновник инцидента).

При внесении в базу утечек каждое сообщение классифицируется по:

- типам данных (относятся ли скомпрометированные сведения к персональным данным, платежной информации, государственной или коммерческой тайне, ноу-хау и т.п.);
- типу канала утечки;
- наличию умысла (если по описанию или имеющимся признакам действия лица (лиц), допустившего утечку, являются умышленными, то утечка классифицируется как умышленная; в обратном случае — как неумышленная / случайная, см. Глоссарий);
- вектору воздействия («внешний вектор»/«внешний нарушитель», «внутренний вектор»/«внутренний нарушитель», «не определено» (неизвестно), «гибридный вектор» — когда утечка связана с скоординированными (совместными) действиями как внешних, так и внутренних нарушителей);
- типу нарушителя (хакер, сотрудник, топ-менеджер, подрядчик и т.п., см. Глоссарий).

В базу также попадают случаи, когда невозможно установить обладателя скомпрометированной информации (название организации, из которой произошла утечка), но 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 «Прочее», поле «название организации» остается пустым.

В ЭАЦ составлен справочник отраслей на базе рейтингов различных аналитических агентств, позволяющий классифицировать организации по отраслям (сферам деятельности), в том числе укрупненным, совпадающим с международной экономической аналитикой.

Выделяются следующие сферы деятельности (отрасли, отраслевые группы):

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

Иных признаков (категорий для классификации) база утечек ЭАЦ не содержит.

Если в сообщении об утечке информации не указаны размер организации и/или отрасль, то они определяются, исходя из сведений в открытых источниках — в первую очередь по данным с сайта организации, а в случае отсутствия

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

[5] 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.

на нем необходимых данных устанавливается на основании поиска по специализированным сайтам и через поисковые Интернет-запросы. В ЭАЦ подготовлена отдельная внутренняя инструкция для поиска информации, которая изменяется по мере появления сайтов, совершенствования языка запросов.

В базу вносится количество скомпрометированных записей, содержащих только ПДн и/или платёжную информацию, т.к. в остальных случаях количественные характеристики обычно отсутствуют или не отражают размер утечки. Например, объемы файлов и/или количество файлов, содержащих коммерческую тайну, ноу-хау в виде чертежей, описаний, формул и т.п., не отражают ценность «утекшей» информации. В части утечек государственной тайны количественные характеристики также не применимы — важен сам факт компрометации такого рода сведений и их содержание, которое влияет на безопасность государства (национальную безопасность) и ущерб для него.

В случае, если в сообщении об утечке указаны ПДн и/или платежные данные, но не указано их количество, в базе в поле «количество» ставится «ноль». При появлении сведений о количестве «утекших» данных в поле «количество» соответственно вносятся ставшие известными сведения о количестве «утекших» ПДн и/или платежных данных. Таким образом, возможно оценивать количество реально «утекших» ПДн и/или платежных данных как превышающее внесённое в базу утечек и опубликованное в аналитических отчётах.

Все перечисленные признаки (конкретные варианты признаков) вносятся при наличии соответствующей информации, а также могут определяться методом экспертной оценки, носить вероятностный характер, если сведения об утечке информации неполные или противоречивые. В случае, если такие сведения приведены, но признак не входит в основной список классификатора, то устанавливается признак «Прочее».

При невозможности классифицировать утечку информации по сведениям из сообщения (нет возможности выбрать из списка подходящий признак и отразить его в базе), в соответствующем поле выбирается значение «Неизвестно».

В целях исследований, проводимых с применением настоящей Методики, все внешние и гибридные утечки (см. Глоссарий) считаются умышленными. Внутренние утечки (внутренний вектор, утечка по вине или ошибке внутреннего нарушителя) могут быть как умышленными, так и случайными (см. Глоссарий).

При анализе публикаций, полученных из закрытых, частично закрытых источников или других источников ограниченного доступа, в т.ч. для доступа к которым необходимо специализированное ПО или допуск со стороны модератора, распространяемые (продаваемые) данные, как правило, считаются аналитиками ЭАЦ «утекшими» в результате внешних или гибридных действий, которые по своему определению являются умышленными. Данный подход определён тем, что лица, имеющие право на публикации в таких ресурсах, как правило, являются хакерами. Но до появления дополнительной информации утечки, опубликованные на закрытых ресурсах, отмечаются в базе и статистике как неизвестные («не определено»).

Аналитики ЭАЦ допускают, что среди данных, распространяемых через подобные ресурсы, могут быть также похищенные и распространяемые непосредственно сотрудниками пострадавших организаций (внутренний вектор/внутренняя утечка), которые одновременно владеют методами и инструментами анонимизации (например, системные администраторы), или переданные ими своим сообщникам-хакерам для реализации, но оценивают их долю как мало влияющую на статистику.

Также аналитики ЭАЦ допускают, что в статистике сведений об утечках информации имеется определенный перекос в сторону внешних умышленных утечек, но на данный момент инструментов и методов выявления случаев распространения информации в ДаркВеб или на других аналогичных ресурсах, полученной внутренними нарушителями, через анализ публикаций о распространении не имеется. В случае появления новых данных, в том числе результатов расследований, сотрудники ЭАЦ вносят в базу утечек ЭАЦ соответствующие изменения, в том числе о виновниках утечек.

В качестве внешних умышленных классифицируются утечки, произошедшие в результате заражения вредоносным ПО, взлома учетных записей и других действий внешних злоумышленников (нарушителей), в том числе в результате фишинговых атак на сотрудников.

Внутренние умышленные утечки определяются наличием умысла со стороны персонала, который обращается к информационным активам организации

Аналитики ЭАЦ считают, что большие шансы получить огласку в СМИ и других открытых источниках, а также стать известными большому кругу лиц, имеют следующие случаи утечки данных:

- кражи данных в целях продажи неопределенному кругу лиц;
- действия хактивистов для достижения общественных и политических целей;
- крупные утечки (объемом более 1 млн записей), утечки из наиболее крупных и широко известных организаций вне зависимости цели кражи;

- утечки из компаний с известными брендами или государственных, или социально-значимых организаций;
- утечки, в которых фигурируют данные известных персон (политики, бизнесмены, артисты, музыканты, спортсмены, писатели, общественные деятели и т.д.).

Такие утечки чаще попадают в сферу внимания СМИ и блогеров, а также надзорных органов, и обычно сопровождаются рекламной кампанией или массовыми рассылками со стороны лиц, распространяющих (продающих) эти данные.

При проведении анализа и подготовке отчётов по его результатам сведения об утечках представляются с использованием исторических данных — количественных показателей предыдущих лет. ЭАЦ регулярно проводит мониторинг источников сведений об утечках информации и отслеживает обновления сведений по ранее зарегистрированным в базе ЭАЦ утечкам информации. Кроме того, в базу утечек вносятся ранее не опубликованные или неизвестные ЭАЦ данные об утечках, произошедшие в предыдущие периоды.

В ходе мониторинга в базу вносятся уточнённые сведения о дате (периоде), когда случилась ранее опубликованная утечка, об объёмах (количестве записей), векторе атаки и других.

Таким образом, при появлении новых сведений, в том числе о количестве утечек информации, векторах воздействия, каналах, суммах штрафов, наложенных на организации, допустившие утечки, и другие сведения о количестве утечек информации за прошлые периоды могут изменяться по сравнению с ранее опубликованными. Но, как правило, вновь полученные сведения не оказывают существенного влияния на общие показатели, отраженные в отчетах, а также на приведённые в исследованиях тенденции.

В основном данные в сравнительных исследованиях (сравнения с аналогичными показателями предыдущего периода) представляются в процентном виде. Исключение составляют: сведения о количестве утечек, включенных в базу ЭАЦ, а также об объеме записей, скомпрометированных в результате этих утечек, объеме скомпрометированных записей в расчете на одну утечку (только в случае утечек ПДн и платежной информации).

Для анализа и корректного расчета среднего числа записей в одной утечке информации сведения об утечках могут быть сгруппированы по количеству:

- до 1 миллиона записей в одной утечке информации;
- от 1 до 10 миллионов записей в одной утечке информации;
- от 10 миллионов записей в одной утечке информации («мега-утечка»).

При анализе выборки утечек информации по определенному признаку и построении сравнительных диаграмм 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.[6] Такой подход позволяет проиллюстрировать динамические изменения отдельных показателей (долей, приходящихся на утечки, обладающие определенным признаком) и выявить тенденции, т.е. решает задачи наглядного представления информации. Но в случаях, когда доля утечек с признаком, классифицированным как «неизвестный», превышает 5%, ЭАЦ приводит полные диаграммы.

Исследования утечек информации проводятся в различных разрезах:

- в отношении утечек в мире в целом и в России;
- по определенным государствам или группам государств, объединённым общим признаком (например, входящие в Евросоюз);
- в определенной сфере экономики;
- по вектору воздействия (например, утечки во вине внутренних нарушителей)
- по другим направлениям и признакам.

В ходе исследования и в рамках подготовки отчётов проводятся выгрузки и сравнения по имеющимся признакам в классификаторах, прежде всего:

- сферам деятельности организаций (отраслей экономики);
- каналам утечки информации;
- видам скомпрометированной («утекшей информации»), в том числе по объемам (в случае наличия данных);
- виновникам утечки (нарушителям);

[6] 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.

- вектору воздействия (умыслу).

В файлах с выгруженными данными отражается информация по вариантам классификаторов, в т.ч. «Неизвестно» и «Прочее».

Сравнения проводятся с аналогичным предыдущим периодом и/или за периоды 3–6 лет при необходимости, например, для выявления закономерностей в росте или спаде утечек информации.

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 организации, воздействующие на веб-ресурсы, информационную инфраструктуру, носители корпоративной информации с целью компрометации информации, и действия внутренних нарушителей (сотрудники организации и подрядчики, получившие права доступа к ресурсам организации), 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).

ГАС «Правосудие» — Государственная автоматизированная система Российской Федерации.

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).

Запись в ГАС «Правосудие» — запись на сайте https://bsr.sudrf.ru/, включающая информацию об одном судебном решении.

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:

1. утрата услуг, оборудования или устройств;

2. системные сбои или перегрузки;
3. ошибки пользователей;
4. несоблюдение политики или рекомендаций по ИБ;
5. нарушение физических мер защиты;
6. неконтролируемые изменения систем;
7. сбои программного обеспечения и отказы технических средств;
8. 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):

1. «Оборудование (сервер, СХД, ноутбук, ПК)», — компрометация информации в ходе обслуживания, в результате кражи или потери оборудования.
2. «Мобильные устройства» — утечка информации вследствие нелегитимного использования мобильного устройства/кражи мобильного устройства (смартфоны, планшеты). Использование данных устройств рассматривается в рамках парадигмы BYOD.
3. «Съемные носители» — потеря/кража съемных носителей (CD, USB, карты памяти и др.).
4. «Сеть (сетевой канал)»:
   - сетевое соединение — проникновение в сеть организации из Интернет или другую сеть общего пользования (взлом, открытый вход, наличие аутентификационной информации), нелегитимное использование внутренних ресурсов сети, в т.ч. FTP;
   - облачные сервисы (неверная настройка внешних ресурсов — серверов в «облаке» и т.п.);
   - нелегитимная публикация информации на внешнем веб-сервисе (сайт организации, GitHub и т.п.);
   - нелегитимная публикация информации на неофициальных (личных) Интернет-сервисах (яндекс-диск и т.п.), в соцсетях или мессенджерах, отправка данных через веб-интерфейс в личную почту, формы ввода в браузере, в соцсети, мессенджеры (ранее — утечка через браузер).
5. «Электронная почта» — утечка данных через корпоративную электронную почту.
6. «Бумажные документы» — утечка информации вследствие неправильного хранения/утилизации бумажной документации, через печатающие устройства (отправка на печать и кража/вынос конфиденциальной информации на бумаге).
7. «IM-сервисы мгновенных сообщений» — утечка информации при передаче ее голосом, в текстовом виде, а также через видео — при использовании мессенджеров.
8. «Не определено» — категория, используемая в случае, когда сообщение об инциденте в СМИ не позволяет точно определить канал утечки.

Критическая информационная инфраструктура Российской Федерации — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

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».

Нарушение с применением средств автоматизации — нарушение положений (требований) статей Кодекса об административных нарушениях РФ или Уголовного кодекса РФ с использованием компьютера, средств связи и сети Интернет.

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 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:

1. 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.
2. Рядовой сотрудник.
3. Топ-менеджер (руководитель).
4. Системный администратор.
5. Подрядчик: сторонние исполнители работ по заказу организации, партнеры и внештатные сотрудники.
6. 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:
- Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.
- 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]

Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры.

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.

Субъекты критической информационной инфраструктуры — государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Судебное дело — совокупность судебных решений всех инстанций, которые относятся к одному факту нарушения Кодекса об административных нарушениях или уголовного кодекса РФ.

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 целях исследований, проводимых по данной Методике, к категории «утечка информации» относится событие, когда в результате умышленных действий внешнего нарушителя, или умышленных или неумышленных действий внутреннего нарушителя, или совместных действий внутреннего и внешних нарушителей обладатель информации ограниченного доступа (организация) утратил контроль над этой информацией.

Утечка информации неумышленная — к данной категории относятся ситуации, если к утечке информации привели действия (бездействие) пользователя (внутреннего нарушителя), которые не носят признаков умысла (случайно отправил данные по неправильному адресу, забыл закрыть доступ к сетевому серверу, Elastic-серверу или GitHub, потерял бумажные документы или другой носитель информации). Если в результате случайных действий пользователя, доступ к данным получило третье лицо, не имеющее корыстных намерений (исследователь сетевой безопасности, в том числе с применением сетевых программ-роботов, этичный хакер, прохожий), такая утечка также признается случайной.

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 организация убытки, связанные с действиями пользователя, причинён ли реальный вред субъектам персональных данных.

В целях исследований, проводимых по данной Методике, к умышленным также относятся те утечки, в результате которых данные получены внешними по отношению к организации лицами, проводившими целенаправленный поиск определённых типов данных и/или искавших возможность получить подобные или любые данные конкретных организаций. При этом на характер умысла не влияет то, вследствие чего получены данные — в результате взлома системы или за счёт ошибки сотрудника организации, не ограничившего доступ к данным. Таким образом решающим фактором при установлении характера умысла в каждой конкретной утечке выступает наличие корыстной заинтересованности сотрудников, подрядчиков и третьих лиц в отношении информационных активов организации.

Также к умышленным утечкам относятся все утечки, спровоцированные хакерскими атаками или физическим доступом извне к носителям информации ограниченного доступа, принадлежащей организации, в том числе в результате совместных действий внешнего нарушителя и внутреннего нарушителя (**гибридные утечки**).